ARTICLE

EU’s Revised Product Liability Directive: The Impact on the Legal, Business, and Operational Landscape

3 February, 2025

AUTHORS

Briony Pollard | Kari Prochaska | Rohit Sethi

Liability laws serve as a cornerstone of protection for consumers and businesses. As digital products become an increasingly integral part of our world, EU lawmakers continue to identify potential gaps in protection for users. On December 8, 2024, the revised EU product liability directive (the “Directive”) entered in force and ushered in significant changes to the EU product liability environment. The Directive widens the remit of the current EU product liability regime so as to capture software and AI systems or models to address and acknowledge the fact that software as a product may cause harm to an individual. As with the recently enacted EU AI Act, the Directive updates the existing legal framework to, in part, provide greater protection and redress mechanisms for individuals who seek to bring a cause of action for the use of defective products. As a result, compliance with updated obligations will involve a number of legal and practical operational considerations for in-scope organisations.

In this two-part article, members of Willkie Farr & Gallagher’s Privacy, Cybersecurity & Data Strategy practice highlight the legal significance of the changes, and Rohit Sethi of Security Compass discusses the myriad operational and technical factors that organisations will face over the next few years as a result of the changes.

EU’s Revised Product Liability Directive: The Impact on the Legal, Business, and Operational Landscape

Understanding the Primary Legal Implications of the Directive

(Briony Pollard and Kari Prochaska of Willkie Farr & Gallagher’s Privacy, Cybersecurity & Data Strategy practice)

Scope, Definitions, and Defectiveness

The expanded scope of the EU product liability regime now includes software (excluding open source) and any component that may be integrated into a software or AI or machine-learning type product. Under the Directive, the definition of “product” has been broadened to implicate software in a variety of uses (e.g., accessed via the cloud, on a device, or supplied through a SaaS model) and the “components” of a product that may include materials or services that are integrated into a product, such as AI systems or software utilised in connected vehicles.

Whilst the existing and revised regimes both provide for “no-fault” (or strict) liability on manufacturers for defective products, the Directive shifts the burden of proof from the individual claimant to the defendant organisation so that an individual is no longer required to prove a causal link between a defective product and damage resulting from that defective product.

The “defectiveness” of the product is presumed under the Directive where it is established that the product is defective and the damage caused is consistent with the defect in question. This means that the defendant organisation will now be required to demonstrate that either the product was not defective at the time the product was placed on or made available to the market or, under an objective standard, that the technical knowledge of or within the organisation at the time the product was placed on the market could not have discovered the defect. Assessing the defectiveness of a product includes, among other things, the foreseeable use of that product (and the other products that the primary product may interact with) by specific user groups (e.g., children) involved in the product use.

Further, the factors for consideration regarding what constitutes a defective product have been broadened to directly include specific considerations that impact software or AI systems, including a product’s ability to acquire new features or its ability to learn. In addition, a causal link between damages and defectiveness of a product will also be presumed where an aggrieved individual or party faces “excessive difficulties” in proving defectiveness due to the nature of the technology. This is intended to address the use of AI systems where the functionality may not be readily understandable to individuals or parties that seek to bring a claim.

Key Legal Implications for Businesses

1. **Timing**

EU member states are required to implement the Directive into local law by the end of 2026. Products placed on the market from that point on will be within the scope of the new law (but products that are placed on the market prior to that point will not). This means that organisations have, at best, a two-year grace period to prepare for compliance with respect to products, or components of products, that are currently in production.

2. Increased Scope of Liability

The Directive increases the scope of organisations that are subject to liability. Individuals or parties may now bring claims against both the manufacturers of products and the manufacturers of components of those products (where the manufacturer agreed to the component’s integration with a product). Under the Directive, the integrated or interconnected digital service components of a product that impact a product’s safety (e.g., traffic navigation systems, health or physical activity trackers) are considered within the “control” of the manufacturer of the product. Notably, the concept of manufacturer control can be extended beyond when a product is placed on the market or integrated into a product through, e.g., a software modification or update, or an AI system’s machine learning or algorithmic functionality. For software that is deployed and then updated where such updates are determined to be defective, liability attaches to the manufacturer when the product or component is under the control of the manufacturer. An individual or party making a claim is not required to maintain a contractual arrangement with a software provider, which means that a broad scope of liability exists for entities that are one step removed from the individual consumer. As a result, it is likely that the introduction of claims from individuals and groups of individuals will increase liability risk for manufacturers of products or for manufacturers of product components.

3. Supply Chain Considerations

Including the components of products within the scope of applicability has implications for supply chain relationships and apportionment of liability considerations as between parties. However, under the Directive, liability towards an affected individual cannot be limited by contract between the parties. Due to liability considerations for manufacturers and the interplay between the product and its components, organisations will need to continually assess their business partner relationships for risk of defectiveness concerns in products or components of products (when integrated). This may occur through extensive vetting of partners and vendors through due diligence.

In addition, claims related to defective products or components may be brought against manufacturers outside of the EU. In the context of a defective software component claim, individuals may seek compensation from a manufacturer of a component that caused the harm. Actions against non-EU entities may now be brought against importers, a manufacturer’s authorised representative, or a fulfilment service provider in the EU. Notably, and subject to certain conditions, where a non-EU party cannot be identified, an individual may also seek compensation from the distributor of the product.

4. Disclosure Obligations

Where aggrieved individuals only need to show facts or evidence to support a claim, defendant organisations must disclose product documentation that is “necessary and proportionate” to the individual’s claim. These disclosure requirements are balanced against an organisation’s right to protect its trade secrets and confidential and proprietary business information; however, it is unclear how determinations regarding what is “necessary and proportionate” will be established without excessively burdening companies. As a result, companies should prepare to produce more documentation in litigation, which will likely increase internal compliance costs.

5. Documentation Considerations

Written documentation maintained by organisations, including risk assessments and other internal processes and procedures, will play a factor in considering how defectiveness may be assessed within software or AI systems or products. Accordingly, organisations should maintain, as applicable, documented product risk assessments, which address software safety concerns, maintain AI-related audits, maintain and keep AI 'explainability' and 'transparency' documents updated, and ensure that any safety and risk considerations with respect to software or AI systems' products or components are sufficiently updated to keep pace with technological developments in order to adequately assess (and address) potential harms. Organisations may consider (to the extent that they have not done so) integrating all relevant stakeholders and teams into the risk management process to ensure that all safety initiatives are documented and tracked.

6. Insurance Coverage

Organisations will need to consider whether their current liability insurance coverage is adequately sized for potential claims under the Directive, or if additional/different coverage is required.

How the Directive Impacts Digital Product Manufacturers

(*Rohit Sethi of Security Compass)*

The requirements in the Directive represent a major change for companies that either build software or use software in their products (i.e., "digital product manufacturers") and mark a turning point in accountability in the digital sphere. The changes made by the Directive will impact information security programs in significant ways, including: (1) alignment of objectives and responsibilities; (2) process change; and (3) change management, which we explore in more detail below.

1. Alignment of Objectives and Responsibilities

Cybersecurity has been a trending topic for boards of directors ("BODs") for years. The National Association of Corporate Directors recommends that cybersecurity risk is incorporated into full BODs' meeting agendas to ensure that cybersecurity discussions are adequately documented in board minutes and the adoption of a framework for managing cybersecurity risk.

BODs facing potential liability for security flaws should be aware of the differences between enterprise cybersecurity and product security. Many frameworks, such as the popular NIST Cybersecurity Framework, are designed to apply broadly to manage cybersecurity risks faced by an organisation, including those specifically related to IT systems, e.g., those relating to email phishing attacks, weak employee passwords, encryption of information on mobile devices, hardening infrastructure, and identity management. The scope is vast and reflects the ever-expanding role of the Chief Information Security Officer

("CISO"). Every organisation that handles personal data needs to implement and maintain some type of a cybersecurity program.

Product security, on the other hand, is specifically focused on the security of products that the organisation manufactures. Most organisations do not need a product security framework. However, digital product manufacturers (including those that produce software embedded in hardware devices) need to consider the specific concerns of their products in addition to their own enterprise security posture. Whilst integrating security by design into the software development process is a small piece of the overall enterprise security set of responsibilities, it is a fundamental aspect to maintaining strong product security. The establishment of a product security incident response team differs in the scope of responsibility from that of a traditional incident response team. For these reasons, BODs should consider adopting more robust frameworks that specifically focus on product security, such as the NIST Secure Software Development Framework ("NIST SSDF"), the Building Security In Maturity Model, the Payment Card Industry Software Security Framework, or the Industrial Society of Automation 62443 set of standards. These serve as complements to (and not as a substitute for) broader enterprise security frameworks. Once a framework has been selected, BODs should continue to seek regular updates from qualified internal and external stakeholders.

The difference between enterprise security and product security may also impact ownership of security responsibilities. Typically, cybersecurity personnel assist development teams with expertise and services within organisations. With respect to software security, this often means that cybersecurity teams lend expertise in risk assessments, security testing, and other consultation services to software development teams. Although software security is often addressed in enterprise security frameworks, it is not covered in the same depth as frameworks such as NIST SSDF.

However, prioritising security activities in the development process, educating development teams on security risks, and remediating identified vulnerabilities fall under the scope of the stakeholder that controls software development. In many organisations, this is a Chief Technology Officer ("CTO") or VP of Software Engineering. The resources allocated for cybersecurity activities are often at odds with more immediate development priorities, such as shipping features or fixing bugs. Issues may include whether the CTO takes part in BOD reporting regarding product security, or whether their objectives and compensation are tied to security outcomes. In our experience, product security initiatives can only be successful if the product development organisation takes ownership of security outcomes.

Practitioners must recognise the significant organisational changes required to integrate security into the development process. Generally, security responsibilities in large organisations fall under the oversight of the CISO, with application security testing handled by security professionals who deliver vulnerability reports to development teams for remediation. This reactive approach, whilst common, does not constitute "secure by design."

A critical aspect of adopting a secure development life cycle is shifting ownership of security responsibilities. This means expanding ownership beyond the security department to include the head of software development, such as the CTO or VP of application development. By making security a shared responsibility, development leaders can ensure that security requirements, threat modelling, and secure coding practices are embedded directly into the development process, fostering a collaborative and proactive approach. If the CTO is not held accountable for security—through job responsibilities, objectives, or compensation—security efforts can conflict with their priorities, such as driving revenue or product delivery speed. However, in heavily regulated industries like banking, technology executives often have compensation tied to risk outcomes, which creates an incentive to prioritise security alongside other objectives.

This shift in accountability also impacts governance. BODs are often left out of discussions on secure development practices, as these are seen as overly technical. However, adopting a standard such as NIST SSDF enables technology leaders to present measurable progress and compliance in a way that BODs can understand and oversee. This approach provides critical visibility into how well security is integrated into the development process, ensuring that governance aligns with security objectives.

2. **Process Change**

Once organisations have created appropriate alignment and incentive structures, they often need to modify their processes to incorporate a more robust approach to building secure products. In our experience, most software organisations at scale have already adopted some security processes though the implementation of annual penetration testing, offering developer security awareness training, and a process for patching vulnerable servers. However, with the potential risks of liability and the need to adopt more robust software security practices, organisations often need to introduce new processes, including the following:

- *'Secure by design' processes*. Secure by design practices involve developers and architects identifying non-functional security requirements, creating threat models, and incorporating security considerations prior to coding.
- *Manage open source risk.* Whilst the practice of vulnerability patching in open source software has improved steadily in recent years, the potential liability arising from a vulnerability in open source software raises the stakes. Organisations will need to exercise rigour when selecting open source libraries that adhere to security best practices, such as the Open Source Security Foundation Best Practices Badge Program.
- *Audit trails.* Many security activities, such as threat or developer education, are done on an ad hoc basis. For example, a security leader and software developers may whiteboard potential risks to the software they are building. The end result is educational but may not produce an artifact or any follow-through regarding which specific risks are addressed in the software. However, lack of evidence will be an issue in the event that the software manufacturer needs to prove adherence to industry-accepted best practices.

The breadth of process change is dependent on the organisation's starting point for maturity. Organisations can use the Software Assurance Maturity Model's self-assessment tool to understand their gaps against best practices.

3. Change Management

In our experience, the most challenging aspect of implementing product security practices is organisational change management. Rolling out changes internally may be fraught with resistance, and adopting these frameworks often come with challenges:

- *Prioritising risk management activities over other business objectives.* Adopting a product security framework often involves adding new responsibilities to software development teams. These teams are often already stretched to meet demands for new features and fixing defects. The additional work puts strain on fulfilling immediate customer requirements.
- *Lack of awareness of security risk.* Technical professionals do not always understand the full range of cybersecurity risks. As a result, they may have a misplaced belief that their software is already sufficiently safeguarded from threats and view any additional investment of effort and time as wasted.
- *Insufficient expertise*. Organisations that appreciate the full breadth of cybersecurity often lack the skills to implement all the new product security processes.

Integrating security into the software development process requires cultural change. Organisations can leverage their existing change management frameworks to address these concerns by mapping out stakeholder needs, defining the benefits for each stakeholder, running pilots and communicating results broadly, and measuring and reporting on progress. In our experience, cultural shifts related to embracing product security take a large organisation approximately two to three years.

With respect to next steps related to the Directive, organisations should evaluate legal obligations alongside their current internal processes and approaches with respect to information security, software development, and change management. Where gaps that directly impact compliance with the requirements of the Directive are identified, organisations should consider documenting such compliance gaps and developing operational strategies to close them. Given that the Directive must be adopted by EU member states within the next two years, organisations that have not yet embarked on compliance analysis should begin as soon as possible.

EU’s Revised Product Liability Directive: The Impact on the Legal, Business, and Operational Landscape

If you have questions regarding the legal implications of the EU’s Revised Product Liability Directive, reach out to the authoring attorneys Briony Pollard (bpollard@willkie.com) or Kari Prochaska (kprochaska@willkie.com) or contact the Willkie attorney with whom you regularly work. If you have questions concerning the impact on digital product manufacturers, reach out to Security Compass (info@securitycompass.com).

This article neither contains legal advice nor establishes an attorney-client relationship in any form. The opinions expressed herein are attributable to the author(s) alone, and they do not reflect the views, positions, or opinions of Willkie Farr & Gallagher LLP or other attorneys at the firm.