

Comply.Land Publishes New Guidance on Emergency Fixes and Manufacturer Obligations Under the EU Cyber Resilience Act

Addressing the question: what happens, when an integrator, service provider or software vendor makes an emergency change to a product it did not manufacture.

BIRGU, MALTA, October 6, 2026

/EINPresswire.com/ -- New dossier addresses when an emergency fix to someone else's product can make the fixer a "manufacturer" under the EU-CRA.

Comply.Land, a Malta-based compliance infrastructure provider focused on the EU Cyber Resilience Act (CRA), has published a new dossier addressing a question that has grown more urgent since the CRA's reporting obligations entered into force on 11 September 2026: what happens, under EU law, when an integrator, managed-service provider or software vendor makes an emergency change to a product it did not originally manufacture.



Downstream Post-Market Modifications and Break-Glass Agreements

The CRA entered into force on 10 December 2024, starting a 36-month transition period for manufacturers to implement it. Notifications of Conformity Assessment Bodies authorised to carry out third-party assessments began on 11 June 2026. The reporting obligations this dossier addresses entered into force on 11 September 2026, requiring manufacturers to report actively exploited vulnerabilities in their products and severe incidents to ENISA and national CSIRTs within 24 hours of becoming aware of them. The Product Liability Directive's transposition deadline follows on 9 December 2026, extending strict liabilities to defective software. The CRA's full application arrives on 11 December 2027, when all products with digital elements placed on the EU market must carry complete technical documentation and the CE marking and manufacturers must have representation in the EU via their own office, an Authorised Representative, Importer or Distributor.

Under Article 22 of the CRA, a party other than the original manufacturer, importer or distributor that carries out a substantial modification to a product and makes it available on the market can itself be treated as a manufacturer under the Regulation, for the part it changed or, in some cases, the whole product. That status carries the full set of Article 13 and Article 14 obligations, including technical documentation and vulnerability-reporting duties, for the affected parties.

The dossier, titled “[Downstream Post-Market Modification and Break-Glass Agreements](#)”, is prepared by Daniel Thompson-Yvetot, and sets out the legal test for when an emergency change crosses that line. It

recommends that organisations put a break-glass agreement in place in advance: a framework that pre-authorises emergency actions, allocates [CRA obligations](#) before an incident occurs, and defines the route back to the original manufacturer’s supported product.

“

Every emergency response plan we’ve reviewed assumes the fix is the hard part”

Daniel Thompson-Yvetot

The dossier is the third in Comply.Land’s CRA Fringe series, published weekly, each addressing a single question inside the Regulation. Earlier issues examined the 24-hour, 72-hour and 14-day reporting cascade that applies once a vulnerability is being actively exploited, and the question of whether a manufacturer’s Article 14 reporting duty survives a product’s support period.

“Every emergency response plan we’ve reviewed assumes the fix is the hard part”, said Daniel Thompson-Yvetot, founder and CEO of Comply.Land. “Under the Cyber Resilience Act, the harder part can be working out afterwards who just became a manufacturer, and by then it is too late to plan for it. That is exactly the kind of question this series exist to answer: not what the Regulation clearly says, but what happens in the cases it does not clearly cover.”

The dossier is available now at: <https://comply.land/dossiers/cra-substantial-modifications-manufacturer-obligations/>



Comply.Land logo

For access to all available dossiers, visit this page: <https://comply.land/shop/#dossier>

About Daniel Thompson-Yvetot

Daniel Thompson-Yvetot is founder and CEO of Comply.Land and CrabNebula Ltd., and co-creator of the Tauri open-source framework, the toolkit behind a generation of secure, lightweight desktop and mobile applications. He lives in Malta, where he was named Malta Information Technology Agency (MITA)'s Cybersecurity Leader of the Year.

Daniel navigates code as effortlessly as he interprets the regulation. He wrote the first book published in Europe on the Cyber Resilience Act (CRA), Manufacturing European Software, and sits on the Open Regulatory Compliance Working Group tracking the CRA and Product Liability Directive's impact on software manufacturers. As an ETSI Rapporteur he has led the drafting of four harmonised standards translating the CRA into European technical reality. He speaks regularly across Europe on [CRA compliance](#), open-source governance, and software security, including a keynote at a European Parliament conference on cyber resilience convened with MEP Peter Agius.

Daniel Thompson-Yvetot

Comply.Land

daniel@comply.land

Visit us on social media:

[LinkedIn](#)

[YouTube](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/946606295>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.