European Semiconductor Industry Association

POSITION

Data Act

Brussels, 26 October 2022

Broad scope

Unveiled on 23 February 2022, the "*Proposal for a Regulation on harmonised rules on fair access to and use of data (Data Act)*"[1] aims at opening new markets for data-driven services and accelerate innovation in the EU Single Market. However, the proposed legislation is handling overly broad definitions that do not sufficiently circumscribe a proper **scope**. Article 2(1) defines "*data*" without differentiating between product-related, technical, non-technical, personal or non-personal data, and Article 24(b) expands the scope to "*all data and metadata created by the customer* […] *including, but not limited to, configuration parameters, security settings, access rights and access logs*"[2]. This also poses questions around the protection of company **intellectual property** and **trade secrets**, a particular concern for the competitiveness of research-intensive sectors as the European semiconductor industry.

Take the example of a product with machine-learning capabilities: In this situation, the machine-learning model would use data generated by the "*use of the product*" as (continuous) training data. Although the intellectual property of the model (at initial product delivery) is proprietary to the product developer, manufacturer, or supplier, it is unclear whether the evolved model must be disclosed to the user or whether the machine-learning process is part of the "*data generated by use of a product*". If so, the intellectual property could easily be reverse-engineered and thus no longer be protected.

Therefore, ESIA would recommend restricting the definition of **"*data*"** as follows:

Article 2(1) 'data' means any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audio-visual recording; excluded are company intellectual property, trade secrets (in accordance with Directive (EU) 2016/943[3]), metadata, product-specific credentials, cryptographic keys and signatures used for authentication of the device, and product specific passwords;

Rue de la Duchesse 11/13
1150 Brussels
Belgium
Tel.: +32 2 290 36 60
Fax: +32 2 290 36 65
secretariat@eusemiconductors.eu
www.eusemiconductors.eu

ESIA is an industry association under the umbrella of
EECA: European Electronic Component Manufacturers' Association
EU Transparency Registry: 22092908193-23

Insufficient protections

To address the potential risk of **reverse engineering** more directly, ESIA suggests prohibiting it by default, unless otherwise agreed among parties (exceptions may include special technical requirements with key customers).

Article 2(11) 'processing' means any operation or set of operations which is performed on data or on sets of data in electronic format, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. For the sake of clarity, reverse engineering, disassembling, or modifying data are excluded;

Furthermore, the definition of "*product*" is very extensive & imprecise and could potentially include components of a product. To provide more legal certainty, ESIA suggests restricting the scope of the EU Data Act to **"*finished products*"** and using that terminology for the scope of the draft regulation:

Article 2(2a) 'finished product' means a product usable for its intended purpose without being embedded or integrated into any other product. Components of a device, such as a processor or a sensor, are excluded;

In addition, the Data Act should include a definition for **"*connected product*"**:

Article 2(2b) 'connected product' means a finished product that is intended to communicate directly or indirectly over the internet. Products that are primarily designed to store and process data, or to display, play, record and transmit content, are excluded;

In accordance with the amended "*data*" and "*product*" definitions above, the obligations of Article 3(1) should also be clarified to make sure that European and national legislation on cybersecurity – such as Network & Information Security (NIS) Directive[4] or the proposed Cyber Resilience Act[5] – are not foiled.

Article 3(1) Products shall be designed and manufactured, and related services shall be provided, in such a manner that data generated by their use that are accessible to the data holder and that the data holder controls are~~, by default,~~ easily, reasonably, securely and, where relevant and appropriate, directly accessible to the user.

It must be ensured that product design provisions of the EU Data Act do not lead to a situation where manufacturers are forced to compromise data security for data access.

For further information:

Hendrik Abma
Director-General
European Semiconductor Industry Association (ESIA)
Tel: + 32 2 290 36 60 • Web: https://www.eusemiconductors.eu/

ABOUT ESIA

The European Semiconductor Industry Association (ESIA) is the voice of the semiconductor industry in Europe. Its mission is to represent and promote the common interests of the Europe-based semiconductor industry towards the European institutions and stakeholders in order to ensure a sustainable business environment and foster its global competitiveness. As a provider of key enabling technologies, the industry creates innovative solutions for industrial development, contributing to economic growth and responding to major societal challenges. Being ranked as the most R&D-intensive sector by the European Commission, the European semiconductor ecosystem supports approx. 200.000 jobs directly and up to 1.000.000 induced jobs in systems, applications and services in Europe. Overall, micro- and nano-electronics enable the generation of at least 10% of GDP in Europe and the world.

[1] EUROPEAN COMMISSION (23/02/2022). *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on harmonised rules on fair access to and use of data (Data Act), COM(2022) 68 final*, EUR-Lex. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022PC0068&qid=1665763079565&from=EN (retrieved 19/10/2022)
[2] *Ibid.*, p. 38 & 53.
[3] DIRECTIVE (EU) 2016/943 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, OJ L 157, 15.6.2016, p. 1-18. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0943&from=EN (retrieved 19/10/2022)
[4] DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, p. 1-30. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN (retrieved 19/10/2022)
[5] EUROPEAN COMMISSION (15/09/2022). *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, COM(2022) 454 final*, EUR-Lex. URL: https://eur-lex.europa.eu/resource.html?uri=cellar:864f472b-34e9-11ed-9c68-01aa75ed71a1.0001.02/DOC_1&format=PDF (retrieved 19/10/2022)