Data Act

2022/0047(COD) - 14/03/2023 - Text adopted by Parliament, partial vote at 1st reading/single reading

The European Parliament adopted by 500 votes to 23, with 110 abstentions, **amendments** to the 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).

The issue was referred back to the committee responsible for inter-institutional negotiations.

Data and scope

Parliament clarified that the proposed Regulation should lay down harmonised rules on:

- the design of connected products to allow access to data generated by a connected product or generated during the provision of related services to the user of that product;

- data holders making available data they accessed from a connected product or generated during the provision of a related service to data subjects, users or to data recipients, at the request of the user or data subject;

- fair contractual terms for data sharing agreements;

- the making available of data to public sector bodies or Union institutions, agencies or bodies, where there is an exceptional need in the public interest;

- facilitating switching between data processing services;

- introducing safeguards against unlawful international governmental access to non-personal data; and

- providing for the development of interoperability standards and common specifications for data to be transferred and used.

Objectives

The Data Regulation aims to **boost innovation** by removing barriers obstructing consumers and businesses' access to data. The legislation will clarify who can access data and under what conditions. It will allow a wider range of private and public entities to share data.

To void the fragmentation of the internal market, it is necessary to lay down a harmonised framework specifying who, is entitled to use accessible data collected, obtained or otherwise generated by connected products or related services, under which conditions and on what basis.

The Regulation:

- obliges manufacturers of connected products and providers of related services to design their products and services in such a way that users of a connected product or related service in the EU can access, in a timely manner, the data accessible from the product or generated during the provision of a related service and that those users can use the data, including by sharing them with third parties of their choice;

- requires data holders to make data available to users and to data recipients designated by those users;

- provides that data holders should make data available to data recipients in the Union on fair, reasonable and non-discriminatory terms and in a transparent manner;

- provides that, if there is an exceptional need, data holders should make data available to public sector bodies of the Member States and to Union institutions, bodies, offices and agencies;

- further aims to facilitate switching between data processing services and to improve the interoperability of data and data sharing mechanisms and services in the Union.

SMEs

Start-ups, SMEs and companies from traditional sectors with less-developed digital capabilities struggle to obtain access to relevant data. This Regulation aims to facilitate access to data for these entities, while ensuring that the corresponding obligations are scoped as proportionately as possible to avoid overreach.

When companies draw up their data sharing contracts, the law will rebalance the bargaining power in favour of SMEs, **protecting them from unfair contract terms** imposed by companies in a much stronger bargaining position.

Compensation for the provision of data

To incentivise the continued investment in generating and making available valuable data, including investments in relevant technical tools, this Regulation contains the principle that data holders may request **reasonable compensation** when legally obliged to make data available to the data recipient in business- to business relations.

Any compensation agreed between a data holder and a data recipient for making data available in business- to- business relations should be non - discriminatory and reasonable. A data holder, a data recipient or a third party should not directly or indirectly charge consumers or data subjects a fee, compensation or costs for sharing data or accessing it.

Members strengthened provisions to protect trade secrets and avoid a situation where increased access to data is used by competitors to retro-engineer services or devices. They also set stricter conditions on business-to-government data requests.

Emergency situations

The amended text also sets out how public sector bodies, in exceptional circumstances or emergencies, such as floods and forest fires, can access and use data held by the private sector where necessary.

Strengthened coordination

Each Member State should designate an independent competent **coordinating authority** (‘data coordinator’) as responsible for the application and enforcement of this Regulation, for coordinating the activities entrusted to that Member State, for acting as the single contact point towards the Commission, with regard to the implementation of this Regulation and for representing the Member State at the European Data Innovation Board.

To further enhance coordination in the enforcement of this Regulation, the European Data Innovation Board should foster the mutual exchange of information amongst competent authorities as well as advise and assist the Commission in certain matters.

Data processing

Union law on the protection of personal data, privacy and confidentiality of communications and integrity of terminal equipment shall apply to any personal data processed in connection with the rights and obligations laid down in this Regulation. Any contractual term in a data sharing agreement between data holders and data recipients which, to the detriment of the data subjects, undermines the application of their rights to privacy and data protection, derogates from it, or varies its effect, will be void.

International access and transfer

Providers of data processing services should take all technical, legal and organisational measures, including contractual arrangements, in order to prevent international transfer and third-country governmental access to such non-personal data held in the Union where such transfer or access would be in contravention of Union law or the national law of the relevant Member State.