Brief Report on the Framework for the Free Flow of Non-personal Data in the European Union (FFD)

The Regulation (EU) 2018/1807

Rahul Patil[1] and Anjula Gurtoo[1]

[1] Centre for Society and Policy, Indian Institute of Science, Bangalore 560012, Karnataka, India

The report covers the provisions of the Framework on Free flow of Non-personal Data relevant to the operationalisation of goods and services related to the non-personal data and its management.

Introduction

The report elaborates on non-personal data, which is at the core of the Regulation. Overall, it has four sections, viz., 1. Basics of non-personal data and its regulatory framework; 2. Shedding of data localisation requirements; 3. Data availability for competent authorities & cooperation among each other; and 4. Data portability for professional users. These four sections detail salient provisions carved under relevant FFD Articles and Recitals, which are also cited.

Under Sect. 1, the notion of non-personal data and the context of the FFD regulations are set along with the need for the various provisions for a data economy and a Single Digital Market in the Union. In the Sect. 2, imposition and repealing of data localisation requirements are discussed. Sect. 3 focuses on the concerns of the public authorities and their duties in monitoring data processing practices and facilitating the regulated data economy. Another important procedural adoption of the regulation, data portability, is discussed further in the Sect. 4.

Corresponding author: Patil, R. (rahulb@iisc.ac.in)

In brief, the Regulation tries to ensure that it is flexible enough to accommodate the evolving needs of the users, services providers, and National or Commission authorities in the Union and the Member States. Even the Regulation follows the principle (as stated in Recital 11) of not detailing the technical rules (i) to avoid the risk of overlaps with existing mechanisms and (ii) to avoid higher burdens both for Member States and businesses

The Regulation (EU) 2018/1807 (i.e., FFD) has 9 articles and 39 recitals and applies to all the organisations in the EU or outside involved in handling data processing in the Union.

Non-Personal Data

↳ Any information not related to an identified or identifiable natural person

FFD

↳ Only applicable, if electronic non-personal data is being processed in Europe

Section 1: More about non-personal data and its regulatory framework

i. Non-personal data:

What is non-personal data?

Non-personal data is data other than personal data as defined in point (1) of Article 4 of Regulation (EU) 2016/679.

Some of the examples of non-personal data cited in the recitals of the Regulation are:

- Aggregate and anonymised datasets used for big data analytics;
- data on precision farming that can help to monitor and optimise the use of pesticides and water;
- data on maintenance needs for industrial machines

ii. FFD Regulation:

What is the scope of the regulation?

1. Applicable to the processing of electronic non-personal data
2. Applicable to the processing of such data as a service in the Union
- independent of the fact whether a service provider is from the Union or not
1. Applicable to the processing of such data by a natural or legal person in the Union for its own need

What is the breadth of the regulation?

Application of Regulation is in the broadest sense

- Encompassing the usage of all types of IT systems (either located on the premises of the user or outsourced to a service provider)
- Covering data processing of different levels of intensity – e.g.:

- *Data storage:* Infrastructure-as-a-Service (IaaS)
- *Processing of data on platforms:* Platform-as-a-Service (PaaS)
- *Application:* Software-as-a-Service (SaaS)

When did the regulation come in force?

Application of Regulation is in the broadest sense

- The Regulation on a framework for the free flow of non-personal data in the European Union (i.e., Regulation (EU) 2018/1807 of 14 November 2018) is entered into force on 28 May 2019.
- The translational period of 24 months starts from the date of application of the Regulation up to 30 May 2021.

What are the provisions of the translation period?

- The translation period allows the Member States to review existing provisions in the national legislative instruments compared to the provision prescribed in the Union legislation.
- Responsibilities of the Member States:
    - Review of existing laws, regulations, or administrative provisions of a general nature laying down data localisation requirements
    - Communicate to the Commission any such data localisation requirement that they consider complying with this Regulation along with the justification for the same

- Responsibilities of the Commission:
  - Examine the compliance of any remaining data localisation requirements
  - Make comments in question to the Member States & can include recommendations to amend or repeal the data localisation requirement

How does the timely relevancy of the FFD provisions get monitored?

The Regulation advises the Commission to evaluate its provisions and report them along with the recommendations in light of the necessary modification.

- The Commission should prepare a report on the implementation and evaluation of the Regulation before 29 November 2022 – detailing:
  - The need for modifications – considering technological or market developments
  - Evaluation of the application of regulation on mixed datasets
  - Implementation of the public security exception

- The Commission should publish (before 29 May 2019) informative guidance on the handling of mixed data sets:
  - For the companies to understand the interaction between GDPR and FFD

iii. Setting the context of FFD and its intention

Achieving data-driven growth and innovation and creating the Digital Single Market are the prime objectives of the European Commission. Previous studies (SMART 2015-0016, 2017) commissioned for the European Commission have shown that the legislative modulations can potentially lead to a high-growth scenario of 4% additional EU GDP (FFD Factsheet, 2019).

What has been agreed?

A single set of rules for all market participants: Key element for the functioning of the internal market – (FFD Recital 7)

- To establish legal certainty
- To avail a level playing field within the Union

Objective: to remove obstacles to trade and distortions of present & likely competition resulting from divergences between national laws

iv. Modes of tackling the obstacles

To harness this potential, the facilitation of cross-border data flows has been highlighted. However, it's prescribed in the FFD recital 24 that the competent authorities of Member States have less preferred cross-border data processing due to a lack of trust in such data processing and presumed unavailability of data for inspection and audit for regularity or supervisory control. Such circumstances lead to data localisation requirements, limiting cross-border data processing activities and reducing the desired data-driven growth and innovation.

The following activities are involved in the data value chain:

- data creation and collection
- data aggregation and organisation
- data processing [*fundamental building block*]
- data analysis, marketing, and distribution
- use and re-use of data

  - The data processing activities are hampered by two types of obstacles:
    i. Data localisation requirements put in place by Member States' authority
    ii. Vendor lock-in practices in the private sector

Section 2: Rights conferred by the CCPA

i. The imposition of data localisation requirements:

Recital 24 of the FFD explicitly highlights that the data localisation requirements stem from a lack of trust from the competent authorities for the cross-border processing by natural/legal persons or any data processor in the Union.

Such imposition of data localisation requirements hampers the effective & efficient functioning of data processing and the development of the data economy. It's been projected that in the absence of the data

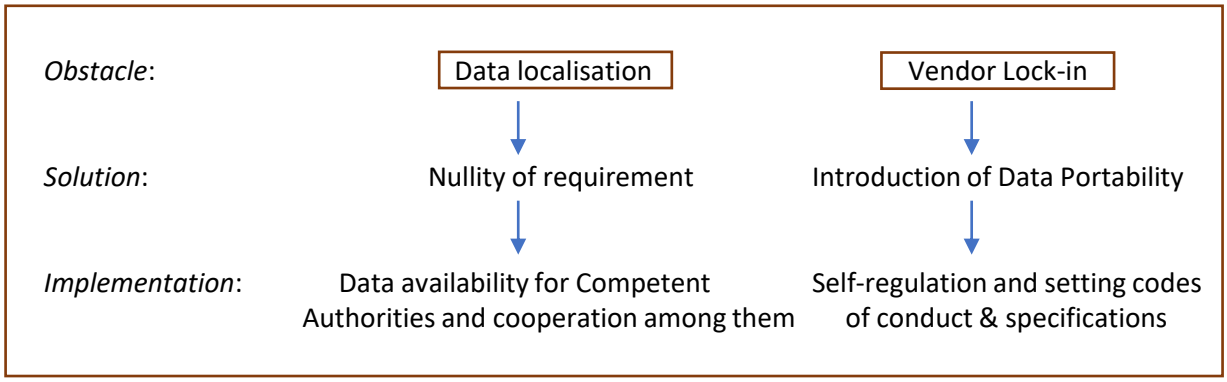

Figure 1: Strategies to tackle data location and vendor lock-in obstacles

localisation requirements high growth scenario can be achieved by adding an extra 4% to the EU's GDP. The analysis has shown that building a data centre in high-cost European locations costs 120% more than in the low-cost ones (SMART 2015-0016, 2017).

ii. Nullity of data localisation requirements:

The primary intention of the Regulation is to nullify data localisation requirements for the data processors imposed by Member States of the EU. However, the Commission believes that the lack of trust from the competent authorities of Member States cannot be overcome solely by the nullity of contractual terms prohibiting lawful access to data by competent authorities to perform their official duties. The Regulation prescribes measures to facilitate their functioning to empower the concerned competent authority. These measures to monitor and scrutinise the practices are enlisted under Sect. 3(b).

The Regulation has formulated a coherent set of rules across the Union while nullifying the data localisation requirement imposed by the Members States:

- No restrictions on the free movement of the non-personal data within the Union by the Member States
    - Exception: when a restriction or a prohibition is justified by public security reasons – only justification for data locations
- No obligations on storage of the different types of data separately

iii. Public authorities and bodies: Setting up an example:

The Regulation highlights that the public authorities and bodies governed under the Union laws or of the Members States handle large amounts of data. Hence, it's important that they lead by example:

- by taking up data processing activities
- by refraining from making the data localisation requirements while using data processing activities

The Regulation does not oblige the Member States to outsource or insource the services that they wish to provide themselves (or organised by means of the other public contracts)

- Public authorities and bodies are encouraged to consider the economic or other benefits of outsourcing services
- They might have legitimate reasons to choose self-provisioning of services or insourcing

Commission also suggests the Member States communicate *any draft act* to the Commission in the cases to prevent the emergence of new barriers to the smooth functioning of the internal market, such as:

- Draft act introducing a new data localisation requirement or modifying an existing data localisation requirement
    - Such *draft acts* have to be submitted and assessed in accordance with Directive (EU) 2015/1535 - a procedure for the provision of information in the field of technical regulations and rules on Information Society services

Section 3: Data availability for competent authorities & cooperation among each other

i. Availing non-personal data for scrutiny:

Recital 24 of the FFD explicitly highlights that the data localisation requirements, which are found to be an obstacle to the data economy to its fullest potential, are imposed by the Member States Authorities due to the presumed unavailability of the data for the scrutiny.

guidance on how to comply with the provisions.

Measures for proper implementation of the Regulation:

To address the concerns of the competent authorities, the Regulation clearly states that –

- It does not affect the powers of competent authorities to request or obtain access to data in accordance with Union or national law.
- Whereas such competent authorities cannot be refused access to data on the basis that the data are processed in another Member State.
- Such competent authorities can impose functional requirements concerning data access, e.g., keeping system requirements in the concerned Member State.

ii. Powers and responsibilities of the Member States and Authorities:

Transparency provisions for proper implementation of the Regulation:

1. To ensure transparency in data location requirements, the Regulation suggests that

- The Member States should publish/update information on requirements on a national online single information point
- The Member States should communicate the address of the national online single information point to the European Commission
- The European *Commission should publish/update this information* on their website

2. The regulation obliges natural or legal persons to comply in –

- providing and *guaranteeing effective and timely electronic access* to data to competent authorities
    - Irrespective of the member state in which data is being processed

3. In the case where natural/legal *person fails to comply with an obligation*:

- The concerned competent authority should seek assistance from competent authorities in other member states
- The competent authority should use specific cooperation instruments in Union law or under international agreements
    - e.g., in the respective subject matter: police cooperation, criminal or civil justice, administrative matters

4. Regulations should not allow attempts to evade the application of law:

- The imposition of (effective, proportionate, and dissuasive) *penalties* by the Member States on users - which prevent competent authorities from receiving access to their data necessary
- The imposition of strictly proportionate *interim measures* by the Member States on uses – where a user abuses its right
    - If re-localisation of data is imposed for more than 180 days (in the case of interim measures), it should be communicated to the Commission for the examination of its compatibility with the Union Law

5. Security requirements applied in a justified and proportionate manner (as per Union or respective national law) in the Member State of residence/establishment of natural/legal person should also be applied in the other Member States.

- Equivalent to reciprocity
- Protection of natural/legal person's rights in the other Member States

- The natural/legal person should fulfil these requirements by themselves or by service providers

6. Security requirements (in the national law) should be proportional to the risks posed to the security of data processing (at national level).

7. While enforcing powers, competent authorities might have to look up provisions of other Union regulations or the laws enacted by the Member States aligned with the Union regulations.

Such provisions might involve the following –

a) Interpretations of the EU Regulations TFEU (Article 52), TEU (Article 5), and the Court of Justice regarding public security and the principle of proportionality

- The Treaty on the Functioning of the European Union – TFEU
- Public security - Article 52
  - Both internal and external security – Court of Justice interpretation
  - Issues of public safety
  - To facilitate the investigation, detection, and prosecution of criminal offences

- *Genuine and sufficiently serious:* threat affecting one of the fundamental interests of society
  - Threat to the functioning of institutions and essential public services and the survival of the population
  - Risk of a serious disturbance to foreign relations or the peaceful coexistence of nations
  - Risk to military interests

- Treaty on European Union – TEU
  - The principle of proportionality – Article 5

b) Provisions of the public procurement: Directive 2014/24/EU

c) Previsions of the contract law (contractual obligations): Regulation (EC) No 593/2008

d) Provisions related to the level of cybersecurity: Directive (EU) 2016/1148

- Data processing services = Digital services
- Service providers should ensure technical and organisational measures to manage the risks posed to the security of network and information systems – such measures should consider the following elements:
  - security of systems and facilities
  - incident handling
  - business continuity management
  - monitoring, auditing, and testing
  - compliance with international standards

iii. Cooperation procedures among authorities:

Under Article 7, the Regulation prescribes the rules to establish and facilitate harmony between competent authorities. Such provisions are particularly of great importance when competent authorities scrutinise the data processing activities across the Member States. Such provisions are also important in cases where multiple subject matters are involved.

1] If the request for assistance (by the authority) involves *access to any premises* of a natural or legal person (including to any data processing equipment and means)

- Such access must be in accordance with Union law or national procedural law
- With the requirement to obtain prior judicial authorisation

2] For requesting assistance between the Member States, there should be a single point of contact between the requesting and requested the Member States.

- Such assistance-related requests should be further transmitted to the competent authority.

- In response, information related to difficulties faced should be provided if the request cannot be fulfilled or the grounds for refusing it.

3] Any information exchanged in the context of assistance requested should be used only for the matter requested.

4] The single point of contact with the competent authorities shall provide users with general information on this Regulation, including on the codes of conduct.

Section 4: Data portability for professional users

i. Data Portability: A measure for ensuring competition in the internal market

A competitive internal market for data processing services can be contributed by –

- Data portability
- Consistent technical requirements
  - technical harmonisation,
  - mutual recognition
  - voluntary harmonisation

Data Portability can facilitate (i) user choice, and (ii) effective competition in the markets for data processing services

- User is not allowed to port their data – who act in the course of their business or professional activities.
  - i.e., during the contractual terms/ before termination of the contract

Professional users should be able to

- Make informed choices
- Easily compare the individual components of various data processing services
  e.g., contractual terms and conditions of porting data upon the termination of a contract

Self-regulation to support the free flow of data:

The Commission encourages industry players to develop self-regulatory codes of conduct at the EU level to foster a competitive data economy

- porting of data to avoid vendor lock-in practices (users cannot switch between service providers because their data is 'locked in' the provider's system)

Work should be considered on the issue of liability:

1. implementation of self-regulatory codes and other best practices
2. taking into account recommendations, decisions, and actions taken without human interaction along the entire value chain of data processing

Include –

- appropriate mechanisms for determining liability
- appropriate mechanisms for transferring responsibility among cooperating services
- appropriate mechanisms for insurance and auditing

ii. Self-regulation of codes-of-conduct

The Regulation encourages and facilitates the development of self-regulatory codes of conduct based on the principles of transparency and interoperability.

It has been stated that such contributions should consider open standards by covering:

- Best practices facilitating data porting in a structured manner, commonly used, and machine-readable format with preference to the open standard format
- Professional users should be provided with the *minimum information* before a contract for data processing is concluded in
  - A sufficiently detailed, clear, and transparent manner
    - regarding processes, technical requirements, timeframes, and charges that apply to the professional user while data porting
- Certification schemes can be approached to facilitate the comparison of data processing products and services.
  - Consider national/international norms
  - Include factors such as quality management, information security management, business continuity management, and environmental management
- Preparation of roadmaps for creating awareness of the codes of conduct among stakeholders

Market players should define the detailed information and operational requirements for data porting:

- In the form of the Union codes of conduct, i.e., model contractual terms and conditions

- Considering alignment with the innovation potential of the market
- Considering the experience and expertise of the service providers and professional users of data processing services

Codes of conduct:

- It should be comprehensive.
- Addressing critical aspects regarding the process of porting data –
  - The processes used for data back-ups & the location of data back-ups
  - The available data formats and supports
  - The required IT configuration and minimum network bandwidth
  - The time required before initiating the porting process and the time during which the data will remain available for porting
  - The guarantees for accessing data in the case of the bankruptcy of the service provider
  - Suggesting vendor lock-in is not an acceptable business practice
  - Providing trust-increasing technologies
- It should be regularly updated to keep pace with technological developments.

iii. Responsibilities of the Commission for self-regulated codes-of-conduct

- The Commission should ensure that all the stakeholders are consulted throughout the process, e.g., associations SMEs & start-ups, users, and cloud service providers
- The Commission should evaluate the development & the effectiveness of the implementation of such codes of conduct

REFERENCES

1. FFD, (2019). Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R1807
2. SMART number: 2015/0016. (2017). Facilitating cross border data flow in the Digital Single Market. European Commission. London Economics. https://ec.europa.eu/digital-single-market/en/news/facilitating-cross-border-data-flow-digital-single-market
3. FFD Factsheet. (2019). Shaping Europe's digital future. Free flow of non-personal data. https://ec.europa.eu/digital-single-market/en/news/free-flow-non-personal-data