Computer & Communications Industry Association

Tech Advocacy Since 1972

CCIA comments on the relationship between GDPR and Free Flow of Non-Personal Data Regulation

CCIA welcomes the opportunity to present its views on the interpretation and application of the newly adopted Free Flow of non-personal Data (FFoD) Regulation. We believe that the free movement of data is essential to build a thriving European digital single market. CCIA supports an ambitious application and enforcement of the principle of free movement of data that is coherent with the spirit of this Regulation and the General Data Protection Regulation.

In our view, a meaningful principle of free movement of data requires a broad interpretation, particularly in instances when personal and non-personal data are mixed, with clearly delineated limitations. For this reason, we believe that **the principle of free movement under FFoD should apply to both personal and non-personal data** w**hen personal and non-personal data are inextricably linked.** Nothing else changes as far as the application of GDPR is concerned: all relevant provisions of the GDPR (particularly chapters 1 to 4, and 9), should be observed by controllers and processors when a dataset qualifies as personal data.

We believe this in line with the spirit of both FFoD and the General Data Protection Regulation:

- While both texts share the objective of facilitating the free flow of personal and non-personal data[1], the relevant provision of GDPR provides Member States more room to restrict or prohibit the free movement of data than the FFoD. One the one hand, Article 1(3) GDPR prohibits data localisation restrictions grounded on the protection of personal data. This means any other grounds can be used to justify localisation restrictions. On the other hand, Article 4(1) FFoD only permits restrictions if they are based on public security. In other words, Member States cannot use any other grounds to justify restrictions.

- In cases where personal and non-personal data cannot be separated, this dissonance between the two texts could raise a tension between national localisation laws and measures that are compliant with the GDPR and the application and enforcement of the FFoD.

[1] See Recitals 3, 6, 9, 13, Article 1(1) and (3) of the GDPR, and the legal basis of the GDPR referred to in Recital 12. See also Recitals 4, 8, 9 and 10 of FFoD, and the very objectives of the Regulation encapsulated in its Article 1 and 4.

- The FFoD addresses this tension in Article 2(2) and provides that it "shall not prejudice the application of Regulation (EU) 2016/679". We believe that this provision should be read in a way that the **principle of free movement under the FFoD be extended to personal data in those instances. We believe this interpretation reinforces, rather than *prejudice*, the principle of free movement of data of the GDPR.** Conversely, using the GDPR more laxed exemption regime to undermine one of the very objectives that it pursues would run afoul the spirit of the GDPR and the lawmakers' intentions.

- We recall that the purpose of the GDPR is "to prevent divergences hampering the free movement of personal data within the internal market" according to Recital 13. The same recital further specifies that "the proper functioning of the internal market requires that the free movement of personal data within the Union is not restricted or prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data."

- In addition, nothing in the GDPR can be construed as granting Member States the power to restrict the principle of free movement of personal data. The only restrictions and limitations to the application of GDPR allowed under Section 5 only apply to the exercise of the data subjects' rights. The explicit restrictions or limitations to the GDPR do not apply to the principle of free movement of personal data under Article 1(3).

As illustrated below, this interpretation is particularly relevant to ensure regulatory certainty for the development and deployment of Internet of Things, artificial intelligence and machine learning beyond industrial applications.

Practical examples

Example 1 -- A new gambling law authorizes online gaming and gambling services providing that regulators have "direct access" to certified IT systems and data held by online gambling service providers. The data which must be held in the country include user account information, wagers made, and winnings paid out.

The primary motive behind this measure is to ensure effective regulatory oversight on gaming and gambling activities, specifically to detect fraud and mitigate adverse effects on public health within the country.

An online gaming operator is considering improving its services and taking action to ensure responsible use of its service by implementing third-party machine-learning technologies. The primary aim of this technology is to detect and prevent cases of addiction or other forms of risky gaming patterns[2]. The technology involves the processing of thousands of gameplays from existing users ("data source"), the anonymisation, aggregation, and analysis of this information

[2] See for instance responsible gambling analytics company Bet Buddy. This company specialises in providing online betting companies with analytics to improve each single user's gameplay experience and detect cases of risky gaming patterns.

to learn from past experience ("data insight"), and real-time analysis of each and every single future gameplay and how they match up with pre-identified risky gaming patterns. In this case, the use of this technology involves both personal and non-personal data at various processing stages, each of which are inextricably linked to one another to deliver the service.

In this scenario, Article 1(3) of the GDPR alone would not prohibit such a data localisation restriction to the extent that the motives behind the measure are not connected with the protection of individuals' personal data, but rather the fight against fraud and public health.

Depending on the wording of the legislation, any further processing that would render personal data as non-personal data - in this case, processing which would detect and prevent risky gaming patterns - could also be subject to the localisation restriction. This could potentially run against the FFoD to the extent that (a) the datasets do not constitute personal data and (b) the national data localisation measure is not "justified on the grounds of public security".

Should the law explicitly permit anonymisation of personal data and subsequent processing of non-personal datasets outside the jurisdiction of the Member State, three questions arise for the online gambling service provider and its third party analytics service provider:

- Can the process of anonymisation take place outside the jurisdiction of the country?
- From a technical perspective, does the IT system architecture of the online gaming operator and the third party analytics service provider permit segregation and subsequent integration of datasets?
- If so, is segregation and subsequent integration a viable way forward financially?

If the answers to these questions are negative, the national data localisation restriction, albeit permitted under the GDPR, would at best restrict the processing of non-personal data within the country. At worst, this restriction would prevent the online gaming operator from implementing this third party service even if the purpose of the service contributes to the public health objective which the data localisation restriction aims to pursue.

Either way, this data localisation restriction would effectively prevent the free flow of non-personal data within the EU, ultimately nullifying the effect of the FFoD.

Example 2 -- An EU Member State adopts a new legislation requiring all establishments governed by its national health service to store copies of all their data, including patient records (personal data), in the National Health Registry. The law does not provide for a possibility of data transfers outside of this system. Healthcare services using patient data (e.g. hospitals, independent healthcare practitioners used for post-op patient treatments and recovery, social security service, and private insurance companies) must obtain attestations of conformity at the national level, and must adhere to nationally defined interoperability and encryption requirements.

The motives behind this restriction are security (e.g. preventing unauthorised access to IT systems and assets), maintaining exclusive control over national healthcare systems, and ensuring availability and access to patient records across healthcare organisations.

A medical research centre is considering partnering with a service provider specialised in providing AI-powered analytics to help health practitioners prioritize care for patients requiring urgent treatment and meet their own care response-time guidelines e.g. in the case of AMD retinal diseases.

The technology involves the processing of as many prior patients' scans and related diagnosis as possible ("data source"), the anonymisation, aggregation, and analysis of this information to learn from past experience ("data insight"), and the analysis of each and every single future scans and how they correlate with pre-identified diagnosis along with corresponding treatments for a given patient. In this case, the use of this technology involves both personal and non-personal data at various processing stages, each of which are inextricably linked to one another to deliver the service.

In this case again, Article 1(3) of the GDPR alone would not prohibit such a localisation restriction of the patients' data processed at the very early stage of the process and before anonymisation (i.e. the data source), and the processing involving the correlation of the insight with the data obtained from scans of a given patient. This is because the motives behind the measure are not connected with the protection of individuals' personal data, but rather public health.

Because the law does not provide for a possibility of data transfers outside the National Health Registry, the processing necessary to perform this kind of scan analytics must be done in-house following an attestation of conformity by the responsible authority. In-house processing would require sufficient computational power for the service to scale and train itself better scans after scans. Above all, the rich dataset borne out of anonymised patients' data along with the pattern of correlation between different scans and corresponding diagnosis and treatments would not be permitted to leave the National Health Registry. This would effectively negate the effect of the free flow of non-personal data regulation.

Contact: Alexandre Roure, Senior Manager, Public Policy: aroure@ccianet.org