

Regulatory Monthly Newsletter

Welcome to the twenty sixth monthly newsletter designed to keep BIIA members informed of the significant developments on the policy dossiers being worked on in Europe and in other geographical territories.

SUMMARY

As you will see from reading this newsletter there has been a lot of activity relating to GDPR since our last communication at the end of July with a number of countries issuing the final regulation to make GDPR effective. We have also seen further guidance materialising from both Brussels and local Data Protection Authorities.

GDPR is also having an impact outside of Europe with a number of countries moving forward with implementing data protection regulation that is aligned to what Europe has implemented – see the ‘Rest of the World’ section for more information.

On a different subject work on Artificial Intelligence (AI) is gaining traction in Europe as regulators seek to understand the benefits and impact of the use of this new technology.

Keep a lookout for further updates on these two key topics and others in our next newsletter.

IN EUROPE

PRIVACY

European Commission: views on legitimate interest

In August, some [comments](#) from the European Commission on the Serbian government’s draft data protection law were published. The comments, written back in April 2018, followed the consultation of the Serbian authorities, which aim to align the legal framework of data protection in Serbia with the framework in the EU.

In those comments, when referring to the issue of legitimate interest, the European Commission states that:

- The GDPR considers as lawful data processing which is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject; and

Regulatory Monthly Newsletter

- Legitimate interests refer to the stake that a controller may have in the processing, or the benefit that it derives (or that others might derive) therefrom (e.g., the interest of a bank to use its customer data to detect fraud or protect against money laundering schemes).

These comments somewhat expand the 'official' interpretation of legitimate interest as provided on the website of the European Commission [here](#). (Click the highlighted text to access the comments and European Commission website)

Spain moves on GDPR implementation

Due to the complex balances inside the Spanish Parliament, Spain has been unable to put in place a new Data Protection Act that develops the GDPR. For that reason, on Friday 27 July 2018, the Spanish Government approved Decreto-Ley on Data Protection Matters (“[RDL 5/2018](#)”) indicating that there were urgent reasons to do so. A Spanish Decreto-Ley is considered technically a Law but it needs to be confirmed by the Parliament within a short timeframe, otherwise, it will lose its legal force automatically.

The scope of the RDL 5/2018 is very limited. It deals mainly with procedural matters. The message behind the approval and publication of RDL 5/2018 is that the Spanish Government is doing whatever it can to move forward the adequate application in Spain of GDPR. The RDL 5/2018 would put some pressure on the Parliament to complete the task with the shortest delays. (Click the highlighted text to access the Decreto-Ley)

Italy moves on GDPR implementation

A [legislative decree](#) integrating the GDPR into the Italian rulebook was recently published on the Official Gazette. The text will be binding with effect from 19th of September 2018.

A key question is how does the new law relate to the existing, pre-GDPR, code of conduct regulating credit bureaus ([here is the text in English](#)). This is dealt with in article 20. According to the analysis by BIIA member, CRIF:

- The existing code of conduct will continue to produce its effects for up to 12 months since the entry into force of the legislative decree, the time varying depending on the procedure described below.
- The time limit indicated above will depend on whether the affected industry associations (credit bureaus, banks, etc.) will activate the procedure to submit a new code of conduct ex art. 40 GDPR or not, and on the length of the approval procedure.

2

Copyright © BIIA 2018 - For Member Internal Use Only –
To Request Permission to Publish Contact: Neil Munroe at neilm@crsinsights.com

Regulatory Monthly Newsletter

- Starting from the entry into force of the decree, the interested subjects will have up to 6 months (= 19th March 2019) to submit the text of a new code of conduct (ex art. 40 GDPR) to the Italian Data Protection Authority. Starting from the date they submit the draft new code of conduct, the approval procedure shall end within max. 6 months.

Should the interested subjects not submit any new code by the first 6-months deadline, the existing code of conduct will cease to be operational. Same if the submitted code of conduct is not approved by the second 6-month deadline. **(Click the highlighted text to access the Decree and code of conduct)**

And finally Belgium also moves on GDPR

On 5 September, the [new Belgian Data Protection Act](#) (in Dutch) implementing the GDPR was published and entered into force. Since December 2017, however, Belgium has had in place a [law](#) implementing many of the more procedural provisions of the GDPR, notably the structure, powers and competence of the new Belgian Supervisory Authority.

The new Belgian Act focuses on the implementation of the remaining (more substantive) provisions of the GDPR, where the text often goes beyond the European framework. Belgium also chose to implement the GDPR's provision allowing Member States to foresee additional penalties applicable to GDPR infringements, and the Belgian Act expressly provides for criminal sanctions.

For a succinct analysis of the main provisions, you can consult the [blog](#) of law firm Sidley here. **(Click the highlighted text to access the Act and the blog)**

French DPA warns two companies for potential GDPR violations

France's Commission Nationale de L'informatique et des Libertés (CNIL) published a formal [warning](#) i.e. no penalty to two companies - Teemo, Inc. (Teemo) and Fidzup SAS (Fidzup) - that allegedly collected and retained geolocation data in violation of the EU's GDPR. The warning provides some insight into how European data protection authorities may approach GDPR enforcement with respect to the consent and data retention requirement.

German DPAs' list of data processing activities subject to DPIA

The German Data Protection Authorities (German DPAs) have jointly released a [list of processing activities](#) that are subject to a data protection impact assessment (DPIA). The List contains 16 examples and thereby the areas that German DPAs consider constituting "high risk" processing activities, including the

3

Copyright © BIIA 2018 - For Member Internal Use Only –
To Request Permission to Publish Contact: Neil Munroe at neilm@crsinsights.com

Regulatory Monthly Newsletter

'aggregation of personal data from various sources and further processing of the aggregated data (e.g. fraud prevention systems or **scoring** by banks or insurances)'.
The list is not exhaustive and is subject to future revisions. (Click the highlighted text to access the list of processing activities)

DATA

A regulatory sandbox for data experimentation?

The UK's Information Commissioner (ICO) is [calling for evidence](#) and initial views on creating a regulatory sandbox. The ICO sandbox will be a safe space where organisations are supported to develop innovative products and services using personal data in innovative ways. Firms will not be exempt from complying with data protection law, but they will have the opportunity to engage with the supervisor; drawing upon the ICO's expertise and advice on mitigating risks and data protection by design, whilst ensuring that appropriate protections and safeguards are in place.

This call for evidence is the first stage of the consultation process. The ICO seeks early evidence and views on the feasibility, scope and demand for a sandbox. This will be used to inform detailed proposals for consultation later in the year. This consultation closes on 12 October 2018.

This initiative is very relevant for the credit reporting industry. Traditionally, the concept of regulatory sandboxes has been discussed in the context of financial supervision. As a result, only credit reporting agencies supervised by financial supervisors could eventually benefit from the sandbox. However, the ICO initiative is horizontal, potentially benefiting any firm that manages and processes data. The ICO initiative can, furthermore, set a precedent for other data protection authorities in Europe. (Click the highlighted text to access the call for evidence)

FINANCIAL SERVICES

Loan-based crowdfunding platforms in the UK

The UK Financial Conduct Authority (FCA) is consulting on its [recommendations](#) for changes to P2P lending regulations for loan-based crowdfunding platforms. The FCA invites responses to rule changes for loan-based firms which cover proposals to:

- ensure investors receive clear and accurate information about a potential investment and understand the risks involved;

Regulatory Monthly Newsletter

- ensure investors are adequately remunerated for the risk they are taking;
- provide transparent and robust systems for assessing the risk, value and price of loans, and fair/transparent charges to investors; and
- promote good governance and orderly business practices.

Interestingly for credit information providers, P2P platforms should offer more information about the creditworthiness of the borrowers on their platforms. **(Click the highlighted text to access the recommendations)**

Global Financial Innovation Network

On 7 August 2018, the UK FCA, collaborating with 11 overseas financial regulators, **announced** the creation of the Global Financial Innovation Network (GFIN) and together they published a **consultation document** about this. The overseas regulators (the Regulators) include regulatory bodies from Abu Dhabi, France, Australia, Bahrain, the USA, Dubai, Guernsey, Hong Kong, Singapore and Canada.

The GFIN aims to provide an efficient way for innovative firms to interact and preserve an open dialogue with the regulators while trying out new ideas. At the same time, the GFIN should:

- act as a network of regulators to collaborate and share experiences with innovation in respective markets, including emerging technologies and business models;
- provide a forum for joint policy work and discussions; and
- provide firms with an environment in which to trial cross-border solutions.
-

The consultation will remain open until 14 October 2018. The FCA and the Regulators committed to engaging in the next two months with interested parties across the different jurisdictions involved in the project. Further feedback and an update on the next steps is expected in the autumn. **(Click the highlighted text to access the announcement and consultation document)**

TECHNOLOGY

National AI strategies

A **recent post** on Medium summarises the key policies and goals of over 10 countries that have published strategies in the last 10 months regarding their AI policies and initiatives. You may wish to bookmark it as the page is continuously updated as new programs are published, or existing ones are updated.

Regulatory Monthly Newsletter

One of those countries is Germany. The German government has recently released a [paper](#) on Artificial Intelligence which shall evolve into a fully-fledged strategy by the end of the year. The paper includes **considerations on algorithms amongst others on the importance of algorithmic transparency, auditability** and control in decision-making to ensure that no discrimination or manipulation is possible when algorithms take decisions or model forecasts. In the following months, the government plans to consult stakeholders across Germany to further develop the strategy which will be presented at a digital summit on the 3rd and 4th December 2018. **(Click the highlighted text to access the post and paper)**

Work on AI ethical guidelines starts

On 20 September 2018, the European Commission's [High-Level Expert Group on Artificial Intelligence \(AI\)](#) will hold the first of three workshops in Brussels. The High-Level Expert Group was set up by the Commission with the aim of developing draft AI Ethical Guidelines and making mid- and long-term policy recommendations on AI-related challenges and opportunities.

The five topics that will be discussed during the first workshop are:

1. Trusted (i.e. responsible and safe) AI
2. Transparency and Accountability:
3. Industry and Ecosystem Uptake of AI
4. AI Infrastructure and Enablers
5. Use-Cases for the Guidelines

Over the next months, the High-Level Expert Group will organise two workshops to gather further input on additional relevant topics. The Commission aims for the draft AI Ethical Guidelines to be formally presented at the first annual assembly of the AI Alliance in Q1 2019. **(Click the highlighted text to access the website for the Expert Group)**

Proposal on cybersecurity

The European Commission has recently released a [Proposal](#) for a Regulation addressing the EU's cybersecurity industry as part of its next step towards a Digital Single Market. The Regulation would establish the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres in order to 'equip Europe with the right tools to deal with an ever-changing cyber threat'.

Regulatory Monthly Newsletter

The Commission is hoping that the creation of this Network will allow the many existing cybersecurity competence centres in the EU to pool and share information and expertise, help deploy EU cybersecurity products and solutions, and facilitate cooperation between industries and communities. The Commission expects that creation of one, centralized framework will allow for increased coordination and exchange of expertise and knowledge, cost savings through co-investment, and opportunity for the EU to become a global leader in cybersecurity. **(Click the highlighted text to access the proposal)**

THE REST OF THE WORLD

Japan and EU in a deal to allow personal data flows

Japan and the European Union announced in July an agreement to recognize each other's data protection regimes as adequate. Once implemented, the agreement will permit the free flow of personal data between the two jurisdictions. The European Union is now taking steps to add Japan to the white list of countries exempt from stricter rules governing personal data transfers, with formal approval expected by the end of the year. To add Japan to this list, the European Data Protection Board must review the proposal. The EU and Member States legislatures must deliberate on the matter before formal approval is given.

In connection with the decision, Japan agreed to implement additional safeguards to align with the EU's standards. Such additional safeguards have not yet been finalized, but will likely include stricter guidelines for the retransfer of personal data that originated from the European Economic Area (EEA) to a third country and additional limitations on the use of sensitive data.

Brazil passes its first General Data Protection Law

In July, Brazil's Federal Senate (Federal Senate) unanimously approved the country's first General Data Protection Law ([Lei 13.709 sobre a proteção de dados pessoais](#)). The law - that is modelled on the European Union's General Data Protection Regulation - establishes a comprehensive data protection system in Brazil and imposes detailed rules for the collection, use, processing and storage of electronic and physical personal data. The regulation will go into effect in February 2020.

Singapore Launches Pilot for Data Protection Trustmark Certification Scheme

The Infocomm Media Development Authority (IMDA) and Personal Data Protection Commission (PDPC) launched an open call for organizations to participate in a pilot for Singapore's Data Protection Trustmark

Regulatory Monthly Newsletter

(DPTM) certification. The scheme aims to foster sound, transparent and accountable data protection practices among Singapore- based organizations and was developed in consultation with the industry.

The open call was announced by Minister for Communications and Information, Mr. S Iswaran, at the 6th Personal Data Protection Seminar today. The pilot will help to finalize the DPTM framework and certification process, prior to the DPTM's launch planned for end- 2018.

Organizations certified under the DPTM scheme will be able to use and display a DPTM logo in their business communications for the duration of the certification, which is three years. The DPTM engenders trust and confidence among consumers as they will be able to immediately identify organizations that have in place data protection policies and practices that had been subject to independent assessment. This, in turn, provides a competitive advantage for these certified organizations.

More regulation for Credit Reporting Agencies likely in US

In a report entitled "[A Financial System That Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation](#)", the U.S. Department of the Treasury recommends that the relevant US agencies use appropriate authorities to coordinate regulatory actions to protect consumer data held by credit reporting agencies. These regulatory actions are likely to lead to credit reporting agencies being subject to supervision for compliance with the federal data security requirements of the Gramm-Leach-Bliley Act.

The report also recommends that the US Congress amends the Credit Repair Organizations Act to exclude national credit bureaus and national credit scorers in order to allow these entities to provide credit education and counselling services to consumers to prospectively improve their credit scores.

The Treasury report contains a series of recommendations that form a proposed national framework for companies engaged in financial technology. Of more relevance from a credit information industry perspective, the report addresses data aggregation. The report encourages banks and other firms that offer consumers financial services to develop mechanisms to enable consumers to provide third parties with access to account information. **(Click the highlighted text to access the report)**

Argentina publishes GDPR-style data protection bill

Argentina is on its way to modernise its data protection law. The President sent the data protection bill to Argentine's Congress on 19 September. Argentina was declared as 'adequate' by the EU Commission under the EU DP Directive 1995, but Argentina's current data protection law of 2000 is not fully aligned with the EU General Data Protection Regulation (GDPR).

Regulatory Monthly Newsletter

The bill defines international transfers of personal data as lawful when, for example:

1. there is express consent by the data subject,
2. the receiving country provides an adequate level of protection,
3. the transfer is necessary for the maintenance or fulfilment of a legal relationship between the data controller and the owner of the data,
4. the transfer is necessary under a contract concluded, or legally required for the safeguarding of a public interest, or for the administration of justice.

The bill also recognises contractual clauses, and other binding self-regulatory mechanisms as suitable for transfers.

* * *