February 2020

ACCIS' contribution to inform the preparation of the European Commission's evaluation report of May 2020 on the application of the GDPR

Established in Dublin in 1990, the Association of Consumer Credit Information Suppliers (ACCIS) represents the largest group of credit reference agencies in the world. ACCIS brings together 42 members across 28 European countries and 8 associate and affiliate members from all other continents.

According to Article 97 of the General Data Protection Regulation (GDPR), the European Commission shall submit a report on the evaluation and review of the GDPR to the European Parliament and the Council. The first report is due by 25 May 2020. ACCIS welcomes the preparation of that evaluation report and invites the European Commission to take note of the experiences of credit reference agencies (CRAs) with the GDPR.

Our contribution consolidates the informal observations that we shared with the European Commission in the context of the stock-taking exercise carried out mid-2019 with our views on the new areas of interest for the European Commission in the context of the ongoing evaluation.

General comments

As organisations that collect and hold people's credit information and other relevant data, CRAs have taken GDPR readiness very seriously. CRAs run multi-annual compliance programmes before the date of application of GDPR i.e. 25 May 2018. Before GDPR came into application, CRAs also undertook root-and-branch reviews of their businesses, including products, services and internal systems.

Some of the main challenges in the run-up to the entry into application of the GDPR were:

- Identification of all the treatments of data and the data assets of the company, including considerations of the legal grounds for processing data, data retention periods, etc.
- Updating or creating privacy notices to meet the GDPR transparency requirements.
- Implementing new procedures to cope with the range of new data subject rights in Chapter III and the obligations to demonstrate compliance under Article 5(2).
- Clarification of Controller and Processor agreements with suppliers and customers (this challenge is ongoing as a consequence of lack of guidance and examples).

From 25 May 2018 onwards, the main challenges for the industry have to do with the lack of a harmonized interpretation by national Data Protection Authorities (DPAs) of some of the provisions of GDPR.

Case Study: Information to data subject on personal data not obtained from him / her

Article 14 regulates the information obligations for controllers in the event personal data have not been obtained from the data subject. Para 5 states that where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall not have to provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2 insofar (letter b) *"the provision of such information proves impossible or would involve a disproportionate effort […] subject to*

ACCIS IVZW • p/a Interel • Rue du Luxembourg 22-24 • B-1000 Brussels
+ 32 2 761 66 93 / secretariat@accis.eu / www.accis.eu / EU Transparency Register: 21868711871-63

the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available".

There is no consistency among DPAs in the way Article 14 (5) (b) should be interpreted. For example, the Norwegian DPA notes that when using publicly available personal data, the data controller may inform the data subject through the data controller's website. However, the Polish DPA will not recognise websites as a means to provide the information notice. In addition, in approving the 2019 Italian code of conduct for credit reporting systems, the Italian DPA has recognised different communication methods such as the use of website privacy notices or different digital methods.

Impact of the GDPR on the exercise of consumer rights

In order to provide sufficient information to the data subjects and to comply with the (extended) transparency obligations under GDRP, CRAs had to update their data protection statements. Generally speaking, information according to Articles 12-14 was (i) made visible to data subjects via the company's website; (ii) was added via a link in all email communications; (iii) was implemented via electronic portals for data subjects, etc.

In some cases, CRAs launched industry-wide public information notices, explaining how those CRAs use and share personal information, the type of information they hold, where it comes from and the legalities of handling personal data[1].

In relation to claims by data subjects, CRAs have registered an overall increase in the number of cases. Full subject access requests have increased. Rectification requests have also increased, as a result of higher GDPR awareness. In some countries, advertising campaigns have encouraged data subjects to access (and then correct) their credit reference data.

Erasure requests tend to be rare.

Data portability requests are very rare. For a majority of CRAs, Article 20 GDPR is not applicable as most data is received from third party data contributors and data is not processed on the basis of consent or contract.

In relation to the facilitation of the exercise of data subjects' rights (in Article 12(2)), CRAs note that data subjects have the possibility to exercise their rights under Articles 15-22 of the GDPR, which may include applying for a copy of the personal data undergoing online processing from the controller, where that controller is in a position to identify the data subject.

CRAs are used to dealing with data subject claims, so they have overall the appropriate resources - via automated systems where feasible - to handle the increased data subject issues.

Complaints and legal actions

In the past months, there have been cases of organisations that have submitted complaints against CRAs before local DPAs. In that regard, CRAs wish to emphasize the importance of ongoing dialogue with DPAs in respect of data subject complaints made directly to them. That dialogue should facilitate the investigation / evaluation of possible situations of non-compliance.

There have also been court actions against CRAs, but in much smaller numbers than the number of complaints. As a result of the volume of records held by CRAs, it is inevitable that some data subjects

[1] For example, the de Credit Reference Agency Information Notice (CRAIN) in the UK (2017).

ACCIS IVZW • p/a Interel • Rue du Luxembourg 22-24 • B-1000 Brussels
+ 32 2 761 66 93 / secretariat@accis.eu / www.accis.eu / EU Transparency Register: 21868711871-63

will resort to court action instead of (or after exhausting) the available data dispute, rectification and complaint processes.

Complaints and court action usually relate to rights of the data subject, especially Articles 15, 17 and 21 GDPR.

Use of representative actions under Article 80 GDPR

ACCIS members have no knowledge of any representative actions being filed against them.

Experience with Data Protection Authorities (DPAs), the one-stop-shop mechanism (OSS) and the consistency mechanism (opinions under Article 64 GDPR):

CRAs - but all business in general - need legal certainty. When this cannot be provided by the law itself - because it is open to interpretation or because it has been interpreted in an inconsistent way across the European Economic Area, CRAs turn to their local DPAs for guidance. It is important that the DPAs are able to focus resource in order to ensure the CRAs have enough advice/guidance to enable the CRAs to navigate their way through the legislation in the way intended by the legislators.

A case in point is the uncertainty as to when the exception in Article 14 (5)(b) can be relied upon (see box above). In some instances, the obligations imposed by Article 14 are not only disproportionate in cost and effort, but in conflict with other business requirements such as environmental standards. Businesses who fall under the obligation of Article 14 need guidance on when the principle of proportionality can be used. For example, it would be useful if there could be an Article 14(5)(b) balancing test available to data controllers that is consistent across the EEA, so that controllers can compare the cost and effort of the information obligation through letters versus the potential disadvantage to the data subject when the information notice is provided on the data controller's website and come to a conclusion that is consistent with other data controllers across the EEA. For instance, when using publicly available data - such as a sole proprietor from Companies House - and where the risk to the rights and freedoms of individuals is low, the principle of proportionality should allow the data controller to communicate through a website privacy notice. Public Sector Information (PSI) initiatives such as the EU Commission Public Sector Information Directive strategy would be hindered if all users of PSI would be required to communicate directly to the data subject in all use cases. If left to the interpretation of Member State DPAs then those will adhere to their mandate without taking into full consideration the wider EU strategy.

In connection to the guidelines issued so far by the EDPB, the perception is that they often seem to be over and above what would be required to comply strictly with the requirements of the GDPR.

Experience with accountability and the risk-based approach

Implementing business controls to meet the requirements of the accountability principle under Article 5(2) was mentioned as one of the key challenges of GDPR implementation.

Clients and consumers of CRAs already have high expectations in respect of information security and availability. That said, it is a common view among CRAs that compliance with GDPR is further enhancing data subjects' trust.

CRAs are very innovative companies, as reported in internationally recognized indexes. There is no reason to think that innovation will not continue even with enhanced oversight from having a DPO and the controls to meet GDPR accountability requirements.

For most CRAs, existing technical and organisational measures were often considered to be suitable for GDPR compliance after review as part of the readiness programmes. In some situations, additional controls and systems were brought in.

ACCIS IVZW • p/a Interel • Rue du Luxembourg 22-24 • B-1000 Brussels
+ 32 2 761 66 93 / secretariat@accis.eu / www.accis.eu / EU Transparency Register: 21868711871-63

Data protection officers (DPO)

The majority of CRAs already had appointed a DPO appointed before GDPR. It is a common view that the appointment of a DPO provides a valuable point of contact in respect of data protection matters and to ensure the business is compliant.

Adaptation/further development of Standard Contractual Clauses (SCCs)

CRAs noted that the existing SCCs do not cover all the scenarios that businesses encounter in their activities. In particular, there are no model clauses to enable a processor in the EEA to send data back out to a non-EEA client. In addition, prior to the GDPR, businesses had the flexibility to amend the model clauses to meet the requirements of particular unique data-sharing arrangements, so long as adequacy of the controls over the data had been assessed as being sufficient. This is no longer available under the GDPR without seeking local DPA approval. Giving businesses greater flexibility in how SCCs can be used and adapted would be a positive development.

Controller/processor relationship

CRAs have updated all current contract templates to align to GDPR and national laws. Having a set of optional standard contractual clauses (SCC) could be a useful addition, especially regarding liability allocation (e.g. Article 79 GDPR: no joint and several liability). This would introduce greater scope in the way SCCs can be used and adapted.

Problems with the national legislation implementing the GDPR

CRAs have noticed some issues, that have been shared directly with the European Commission.

GDPR and new technologies

Broadly speaking, GDPR has made it not easier to enable new technologies and methods. It is a challenge for the relevant business units to explore, implement and service new opportunities within the complex framework of the GDPR.

GDPR should ensure that new technologies are developed in a responsible way. For example, privacy by design requires data protection to be considered right at the start and throughout the life cycle of a product. Since the GDPR itself is intended to be technology neutral, overall its impact has been to ensure products are created with privacy in mind.

It has been argued that GDPR provides sufficient protection for the trustworthy development of new technologies such as artificial intelligence. CRAs have mixed views on this matter. Whist it is accepted that the current safeguards are a good start, some CRAs think that - by ensuring they are properly enforced - they could be sufficient to grant fair and trustworthy data handling regarding artificial intelligence. Other CRAs think that additional rules / guidance are needed to clarify how the data protection principles should be applied in practice given the complexity of the processing.

In respect of artificial intelligence, controllers are already providing information to the data subject about the origin and destination of the personal data (transparency) and about the context and the extent of the processing. As mentioned above, clarification as to how the GDPR requirements should be applied in practice would be helpful, for example a as regards the use of personal data in a fair way.

Codes of conduct (under Article 40 GDPR)

ACCIS as such has not been engaged in the preparation of a Code of Conduct. Some members of ACCIS have, however, developed them:

ACCIS IVZW • p/a Interel • Rue du Luxembourg 22-24 • B-1000 Brussels
+ 32 2 761 66 93 / secretariat@accis.eu / www.accis.eu / EU Transparency Register: 21868711871-63

- In Germany a Code of Conduct regarding retention periods for consumer credit information suppliers has been in force since 25 May 2018. The preparation was characterized by an intensive dialogue between the German association of credit information suppliers (DW) and the German data protection authorities.

- In Italy, there was already a code of conduct regarding consumer credit, creditworthiness and punctuality in payments. In 2019, an updated code was adopted. Concerned CRAs report that the experience with the code is very good as the code establishes different rules and removes doubts about what's possible to do with the data or not.

Data breach notifications (under Article 33 GDPR)

Some members of ACCIS have notified a data breach. It should be underlined that the necessary processes for assessing potential breaches and report detected breaches are well implemented, so documentation and, if necessary, notification to the competent DPA and / or the data subject are secured. Having said that, there is perception that preparation of the report is very time-consuming and provides relatively little. Also, that being frightened of an unbearable fine, there is a risk that controllers might overreact when it comes to notifying a data breach and notify in circumstances where notification was not essential thereby putting unnecessary strain on DPAs.

Adequacy decisions and other transfer tools

Adequacy decisions are quite important for the international transfer of consumer credit information. Many CRAs engage in that activity. The main destinations vary according to the individual CRAs' focus of interest and geography. Mentioned countries include Switzerland and the US.

According to those CRAs that report any experience on the matter, using adequacy decisions is very easy and useful because the transfer has been approved by the European Commission and also because there are not required further obligations/documentation (except in relation to transfers to the US where transfers are limited to the Privacy Shield framework).

The United Kingdom in a post-Brexit scenario and Hong Kong are the priority third countries that should be considered by the Commission in view of a possible adequacy decision.

CRAs think that Standard Contractual Clauses and processor to sub-processor clauses are other transfer mechanisms from the GDPR toolbox that should be developed as a matter of priority.

ACCIS IVZW • p/a Interel • Rue du Luxembourg 22-24 • B-1000 Brussels
+ 32 2 761 66 93 / secretariat@accis.eu / www.accis.eu / EU Transparency Register: 21868711871-63