FEBIS REGULATORY COMMITTEE MEETS TO DISCUSS A DRAFT FEBIS CODE OF PRACTICE ON DATA PROTECTION

On 11 October 2016, the FEBIS Regulatory Committee held a physical meeting in Paris to discuss the possibility to come up with a FEBIS code at European Level on data protection and compliance and application of the GDPR.

After a tour de table on the national sensitivities towards implementation of the GDPR, the group agreed that a good way forward would be to take the Italian Code of Ethics as a basis for a potential FEBIS code. A mail was therefore sent to all FEBIS members asking them to look at the Italian Code at http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/5483022 (now published as a law in the Italian Official journal) and to send us their comments by 15th November 2016 on the following issues :

- Do you agree with the proposal to use the Italian code as a basis for a European code at FEBIS level?
- What comments do you have on the content of the code?

The minutes of the meeting of 11. 10.2016 are available upon request, just email Stephanie at stephanie@svmconsult.com

Contents

EUROPEAN COMMISSION PUBLISHES A REPORT ON THE STATE OF THE CREDIT RATING INDUSTRY

On 19 October 2016, the European Commission published a report on the state of the credit rating industry and the possible alternative tools to credit ratings, aiming at outlining the existing instruments and the possible alternative tools that can be used.

Several references are made to the credit reference service providers and the report notably has a whole chapter entitled “alternative to rating”. In this chapter, reference is made to scoring as an alternative to rating. Though

the mention is made of both scoring by central banks and scoring by private companies, the majority of the reference made are about scorings by central banks (cf. descriptive paragraph below)

The report also notably refers to the problem of the lack of obligation of publication of accounts in Europe as an impediment in the chapter on "accounting based measures".

The report also questions the possibility to create a European credit rating agency

Scorings by Central Banks

Central Credit Registers (CCR) and Central Financial Statements Databases (CFSD) are relevant examples of scoring tools which are either owned or managed by central banks. CCRs and CFSDs' techniques are largely applied to corporate debt instruments but their geographical and sectoral coverage vary from country to country depending on parameters such as the eligibility of the instruments as collateral for monetary policy operations. The main drawback of CCRs and CFSDs is their limited country and asset class coverage as well as limited access to data. They are also limited in their application to corporate debt and their coverage of non-financial corporations in some countries is negligible. Scorings can be an important tool for smaller companies, as they allow a cheaper means of obtaining a credit assessment (compared to credit ratings by CRAs). However, scorings do not seem sufficient to provide a feasible full alternative to external credit rating systems but should rather be employed as a useful complementary source of information about the ***creditworthiness of a financial product***

ECJ RULING QUALIFIES DYNAMIC IP ADDRESSES AS PERSONAL DATA

The ruling of the European Court of Justice in the case known commonly as "Breyer" may have serious implications ***as it clarifies the definition of personal data, which will make it more difficult for organizations to pseudonymize or anonymize personal data. In short, IP addresses may be personal data even though information may have to be sought from third parties to identify the subjects***. A further complication is how this ruling will stand once the GDPR comes into force in 2018.

EU data protection law only applies to the processing of personal data, which it defines as "any information relating to an identified or identifiable natural person." Anyone to whom EU data protection law applies needs to correctly distinguish the personal data that they process from any other information that they hold. It is important that this is done at present, but it will become essential after May 25, 2018, when the EU's new GDPR will apply.

The GDPR makes controllers accountable for the processing of personal data, requiring that they demonstrate compliance. Demonstrating compliance may mean appointing data protection officers, undertaking data protection impact assessments and implementing data protection by default and design. Controllers that fail to do so may be face fines of up to four percent of their annual turnover worldwide. They may also face actions for damages, which may be brought by way of class action and so prove even more expensive.

The judgment of the European Court of Justice in Breyer is particularly significant in this context. ***The CJEU was not considering pseudonymization directly, but rather the definition of personal data and whether or not a dynamic IP address could be personal data.***

These obligations of accountability and compliance may all be avoided if a controller can demonstrate that they are not, in fact, processing personal data. At present the Data Protection Directive 95/46 encourages controllers to anonymize personal data. Anonymization should mean " … irreversibly preventing the identification of the individual to whom data relates." Whist possible in theory, anonymization has proven impossible to perfect in practice. So the GDPR now suggests pseudonymization, which it defines as: " … the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person." The GDPR suggests that pseudonymization may ensure the security of data, the lawfulness of processing or enable research.

The Breyer case was referred to the CJEU by the German Courts. The public websites of many German federal institutions, according to court documents, "… store information on all access operations in logfiles. Even after access has been terminated, information is retained in the logfiles concerning the name of the file or web page to which access was sought, the terms entered in the search fields, the time of access, the quantity of data transferred, an indication of whether access was successful and the IP address of the computer from which access was sought." The institutions that store this information do so to prevent cyber-attacks and enable the prosecution of cyber-attackers. Patrick Breyer objected and sought an injunction from the German courts seeking to prevent the processing of this information. This led to the German Courts referring two questions to the CJEU.

The first question asked of the court was ***whether a dynamic Internet Protocol address (IP address) can be personal data.*** An IP address is a sequence of numbers assigned by an internet service provider (ISP) to each computer that accesses the internet. Some internet users have static IP addresses that are permanently assigned, but most have dynamic IP addresses, which are temporarily assigned to each computer as it goes on-line and reassigned when it goes off-line. As a result, dynamic IP addresses cannot be used to directly identify the computer from which access had been sought. If one of the German federal institutions in question wanted to identify which computer had been assigned a particular IP address, then it would have to request that information from the ISP that had originally assigned the IP address.

The CJEU observed that in the event of a cyberattack, German law appears to provide for website operators to contact the appropriate authorities, who might then take the steps necessary to obtain information from ISPs and bring criminal proceedings***. This observation led the CJEU to conclude that dynamic IP addresses are personal data if website operators have "legal means" enabling the identification of the person associated with the IP address with the help of additional information which that person's internet service provider has***.

The judgment in Breyer suggests that data will still be personal even if it requires legal means to make a person "identifiable." This suggests that the meaning of "identifiable" is very broad. It may prove difficult to construct " … technical and organisational measures" that go further than the "legal means" referred to in Breyer. If the

CJEU judgment in Breyer applies to the GDPR, then pseudonymization may prove as difficult to perform as anonymization.

It is true that the GDPR does not yet apply and so was not directly considered in Breyer, but the definition of personal data in the new GDPR is largely the same as that in the old Directive 95/46. The GDPR specifies some new factors that an identifier can contain such as name, location data, online identifier and genetic data. It also clarifies that the data of dead or legal persons such as companies cannot be personal data. Otherwise old and new definitions are the same. Hence, it cannot be assumed that the CJEU will not apply Breyer to its interpretation of the GDPR after May 25, 2018. Where this leaves the concept of pseudonymization remains to be seen.

The second question asked of the CJEU was whether German law could permit the processing of personal data for the purposes of facilitating and charging for access to services after a connection had been terminated. The CJEU held that the objective of ensuring the general operability of services cannot justify the use of such data after those services have been accessed. However, the CJEU did suggest that those who provide internet services might have a legitimate interest in ensuring the continued functioning of their websites which goes beyond each specific use of their publicly accessible websites.

EUROPEAN PARLIAMENT DISCUSSES THE HARMONISATION OF EUROPEAN CODE FOR BUSINESS LAW

The JURI (legal affairs) committee of the European Parliament discussed mid October 2016 a draft report aiming at having a better harmonisation of European business law, especially in the field of class action and collective redress possibilities. The report which as presented outlined again the benefits that would come from having a European company statute and also calls for the possibility to have a European Code of business case law, to avoid having too different interpretations of the national laws applicable to business issues.

The discussion was webcast on the European parliament web site and can be seen at http://www.europarl.europa.eu/ep-live/en/committees/video?event=20161013-0945-COMMITTEE-JURI

FEBIS– Federation of Business Information Services

Benefiting from the opening of markets within Europe and overseas, world-wide business has experienced substantial growth. As business grows so does the demand for business information, in particular, intelligence for cross-border business activities.

In 1973, leading European credit information agencies joined forces to form the Federation of Business Information Services FEBIS (initially known as FECRO), with its registered office in Frankfurt. Today, FEBIS has developed into a sizable organization comprising more than 60 full Members from all over the world involved in providing Business Information and Debt Collection services of National and International importance.

Supported by a combined workforce of more than 20,000 staff, FEBIS Members generate over 180 million Business Information and Consumer reports annually for over 500,000 organizations, providing these clients with invaluable business support. Aggregate sales turnover of FEBIS Members is in excess of €2.5 Billion.

As the industry association, FEBIS strives to look after common interests of its members. While monitoring new legislation like data protection laws and insolvency laws, FEBIS also oversees and the application of public sources and information.