TO:
Role/Insitution
email

Brussels, 14 September 2015

Subject: The Data Protection Regulation and sound lending practices

Dear _____,

ACCIS, **Eurofinas, European Banking Federation** and **European Mortgage Federation** representing the European lending and credit reporting sectors, support the on-going efforts of the European Institutions to update the European data protection framework and make it fit for the digital era.

Although we appreciate that the Proposal for a General Data Protection Regulation (GDPR) is a horizontal instrument applicable across all sectors, we are concerned that some of the provisions could unintentionally affect our ability to carry out sound lending practices and to protect our customers.

We are committed to contributing to the European Institution's on-going efforts to achieve a well-balanced and workable regulatory framework. A balance between the protection of data subjects' rights and the ability for European businesses to remain innovative and competitive needs to be found.

Therefore, the signatories would like to call on the European Parliament, the Council and the European Commission to take these concerns into account when discussing the final text of the Regulation. The arguments presented in this letter are the key concerns fully shared by the co-signing organisations and thus represent the views of the majority of companies active in the EU consumer credit, credit reporting and banking industries. Each of the co-signing organisations may have additional arguments regarding the draft GDPR, specific to their industries, and may present such arguments separately from this letter.

We hope the points outlined below will prove useful in the forthcoming discussions and we remain at your disposal to elaborate further and to discuss with you the elements presented in this letter.

Principles relating to personal data processing (Article 5)

Many different types of data are used out of necessity on a daily basis by banks, consumer credit providers and credit information suppliers. They are used *inter alia* to satisfy regulatory requirements, tackle fraud and money laundering and to assess objectively the creditworthiness of applicant borrowers, in order to ensure sound and safe lending practices.

Legislation in force - such as the Consumer Credit Directive,[1] the Capital Requirements Directive[2] and the 3rd Anti-Money Laundering Directive[3] - place an obligation upon consumer credit providers to use data when conducting a creditworthiness assessment, for risk analysis and for identification purposes (*know your customer*). National legislation also often provides in extensive detail the kind of data to be collected.

In order to carry out accurate creditworthiness assessment, adequate breadth and depth of data is required. To limit data processing to the minimum necessary (the principle of data minimisation), would present an obstacle to consumer credit providers' ability to adhere to the aforementioned legislation and to carrying out sound and responsible lending practices.

We support the wording, which was already part of the 1995 Directive, **requiring the processing of personal data to be adequate, relevant and not excessive.**

Lawfulness of processing (Article 6)

In many Member States, further processing based on legitimate interest, by the controller and/or 3rd party with whom the controller shares the data, is key in order to perform processes such as ID fraud prevention, ID check, portfolio management, credit transfer and other activities that are linked to credit risk prevention and creditworthiness assessments and preventing over-indebtedness.

Credit reporting agencies (CRAs), acting as a 3rd party in relation e.g. to the banks and consumer credit providers, are dependent on receiving data from the original collector of the data, e.g. lenders, insurers, utility companies, etc. This dependency contributes to financial stability and facilitating access to credit for consumers, by lowering risks connected to lending and consequently lowering credit prices.

Further processing based on legitimate interest needs to take this into consideration and be wide enough to allow CRAs, consumer credit providers and banks to perform their work. Otherwise CRAs' databases would be drastically affected and - consequently – risk assessment would be less accurate and prices for credit would rise.

Moreover, for statistical purposes, further processing of personal data is essential for banks and consumer credit providers. This allows for the preparation of appropriate and tailor-made offers to their clients, reflecting their needs and expectations. Further processing also allows credit and financial institutions to create general profiles of clients to raise the effectiveness of tackling fraudulent and money laundering activity which is detrimental for both the client and the bank, as well as creating systemic risk in the banking sector.

---

[1] *Directive 2008/48/EC of the European Parliament and of the Council of 23 April on credit agreements for consumers and repealing Council Directive 87/102/EEC.*

[2] *Directive 2006/48/EC of the European Parliament and of the Council of 14 June 2006 relating to the taking up and pursuit of the business of credit institutions (recast).*

[3] *Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing.*

We think it should be clearly stated that the processing of data is considered as lawful when the processing takes place within a group. Financial institutions often need to process personal data within the group of which they are members in order to achieve aims, such as offering a broader variety of products to the clients, or, efficiently tackling fraud.

Thus, it should be ensured that the processing and transferring of data amongst the entities in the same group is lawful and does not require the data subject's consent each time the data is transferred within a group, provided that one of the preceding grounds for processing is fulfilled.

We believe that the Council's position takes due account of this.
However, further legal clarity is needed particularly when further processing is carried out by another controller. If the final text differs from the Council's position it should at least reflect the need for further processing of data in case of justified and legitimate interest of the controller which is not against the interest of the data subject and is executed in conformity with the GDPR principles. In this case, further processing should be defined as "compatible".

Special categories of data (Article 9)

Gender identity

We fully agree that data concerning sex life should not be used to discriminate individuals. Nonetheless, collection of gender data should remain possible and not considered a special category of data. The term "gender identity" could be construed as having a far broader scope of remit (e.g. capturing simply title data i.e. Mr/Mrs). To remove any reference to the gender identity of a consumer would be very difficult considering that in many countries national numbers identify gender.

Administrative sanctions & judgements

Court debt judgments and insolvency/bankruptcy data are vital data sets which are processed to allow lenders to make informed lending decisions. The processing of these data contributes to a safer financial environment, lowering credit risks which ultimately benefits consumers by lowering the cost of lending. The importance of this data is recognised by authorities and in fact, in many EU countries this information is made available in public registers. Therefore the processing of such data should be allowed for these particular purposes.

Fraud databases

In some Member States credit and financial institutions as well as banks can set up databases which contain data on fraud committed against consumer credit providers. Processing and sharing of these data with other providers is permitted in order to allow credit providers to prevent fraud and minimise risks.

Due to the restrictions in article 9, the processing of data related to criminal convictions and similar security measures, it is unclear whether these databases, whose existence is essential to protect both consumers and businesses, can be maintained in the future.

Right to be forgotten and the right to object (Articles 17 & 19)

A lack of sufficient data – including on administrative sanctions and judgement - can lead to an inefficient allocation of credit as well as an additional and unreasonable cost for the large majority of the EU consumers.

In our view, it is important that the text of the Regulation does not represent a risk to the process of conducting reliable creditworthiness assessments, which are crucial for sound lending practices. In some situations, e.g. data on a social media network, we believe that the data subject should have the right, at any time, to object as well as to be forgotten. On the other hand, Member States already have clear rules regulating the length of time for which data can be used by lenders and CRAs. The right to be forgotten in terms of old data in the field of credit risk assessment is therefore already implemented.

In our industries, some data, especially negative data which the consumer would most probably like to erase, are vital to make accurate assessments before granting a loan. This is also true for positive data which the consumer would like to withdraw in order to obtain additional credit, thus exposing himself to the risk of over-indebtedness.

In this context, we believe that data subjects should present a justified reason to erase or object to the processing of their data. For instance, their data should be removed when inaccurate or when they have been retained longer than the terms allowed by law. However, negative but correct data should not be erased or objected to, since they are fundamental to creating a reliable database. Access to data concerning the negative credit history is of vital importance for lenders, for portfolio management, managing cases of delinquency, developing future underwriting strategies and for fulfilling their legal obligations. Last but not least they are of high importance for evaluating the creditworthiness of the consumer, protecting consumers from over-indebtedness, sustaining responsible lending and borrowing practices.

When deciding whether or not to grant a loan to an applicant borrower, consumer credit providers assess a large range of data to assess the creditworthiness of their customers and satisfy regulatory requirements. We wish to stress that if insufficient data is available due to the customer having requested the erasure of his data, this will result in the credit provider being unable to perform the required verifications and risk assessment. The lender will consequently be unable to grant a loan.

Automated processing / profiling (Article 20, Recital 58)

We fear that the proposed provisions on automated processing/profiling could prohibit or restrict risk assessment as part of lending practices. Too restrictive rules on automated processing/profiling would be to the detriment for both consumers and businesses alike.

Mandatory human assessment on all decisions based on automated profiling would stretch waiting times for consumers or prohibit consumer lending directly at the point-of-sale and increase the risk of bias in the decision-making process as well as the risk of fraud. It would jeopardise the application of automated decision-making mechanisms used by consumer credit and credit scoring professionals to make prompt, objective and accurate assessments. Credit scoring and risk assessments are instrumental to ensure sound lending practices. Their use has been judged by regulators in many countries as being beneficial to the consumer, the lender and the economy. The World Bank in particular supports its use.

We support the possibility to request human assessment by the consumer if and when he/she thinks that he/she has not been treated fairly or when information is believed to be inaccurate. This possibility guarantees the consumer's rights and is already provided for by the current Data Protection Directive 95/46/EG.

To evaluate creditworthiness as objectively and accurately as possible, credit scoring systems carefully and precisely process data on the customer. Obviously, it is not in the best interests of lenders to turn down good payers or accept those that do not pay. For this reason, those using scoring systems keep them under constant review and check that the systems and data are up-to-date and accurate.

We would like to emphasise that in light of the creditworthiness assessment which consumer credit providers and CRAs perform in view of entering into a contract with an applicant borrower, the Regulation should also allow automated processing/profiling when the parties concerned are in the throes of entering a contract (as already allowed by the 1995 Directive).

It should be further underlined that profiling is a crucial tool for banks and consumer credit providers to prevent fraud and money-laundering or to support the development of "tailor-made" products or services for customers. Profiling should not be perceived as simply negative– it is based on a balance of interests: preventing criminal actions and building consumers' trust in the digital economy as well as developing e-commerce.

The opt-out concept, (the data subject shall have the right to object, i.e. to opt-out), instead of the largely proposed opt-in concept (i.e. the right not to be the subject) is preferable. However, the right to object cannot apply if profiling is requested by law or legal requirements (e.g. Anti-Money Laundering requirements, combating fraud or assessing borrowers' creditworthiness). We also propose that exclusion of low-risk automated data processing should be clearly stated. Moreover, we suggest that the lawfulness of processing and profiling for the monitoring and prevention of fraud and money laundering should be included in the article itself and not only mentioned in Recital 58.

Representation of data subject

We would like to raise our concerns regarding Article 76 allowing the data subject to have the right to mandate a body, organisation or association, to lodge a complaint on his or her behalf and to exercise the rights referred to in Articles 73, 74 and 75 on his or her behalf.

The introduction of EU representative actions has already been covered by the European Commission's recommendation[4] on Common Principles for Injunctive and Compensatory Collective Redress Mechanisms in the Member States concerning Violations of Rights granted under Union Law published in the Official Journal of the European Union. Therefore, it would be more appropriate to wait for the outcome before including any such provisions in the EU legislation, especially in the General Data Protection Regulation.

The ability for individuals to bring collective actions against entities in case of negligence could have negative unintended consequences. Hence, we are not in favour of collective actions with regard to such individual rights as privacy and data protection. The current system containing a relevant oversight regime is sufficient.

Sanctions

[4] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013H0396&from=EN

Article 79 uses a mandatory language and states that supervisory authorities "shall impose a fine" in the situations described. This leads to a situation in which very little margin of appreciation is left to the supervisory authorities to impose or not a fine or other measures.

National regulators should have the ability to set the appropriate penalties. In order to ensure clarity and certainty of the obligations set out in the proposed Regulation, sanctions should not be systematically imposed, and a margin of discretion in deciding whether or when to impose a fine, should be left to the supervisory authority.

Regarding the thresholds of the sanctions, it should be mentioned that they are highly disproportionate. A system of sanctions based on the model of sanctions of anti-competitive behaviour cannot be adapted to the data protection context. The impact of data protection violations is not comparable to anti-competitive behaviour. Indeed, in competition law the evaluation of the sanction is based on economic studies and on the analysis of the negative impact of anti-competitive behaviour on the market.

We consider that the sole criteria of the annual worldwide turnover of enterprises could lead to very disproportionate amounts of fines; hence administrative sanctions should be limited further.

Moreover, we support the thresholds of fines proposed in the Council text and strongly oppose the limits proposed in the European Parliament text which we consider disproportionate and unjustified.

With kind regards,

Jeroen Jansen
Secretary General
Association of Consumer
Credit Information Suppliers (ACCIS)

Tanguy van de Werve
Director General
Eurofinas

Wim Mijs
Chief Executive
European Banking Federation (EBF)

Luca Bertalot
Secretary General
European Mortgage Federation (EMF)