eurofinas

SPECIALISED CONSUMER CREDIT PROVIDERS IN EUROPE

Eurofinas Contribution to the Questionnaire for Stakeholders Consultation 01/07/2010

July 2010

Eurofinas AISBL
Boulevard Louis Schmidt, 87
B-1040 Brussels

RPM Bruxelles 0408.299.625

ABOUT EUROFINAS

Eurofinas, the European Federation of Finance House Associations, is the voice of the specialized consumer credit providers in the EU. As a Federation, Eurofinas brings together associations throughout Europe that represent finance houses, specialised banks, captive finance companies of car, equipment, etc. manufacturers and universal banks. It is estimated that together Eurofinas members financed over 320 billion euros worth of new loans during 2009 with outstandings reaching 720 billion euros at the end of the year.

For further information about this Eurofinas questionnaire response, please contact r.bhatiani@eurofinas.org or visit www.eurofinas.org.

Eurofinas is entered into the EC Register of Interest Representatives with ID N°83211441580-56

1. Should the principle of "data minimisation" be explicitly introduced in the legal framework?

The explicit introduction of the principle of “data minimisation” would be inappropriate. Many different types of data are used out of necessity, on a daily basis, both on- and off-line.

Credit providers represented by Eurofinas need to use a certain amount of personal data in order to i) satisfy regulatory requirements and ii) assess objectively the creditworthiness of their customers.

This data comes from various direct and indirect sources such as:

- the loan application form and other information supplied by the customer to the lender (income, family status, length of employment, number of loan applications, etc.);
- experience of business relations with the customer to date (credit history, including current and past credit commitments);
- credit bureaux/credit risk agencies whose role is to provide credit information on consumers; and
- depending on the country, public sources including bad debtor lists, court judgements or bankruptcies in the applicant’s name.

2. Should the current provision on automated individual decisions be made more explicit, namely by clarifying that “profiling” is prohibited?

The wording used in this question is unclear. Before answering any such question the term ‘profiling’ needs to be accurately defined.

Profiling should not mean ‘risk assessment’

Risk assessment must not be prohibited. Lenders need to assess risk as part of their sound lending practices, which can help reduce levels of consumer over-indebtedness.

Effective lending checks (including risk assessments made possible through the access to, and exchange of, the applicant borrower’s credit and fraud data) allow lenders to effectively identify and *accept* potential ‘good’ applicant borrowers during a creditworthiness assessment.

Conversely, effective lending checks help identify and *decline* potential ‘bad’ applicant borrowers during a creditworthiness assessment.

Credit scoring

Such risk assessments often include a credit scoring element. Scoring systems typically weigh up and decide the contribution of individual information items commonly taken from the sources outlined in the response to question 1 above. This means a score can comprise a large number of items of relevant criteria, each weighted differently and with no single item dominating. No one factor is ever decisive in itself though some factors can be significant.

When calculating a scorecard, credit providers only use data that is statistically suitable for predicting the probability of default and whose effectiveness can be economically or objectively explained. Again, by complying with anti-discrimination rules, sensitive factors such as race and religion are not included as information to be provided to the lender in the application forms and therefore are not taken into account by credit scoring.

Scoring disclosures

Details of existing scoring methods and how they work are confidential trading information that belong to (and confer economic benefits upon) the lenders using them.

Were any proposed revisions to the current European data protection regime to require detailed disclosures of consumer credit scoring methods (as is under discussion in certain national jurisdictions), both lenders and consumers would suffer.

If, as a result of such detailed disclosures, competing lenders knew each others scoring methodologies (i.e. specific IT system configurations/scoring software) there would be no incentive for lenders' continued investment in developing new, innovative and ever more precise IT systems/software that are key in managing risk.

Consumers would then suffer due to higher interest rates compensating for less precise risk management strategies.

Of even greater importance, if the details of such scoring methods were to be disclosed (as a result of a change to European data protection legislation or through other (legal) requirements), the security and accuracy of the credit referencing system would be greatly reduced.

This could be the case where either a loan applicant or a finance company employee - such as the loan officer in charge of granting the credit uses the disclosed information to make fraudulent applications. By knowing which information items are taken into account in the score or which criteria have a larger weight within the overall score, the applicant borrower or employee may falsify the data when applying for the loan thus reducing the predictive power of scorecards.

The costs related to this increased fraud risk would be passed on to borrowers through higher interest rates on loans thereby greatly reducing loan affordability.

The trust between a lender and a borrower is key to having a mutually beneficial business relationship. If lenders were to inadvertently aid fraudsters by disclosing detailed consumer credit scoring methods then the image of the industry would suffer as this trust is lost.

Against this background, Eurofinas stresses that there should be no duty (nor any indirect requirement), to disclose **detailed** consumer credit scoring methods as a consequence of any future legislative review.

That being said, credit providers and their trade associations can (and do[1]) disclose to consumers the **general principles** of credit scoring. Indeed, helping potential borrowers understand the underlying mechanisms of credit scoring is one way in which a lender can contribute to a borrower's financial education in the context of responsible lending and borrowing.

3. Should the current categories of "sensitive data" be extended to cover (and if so why):

- data of a financial nature ?

Accessing data of a financial nature would become burdensome, bureaucratic and time consuming if the current categories of sensitive data are extended to cover data of a financial nature. As such Eurofinas opposes data of a financial nature being classified as sensitive data.

For reasons of inter alia risk assessment and Anti-money Laundering (AML) compliance, it is important for the European Commission to ensure that **all lenders** are able to easily access and exchange customer data of a financial nature (such as AML and credit data) both at national level and in a cross-border pan European context.

---

[1] *For example, see http://www.eurofinas.org/uploads/documents/reports/E-publication_FinancialEducation.pdf. See also http://bfach.digramm.com/media/file/3331.Scoring_Kundenmerkblatt_bfach.pdf, an educational document on scoring produced by Eurofinas' German member Bankenfachverband.*

5. Should there be specific conditions for collecting personal data if they are not directly collected from the data subject?

In situations where personal data is not directly collected from the data subject, existing rules remain sufficient. Should specific conditions be introduced in the future, for such a situation, then these conditions must be widely consulted upon and a thorough impact assessment made.

This issue of indirect data collection is particularly important for lenders as typically a wide variety of data is not directly collected from the data subject. This data can include:

- any known current or recent credit arrangements with the lender;
- public information confirming domicile (e.g. an extract of the electoral register), court judgments and/or bankruptcy information;
- credit histories with other lenders;
- scores calculated by the lender and/or 3rd party (normally the credit register);
- data checks to comply with anti-money laundering obligations and fraud prevention; and
- data contained in other registers of excluded or politically sensitive individuals.

Such data usage has allowed for the development of a thorough risk assessment process leading to better targeted products, cheaper credit products (due to more accurate pricing of risk), wider credit availability for consumers and better management of consumers.

6. How could the "right to be forgotten" be strengthened in view of data retention and the right of deletion, particularly with reference to data protection in the on-line environment? Could the introduction of an autonomous right of the data subject to, for example, explicitly ask for withdrawal of his/her personal data from a website be an effective means of addressing this issue?

Eurofinas warns against an absolute right to be forgotten. Access to historic data is needed by lenders for reasons of portfolio management.

Lenders need to understand the repayment behaviour of their customers over the credit lifecycle, and after the expiry of the credit agreement, for reasons related to managing their loan portfolios.

This data needs to be retained as past repayment behaviours and loan portfolios need to be compared against a lender's own expectations for its existing loan portfolio in order to assess the portfolio performance.

Additionally, having access to historic credit data allows lenders to quickly research the causes of any changes in current repayment patterns (such as growing delinquency). Such access places lenders in a better position to quickly respond to changes in repayment behaviour and to anticipate a rise (or fall) in levels of bad debt.

In cases where a borrower is unable to repay a loan within the timeframe set down by a consumer credit agreement, continued access to a borrower's credit data is necessary. In such situations, credit data access after the expiry of the credit agreement aids lenders in managing cases of delinquency, developing their future underwriting strategies (e.g. by refining creditworthiness assessments and scorecards) and optimizing the effectiveness of their collections' operations.

7. Is there a need to strengthen the control of a data subject's own personal data? Could the current data protection legislation be improved by establishing a 'property right' over individuals' personal data ("data ownership")?

Existing controls are sufficient. Strong controls are built into the Data Protection Directive 95/46/EC (DPD) through stringent obligations placed upon the data controller and through the extensive rights of the data subject. These rights include a clear right of access to data, a right to erase data, a right to rectify data and a right to block data (Article 12 DPD) as well as a right to object to the processing of data (Article 14 DPD).

Establishing a 'property right' over personal data would mean additional bureaucracy for both data users and data subjects. Property rights would be almost impossible to supervise in practice as data is often separated or combined and/or processed into a product calculated by the data processor (e.g. a credit score).

8. Is there a need to address the issue of "data portability" in particular in the context of protection of personal data on the Internet, but also in the offline world? Should individuals always be able to permanently retrieve their own personal data from a certain application, and move it to another without being prevented by the data controller from doing so, either practically in terms of technical standards or contractually?

Data portability in the field of the cross-border access to, and exchange of, credit data has been extensively discussed by the Expert Group on Credit Histories (EGCH), set up by DG MARKT in 2008. Notwithstanding the comments below, Eurofinas agrees with the EGCH that it should be left to each individual lender to decide which data access model offers the most convenient and cost-effective solution to data portability in light of (i) the current low volume of cross-border credit database consultations and (ii) its own situation. In the field of credit data portability, we urge DG JUSTICE to take into account the views of the EGCH report[2] in the light of the comments below:

The report portability model

Eurofinas does not favour the report portability access model due to the risk of fraud associated thereto. This model is open to abuse as an ill-intended applicant borrower may alter the data in between receiving the credit history in country A and presenting it to a lender in country B.

A further difficulty therein can be if the data supplied is in a different language and/or uses differently defined terms which the lender may not be aware of.

The right-of-access model

The right-of-access model may be appropriate in certain situations where a lender needs to access a credit database but cannot due to the restrictive access conditions of the credit database.

The report portability and the right of access models may not adapt well to the principle of reciprocity however.

The indirect access model

The indirect access model may offer a convenient solution for lenders who:

- only rarely need to consult a foreign credit database; and/or
- do not have the resources to directly access a foreign credit database and interpret the data contained therein.

[2] *Report of the Expert Group on Credit Histories, May 2009, DG Internal Market and Services, available at: http://ec.europa.eu/internal_market/consultations/docs/2009/credit_histories/egch_report_en.pdf*

Eurofinas agrees with the EGCH suggestion that this model may be the most suitable for use as a first step in facilitating the cross-border access to, and exchange of, credit data considering the current low levels of cross-border lending.

The direct access model

The direct access model may be suitable for lenders making (or planning to make) a high volume of cross-border credit database consultations, which can justify the infrastructure costs of joining the foreign credit database. Nevertheless, it may be difficult for a lender in country A to comply with:

- the legislation in country B regarding data access; and
- some of the formal rules of the credit database in country B (e.g. as regards the updating frequency of the repayment history and data retention periods).

10. Is there a need to improve the modalities of individuals' right of access to their own data, particularly in the online environment?

Rights of the data subject

Before even considering modalities, data subjects need to firstly be made aware about the rights conferred upon them by the DPD in order to obtain the benefit thereof.

Thus **access to information** on the data subjects rights set down in the DPD **is key**.

This information should be easily obtainable and should include some explanation on the various redress mechanisms available in case a data subject's data set is inaccurate.

Relevant information campaigns supported by the European Commission would therefore be of value.

Eurofinas notes that conferences such as the 19-20 May 2009 conference organised by the European Commission entitled *Personal Data, More Use More Protection* are useful reference points for all parties interested in the rights and obligations stemming from the DPD.

Improving modalities

With regard to improving modalities, a stock taking exercise should first be carried out either by the European Commission, or by the Article 29 Working Party on existing methods of data access. Best practices from this stock taking exercise should then be circulated to stakeholders by the European Commission.

11. Should data controllers be entitled to charge for a data subject's access to one's own personal data, or should this be always free of charge? Should such provisions also apply to the exercise of the data subject's right to correct, erase and block data?

Eurofinas supports maintaining the *status quo.* An appropriate contribution by the consumer should be requested for data access (including for correction/erasure and blocking of data).

It is clear from Article 12(a) of the DPD that an appropriate contribution can be requested from data subjects for such access.

The provision of data held within a database has a cost. Thus if credit databases are forced to give consumers access to their credit data 'free of charge', any administrative costs incurred would likely be borne by the lenders who consult the credit data.

Ultimately, lenders would recover any extra expenditure by passing these costs to consumers through (*inter alia*) product fees and/or interest rate adjustments.

In countries (such as the UK) where an appropriate contribution[3] is usually paid by a consumer for accessing their credit data, Eurofinas notes that no decline in the number of consumers consulting their data has been recorded.

Fraud deterrence

In addition, it should be recognised that requesting an appropriate (not for profit) contribution by consumers for data access is critical in deterring fraudsters from obtaining high volumes of consumers' credit data.

If data access upon request were to become free of charge then consumers would face an increased risk of frauds (e.g. 'account takeover') with its attendant detrimental consequences.

12. Should precise deadlines be introduced for the controller to:

- comply with access requests by data subjects?

- comply with the obligation to rectify or delete data processed in breach of data protection?

In principle, we are not opposed to sensible deadlines.

We caution that deadlines need to be realistic and must take into account the specificities of individual industry sectors and market participants who need time to collect data that may potentially be stored in different ways across different subsidiaries.

14. Is there a need for introducing an explicit principle of transparency into the legal framework in order to ensure that data subjects receive adequate and sufficient information about the collection and processing of their personal data and to enable them to make an informed choice?

There is no need to introduce an explicit principle of transparency into the legal framework in order to ensure that data subjects receive adequate and sufficient information about the collection and processing of their personal data.

Credit providers already promote transparency in data processing. As mentioned earlier, credit providers and their trade associations[4] disclose to consumers easily understandable and clear information on the collection and processing of their personal data.

There is no need to standardise such information in a uniform EU 'privacy notice' as information disclosure, to an extent, must be tailored in the light of the service/product provided by the company processing the data.

[3] Circa *£2 in the UK.*

[4] *For example, see http://www.fla.org.uk/filegrab/1Yourcreditexplained_19_01_07.pdf?ref=20*

15. Is there a need to increase data subjects' general awareness of their rights?

Data subjects need to be made aware about the rights conferred upon them by the DPD in order to obtain the benefit thereof (see response to Q. 10).

23. Is there a need to strengthen the current provisions on judicial redress? More specifically: should the possibilities for judicial redress be extended, in particular by way of "collective redress" in data protection matters?

We oppose strengthening the current provisions on judicial redress. They are fit for purpose in their existing form.

Eurofinas sees the development of alternative dispute resolution schemes as a viable alternative to extending judicial redress by way of 'collective redress' in data protection matters. Eurofinas therefore strongly supports, subject to a full cost/benefit analysis being carried out, the introduction and the promotion of out-of-court settlement mechanisms that comply with the principles of impartiality, transparency, effectiveness and fairness.

Rather than strengthening judicial redress, the Commission should make sure that data subjects have access to individual alternative dispute resolution mechanisms and that all types of sectors are covered. Member States should remain free to assess whether such schemes should be promoted on a self-regulatory or statutory basis.

24. Is there a need to develop alternative dispute resolutions (ADRs) and out-of court proceedings in data protection matters?

In addition to the comments above, we recognise that access to justice will help data subjects to seek redress in case of a breach of their rights guaranteed by the DPD.

However, justice served through the courts can be an expensive and time consuming process for all parties involved.

Improving access to justice through the development of an ADR system which addresses the specific concerns raised on specific issues (e.g. for credit providers, on the issues related to the access to, and exchange of, credit data) would be more effective.

A self-regulatory or statutory ADR system would offer data subjects a quick, uncomplicated, easily-accessible and cheap means of redress by avoiding the complexities and delays of a judicial process.

27. In general, should the data subjects' rights be made more explicit, in order to mirror the data controller's obligations?

Data subjects' rights are *already* very explicit (see answer to Q.7). It would be difficult to develop them any further.

It would be illogical for data subjects' rights to mirror the data controller's obligations as they serve different objectives. Whilst the rights of a data subject promote principles of transparency, accuracy and ownership, the obligations of a data controller reflect considerations of security and confidentiality.

28. Is there a need for further harmonisation of the data protection rules at EU level? Are there practical problems affecting the free movement of data?

Eurofinas holds the view that the current Directive is a gold standard in data protection and we see it as premature for the European Commission to propose a new DPD. As such, we support a process of evolution of the current Directive through improved interpretation and implementation to assist pan European data flows.

Greater harmonisation of existing rules would be beneficial for both consumers and businesses. It would reduce or remove data protection rules as a barrier both to firms engaging in cross border activity and to consumers wishing to access goods and services from outside their own Member State.

Upholding a more consistent interpretation of data protection rules for individuals throughout the EU would also lend increased strength to educational efforts in this area. This would reduce the potential for providing 'mixed messages' to data subjects resulting from the differences in data protection rules between Member States.

Credit provider specific concerns

Eurofinas stresses that national Data Protection Authorities should work towards more convergence or harmonisation in the interpretation of data protection rules and practices in order to facilitate, for lenders, the process of *cross-border* data exchange. We acknowledge that the DPD has been interpreted differently across the EU 27.

Particular differences exist in the interpretations of the:

- 'authorised purposes' of using credit data; and
- 'authorised actors' for exchanging credit data

which have been interpreted narrowly or broadly dependant upon the jurisdiction involved. This has led to divergent credit data access/exchange landscapes within the EU.

DPD implementation

At the very least, reviewing the way that the DPD has been interpreted, with a view to *fully* harmonising the ability of all lenders and credit bureaux/registers to access and exchange credit data, would facilitate, in particular, the *cross-border* access to, and exchange of, credit histories.

Reviewing the way that the DPD has been interpreted with a view to facilitating the fight against fraud also has merit.

In 2007, Eurofinas held a Discussion Day on Fraud to create a forum where Eurofinas members presented their local situations regarding *inter alia* the use, and exchange of, fraud data. The main obstacle to the effective use, and exchange, of fraud data as cited by members was their local data protection laws, which prevent the use/exchange of such data. Moreover, the participants noted that the fraud data which is available does not exist in any homogenous and comparable forms.

The Eurofinas 'Discussion Day' also highlighted the need for a common definition of identity theft at EU level; a new penal legislation which deems identity theft in the sphere of financial services to be a criminal offence in all Member States; and EU wide statistical data on the issue.

At the Discussion Day, a specific reference was made to Schengen rules which do not permit access by industry in one Schengen country to databases on stolen IDs of other Schengen nationals. While the information does exist, it may only be accessed by police forces.

Another problem highlighted was that consent (from fraudsters!) may be required before being able to consult the relevant fraud data. An additional point was made that fraud data sharing may in some instances

not be allowed cross-border. With criminals often operating across borders, the possibility to be able to share such data is essential.

29. Is there a need to further harmonise, reduce and/or simplify the notification procedures to the DPAs and to ensure an effective follow-up of notifications by the national data protection authorities?

The notification procedures should be limited to certain categories of processing operations most likely to affect the rights and freedoms of data subjects.

31. Should a general obligation for the data controller to take appropriate measures to ensure and demonstrate the compliance with data protection law be introduced?

We oppose any general obligation for the data controller to take appropriate measures to ensure and demonstrate data protection compliance. Compliance should be presumed until proven otherwise by a complaining party.

Requiring compliance to be demonstrated as a general obligation would only add to administrative burdens and increase costs for those needing to process personal data. Such costs would inevitably be passed on to data subjects, in a consumer credit context, via increased interest rates and/or product fees.

32. Should the obligation to conduct a PIA be introduced? Should it be mandatory for the controller? If yes, what would be the threshold for such obligation?

Privacy Impact Assessments would potentially add yet another layer of bureaucracy to an already complex legal framework. Should any such obligation be imposed, it must be restricted to categories of data processing that are most likely to affect the **fundamental rights and freedoms** of data subjects.

36. Should the principle of 'privacy by design' be introduced and if so how should it be implemented concretely?

The principle of 'privacy by design' has different interpretations. Before discussing the introduction and implementation of any such principle, the European Commission must first define what precisely it means by 'privacy by design'.

38. Should the obligation for reporting personal data breach notifications – as currently provided for by the e-Privacy Directive - be extended? If yes, are there specific sectors where personal data breach notifications should not apply? Should a threshold be set, and if yes, where?

There would be real difficulty in establishing thresholds for any obligation to report personal data breach notifications due to the mix of different factors involved. We believe Member State regulators are best placed to determine where notification or other action may be appropriate, on a case by case basis.

40. Is there a need for specific rules on personal data processing by law enforcement authorities within the future data protection framework?

Lenders often work together with law enforcement authorities to fight fraud. Experience has shown that it remains difficult for lenders to access/exchange data on fraudsters in conjunction with those authorities.

Such data exchanges should be facilitated, where appropriate, by way of specific rules. This practical step would begin to address existing difficulties in the access to, and exchange of, fraud data.

This is a major issue for the specialised lenders that Eurofinas represents as both credit data and fraud data are necessary for lenders to grant loans responsibly. Responsible lending includes not only the creditworthiness assessment of an applicant borrower but also understanding the likelihood of a fraudulent application and the prevention of frauds such as identity theft.

Moreover, the sharing of fraud related data is necessary to protect the consumer. Once a consumer's identity becomes compromised or is stolen, it is in his or her interest that consumer credit providers prevent the use of this identity by fraudsters in loan applications (see also response to Q. 28).

59. Should the current role of the Article 29 Working Party on Data Protection be changed? If so, how?

The current status and role of the Article 29 Working Party should be maintained.

We welcome the fact that lenders' concerns, such as AML compliance have previously been addressed by this Working Party.