ECRI COMMENTARY
European Credit Research Institute

Data protection at the cost of economic growth?

Elina Pyykkö*

ECRI Commentary No. 11/November 2012

The Data Protection Regulation proposed by the European Commission contains important elements to facilitate and secure personal data flows within the Single Market. A harmonised level of protection of individual data is an important objective and all stakeholders have generally welcomed this basic principle. However, when putting the regulation proposal in the complex context in which it is to be implemented, some important issues are revealed. The proposal dictates how data is to be used, regardless of the operational context. It is generally thought to have been influenced by concerns over social networking. This approach implies protection of data rather than protection of privacy and can hardly lead to more flexible instruments for global data flows.

Building and ensuring consumer trust in the economy is essential for economic development. This is of particular importance in a post-crisis Europe where digital commerce is to be promoted for its enormous potential contribution to economic growth. However, as more and more private data are processed and distributed within the Single Market the current data protection legal framework is proving to be outdated. All 27 EU member states have different data protection legislations, which are more or less based on a directive that was first adopted in 1995.[1] Consequently, the European Commission has worked extensively on the reform of the data protection legal framework. Earlier this year it published its proposal for a Data Protection Regulation,[2] which aims to secure the privacy and ability of individuals to consume confidently within and across the internal market. Instead of another directive, a regulation is proposed to

[1] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
[2] COM(2012)0011 (http://ec.europa.eu/justice/data-protection/law/index_en.htm).

ECRI Commentaries provide short analyses of ongoing developments with regard to credit markets in Europe. ECRI researchers as well as external experts contribute to the series. External experts are invited to suggest topics of interest for ECRI Commentaries.

Elina Pyykkö is a Research Fellow at the European Credit Research Institute within CEPS in Brussels.

harmonise data protection rules across the EU. This is intended to bring clarity and decrease associated costs for businesses; facilitating freer and more flexible flows of personal data.

All this is to be achieved through a regulation that puts individuals more firmly in control of their data. In particular, consent for collecting and processing data on the individual is to be given explicitly, when required, and individuals are provided with a 'right to be forgotten.' Individuals are also to receive better information about the processing of their data, and through a concept of 'data portability' they should have greater rights of access to this data. Data controllers are now also dealing with more strictly defined and lawful data processing, depending on either the (explicit) consent of the data subject or the legal obligations regarding the processing of data.

However, the proposal regulates protection of data with no regard to the operational context of the data controller. This is in contrast to the Report on Completing the Digital Single Market[3] adopted by the Committee on the Internal Market and Consumer Protection of the European Parliament, which stresses the need to implement the European Commission's proposed new data protection regulation in a way that allows sufficient flexibility for companies to develop their business without disproportionate costs, while still protecting privacy and safeguarding fundamental rights. If the proposal is to promote a free flow of information that respects privacy, then it is important to not merely set data protection rules without allowing for the context. In its current form, the proposal does exactly this because it regulates how data should be used rather than ensuring privacy in a pragmatic and practical way, without disproportionately interfering with the operations that are necessary for the technological advances observed in previous years.

When the protection of data is the main objective, with no regard to the operational context, it is inevitable that from the perspective of organisations operating in different industries some requirements prove to be disproportionate or even counter to industry-specific regulations. The financial services industry is one of the sectors where some of the requirements in the proposal are disproportionate or even conflict with legislation already in place. In the post-crisis world of responsible lending and more efficient financial services, the focus on data protection jeopardises the recent emphasis on these principles. This risk should not be underestimated, since the evidence shows that the existence of credit reporting is associated with an increase in credit availability, as well as with reductions in borrower and lender risk and in the cost of credit for firms (Jappelli and Pagano 2002; Brown, Jappelli, and Pagano 2009). Furthermore, Houston et al. (2010) have found that greater information sharing leads to a reduced likelihood of financial crisis and higher economic growth. Credit reporting is a vital part of a country's financial infrastructure and is an activity of public interest (World Bank, 2011).

Operational implications for the financial services industry

The financial services industry has a special role in the everyday lives of consumers, businesses and in the economy as a whole. Well-functioning financial services for individuals are one of the cornerstones of economic growth, and difficulties in these services, for instance in granting credit, has far-reaching consequences. For these services to work in a way that promotes

[3] See: (http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2012/2030(INI)).

financial stability, the use of credit data on individuals and businesses is of utmost importance. On the other hand, individuals know that access to this information is necessary for them to obtain credit and on better terms. Credit Reference Agencies are important mediators of this information, working for the benefit of both credit providers and borrowers. All these stakeholders have the incentive to keep this information flowing, as long as privacy is respected appropriately. Indeed, for the most part, Credit Reference Agencies have a critical responsibility to build confidence in their model because guaranteeing the safe supply and flow of comprehensive information is their core business.

Introducing data protection rules that tightly and disproportionately regulate how the data is to be used could disrupt these data flows and have negative implications for all stakeholders. The general one-size-fits-all approach of the proposal has several new elements in comparison to the Directive 95/46/EC with respect to the rights of consumers and enforcement that are likely to have significant and disproportionate impacts on financial services. The proposal has several requirements for the lawfulness of data processing that might risk efficient consumer credit data sharing, making granting credit more risky and costly for the creditor. In addition, limiting the use as well as the control of data by data controllers might stifle the functioning of the credit reporting systems, thereby risking the development and investments towards more security and efficiency.

One of the most controversial principles of the proposal from the perspective of financial service providers is the 'Data Minimisation' principle introduced in Article 5, which states that the use of personal data must be limited to the minimum necessary. Using the full range of relevant personal data is, however, necessary for secure and efficient financial services for consumers. This is why the Consumer Credit Directive and the Capital Requirements Directive set an obligation for consumer credit providers to assess the creditworthiness of the consumer using necessary data, also for the purposes of risk management and identification. However, without further clarifications, the principle of data minimisation might present an obstacle for financial service providers to use the right level of personal data in the above-mentioned way. Therefore, this principle should be clarified in relation to the industry needs and objectives. In addition, 'data minimisation' might prevent the creditor from using the information needed for it to grant credit in a responsible manner to promote financial stability.

The 'Right to be forgotten' stated in Article 17 also has the potential to harm the existing important functions of using personal data in credit decisions. It implies that the data on the individual is to be erased if that data is no longer necessary for the purposes for which it was collected, or if the data subject withdraws the consent necessary for collecting and processing the data. This right is in principle a good notion, but in the context of credit data for crediting purposes, it could ultimately disadvantage the consumer. If there is no data about the consumer, on what can the lender base his/her credit decision? Financial service providers need historical consumer data for risk management, managing cases of delinquency, assessing creditworthiness, preventing over-indebtedness and, in most cases, for fulfilling their legal obligations. Also, after the settlement of the credit contract, the financial service provider can use this data as a proof of consumers' creditworthiness in future financial service granting decisions. Through Credit Reference Agencies, other financial service providers can also use this information for this purpose. This aspect – benefiting both consumers and the financial service providers – could be at risk through an established right to be forgotten, as the current proposed requirement might actually mean that once the loan is paid off, the data holder erases the data completely. This might lead to consumers with perfect credit files not having any credit

information to prove their creditworthiness, possibly precluding them from future credit and potentially even leading to financial exclusion. Consumers should therefore be aware that it is problematic for lenders to grant credit without any information about the creditworthiness of the consumer.

The proposal also sets out the principles for what is to be considered the lawful processing of personal data. Following the preceding Directive 95/46/EC, Article 6 states that the data can be processed if based on legal obligation, if necessary for the performance of a contract, if based on the purposes of the legitimate interest of the controller, or on the basis of consent. With the Directive, creditors have generally conducted processing based on the (prospective) contract with the consumer, or on the grounds of consent, while credit registers as third parties have operated under legitimate interest for processing. However, unlike the Directive, the Regulation proposal no longer refers to the legitimate interest of third parties to whom the data is disclosed. This might lead to credit registers having to resort to obtaining explicit consent from consumers to process their data.

Article 7 of the proposal states that in order to ensure free consent, it should be clarified that consent does not provide a valid legal ground where the individual has no genuine and free choice and is subsequently not able to refuse or withdraw consent without detriment. The relationship between the creditor and the consumer is, however, very complex, as the consumer has the choice of not providing certain information, but this might lead to the consumer not obtaining the credit or service provided on credit. This complexity has implications also for the functioning of credit registers as the third party in the middle of this relationship. On the other hand, the adequacy and consistency of credit registers would be compromised if credit reporting were dependent on individuals' consent. Consent as a basis for data processing therefore does not work well in the credit data context.

In addition to limiting the use of personal data by the data controllers, the proposal aims to increase data subjects' control of their own data by giving them more direct access to it. Article 18 of the proposal states that the data subject shall have the right to obtain from the controller a copy of data and allow further use by the data subject. While data subjects already have the right of access and correction in their personal data, the data portability aspect goes further. Data portability creates a significant risk for the system as data subjects might be persuaded to provide their personal data to another party, thereby increasing the risk of identity theft.

The data portability principle facilitates the uncontrolled free flow of data that creates risks in addition the risk of crime and fraud. While the concept of data portability was conceived to help data subjects in the use of social networks or energy contract negotiations, this free distribution of data carries the risk of undermining the whole ethos of credit data sharing, which is based on reciprocity. Reciprocity is an important principle in credit reporting, applied to ensure that access to data is only allowed for those who also, in turn, supply their own. This requirement should, therefore, be seen in conjunction with the banking secrecy rules. This provision could require organisations to disclose trade secrets, and for companies in the data processing business, this might come at the cost of their business. The data portability requirement in its current form also carries the risk of imposition of technical requirements to enable personal data to become portable. This would be a significant cost for businesses, which would then be passed on to consumers. In addition, if the data on individuals becomes a common product that the data controller is obliged to distribute further, this might disrupt the functioning of the consumer credit data markets. The credit and credit data reporting industry is continuously

investing in better applications to make the markets more efficient and secure. The obligation for data portability might disincentivise these operations as the data controllers would no longer be in full control of the data they created.

Broader implications

The proposed regulation has been put forward mainly to find new ways to ensure accountability on the internet. For e-commerce to prosper, the Commission wants to ensure transferability of data, establish the right to be forgotten and adapt the legislation to new challenges, such as cloud computing. However, making the credit and financial services industry obey the same rules as social networks creates a risk that credit providers adjust their portfolios to allow for the greater credit risks they have to bear because of the lower level of information available. This might result in lower consumer credit volumes and in lower technological innovations in the industry. EU legislators are working hard to promote e-commerce for its great potential in future economic growth, but the growth of the e-commerce might be stifled if consumers cannot access credit or if retail payments are not efficient because of disproportionately strict data protection rules.

Using consumer credit data in credit decisions and for identification is of crucial importance for responsible lending practices, which is also reflected in the creditworthiness assessments required by the Consumer Credit Directive and the Capital Requirements Directive. It also provides critical support for access to services used via internet or mobile phones, where identity systems enable providers to confidently transact with applicants they never actually meet. The use of consumer credit data for these purposes does not function efficiently without sufficient credit reporting systems, which have become a significant building block for consumer credit in many countries after continuous development and investments in new technologies, in cooperation with legislators and consumers. This achievement might be compromised, however, if some of the elements of the Data Protection proposal are adopted without further assessment or clarifications. As mentioned in the previous section, rendering consumer credit reporting under consumers' consent might compromise the adequacy of the available credit data as consumers can then choose which data to report. Similarly, the 'right to be forgotten' might lead to similar consequences if the consumer is able to selectively edit which of the data stored on them is to be erased and which is kept. The resulting incomplete credit files would risk the crucial contribution that the credit registers provide for responsible and efficient lending practices, financial inclusion, consumer choice, financial stability and economic growth.

Conclusions

One of the objectives of the Data Protection Regulation proposal is to promote sustainable economic growth and consumer confidence. Many of the requirements stated in the regulation proposal are called for to harmonise and clarify the rights of consumers in the world of fast-changing internet and big data. However, when assessing the need for regulation, regulators should carefully weigh the intended benefits against the potential negative consequences that such new rules may have on different industries and the economy as a whole.

For the credit industry, efficient and comprehensive information networks are crucial for responsible, sustainable and secure services for consumers. Data protection regulation that harmonises the use of data to the same level as in other industries might risk this essential

information flow. Therefore, prescriptive regulation should be carefully avoided to prevent disruption of the information networks that are at the heart of efficient credit-reporting systems and are already operating in secure and effective ways. The improved consumer confidence might be outweighed by less functional services and disrupt credit providers' ability to provide the services.

In summary, there is a fundamental distinction between protecting data per se and protecting the privacy of individuals. Instead of universally ruling on how to use data, the Data Protection Regulation should provide more principle-based rules to ensure efficient operations that respect the individual's privacy at a level that is appropriate for the purpose. Only this approach can facilitate the creation of more flexible instruments for global data flows and contribute to economic growth in the future.

References

Brown, M., T. Jappelli, and M. Pagano (2009), "Information sharing and credit: Firm-level evidence from transition countries", *Journal of Financial Intermediation*, Vol. 18, pp. 151-172.

Houston, J. F., C. Lin, P. Lin, and Y. Ma (2010), "Creditor rights, information sharing, and bank risk taking", *Journal of Financial Economics*, Vol. 96, pp. 485-512.

Jappelli, T. and M. Pagano (2002), "Information sharing, lending and defaults: Cross-country evidence", *Journal of Banking & Finance*, Vol. 26, pp. 2017-2045.

World Bank (2011), *General Principles for Credit Reporting*, World Bank Task Force Report.

European Credit Research Institute

The **EUROPEAN CREDIT RESEARCH INSTITUTE** (ECRI) is an independent research institution devoted to the study of banking and credit. It focuses on institutional, economic and political aspects related to retail finance and credit reporting in Europe but also in non-European countries. ECRI provides expert analysis and academic research for a better understanding of the economic and social impact of credit. We monitor markets and regulatory changes as well as their impact at the national and international levels. ECRI was founded in 1999 by the **CENTRE FOR EUROPEAN POLICY STUDIES** (CEPS) together with a consortium of European credit institutions. The institute is a legal entity of CEPS and receives funds from different sources. For further information, visit the website: www.ecri.eu.

ECRI Commentary Series

ECRI Commentaries provide short analyses of ongoing developments with regard to credit markets in Europe. ECRI researchers as well as external experts contribute to the series. External experts are invited to suggest topics of interest for ECRI Commentaries.

ECRI Task Force on Credit Reporting

ECRI is running a Task Force to assess the concrete next steps in consumer credit data sharing to contribute to the development towards more efficient and secure retail financial services in the cross-section of responsible lending, financial inclusion and data protection legislation revision. For more information visit our website: www.ecri.eu or contact Elina.pyykko@ceps.eu.

The Author

Elina Pyykkö is a Research Fellow at the European Credit Research Institute of CEPS in Brussels. She holds a PhD in Economics and Business Administration from the University of Oulu, Finland.

European Credit
Research Institute (ECRI)
Place du Congrés 1
B-1000 Brussels, Belgium
Tel.: +32-2-2293911
Fax: +32-2-2194151
Email: info@ecri.be
Web: www.ecri.eu