New data protection law poses threat to lenders and consumers

By Alasdair Warwood

EFFORTS BY THE EU to harmonise regulations in the consumer credit industry will have severe implications for lenders and the way they handle their customers' personal data.

In September 2002, the European Commission published the Consumer Credit Draft Directive which will significantly extend the scope of data protection legislation in the field of consumer credit. The directive places significant restrictions on the collection and use of customer data by both lenders and credit reference agencies. These restrictions may lead to greater social exclusion, higher costs for credit, and an increase in fraud and money laundering.

In an attempt to create a Single Market for consumer credit the EU has, for the first time, turned its attention to the way customer information is collected and used by the consumer credit industry. To the consternation of many in the credit industry throughout Europe, the "model" the Commission appears to have chosen as a basis for developing its proposals, a combination of the French and Belgian systems, is, in data protection terms, the most narrow and restrictive in Europe.

The draft directive has run into opposition – some, but not all, relating to the data protection issues – with a number of member states threatening to block the directive unless they get their way.

COLLECTION AND USE OF INFORMATION FOR MARKETING

Article 7 specifically forbids the sale or use of customer data that is collected before entering into a contract, generated during the term of an agreement for advertising and marketing by the lender, and for offering insurance to customers. It also forbids the sale of information to third parties.

Article 6(1) states that creditors and intermediaries may collect only information which is "adequate, relevant and not excessive…[for] assessing their financial situation and ability to repay."

> The directive places significant restrictions on the collection and use of customer data by both lenders and credit reference agencies.

Article 8 of the directive states that information obtained from consumers, guarantors or credit reference agencies may be obtained only on a case-by-case basis and may be used only for risk assessment purposes.

In other words, lenders may not collect data for marketing or other purposes, even with the consent of the customer. Article 30 reinforces these restrictions. Article 30(4) says: "Consumers and guarantors may not waive the rights conferred on them by this directive."

These provisions, therefore, ban lenders from using their own customers' data for marketing additional products to them. It also bans the sharing of data by lenders for the construction and use of risk modelling and screening systems for marketing purposes. The odd consequence of this is that consumers could end up receiving more credit-related junk mail, only to be rejected when they apply – hardly an outcome one would have expected the EU to favour.

COLLECTION AND USE OF INFORMATION FOR RISK ASSESSMENT

Article 6 of the directive is likely to require lenders to ask for more detailed information on applications – both from consumers and guarantors – for assessment purposes. Any future action against a consumer for recovery of debt will involve an assessment of whether the lender had asked for sufficient information and had properly taken it into account when making its credit decision. These provisions will have a significant impact on the application assessment process; particularly with regard to the use of credit risk scoring techniques and of automated application processing systems.

In addition, Article 29 requires credit intermediaries, when putting a proposal to a lender, to provide the lender with information about "the total amount of other credit offers he has requested or received for the same consumer or guarantor during the two months preceding conclusion of the credit agreement."

Risk management and the use of credit reference agencies

Article 8 requires member states to ensure the establishment of a central default database or network of linked databases. Such databases already exist in one form or another in all member states. Some are run by trade associations and some by commercial organisations. All are subject to national data protection legislation and to agreements between subscribers as to how their data may be used. Only in France and Belgium are they state run or directed.

A number of member states, including Germany and the UK, have made it clear that they oppose any suggestion that such databases should be state run. In one of only two derogations permitted by the directive, member states "may include the registration of credit agreements and surety agreements." The French and the Finns, in particular, are bitterly opposed to any proposal for the mandatory sharing of such data. What, in any event, is not clear is whether the European Commission had in mind the sort of performance data currently shared in many countries including the UK, or whether they have in mind only static data about the consumer's total level of credit commitments.

Where such databases already exist – whether state or privately run, for profit or otherwise – they may continue, but for the first time there will be legal restrictions on how they operate.

The database must provide guaranteed access to all lenders. Articles 8(1) and 8(2) place an obligation on lenders to carry out checks on all consumers and guarantors on the databases in their member state and, where applicable, other member states before granting credit. Where there is more than one database – in the UK there are currently three major bureaux – either lenders must subscribe to all three or the bureaux will have to link up or share data to ensure that lenders get the complete picture. Such a legal requirement will involve massive investment by both lenders and bureaux to redevelop their systems.

Article 8 states that credit reference agencies may not provide lenders with information about previous searches for credit assessment purposes. Previous search information is a vital tool in preventing overcommitment and fraud by making it difficult, if not impossible, for consumers to make multiple simultaneous applications for credit. Search data may only be held and used by the bureaux for audit purposes, to prove the lender made a search.

> ...lenders may not collect data for marketing or other purposes, even with the consent of the customer.

Responsible lending

As well as undertaking searches in the consumer's home country and other member states before lending for the first time, lenders are also required to search these databases prior to the offering, or the accepting, of a request for a credit limit increase. If it can be established that the lender has not made such searches they will be deemed to have lent irresponsibly.

Restrictions on the holding and use of consumer data

As noted above, Article 7 places severe restrictions on the uses to which information collected from consumers, guarantors and credit reference agencies may be put. Information obtained by a lender may be obtained only on a case-by-case basis and may be used only for assessing the immediate application. This puts at risk the use of customer and bureaux data for risk scorecards, fraud and money laundering prevention, customer management and other model building purposes.

Article 8(3) requires that once the credit decision has been made any bureau data held by the lender must be destroyed. This provision has already been condemned by the Commission itself and by influential MEPs as "a mistake". The German Federal Ministry of Justice condemned this provision as absurd and expressed concern at the restrictive language in which Articles 7 and 8 are couched.

A measure such as that proposed by Article 8(3) would undermine risk management and fraud tools which compare data provided by bureaux and consumers to identify discrepancies and links within fraud rings.

Article 8(1) also requires that when a lender makes a search of the database(s) it must, if requested by the consumer or guarantor, immediately provide the results of the search free of charge to the consumer. This provision seems to be based on the assumption that credit applications are dealt with face to face in a banking environment.

Not only would such a provision involve major costs for both lenders and bureaux in producing a response, which would be compatible with the subject access provisions of the Data Protection Directive, it could lead to breaches of a consumer's privacy if operated in a retail environment. Furthermore, it could lead to serious customer disputes with those who are turned down at point-of-sale since the retailer is rarely, if ever, the lender and has no more information than the consumer does as to the processes involved in the credit assessment. Finally, this provision could have adverse implications for fraud prevention systems if it allowed the applicant to identify the information which had revealed their application to be fraudulent.

Collections and recovery

Article 27 includes a number of specific restrictions on the collection and

use of personal data for collections and recovery purposes. No envelope may carry any inscription which "makes it clear that the correspondence concerns the recovery of a debt." It also prohibits "any contact with the neighbours, relatives or an employer of the consumer…especially any communication of, or request for, information on the solvency of the consumer…"

While the Explanatory Memorandum seems to suggest that it is permissible to ask for information regarding changes of address, referred to by the directive as being "in the public domain", this would have to be done in such a way that those third parties were not aware of the identity of the enquirer, or their purpose in seeking the information. Collecting data in such a way would, however, be likely to constitute a breach of the data quality principles established by Article 6 of the EU Data Protection Directive.

TOTAL HARMONISATION

Given that Article 30 prevents member states from introducing legislation which is more, or less, restrictive than the draft directive and prevents consumers from consenting to any wider use of their data than permitted by the directive – a question mark must hang over the use of at least some of the data collected and shared before the directive comes into force.

TIMETABLE

The timetable for the directive is not yet clear. The text has, for the time being, passed out of the hands of the European Commission and into the hands of the European Parliament where it will be given to the independent Economic and Social Committee for examination before being considered formally by the full Parliament. The full Parliament is not expected to consider the directive before the end of 2003.

However, once the directive does come into force member states will have only two years to bring in national legislation; an impossible timetable in view of the scope of the necessary systems and other changes which will need to be implemented during the two years in which the enabling legislation is being hammered out.

Alasdair Warwood runs a UK-based data protection consultancy business and is the author of the second edition of the BSI's "Guide to the Practical Implementation of the Data Protection Act 1998". He is also a member of the Information Tribunal. He was formerly Director, Consumer and Legal Affairs at Experian and Assistant Secretary at the then Finance Houses Association where he was responsible for encouraging the development of data sharing and the use of credit scoring. From 1991-96 he was also Secretary General of ACCIS – the European Association of Credit Reference Agencies and an Alternate Director of Registry Trust. He also helped in the establishment of the Consumer Credit Counselling Service in Nottingham.

Contact:
Tel: +44 (0)1273 736749,
07771 701678,
E-mail: alasdair.warwood@talk21.com
Alasdair Warwood Consultancy Ltd
7 Selborne Road,
Hove BN3 3AJ, UK

continued from page 13

• ensuring compliance with the data protection law and its executive regulations with regard to security and confidentiality of processing

• receiving notifications and preliminary authorisations; and

• advising the government on possible amendments to the law in the light of new technologies.

TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

In compliance with the EU directive, the law provides that the processing of personal data that is outsourced outside the country may take place only if the country in question ensures an adequate level of protection.

CONCLUSIONS

Luxembourg's new data protection law has a wider scope than the EU Data Protection Directive. Moreover, the provisions are technology-neutral and apply to personal data in all forms. As a result, it is flexible and confronts many of the issues that may arise in the future with regard to the processing of personal data. In conclusion, it transposes the directive appropriately, taking into account today's technological and social changes.

A pdf copy of the new law, entitled "Protection des Personnes à L'égard du Traitement des Données à Caractère Personnel" can be found at: www.etat.lu/memorial/memorial/a/2002/a0911308.pdf

Luxembourg's data protection authority, La Commission Nationale Pour la Protection des Donnees (CNPD) is headed by Monsieur Gérard Lommel.

For further information and to contact the CNPD, see the details below:

Tel: +352 26 10 60-1, Fax: +352 26 10 60-29, E-mail: info@cnpd.lu, Address: 68, route de Luxembourg L-4221 Esch-sur-Alzette, Website: www.cnpd.lu