

Bank insurers and privacy

Data processing in financial conglomerates

In chapters 4 to 8 a number of conclusions have already become apparent. One general conclusion from the fact-finding is that bank insurers (with regard to the character of their products and services) sell 'trust' to their clients. Evidence of this can be found in policy statements which focus on social responsibility and solidarity and emphasize attributes such as carefulness and confidentiality. The banking sector also refers to 'the duty to care' for the client's needs. Trust and this 'duty to care' can be regarded as privacy-enhancing mechanisms. Privacy as an individual need is therefore an integral part of bank insurers' corporate policy. Further down in the organization, however, the situation becomes significantly more subtle. When banks say 'we as bank insurers abide by the law and the mutually agreed codes of conduct', they are in fact seeing how far they can go within the boundaries of the law, for organizational reasons. Privacy is not a selling point in the struggle to win the consumer's favour, as all conglomerates closely adhere to the applicable codes of conduct, including those governing the description of purpose.

The descriptions of purpose in the privacy regulations are formulated to refer to all corporate activities, not only to the purpose for which the client first gave the insurer the data, namely the acquisition of a certain product or service. Some bank insurers market themselves as 'all-round financial advisors'. The question remains whether the client is aware of this or just sees himself as a purchaser of a single product. In view of the extreme complexity of offerors and products, the practice of describing the purpose in such broad terms should be given renewed attention with the aim of providing the client with more transparency. In addition to the information in general conditions, privacy regulations and notifications to the Dutch Data Protection Authority, bank insurers will also have to take greater account of how to apply the tightened rules on the duty to provide information under Articles 33 and 34 of the Dutch Data Protection Act (Wet Bescherming Persoonsgegevens - WBP). This study has revealed that insufficient attention is currently given to the promotion of transparency in the handling of personal data within financial conglomerates.

In practice, there are various mechanisms which support the client's privacy, including material concerns of the bank insurers themselves. 'Direct writers' in particular regard their clients' data as an asset to be handled with the utmost care, so as to prevent the clients from going elsewhere. The targeting of selected clients for marketing campaigns is geared towards minimum irritation and maximum response on the part of the client. Analyzing complaints is another important gauge. Additionally, the organization of the bank insurance company as a financial conglomerate can also have its advantages as regards client privacy. Although the front office is directed towards integral customer care, the amount of data available in that department is in fact limited. Product details are only accessible via the back offices, which are organized according to the different product lines. No personal data relating to products are exchanged between subsidiaries (each operating under its own brand name) unless they have an intermediary relationship.

In the insurance sector in particular, there is often no direct relationship with the consumer as a premium payer, as insurers generally work with intermediaries. One of the consequences of this is that the insurer has or feels no responsibility towards customer contact. This marks a break in the product chain between supplier and end-consumer. The consumer finds himself in the role of claimer, whose interests are directly opposed to those of the insurer. The conglomerate considers that intermediaries are themselves responsible for how they deal with personal data, and no further detailed agreements are made with them regarding the protection of those data.

Furthermore, subsidiaries within the same financial conglomerate often operate as each others' intermediary, for example in bank branch offices. In terms of distribution of responsibilities they then operate in the same way as independent intermediaries, the difference being that they have streamlined (automated) the exchange of data. This means that the subsidiary operating as intermediary can access product data it has received from other subsidiaries and use them for

marketing campaigns, for example. In future, the relationship between conglomerates and intermediaries must be considered with more depth with a view to the provision of privacy guarantees. Another point of particular interest is the promotion of transparency in the handling of data by both parties, at all stages of the relationship with the client.

A further aim of the study was to view the consequences on privacy of the clustering of products and the use of data about other products when dealing with one particular product. This is clearly not yet widespread practice. Data which pertain to different products are combined for marketing campaigns and fraud prevention, but not for acceptance procedures or when dealing with claims. After the front office has received the application for a cluster product, further processing takes place in the back office according to separate product lines. Furthermore, subsidiaries differ in their procedures and data management practices. Combining data in the framework of marketing campaigns and for fraud prevention, such as can be found in practice, is a subject which requires more close attention with regard to its consequences on privacy, especially in the light of pending legislation.

Furthermore, integrated ICT infrastructure has not developed as far as expected. The use of integrated ICT infrastructure to link subsidiaries in a financial conglomerate has not yet gone beyond the planning stage. Plans do exist for index or shell systems at conglomerate level to make clients' data accessible, but they have not yet been implemented. At subsidiary level, such developments have been realized, especially in the case of 'direct writers'. Subsidiaries with a mutual intermediary relationship have also technically streamlined their data exchange.

Final remarks

In view of the fact that conglomerates do have policy plans for further integration, especially concerning organization and ICT infrastructure, this study came at an appropriate time. In the course of the study, the researchers witnessed how conglomerates are beginning to attribute a certain increased importance to privacy concerns. They also found that in practice a balance has to be struck between the interests of the company and the interests of consumer privacy, and that this involves considerable risks. Furthermore, the study revealed that conglomerates are prepared to review protection measures which have been sufficient up until recently but may not be adequate in changed circumstances.

This study has given the Dutch Data Protection Authority (DPA) clearer insight into the practices of data processing in financial conglomerates and the associated privacy issues. Privacy and trust issues related to data processing within conglomerates need to be further elaborated under the WBP. In various conglomerates, there were aspects of business practice which left room for improved security measures in the light of advancing developments and future policy designs. By bringing these aspects to light, the timely conduction of this study provides opportunities for careful implementation of security measures in the future. The responsibility to take these necessary steps of course lies with the conglomerates themselves, both in a social context and within the framework of the WBP.

As supervisory body, the Dutch DPA will closely follow how the conglomerates rise to this responsibility. One obvious way of monitoring this process is by assessing the draft codes of conduct which the banks and insurance companies shall be expected to submit to the Dutch DPA under the WBP. The Dutch DPA will also confer with the other supervisory bodies concerned, some of them members of the Council of Financial Supervisors (Raad van financiële toezichthouders), so that activities can be coordinated so as to promote as effectively as possible the careful use of personal data in financial conglomerates.