Source: Joop Verbeek **Version v0.3/02.09.2009**

Document for:

Decision	**x**
Discussion	
Information	

Privacy-consistent banking acquisition

CEPIS

The Council of European Professional Informatics Societies (CEPIS) is a non-profit organisation seeking to improve and promote a high standard among Informatics Professionals in recognition of the impact that Informatics has on employment, business, and society. CEPIS – which represents 37 Member Societies in 33 countries across greater Europe – has agreed on the following statement:

1. Background

With a view to the Single Euro Payments Area (SEPA) [1], some banks within Europe have developed the practice to ask specific clients in a very intrusive way all kinds of questions about their personal life. The bank employees who are appointed to ask these questions are usually called 'advisors'. Their goal is most probably to get the active property of their clients, which is on the accounts of other banks, on their accounts. It seems to be in other words an acquisition policy.

From an ICT perspective the problem that arises is twofold. 1. Almost every bank employee has more access rights than strictly necessary for the specific task of the employee. 2. The so-called advisors have even more possibilities and access rights to look into the details of the data of many specific clients. They can easily combine these data. In some cases even insurance data is part of the data at their disposal.

2. Concerns

From the perspective of the protection of the privacy of the European citizen, the situation mentioned in the previous paragraph is a serious threat. From a legal point of view the necessity and proportionality principle [2] is at stake. Even if the clients give their consent to an interrogation, the average European citizen is not completely aware of the repercussions and the intrusiveness of the questions with respect to his or her personal life. Clients who are not aware of their privacy (rights) give away too much personal information without existing need, because of the intrusiveness of the questions. Banks try to defend this existing practice by referring to their general conditions. However, these general conditions might very well be in contradiction with the necessity and proportionality principle within European legislation and hence illegal. CEPIS

would like to urge the European banking community to stop the current practice described above and bring their practice in accordance with the necessity and proportionality principle within the specific European (data protection) legislation.

In our opinion it is in the interest of the European banking community itself to investigate the mentioned issues because the relationship bank-client could be seriously compromised because of the mentioned privacy-sensitive practice within some European banks. Acquisition should be in accordance with European privacy regulations.

3. Recommendations

In particular the following points need to be considered.

1. The access rights of the employees should be in accordance with their specific task.
2. Advisors should not have access to too much information about too many clients.
3. The information gathered with the consent of the client should be deleted as soon as possible.
4. Cross-branch access to data, *e.g.*, to insurance data and banking data should be avoided.
5. Interrogation of clients should be limited to questions, which are strictly necessary for the daily banking operation and should never be too intrusive with respect to the privacy of the European citizen.
6. Accessing data by employees should be logged in order to be able to judge after the necessity of the data access. This is also a preventive measure to prevent unnecessary data access.
7. The account data displayed on ticket machines and other machines of the bank should be limited to the data strictly necessary, in accordance with the specific wishes of the individual client. For instance, the client should be able to avoid the displaying of information about specific savings accounts.
8. The European banks should alter their general conditions in such a way that they are in full compliance with the necessity and proportionality principle. [3]
9. It is advisable that the data protection regulations, both European and domestic, should be applicable to the mentioned type of information and that bank employees and the banks themselves should be liable if any infringement is committed.

References

[1] For more information see: http://www.ecb.int/paym/sepa/html/links.en.html
[2] The principle of proportionality ensures that the processing of a person's personal data is limited to cases where there is a direct connection with the initial purpose of the processing. The information must not only be useful, but also necessary to whoever is processing a person's data. The data being processed must not be excessive in relation to the aim pursued.
[3] On the basis of the Data Protection Directive at least the following issues are at stake, see: 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, Official Journal L 281, 23/11/1995, p. 0031-0050;
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML

Personal data may be processed only insofar as it is adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed. The data must be

accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified; The data shouldn't be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use. (art. 6)

When sensitive personal data (can be: religious beliefs, political opinions, health, sexual orientation, race, membership of past organisations) are being processed, extra restrictions apply. (art. 8)

The data subject may object at any time to the processing of personal data for the purpose of direct marketing. (art. 14)

A decision which produces legal effects or significantly affects the data subject may not be based solely on automated processing of data. (art. 15) A form of appeal should be provided when automatic decision making processes are used.