Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Data protection and e-commerce: implementation aids and realisation proposals by the Federal Data Protection Commissioner

Electronic business – e-commerce – permits the worldwide exchange of goods and services. A great future is forecast for this new form of business. The analysts expect sales of up to 500 billion dollars in the year 2002. Even if it seems that the technical problems can be resolved there is a lack of confidence and above all legal security with respect to e-commerce.
The conventional world of business is well regulated. Thanks to the existence of these regulations there is a certain transparency and legal security for all concerned. These laws establish security which leads to the feeling of confidence. In other words fixed rules are the basis for confidence. But what legal culture provides the basis for commerce on the Internet? Additional legal and technical outlay are both necessary to ensure that data are not abused on the net and that legal disputes can be dealt with immediately and efficiently as in traditional business transactions.

In real world business transactions client models arise which are not very clearly defined. No one would want to fill in a questionnaire every time they visit a department store. As a rule the acquisition and passing on of data is limited to a restricted circle in the local environment. In the case of e-commerce, in contrast, everything is based on data. Every purchase permits deductions about the person, his needs and his financial position. Consequently, data protection is of prime importance.

To reinforce user confidence in e-commerce and to protect personal data the Federal Data Protection Commissioner presents a series of implementation aids and realisation proposals which can be helpful to enterprises in the implementation of a customer-friendly, transparent data processing policy which complies in full with the provisions of the law.

Feldeggweg 1, 3003 Berne
Phone +41 58 463 74 84, Fax +41 58 465 99 96
www.edoeb.admin.ch

Minimum requirements for the protection of privacy in the electronic commerce environment

- The provisions for the protection of privacy contained in the Data Protection Law (DPL) can reinforce the generation of user confidence in the services offered by electronic commerce.
- The Swiss Data Protection Law offers flexible solutions for the processing of personal data by private individuals (Art. 4 and 13 DPL) and is compiled on a technologically neutral basis. Consequently an amendment of the law is not immediately necessary.
- However, legal provisions alone are not sufficient to protect the privacy of e-commerce users. In particular the users must be informed and their awareness heightened.
- Mid-term user awareness should be promoted by further education measures.
- To reinforce user confidence in electronic business the service providers should (as stipulated by the DPL) process client data transparently. The operators should inform the user on which personal data they want to use and for what purpose. When personal data from a contractual relationship are processed for other purposes (e.g. marketing, publicity) the user should have an option.
- Technologies such as cryptographic procedures, authentication procedures and other data protection-friendly technologies, e.g. the utilisation of anonymisation tools, are suitable for data security. These should be used in the electronic business environment and made available to the user.
- Finally the protection of privacy, in particular transparent data processing, can reinforce user confidence in electronic commerce. This can certainly be used as a competitive advantage for Swiss enterprises.

Key elements for the development of electronic commerce

- E-commerce is ”one-to-one-business” i.e. it is based exclusively on personal contact. Consequently the consumer will react cautiously if he is flooded with advertising and information without flanking confidence-forming measures. Many enterprises already compile databases in order personalize their offer. This further weakens consumer confidence if the persons concerned are not duly informed.
- Authorities hold a key position in the construction of the ”framework” within which e-commerce should be conducted. Protection of privacy heads the list of priorities.
- The problem “privacy” must be adequately resolved to stabilise the market for the long-term success of e-commerce. A significant factor in this respect is which law will be applicable for the pursuit of claims. In the USA the law of the supplier is applicable in litigation. However, the law at the consumer's domicile should be applicable. Only like this will the consumer be able to win confidence in the range of e-commerce services offered in the future.

On international level, the emphasis should be placed on the following aspects:

- Confidence forming measures (in particular protection of privacy) must be implemented efficiently.
- The synthesis of state regulations and codes of conduct as well as technological solutions such as digital signature, privacy enhancing technologies (PET) must be interoperable and internationally recognised.
- The OECD should contribute to the implementation of the above-mentioned points in dialogue with all concerned (business, authorities, consumers and other international organisations).

In Switzerland the emphasis should be placed as follows:

- Swiss representatives on international bodies continue to support further measures to establish consumer confidence in e-commerce.
- A combination of both models state regulations and codes of conduct is certainly welcome. The codes of conduct, however, must protect consumers at least as effectively as state regulations. If the codes of conduct are not able to develop the required degree of efficacy, state regulations for consumer protection are required.
- The e-commerce plan of action that already has been compiled in Switzerland must be implemented rapidly. In particular, confidence forming measures (education, information, protection of privacy) must be in the front line of the public approach.

Data protection conform configuration of a website and the advantages entailed

We recommend that website operators develop a policy for the protection of privacy, on the one hand to meet the legal requirements (transparency, information, options, security, authorisations). On the other hand the confidence of their customers and future users can be built up in this way.

In particular the following aspects should be covered:

- Information on the data protection legislation the specific offer is subject to should be placed where it is easily visible. Further, data protection practice on the website should be explained in easily understandable language. In particular, a statement of which data are acquired and used and for what purpose is essential.
- The user should also be given a choice with respect to the restriction of utilisation (e.g. compilation of customer profiles) and the passing on (e.g. for advertising purposes) of his data.
- Appropriate security measures must be taken in the framework of the intended purpose with respect to the correctness and completeness of the data (e.g. encoding and authentication methods) and to ensure they are up-to-date.
- Finally reference should be made to the mode and manner of implementing legal claims.

Certain processing operations with Internet user data could violate the data protection provisions.
Consequently personal data should not be acquired, passed on or made accessible to third parties without the knowledge of the user.

Hints on the compilation of a data processing statement for Internet services

Data processing statements should inform the user of a website on the protection of privacy procedures practised by the service provider. This is a significant step towards gaining the user's confidence. Prerequisite is that the statement shows the required precision. Only like this the user will be put in the position to decide freely whether and how he wants to allow his personal data to be processed.

We recommend that Swiss companies offering services via the Internet practice a transparent data processing policy by developing such statements and featuring them on their website.

The data requirement of the company must be examined, the current data protection practices analysed and clear guidelines on the handling of personal data drawn up before beginning with the compilation of a data processing statement. The data processing statement can be drawn up on the basis of these facts. It has to comply with data protection law and correspond to the effective data processing.

We recommend not to start drawing up the data processing statement until at least the following questions have been answered:

- How are personal data acquired and where from (internal / external sources)?
- What purposes are personal data collected for?
- What purposes are personal data used for?
- Who is responsible for the control of the personal data collected?
- How and where are personal data stored?
- For what purposes are personal data exchanged with third parties?
- Are there already any guidelines or provisions for the collection, processing and the passing on of this data?
- Is viewing and correcting the data already possible?

The statement should inform the user at least about the following factors:

- What legal provisions govern the provider's data processing practice?
- What personal data are collected and for what purposes?
- What data are passed on to third parties and for what purposes?
- What choices are open to the user for the processing of his data?
- What rights (in particular the right of information and correction) has the user?
- Who answers questions on the processing of personal data?
- What security measures are applied for the protection of personal data?

Finally, the statement must be positioned on the website easily accessible for the user.

Efficacy of protection of privacy with self-regulation models

The most important criterion in the evaluation of codes of conduct for the protection of privacy is their implementability. The percentage of association members who keep to the rules and whether it is possible to impose sanctions against a member for non-compliance with the code of conduct play a significant role in the evaluation of implementability. Further such a code of conduct must be transparent i.e. set out in generally understandable language.
Respect of the code of conduct ought to be a prerequisite for admission to the relevant business association. Binding external controls or sanctions should back up compliance with the code of conduct. After all, it is of decisive importance that the persons concerned are not left to their own devices but receive assistance and support. Apart from this, at least the following fundamental principles must be integrated in the code of conduct:

- Clear information of the persons concerned on the type of data acquired, the utilisation purpose, the recipient and the choices for restriction of utilisation and communication.
- Grant of the rights of information and correction and measures for data processing security.
- Right of appeal to an independent instance.

Criteria for the protection of privacy by means of a code of conduct

A code of conduct can be useful for the establishment of confidence. Nevertheless, codes of conduct are no alternative to laws; they are merely a complement to legal provisions.
Every effort must be made to ensure that such codes of conduct include at least the following elements:

- Clear and understandable information, above all with respect to the nature and way in which personal data are processed.
- User's fundamental right to options on the utilisation of his data.
- Effective legal enforcement mechanisms.
- Creation of uniform criteria for the recognition of codes of conduct (international criteria).
- It is imperative that both the authorities and the business world be integrated in the recognition of code of conduct process.
- The content must provide information on data processing, delivery, compensation as well as on the law applicable in the event of dispute.

Last update: March 2012