

New Data Protection Act in Switzerland: More transparency, additional costs

The Swiss Parliament has partially revised the Federal Data Protection Act. It is currently expected to come into force in Summer 2007. By **David Rosenthal**.

While it will make the processing of personal data more transparent for private individuals, it is also likely to increase the costs of data protection compliance in Switzerland. In the short term, companies will have to put more focus on their privacy statements and review their processing of customer profiles. In the mid to long term, many businesses will consider appointing a privacy officer to avoid burdensome obligations to register their data collections.

More than 10 years after the Federal Data Protection Act came into force in Switzerland, the Swiss Parliament has partially revised it for the first time.

Some of the changes were necessary in light of Switzerland's adoption of the Additional Protocol to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, concerning supervisory authorities and transborder data flows. Other changes have been adopted to bring the Data Protection Act into closer alignment with EU Directive 95/46/EC, although full compliance has not yet been achieved. Nevertheless, as far back as 2000 the European Commission ruled that Switzerland was already offering an adequate level of privacy pursuant to Article 25(2) of the directive.

Some peculiarities of Swiss privacy law – such as the extensive protection of data relating to identified or identifiable legal entities (most jurisdictions protect only the personal data of private individuals) – have not changed. Another unique feature of Swiss data protection law is the increased protection of “personality profiles”, that is, any collection of data allowing the appraisal of fundamental characteristics of an individual's personality. Under the current and new Data Protection Act, all rules governing sensitive personal data also apply to personality profiles.

Finally, Swiss law does not distinguish between the obligations of the

data controller and those of the data processor in the same way as EU Directive 95/46/EC. Under Swiss law, it is not only the responsibility of the data controller to ensure compliance with the basic principles for processing personal data. The processor also remains fully liable for ensuring that data processing is compliant with the Data Protection Act. Hence the data subject may also sue the data processor in case of an infringement of privacy. The main difference between the data controller and the data processor is that in most cases it is the sole responsibility of the data controller to comply with information rights and with notification

subject has consented to such a lack of protection.

The amended Article 6, which governs transborder data flows, now contains a conclusive list of acceptable methods to ensure such protection. Overriding private interests of the data controller or processor as such are no longer sufficient. Instead, one of the following conditions must be fulfilled:

1. *The country of the importer provides an adequate level of data protection.* This requirement is not new. Data protection laws complying with the requirements of the Convention for the Protection of Individuals with regard to Automatic Processing of

Swiss law does not distinguish between the obligations of the data controller and those of the data processor

or registration obligations.

TRANSBORDER DATA FLOWS

One major point of the revision touches on the rules governing transborder data flows. Under the revised Act, it is no longer necessary to notify the export of personal data to the federal Data Protection and Information Commissioner, although this obligation has never really been a problem in practice. There is still an obligation to ensure an adequate level of data protection in the country of the importer (ie. the country to which the data will be exported). In the current version of the Data Protection Act, there is no express rule on how to achieve such protection, although it is accepted that in the absence of statutory data protection the use of transborder data flow agreements is acceptable. It is even permissible not to ensure any protection of the data abroad (or to provide only for a reduced level of protection), as long as this can be justified by an overriding private or public interest or the data

Personal Data are generally considered to provide such protection. The Swiss Federal Data Protection and Information Commissioner (at website www.edoeb.admin.ch) has also published a non-binding list of countries with adequate data protection. However, if the personal data at issue relates to legal entities, most foreign privacy laws are insufficient in this respect as they protect only the personal data of individuals.

2. *There are “sufficient warranties” ensuring an adequate level of protection abroad,* such as a transborder data flow agreement. The reliance on contractual instead of statutory data protection is not new, and the website of the Federal Data Protection and Information Commissioner has already published a model contract drafted for the current Data Protection Act (no major changes are to be expected for the revised Act). The revised Act introduces a requirement that the Commissioner be “informed” about such agreements or other warranties (presumably by the exporter). The meaning of this notifica-

tion obligation in practice is unclear since the necessary guidelines have not yet been issued (a first draft is expected by the end of 2006). This notification obligation has already been sharply criticised as impractical and burdensome for affected businesses (and possibly also for the Commissioner, given the popularity of transborder data flow agreements).

One possible compromise could be that only those transborder data flow agreements deviating from acceptable model contracts be made subject to this notification obligation. Still, this would not solve the problem where the counterparties have not entered into a separate agreement to regulate transborder data flows. For example, transborder data flows in the context of outsourcing arrangements are commonly governed by the provisions of the outsourcing agreement. In such a situation, the new Data Protection Act might require notification of the (relevant portions of the) agreement to the Commissioner (it is not yet clear whether such notifications will remain confidential). Wilful failure to comply may be prosecuted as a criminal offence. The notification obligation is not limited to the transfer of entire databases but also applies to the transfer of individual records of personal data, even if the person affected is aware of the transfer.

Transborder data flow agreements are not to be the only admissible forms of a "sufficient warranty" pursuant to Article 6 of the revised Act. The "safe harbour" concept implemented in the United States is another possible means of ensuring an adequate level of privacy, and other concepts may be developed in the future.

3. *There is a binding corporate rule in place which sufficiently ensures data protection in the case of transborder data flows within a single legal entity or a group of companies.* On the face of it, this provision appears to make intra-group data transfers easier. In practice, however, the opposite might be true since such binding corporate rules must be notified to the Commissioner, which may complicate amendments even if they do not affect the level of data protection. Again, the rules for notification are not clear, but no such obligation exists today. This is one reason why it is

not expected that this provision will lead to major gains in efficiency for intra-group data transfers. Also, eligible binding corporate rules will have to provide for a similar level of enforceability as transborder data flow agreements. This may eliminate the advantage of using binding corporate rules instead of implementing a basic transborder data flow agreement (in fact, many international businesses have already implemented generic, multiparty, intra-group transborder data flow agreements to ensure data protection compliance in addition to their binding corporate rules). This may remain a necessity, bearing in mind that not all countries recognise binding corporate rules for ensuring an adequate level of data protection in case of intra-company or intra-group transborder data flows.

4. *The data subject has consented to the particular export at issue.* According to the revised law, consent must be given for one "individual case". While generic consent will not suffice, it is not necessary to obtain the data subject's consent for every single transfer if the transfer forms part of an overall transfer scheme which has been approved by the data subject. This provision is not expected to create major problems since the data subject's consent is not required if one of the other means to ensure an adequate level of data protection is implemented. In other words, the data subject's consent is necessary only if no adequate level of data protection is ensured. Further, consent may be implicit, except in the case of sensitive personal data or personality profiles.

5. *The export of the personal data at*

important for companies in Switzerland which are involved in legal proceedings abroad and are increasingly confronted with the need to produce evidence before a foreign court which offers no confidentiality and privacy guarantees (however, other provisions of Swiss law may still restrict such disclosure).

7. *The export of the personal data at issue is necessary to protect the life or physical integrity of the data subject.* A similar provision already exists under Directive 95/46/EC.

8. *The data subject has made the personal data publicly available and has not expressly prohibited the processing of such data.*

At first glance, transborder data flows are likely to become less burdensome than they are today, since data subjects need no longer be informed in cases where the data exporter does not want to notify the commissioner of its intended data transfer (even though such notification usually has no negative consequences and is not public).

However, this efficiency gain may well be negated, depending on how the statutory obligation to notify transborder data flow agreements and binding corporate rules to the commissioner is implemented by the legislature and complied with in practice by private businesses. A first draft is expected by the end of 2006. In truth, the commissioner does not have the resources to examine in depth a large number of notifications. It is also doubtful whether private businesses will comply fully with the notification obligation since it is not limited to the export of an entire database but applies

Wilful failure to comply may be prosecuted as a criminal offence

issue is required for the conclusion or performance of a contract with the data subject. A typical example could be the transfer of certain personal information of a bank customer in order to effect a money transfer to a recipient abroad.

6. *The export of the personal data at issue is necessary to maintain overriding public interests or to establish, execute or enforce legal rights in court proceedings.* This latter provision may be

to any transfer of personal data abroad for which data protection is warranted only by means of a contract or policy. Many such transfers may not even be obvious at first sight.

NEW OBLIGATIONS TO INFORM DATA SUBJECTS

Other important changes in the revised Data Protection Act create new obligations to inform data subjects about the

processing of their personal data. The effect of these changes will not only increase transparency but is also intended to discourage the processing of sensitive personal data and personality profiles.

Article 4(4) of the revised Act expressly requires that the data subject be aware of the collection of personal data and the purposes for which it is being collected. Previously, this requirement applied only to data processed by federal authorities and was limited to sensitive personal data and personality profiles. It does not necessarily require that the data collector actively inform the data subject; if it is sufficiently clear from the circumstances that personal data is being collected and used for certain purposes, no express information is necessary. If a customer is asked to complete a form to make an order, it is obvious that this data will be used to fulfil the order. It may also be argued that a customer will also expect to receive promotional information from the company in the future. However, the customer will normally have no reason to expect that the company will share his or her address, or even more information, with third parties for their own marketing purposes. In such situation the customer will have to be actively informed in the future. Online, this might be done by posting a privacy policy. On a paper form, the necessary information could be provided in fine print. In the case of "covert" data collection devices (such as certain closed-circuit television cameras), signs must be mounted informing persons of the device and its use.

It may be argued that this is not really a new requirement because the existing law already requires any processing of personal data to happen in good faith. Also, according to Article 4 of the existing Data Protection Act, personal data may not be processed for a purpose which is not provided for by law, was not communicated and was not apparent from the circumstances at the time of the data collection.

However, there is one major difference under the revised Act. Under the current Act, it has always been possible to justify non-compliance with Article 4 to the extent that the data controller or processor has an overriding private

or public interest, can rely on a provision of law for such noncompliance or has the consent of the person affected. The Swiss Parliament wanted to cut off this route by specifically removing the reference to a possible justification in Article 12 of the revised Act. Accordingly, a breach of the basic principles of personal data processing as laid out in the Act shall always be illegal, even if the interests of the data controller or

found in Article 7a of the revised Act. It requires the data controller (but not the processor) of a "data collection" to inform the data subject whenever sensitive personal data or a personality profile is gathered (this may also apply to the gathering of information to expand an existing profile). This obligation also applies where such personal data is obtained from a third party (ie. indirectly), in which case the data

It will become illegal to use customer data for fraud prevention if the customer is not informed in advance

processor in not informing the data subject outweigh the interests of the data subject in being made aware of the data collection and the purposes for which the data will be used.

For example, it will become illegal to use customer data for fraud prevention if the customer is not informed in advance. As another example, speed and other traffic controls that collect data relating to identified or identifiable individuals which is used to execute federal law may violate the revised Act unless they are made easily recognisable by car drivers (or unless a specific provision of law allows for covert speed controls). However, the revision to the Data Protection Act is not entirely clear in this regard. It is the result of a last-minute change which was not properly thought through. Most experts consider the change simply as a mistake and have even called for ignoring the new law in this respect. For instance, it is unreasonable to require the implementation of a certain level of technical and organisational measures to prevent unauthorised data processing if the person affected has (voluntarily) consented to a lower level of protection (such as in the case of a service provider which will charge extra for better security). Although Swiss lawmakers have expressly removed the possibility of justifying violations of the basic principles for data processing on a case-by-case basis, it is foreseeable that several legal theories will emerge with the purpose of maintaining the fundamental principle that certain violations of privacy may be justified and are, therefore, not illegal.

Another important new provision is

subject must be informed at the latest before the data is stored or disclosed to third parties, if no storage takes place. There are three exceptions to this information requirement:

- The data subject has already been informed (for example where the data was gathered by a third party and subsequently passed on. In such a case it would be advisable, for the limitation of liability, to request an appropriate representation and warranty when obtaining sensitive personal data or personality profiles from third parties);
- The data has been obtained from a third party, and a statute expressly provides for the storage or disclosure of such data;
- The data has been obtained from a third party, and it is not, or not reasonably, possible to inform the data subject (this will likely be interpreted narrowly; it has been stated that the data controller must at least try to comply with the obligation before being entitled to argue that informing is not reasonably possible).

Furthermore, as with the existing right of access, informing the data subjects may be denied, limited or delayed to the extent that

- the data controller has an overriding private interest, provided the personal data is not disclosed to third parties. For example, if a company shares sensitive personal data or personality profiles with a parent company or other affiliates in a group of companies, it will not be able to deny, limit or delay the information of the data subjects

based on its overriding private interest;

- a formal law provides so; or
- this is necessary to protect overriding interests of third parties.

DUTY TO INFORM INDIVIDUALS

It appears that the obligation to inform does not apply to single instances of the collection of sensitive personal data or personality profiles. Since the provision refers only to the controller of a “data collection” being subject to the obligation, it may be assumed that the obligation to inform applies only where sensitive personal data or personality profiles are stored in a manner that allows for a search to be conducted with regard to a particular data subject. The data subject must be informed of:

- The identity of the data controller;
- The purpose of the data processing; and
- Where the personal data is to be disclosed to third parties, a generic description of such intended recipients.

Intentional failure to comply with this obligation to inform may be prosecuted as a criminal offence.

For companies operating in the European Union, this type of provision is not new. What is different under the Data Protection Act is that Swiss law treats personality profiles (ie data collections which allow the appraisal of essential characteristics of individuals) in the same manner as sensitive personal data. Accordingly, under Swiss law, a consumer purchase profile, for example, receives the same level of increased privacy protection as, for instance, personal data concerning the health or sexuality of an individual. This can prove tricky in practice because personality profiles can emerge over time simply as a result of collecting more and more information about individuals.

There is also no privilege for transfers of personality profiles or sensitive personal data within groups of companies and among affiliated legal entities. Accordingly, if one entity within an international concern wishes to transfer profiles of consumer customers to an affiliate (profiles of legal entities are not included in the term “personality profile”), the data subject must be informed that such data may be shared

with other group companies at the time the data is gathered. Under the existing Act, the disclosure of personality profiles or sensitive personal data to a third party (including affiliates and parent companies) requires the (express) consent of the data subject, unless there is an overriding private or public interest or a statute of law justifying such disclosure. In future, a company wishing to share personality profiles or sensitive personal data with others will usually be forced to disclose this to the data subject. Notably, this will not necessarily prevent the company from processing such data, even where the data subject objects to the processing, because the company may be able to rely on an overriding private interest that justifies its processing of the data against the express will of the data subject.

The rationale behind these new information obligations is to give data subjects greater control of their privacy rights. Even though they may ultimately be unable to prevent the processing of their personal data, they will at least be aware of it and may object. Data controllers have one year from the date on which the revised Act takes effect to implement the necessary measures to inform data subjects of personal data that has already been collected.

NEW DATA PROTECTION PROVISIONS

A pending revision of the Swiss Telecommunications Act, expected to come into force in April 2007, will also introduce new data protection provisions that will require companies to inform customers more actively. The most important change in this respect is the new Article 45c, which prohibits the processing of “data on the computer” of another person by use of telecommunications tools unless: (i) the “user” has been informed of such processing, the purpose of such processing and the possibility to object to it, or (ii) the processing is needed for the provision and billing of a telecommunications service. The provision is comparable to Article 5(3) of the EU Privacy and Electronic Communications Directive (2002/58/EC), which governs, among other things, the use of

internet cookies. Companies in Switzerland that use such techniques to track and trace users of their websites (even if they collect no personal data) will be required to inform their users about their practices in the future, as is already commonplace in the European Union.

PRIVACY OFFICER NOT MANDATORY

The basic right of a data subject to review the personal data processed by a data controller or processor remains largely as it is today, with one exception. The data controller must inform the data subject not only of which personal data is being processed and the purpose and legal basis of such processing, but also of the source of the personal data at issue. As practical experience bears out, such information is crucial for a data subject to their privacy rights where data is used for commercial communications. The reason is that such data is often traded among businesses without the data subject’s knowledge. Without information on the source of data, the data subject will often be unable to trace back their personal data and prevent its further distribution. Unfortunately for consumers, the revised Data Protection Act does not envisage any obligation to collect and retain such “source” information. It may thus be expected that data controllers will usually argue that they no longer have any information on the source of the personal data relating to one particular data subject.

AUDITS AND CERTIFICATION

A further change concerns the introduction of data protection and privacy certification. The exact rules have not been set out, but the idea is to allow vendors of data processing systems and software, private individuals and federal authorities to have their systems, procedures and organisations audited and certified through independent, officially recognised certification authorities. There is no obligation to obtain such certification, and there is limited legal incentive to undergo such procedure. It remains to be seen whether businesses and public authorities will really invest in such a “privacy label” as provided for by the revised Act.

Likewise, there will still be no obli-

gation for private businesses, including large organisations, to institute a privacy officer. However, there is at least one legal benefit in appointing a privacy officer (or obtaining privacy certification). This concerns the obligation to register data collections with the federal data protection and information commissioner as currently stipulated in Article 11 of the Data Protection Act.

A private data controller must register data collections with the Commissioner (the register is publicly accessible) where it either regularly processes sensitive personal data or personality profiles or regularly discloses personal data (of any kind) to third parties (again including disclosures to affiliates, should such disclosures not become generally exempted). Under the current law, no registration is necessary if the data subjects were aware of the processing. Businesses have usually chosen to avoid registration by informing data subjects of the

processing (such as through the use of privacy policies or privacy clauses in general terms and conditions).

Under the revised Act, this exemption will no longer be available (which is yet another change which is not well thought out). The obligation to register will remain the same (it will be moved to Article 11a), but will become more difficult to avoid if data is not processed due to a statutory requirement. Although there are certain exemptions for journalists and the media, and although the Federal Council will likely define additional exemptions (one such exemption might be for archived data collections), the only way most businesses may avoid registration is either to appoint an independent privacy officer (which satisfies certain criteria still to be defined) or to obtain a privacy certificate and notify such certification to the Commissioner.

Many businesses that regularly process personality profiles or sensitive

personal data, or regularly disclose personal data to third parties, will probably consider appointing a privacy officer as this may be regarded as the lesser evil to circumvent registration of their data files. On implementation of the revised Act, it is expected that a number of independent consulting companies will start offering small and medium-sized enterprises the option of outsourcing the privacy officer function. This will further increase the costs of data protection compliance in private industry without really improving the situation of the data subjects.

• See www.edoeb.admin.ch/org/00828/index.html?lang=en for text of 1992 law.

AUTHOR

David Rosenthal is Counsel for IT and Telecommunications Law at Homburger, Attorneys-at-law, Zürich, Switzerland, (www.homburger.ch) and lecturer at the University of Basel Law School and Swiss Federal Institute of Technology, Zürich. E-mail: david.rosenthal@homburger.ch