Compliance has pulling power: implementation of changes to the Swiss Federal Data Protection Act

Ueli Sommer
Walder Wyss & Partners, Zurich
usommer@wwp.ch

Data protection is a very hot issue, especially among employees. They expect an attractive employer to treat sensitive data with the utmost care. By contrast, large international groups are often criticised by consumer organisations for their handling of sensitive data. Consequently, an employer may enhance its attractiveness by 'selling' its full or even over-compliance with the applicable data protection laws.

In Switzerland, the Swiss Parliament has adopted various amendments to the Swiss Federal Data Protection Act (SDPA)which will create additional disclosure, registration and organisational obligations for employers, but will also simplify cross-border data transfers. Even though these amendments will not become effective before 1 July 2007, it seems important for employers to amend their procedures and policies as soon as possible. Further, very fast implementation of the new standards and compliance therewith can be marketed to enhance a company's reputation and attractiveness as an employer.

Increased employee sensitivity

The growing digitalisation of today's business world makes it possible for data to flow very fast and very efficiently within large business organisations. Furthermore, the outsourcing of information technology and human resources services is common practice. Consequently, transfers of sensitive data, especially employee data, have increased substantially. While employees and employee representations, at least in Switzerland, used to be quite passive regarding the protection of sensitive employee data in the past, data protection has developed into a hot issue recently. Nowadays, employees and potential prospects want to know from their current or future employer what kind of data is stored, how long it will be stored and, especially, which persons inside or outside the organisation will have access to the stored data. Employees and candidates are starting to expect an attractive employer to treat sensitive data with the utmost care, meaning that employers do not only comply with minimum legal requirements but with best business practices. Moreover, they expect that access to their data will be very restricted and that their data will be protected by the latest available technology. Finally, employee representations are increasing their pressure for the implementation of limits on data collection.

Large international groups are often questioned and criticised by consumer organisations regarding their handling of sensitive data. Consequently, it seems important for an employer not to be listed or flagged for careless handling of data. Furthermore, an employer may address the increased data protection sensitivity by highlighting and marketing its full or even over-compliance with applicable data protection laws and best practice standards. Thus, a company may also enhance its reputation and attraction as a current or future employer.

Amendment of the Swiss Federal Data Protection Act

Background

The amendments to the Swiss Federal Data Protection Act of 1992 have two main objectives:

(1) to update the SDPA and, in particular, to make the subjects of data collection and processing aware of the purposes and uses of such data collection and processing; and

(2) to make the necessary adjustments for compliance with and to permit ratification of, the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

The amendments do not attempt to implement the EU Directive 95/46/EC on Data Protection, although they are, in part, derived from it.

The SDPA protects the data of both natural persons (individuals) and legal entities (for example corporations). The protection of data relating to corporations and other business organisations is a special feature of Swiss law and it creates difficulties in respect of cross-border data transfers. Indeed, only a few other countries provide an equivalent level of protection for such data.

The amendments were enacted on 24 March 2006 and are expected to become effective in the second half of 2007 although the Federal Council has not set a final enactment date yet.

Key elements of the amendments in general

Transparency

The collection of personal data and, in particular, the purposes for which it will be used, must be apparent to the person or entity whose data is being collected. This requirement does not always lead to a specific disclosure obligation, but it will be necessary to give notice of any purpose or use of collected data which the subject of the data cannot infer from the circumstances. For example, if personal data is collected in the course of concluding and performing a contract, but if the recipient of the data intends to use the data for purposes outside the scope of the contract or for the benefit of third parties, then such uses of the data will have to be disclosed by appropriate means.

Information for special categories of data

The amendments will require the person who owns or controls a data collection to inform the subjects thereof if sensitive personal data is collected or personality profiles are maintained. The disclosure must at least identify the person who owns or controls the relevant data collection, the purpose of the data processing and the categories of data recipients.

Consent

The amendments make it clear that if the consent of the data subject is required for data processing, such consent will only be valid if given freely after adequate disclosure of the purpose and use of the data collected and processed. Such consent may only be freely given if the subject of the data is aware of the consequences that would arise if consent to having its data collected were not given. Any consequences would thus have to be appropriate.

Furthermore, the consent will have to be explicit, rather than merely inferred from the surrounding circumstances, if sensitive data are processed or personality profiles are maintained.

Cross-border data transfers

Under current law, cross-border data transfer is only possible if the legislation of the country of destination provides a level of data protection equivalent to that under Swiss law, if a cross-border data transfer agreement has been made or if the subjects of the relevant data have given their consent to the transfer. This regime is especially cumbersome because the laws of most countries do not protect data relating to legal entities and therefore do not afford an equivalent level of data protection.

The amendments state that the country of destination must have data protection legislation which provides 'appropriate' protection, rather than protection 'equivalent' to that available under Swiss law. This should be understood as a change in form rather than a change in substance. The amendments, however, do provide a list of exceptions allowing for data transfers even in the absence of legislation providing 'appropriate' data protection. In addition to reliance on either a cross-border data transfer agreement or the consent of the data subjects, the amendments would permit data transfers between two legal entities which are subject to common management and to data protection policies providing for 'appropriate' data protection, for example, a corporate group data protection policy. In order to rely on the exception, the group data protection policy must comply with the SDPA.

Another exception will be granted if there is a direct need to transfer data in order to conclude a contract or perform contractual obligations and if the transaction involves the data of the contractual counterparty. Unlike the provisions of the EU Data Protection Directive, under Swiss law, there will be no exception regarding the conclusion or performance of a contract concluded between the party controlling the relevant data and a third party which is in the interests of the data subject.

Current law requires notice to be given to the Federal Commissioner for Data Protection of a data transfer abroad if the data subjects do not have knowledge of the transfer. The amendments will replace this requirement with an obligation to notify the Commissioner of the cross-border data transfer agreements or data protection policies under which data transfers will be made (but only in the case of transfers to countries not providing 'appropriate' data protection).

Data processors

Under the amendments, the person who owns or controls a data collection will have to verify that any third-party data processor processes the relevant data in compliance with the law and will be liable to the subjects of the data if it fails to perform this verification.

Registration of databases

Databases will have to be registered with the Federal Commissioner for Data Protection if sensitive data or personality profiles are regularly processed or data is regularly disclosed to third parties. Currently, no registration is required if the data subjects have knowledge of the processing. In the future, this exception will cease to exist. However, no registration will be required if the person with ownership or control of the data has either:

(1) obtained a data protection quality assurance certification from a recognised, independent third party; or
(2) designated an internal data protection officer who has authority to independently monitor compliance with data protection rules and keep records of the data collection being maintained.

No exception to the principles

The SDPA in its current form specifies that data may not be processed in violation of the principles set out in the law without justification. The amendments will remove the exception for 'justified' non-compliance with the principles of the SDPA. This small, perhaps even unintended change means compliance with the principles of the SDPA will be an absolute requirement. An example of this is the principle that data may only be processed for the purpose for which it was collected or which is evident from the circumstances and that such data cannot be compromised, even if the person who owns or controls the data collection claims an 'overriding interest' as a justification for processing of data in a manner otherwise not permitted by law. It is therefore crucial that all potential uses or purposes for the collection and processing of data are disclosed when the data is collected.

Consequences for employers

Additional disclosure obligations

Employers often collect sensitive personal data (for example information regarding health, religion or race) regarding their employees. In addition, personality profiles are also quite often established and maintained for the assessment of performance and career development. Under the amended SDPA, the employer will need to disclose to the employee which legal entity owns and controls such sensitive personal data, the purpose of the data processing and the categories of people having access to the data (eg HR managers, supervisors, etc). If the employer is required to collect sensitive personal data by law, no special disclosure is required.

It is recommendable for employers to limit the collection of sensitive personal data to the absolute minimum required for the conduct of the business in order to limit the administrative work necessary to comply with the additional disclosure requirements.

Explicit consent of employees

Until now, employers have mostly been able to rely on the provision that the purpose for which personal data (including sensitive personal data) is collected is apparent to the employees. However, under the amended SDPA, employers will need to obtain the explicit consent of each employee for the collection of sensitive personal data and the maintenance of personality profiles, which is only valid if the disclosure obligations are fully complied with, as outlined above under 'Consequences for employers: additional disclosure obligations'.

Employees need to be given the possibility to opt out of the data collection and processing process. However, any consequences (such as disadvantages) resulting from opting out need to be:

(1) reasonable; and
(2) disclosed to the employee.

Which sanctions for an opt-out are deemed adequate will be up to future court rulings to clarify.

Intra-group cross-border data transfers

Employees' consent to intra-group cross-border data transfers and cross-border data transfer agreements will remain an important element to enable intra-group cross-border data transfer. However, for international groups the most efficient way to enable such transfers will be to establish and maintain a data protection privacy policy complying with the requirements of the SDPA. With such policy, it will be possible to avoid concluding cross-border data transfer agreements with each group entity.

In the event of cross-border data transfers to countries not providing an appropriate level of data protection according to the SDPA, the Federal Commissioner for Data Protection will need to be informed of the content of cross-border data transfer agreements or the applicable group data protection and privacy policy.

Registration of databases

As the HR databases of employers normally contain sensitive personal data, or are disclosed to other group entities, employers will need to register the database with the Federal Commissioner for Data Protection under the amended SDPA.

Registration will not be required if the employer obtains a data protection quality assurance certification from a recognised, independent third party, or if it designates an internal data protection officer having the authority to independently monitor compliance with data protection rules and keep records of the data collection being maintained. Currently, the Federal Council has not established rules with regard to the certification process and its requirements. It seems that the appointment of an internal data protection officer will be the more efficient way to action compliance with the SDPA.

Appraisal

In general, the new requirements will be familiar to companies operating in the European Union, because they are derived from the EU Directive on Data Protection. Although some of the amendments to the SDPA will simplify compliance for employers in certain areas, such as intra-group cross-border data transfers, they also place additional compliance burdens on employers. Especially with regard to the collection and processing of sensitive personal data, employers will need to inform their employees in more detail and to obtain written consent from each employee. Moreover, it will become necessary to register HR databases with the federal data protection officer if no data protection quality assurance certificate has been obtained or if an internal data protection officer has not been appointed.

Recommendations to enhance employer attractiveness

An employer could use the necessary revision of its data protection policies and guidelines to highlight its pronounced willingness to comply not only with the statutory minimum standard but also with best practice standards. For instance, a launch of new or revised data protection policies may be used to promote the employer's data protection and privacy standards. The following could be considered:

- early launch in advance of coming into force of the amended SDPA;
- fast obtainment of data protection quality assurance certificate from one or even several of the most recognised providers;
- voluntary registration of database with a Swiss federal data protection officer;
- appointment of an independent data protection officer at top management level;
- restriction of access to sensitive data to a very small number of people;
- protection of all collected data by latest data encryption technology;
- limitation of collection of non-sensitive and sensitive personal data to the absolute minimum required for the conduct of the business;
- full information to each employee about data collected and reason for collection;
- provision of opt-out possibilities to the extent possible;
- granting easy access to data collection for data subjects (no administrative obstacles); and
- only internal processing of sensitive data (no outsourcing).

A company may announce the measures taken internally and externally with the help of marketing professionals with the clear aim of enhancing its reputation and, as a consequence, enhancing its attractiveness as an employer.