ABA International Employment Law Committee
American Bar Association - Section of International Law

Switzerland

Changes to the Swiss Federal Data Protection Act ("SDPA")

by Ueli Sommer, Dr.iur, LL.M.
Walder Wyss & Partners

Various amendments to the SDPA were adopted last year. The amendments create additional disclosure, registration and organizational obligations for employers, but they also simplify cross-border data transfers for international groups. In general, the new obligations are familiar to those companies operating in the EU because they are derived from the EU directive on data protection.

Background

The main objectives of the amendments are to make the subjects of data collection and processing aware of the purposes and uses of such data collection and processing, and to make the adjustments necessary to comply 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 individuals and legal entities. The protection of legal entities is a special feature of Swiss law and it creates difficulties in respect of cross-border data transfers because only a few other countries provide an equivalent level of protection. The amendments are expected to become effective on 1 July 2007 although the federal council has not set a final enactment date yet.

Consequences for Employers Additional disclosure obligations

Employers often collect sensitive personal data (e.g. information regarding health, religion or race) and establish and maintain personality profiles for the assessment of performance and career development. Under the amended SDPA, the employer will need to specifically 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 (e.g. HR managers, direct manager, 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.

Switzerland

Changes to the SDPA - Continued

Explicit consent of employees

Until now, employers could mostly rely on the statutory provision that the purpose for which personal data is collected must only be apparent to the employees. However, employers will now need to obtain the explicit consent of each employee for the collection of sensitive personal data and the maintenance of personality profiles. Employees need to be given the possibility to opt out from the collection and processing. However, any consequences (such as disadvantages) resulting from the opt-out need to be adequate and disclosed to the employee.

Intra-group cross-border data transfers

The consent of employees to intra-group cross-border data transfers and cross-border data transfer agreements will remain important elements to enable intra-group cross-border data transfer. However, the amended SDPA provides a new solution regarding international groups: cross-border transfers will be allowed if the group establishes and maintains a data protection and privacy policy in compliance with the SDPA.

In case 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 existing cross-border data transfer agreements and/or the applicable group data protection and privacy policy.

Registration of databases

As HR databases 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. A registration is not needed if the employer obtains a data protection quality assurance certification from a recognized service provider or designates an internal data protection officer who has the authority to independently oversee compliance with data protection rules and maintain records of all data collection.