

## Frequently Asked Questions by Category

### A. General

Question: Is personal data regarding legal entities (companies, associations, etc.) subject to the Swiss data protection laws and regulations?

Answer: Yes, unlike other jurisdictions, the Swiss data protection laws and regulations also apply to legal entities.

Question: Are IP addresses considered personal data under the Swiss data protection laws and regulations?

Answer: Yes, according to scholars and a not yet final decision dated 27th May 2009 of the Swiss Federal Administrative Court, a static or dynamic IP address is considered personal data, provided that the person who processes the IP address is either already aware of the identity of the person using such address or can reasonably be expected to make the necessary efforts to identify that person. The court held that the processing of dynamic IP addresses by a supplier based in Switzerland (the supplier was extracting the dynamic IP addresses of persons uploading copyright-protected works to P2P networks and forwarding the IP addresses to the relevant rights holders in order to allow them to identify the persons using the IP addresses by filing criminal complaints against “unknown” persons) is subject to Swiss data protection laws and regulations. This decision has been appealed to the Swiss Supreme Court and pending its decision the issue of whether IP addresses are protected personal data under the under the Swiss data protection laws and regulations remains unsettled.

### B. Transfer abroad

Question: May we freely and without restrictions transfer personal data from Switzerland to a foreign country or provide access to personal data to persons in a foreign country?

Answer: No. If the legislation of the foreign country does not afford adequate protection for the personal data to be transferred or accessed, under Swiss data protection laws and regulations, transfer or access outside Switzerland is allowed only if certain specific requirements with respect to such disclosure abroad are met.

Question: We intend to transfer personal data from Switzerland to Germany (or to provide access to personal data to persons in Germany). We assume that such transfer or access is possible without meeting any specific requirements under the Swiss data protection laws and regulations because Germany’s legislation provides for adequate protection of personal data. Is this assumption correct?

Answer: It depends on whether the personal data transferred or accessed pertains to natural persons or legal entities. If the transfer or access only pertains to natural persons, a transfer from Switzerland to Germany or access in Germany is not subject to specific requirements under Swiss data protection laws and regulations.

However, if the transfer or access includes personal data concerning legal entities, specific requirements under the Swiss data protection laws and regulations with respect to such transfer or access need to be met unless certain exceptions apply. Compliance with these requirements must be assured before the transfer or access takes place.

Question: We intend to transfer personal data from Switzerland to the U.S.A. (or to make personal data accessible to persons in the U.S.A.) The company receiving the personal data in the U.S.A. has certified its adherence to the **EU-U.S. Safe Harbor Principles**. Do we have to take any specific measures, in particular notify the transfer or access to the Swiss Federal Data Protection and Information Commissioner before it takes place?

Answer: Yes, unless the recipient in the U.S.A. has certified its adherence to the **U.S.-Swiss Safe Harbor Principles** or certain exceptions apply, the data exporter and the recipient in the U.S.A. need to enter into a cross-border data transfer agreement to provide for an adequate protection and the agreement must be notified to the Swiss Federal Data Protection and Information Commissioner before the first transfer or access occurs.

It however needs to be noted that the U.S.-Swiss Safe Harbor Framework is limited in scope since it covers only the transfer of personal data concerning natural persons (and not legal entities). In addition, certain types of data or methods of data processing might not be included in a particular certification. Therefore, even if a recipient has given a certification under the U.S.-Swiss Safe Harbor Framework, it is important to ensure that the personal data to be transferred and processing methods are actually covered by the certification. If the data or processing methods are not covered and unless other exceptions apply, it is still necessary to enter into a specific cross-border transfer agreement and inform the Federal Data Protection and Information Commissioner before the transfer is made or access to the data is provided.

### **C. Registration of data files with the Swiss Federal Data Protection and Information Commissioner**

Question: As an employer, we regularly process personal data relating to our employees (name, occupation, salary, health, appraisals, etc.) in Switzerland. Do we have to register such processing with the Swiss Federal Data Protection and Information Commissioner if we have not either designated an internal data protection officer or acquired a data protection quality mark?

Answer: Unless you process the data in terms of a statutory obligation, registration is necessary if the personal data of the employees includes personality profiles or sensitive personal data. In general, employee data contains sensitive personal data (such as, for example: information about health, trade union beliefs, etc.). Often employee data also may constitute personality profiles because the data might reveal essential characteristics of employees.

In many cases, the processing of sensitive personal data and of personality profiles of employees is based on a statutory obligation of the employer (e.g. the obligation to provide a certification of employment; process certain health data to meet social security requirements, etc.). However, this might not always be the case. For example, if more than objectively necessary information about employees is processed and such information is shared with

other group companies, this would go beyond merely meeting statutory requirements and the prior registration of the data file with the Swiss Federal Data Protection and Information Commissioner would be required.

**D. Data Access and disclosure within a Group of Companies**

Question: Our company is a Swiss subsidiary/branch of a multinational corporate group. Our parent company's headquarters in Norway intends to centralize the human resources data file of the whole group in Norway. Are there any restrictions applicable to such centralization?

Answer: Yes. The intended centralization involves a disclosure and transfer of personal data abroad which is – even within the same group of companies – only permitted under certain circumstances (see section B above). Further, under Swiss employment law, the employer may only collect and process data about employees which are necessary for the performance of the employment relationship. As files of human resources data often contain sensitive personal data or personality profiles, the employees must give explicit consent to the transfer of their data abroad. Additionally, a registration of the data file with the Swiss Data Protection and Information Commissioner might be necessary (see section C above).