The Impact of the Revision of the Swiss Federal Act on Data Protection on Employment Law - The Most Important Questions and Answers

---

On 1 September 2023, the revised Swiss Federal Act on Data Protection (**FADP**) will enter into force. The FADP regulates various new obligations for companies with regard to data processing and also provides for stricter sanctions in the event of breaches of obligations. To what extent the revised FADP will also affect the handling of job applicants' and employees' data is explained below in the form of a brief overview (without claim to completeness). For general information on the revision of the FADP, please refer to the other articles published by MLL Legal (in particular FADP Revision: FAQ Part 1 and FADP Revision: FAQ Part 2).

1. Which changes in data protection law have an impact on employment law?

As of 1 September 2023, a ***formal duty to inform*** will be introduced for all data processing. Companies that process personal data must adequately inform the persons concerned about the acquisition and processing of the corresponding personal data (cf. Art. 19 FADP). This duty to inform includes the disclosure of the identity and contact details of the data controller (i.e., the employer), the purpose of the processing and the recipients or categories of recipients to whom personal data are disclosed. In addition, the revised FADP stipulates which duties to inform exist for companies in the case of cross-border data transfer and acquisition of personal data that is not obtained from the persons concerned/data subject.

Furthermore, from 1 September 2023, companies are obliged to keep a ***register of processing activities*** (cf. Art. 12 FADP). This register must record all of the company's data processing activities, whereby precise information must be provided on the purpose of the processing, the categories of personal data processed, and the persons concerned, as well as the retention period for the personal data. Companies are exempted from the obligation to keep a corresponding register only if they employ fewer than 250 employees as of 1 January of the year in question and also neither "process personal data requiring special protection on a large scale" nor "carry out high-risk profiling" (cf. Art. 24 of the new Ordinance to the Federal Act on Data Protection, ***DPO***). Whether the conditions for exemption from the obligation to keep a register of processing activities are met must be determined on a case-by-case basis through careful examination of the actual circumstances of the individual case.

The introduction of both, the formal duty to inform and the newly applicable duty to keep a register of processing activities mean that ***employers*** must ***firstly*** become aware of which personal data they process in connection with job advertisements and employment relationships, so that they can ***secondly*** fulfil their duty to inform the persons concerned to the extent determined by law.

2. How can these new data protection obligations be implemented in practice from an HR perspective?

Before a company can fulfil its legal duty to inform (former) employees and job applicants, it must **firstly** determine which personal data of employees and job applicants are processed and to what extent. This is done by creating a ***register of processing activities***. Even if a company is not legally obliged to do so, it is still advisable to create such a register. In this case, the register can be limited, in the sense of a minimum scope, to the information that must be provided anyway in accordance with the formal duty to inform (Art. 19 FADP). Only if a company knows what personal data is being processed in the first place, it is able to provide information on the acquisition and processing of personal data to the extent determined by law.

If a company has already initiated a project to create a register of processing activities, it is advisable to also involve HR. In this case, HR must check to what extent personal data is being processed in connection with job advertisements and existing as well as former employment relationships. Subsequently, the corresponding data processing procedures must be recorded in the register of processing activities in accordance with the legal requirements.

Based on the register of processing activities, HR must then draw up a ***data privacy policy for employees*** in a ***second step***, which fulfils the company's formal duty to inform. With the data privacy policy for employees, the company informs employees (as well as job applicants, if applicable) about the following among other things, (i) what personal data is being processed and for what purpose, (ii) to whom personal data is disclosed and (iii) to what extent personal data is also disclosed across borders (cross-border data transfer). When drawing up the data privacy policy for employees, it must be determined whether there is an exemption from the duty to inform pursuant to Art. 20 FADP for specific data processing or information (e.g., if the data processing is required by law). However, according to the will of the legislator, exceptions are to be handled restrictively, i.e., in case of doubt, information is to be provided.

In respect to job applicants, it regularly makes sense to integrate the duty to inform directly into the company's general data privacy policy. Depending on the specific implementation, it may no longer be necessary to inform job applicants in the data privacy policy for employees, as this is done directly through the general data privacy policy, e.g., on the company's website.

3. What form does the data privacy policy for employees need to take and what should HR pay attention to?

For reasons of evidence, the data privacy policy for employees should be ***in writing*** and ***made accessible*** to the employees ***before*** any data processing is to take place. Making it accessible means that the company must ensure that the persons concerned have the ***opportunity to take note*** of the corresponding data privacy policy. It is therefore not necessary for the persons concerned by the data processing to actually take note of the data privacy policy for employees.

Since the individual scope of the company's formal duty to inform can always change, it is advisable to issue the data privacy policy for employees in a ***separate document*** and thus ***detached from the employment agreements***. In this way, the company ensures the greatest possible flexibility with regard to the content of the data privacy policy for employees and can, if necessary, unilaterally amend it at any time. Of course, this also requires HR to ***constantly and repeatedly review*** to what extent data processing with regard to employees (and job applicants, if applicable) has changed within the company, so that the actual circumstances can also be reflected in the data privacy policy for employees.

4. What should be considered with regard to existing employment agreements and regulations due to the revised FADP?

In existing employment agreement templates, personnel regulations and employer instructions, companies should check whether the data protection provisions contained therein are compliant with the revised FADP or whether the aforementioned documents may need to be amended.