PESTALOZZI

ATTORNEYS AT LAW

100 years 1911 2011

Data Mapping

MAIN QUESTION

Where does our company use **What** kind of data in **Which** manner and by **Which** means for **Which** purpose and by **Whom**?

SPECIFIC QUESTIONS

The data mapping of personal data collected and/or processed in Switzerland should provide answers to at least the following questions:

- Whose personal data does your company collect and/or process?
- Which categories of personal data does your company collect and/or process? Do they contain sensitive personal data?
- Which data processing is performed and by whom, i.e. by your company itself or by a third party acting for your company?
- What are the purposes of the processing?
- Are the data processed for other purposes than those for which they have been originally collected?
- Who has access to personal data stored, be it within your company, within the group of companies, or third parties?
- To which countries does your company transfer personal data? Are they located outside the EU/EEA?
- Which IT resources, such as software or applications, does your company use in its contacts both with employees and customers and what personal data do they collect?
- Does your company generate own databases containing personal data?
- Does your company conduct profiling activities?
- Do foreign group companies access personal data collected and/or processed by your company?
- Does your company access foreign databases containing personal data from Switzerland?
- Are there internal (group) policies covering the data processing actions, such as data privacy policies, general terms and conditions, IT policies for employees, cookies policy, etc.?
- Does your company use means of mass-communication, such as newsletters? If so, what is their set-up regarding opting-in/sign-out procedure?

PROVIDING ANSWERS

The following tasks, duties and responsibilities (inter alia) depend on a comprehensive (correct) data mapping:

- General assessment of current compliance level
- Assessment of measures to be taken in order to improve insufficient compliance level
- Assessment of measures to be taken in order to ensure compliance with new laws
- Granting of the individual's right to information/right of access by the data controller (art. 23 D-FADP; art. 15 GDPR)
- Comply with an individual's request for deletion or correction of data (art. 28 D-FADP; art. 16 et seq. GDPR)
- Maintaining data controller's and data processor's inventories of processing activities (art. 11 D-FADP; art. 30 GDPR)
- Comply with the data controller's duty of information upon data collection (art. 17 D-FADP; art. 13 et seq. GDPR)
- Performance of a Data Privacy Impact Assessment by a data controller (art. 20 D-FADP; art. 35 GDPR)
- Management of data breaches and cybercrimes by data controllers and data processors as well as respective notification obligations (art. 22 D-FADP; art. 33 et seq. GDPR)