ATTORNEYS AT LAW

SCHELLENBERG WITTMER

SEPTEMBER 2015

Newsletter

Author:
Roland Mathys

INFORMATION TECHNOLOGY / DATA PROTECTION

Increasing Importance of Data Protection Compliance – a Practical Guide for Compliance Programs

In recent years, the relevance of questions and issues related to data protection laws has increased significantly. Accordingly, companies pay more attention to data protection compliance. However, many companies find the introduction of compliance programs difficult – a practical guide on how to proceed can be of help.

1 INTRODUCTION

The **relevance of data protection** has increased significantly in recent years: Not long ago, data protection enjoyed no more than a shadowy existence, whereas today questions and issues related to data protection law are prominently discussed.

This development can be traced back to various **causes**: The establishment of new technologies strongly connected to personal data (e.g. social networks, portable devices such as fitness trackers or big data analysis); the authorities' and courts' increased focus on data protection (e.g. decisions regarding Google Street View in Switzerland or the „right to be forgotten" in the European Union); individual incidents, in which data protection took the centre stage, were widely echoed in the media (e.g. the „NSA-affair").

This trend will persist in the future. In any case, the **legislative efforts** in the European Union regarding the soon to be finalized draft for a General Data Protection Regulation as well as corresponding revisions in Swiss data protection law point in that direction. For example, under the new EU Regulation, non-compliant companies can be sanctioned with penalties up to 5% of their worldwide yearly turnover or (if higher) up to EUR 100 million.

Accordingly, **data protection compliance** has become more important for companies: A few years ago compliance with data protection laws was primarily considered obstructive to business and costly. Today, it is a central pillar of corporate compliance. Compliance with the applicable legal and regulatory provisions is no longer an end in itself, but often intends to award the company a

„seal of approval" with regard to data protection, which can be used proactively for reputation purposes and as a selling point.

"Until recently, data protection was primarily considered obstructive to business and costly. Today, it is a central pillar of compliance."

For many companies, data protection compliance is legal new ground. Accordingly, they tend to have difficulties with the **development and the introduction of adequate compliance programs**. Questions arise with regard to how to structure such a program, where to begin, where the need for action is most urgent, or what must be considered within a global corporation or in general in an international environment. This newsletter aims to answer these and further questions and to provide an action plan for data protection compliance programs.

2 INITIAL ASSESSMENT

A compliance program begins with the establishment of the **current situation with regard to data protection**. On one hand, a company must analyze which personal data is actually being processed; on the other hand, the data protection instruments (e.g. regulations, processes, structures) already existing within the company must be identified.

2.1 DATA-RELATED ANALYSIS

Firstly, it must be determined **which personal data** is collected and processed within the company. Typical categories of personal data are employee, customer or supplier data. In this context it must be considered that certain countries (such as Switzerland) not only protect data related to individuals, but also to legal entities. The data must be reviewed in order to determine whether it includes sensitive personal data (such as health-related data) or personality profiles to which higher protective requirements apply. The data must also be examined in order to determine whether an anonymization or pseudonymization takes place, to which data protection laws do not apply, and if so in which stages of processing these measures are taken.

For any data collection, the question arises whether the company acts as the **owner of the data collection** ("controller") or merely processes the data on behalf of a third party ("processor"). The company must examine which data processing activities were transferred to a third party (e.g. in the context of outsourcing). Similarly, it must be determined for every data collection if it is registered with the Federal Data Protection and Information Commissioner ("**FDPIC**").

The **assessment of the processing purposes and activities** is of central importance. Due to the principle of purpose limitation in data protection law, personal data can only be processed for purposes which have been communicated to the individual or are apparent to him or her. The processing activities can be identified based on the data's lifecycle from collection to evaluation, use, modification, storage, publication, retention up to deletion. It is advisable to analyze the typical processing scenarios of the specific corporate units more closely (in the HR division e.g. job applications, qualifications, absence management, private internet and email use, employee evaluation, resignation).

Data security constitutes an important component of data protection and must be included in the analysis. Personal data is regularly classified based on confidentiality and protected from alterations or unauthorized access by technical (e.g. encryption) or organizational (e.g. access restrictions) measures.

In the globalized economic environment, data traffic is hardly ever limited to Switzerland. **Cross-border data flows** are the rule, in particular for internationally active corporations. The different data protection levels under different legal systems require an examination with regard to the countries in which personal data is stored, from which destinations it is accessible and which data is transferred between which countries within and outside the corporation.

"Cross-border data flows are the rule, in particular for internationally active corporations."

2.2 COMPANY-RELATED ANALYSIS

From an **organizational point of view**, the question arises whether the company has appointed an internal data protection officer, which might not be a legal requirement but can lead to certain administrative relief. Furthermore, it must be clarified which divisions within the company are responsible for data protection (e.g. the legal department, compliance, HR, IT).

With regard to existing instruments, an inventory of all **relevant documents** in the area of data protection should be compiled. This includes guidelines (e.g. in HR or IT), regulations for data collections, contractual agreements (e.g. in the context of delegated data processing or data transfer), declarations of consent or corporate data protection rules ("Binding Corporate Rules").

Finally, the company's internal **processes** should be assessed: Which quality control measures have been taken (e.g. audits, certifications), how are incidents related to data protection laws processed (e.g. reporting on data leaks, information or rectification requests), which efforts are made with regard to formation (e.g. internal or external training)?

3 IDENTIFICATION, PRIORITIZATION AND CORRECTION OF TYPICAL PROBLEM AREAS

As a next step, the established current situation must be compared with a **fully compliant situation** and problem areas requiring action with regard to data protection laws must be identified and sorted based on priority.

3.1 IDENTIFICATION OF TYPICAL PROBLEM AREAS

The areas requiring action with regard to data protection laws depend on the assessment in each individual case. Based on general experience, the **following business functions** can be classified **as sensitive**:

> **IT**: In a company's IT department, gaps in data protection often arise when the individual services are centralized internally or outsourced to an external provider. This is

accentuated when data is transferred to the cloud, where the company no longer knows (yet alone can influence) in which country the data is ultimately stored. Regularly, action is required in the area of IT security (e.g. lack of staggered authorizations for data access).

- **HR**: The HR department often processes and stores sensitive data (e.g. health-related data connected to illnesses or accidents) or personality profiles (e.g. application dossiers with references, assessments). Accordingly, the requirements for data protection conformity are higher. Common problem areas include the recruiting process (e.g. the retention of personal files of rejected applicants), the regulations regarding the utilization of the company's infrastructure (internet, email) for private purposes or the use of private infrastructure for work purposes ("Bring Your Own Device"), the question of the permissibility of employee surveillance as well as the processing of employee data following resignations or during absences.

- **Marketing / Sales**: In marketing and sales, comprehensive data processing is carried out, e.g. for the purpose of evaluating personal data and clustering or for direct marketing activities. This can be taxing on principles such as transparence (Does the individual know what his or her data is used for?), purpose limitation (Is a processing purpose legitimate?) and proportionality (Is only as much data processed as necessary?).

- **Records Management**: Data retention is data protection compliance's stepchild. Often there are no clear regulations regarding data archiving (e.g. term, form), or incorrect requirements are assumed (e.g. observance only of the retention duties pursuant to commercial law).

- **Communication**: The term communication includes all the company's activities related to offline and online media, in particular websites, social networks, posts and blogs. Data protection policies are now common on websites, however they are often merely adopted from other sources and are therefore not adjusted to the company's specific online presence.

"The areas requiring action with regard to data protection laws depend on the assessment of each individual case."

Further areas requiring an advanced assessment are determined based on the company's specific industry and business sectors (e.g. data sensitivity in the health sector, comprehensive data mining in the retail industry).

3.2 PRIORITIZATION OF ACTIVITIES

The potential variety of areas requiring action does often not allow for parallel implementation. In order to group resources, the individual deficits should be **eliminated gradually**, leading to the question of prioritization.

In order to prioritize the measures it is advisable to use a **risk matrix** with the central criteria of the probability of a data protection breach and the consequences of a breach (e.g. number of affected persons, gravity of the breach, negative publicity and possible reputational damages, risk of claims under civil law, FDPIC administrative proceedings or even criminal sanctions).

The ranking can be influenced by **additional factors**, such as the opportunity to integrate specific measures into ongoing or imminent projects or the option to implement workaround solutions.

Under the aspect of prioritization, international corporations must decide how to ensure **compliance in a vast number of countries**. In this situation, the gradual approach, according to which implementation is initiated in one country (often at the corporation's headquarter or in its most important market) and then extended to further countries (by involving local internal legal departments or external advisors), has prevailed.

3.3 IMPLEMENTATION OF MEASURES

There is no general answer as to which measures should be implemented in the individual case in order to achieve data protection compliance. The **spectrum of possible measures** is very broad and primarily consists of the following elements:

- Complete **termination or adjustment** of non-conform data processing;
- **Information** of the affected persons, possibly coupled with obtaining their consent for specific processing;
- Establishment or amendment of **contractual provisions, guidelines or processing regulations**;
- **Registration** of data collections with the FDPIC;
- Organizational measures such as the appointment of an **internal data protection officer**;
- Establishment or adjustment of the documentation of the required **processes**;
- Internal and external **information and communication**;
- **Training and auditing**.

4 CLOSING REMARKS

The above demonstrates that data protection has become an **important element of corporate compliance**. Compliance programs contribute to ensuring conformity with the applicable laws and to awarding the company a good rating regarding data protection.

In order for a compliance program to achieve the pursued objective, it must be prudently planned and from the outset accompanied legally as well as by the required **management attention**.

Contacts

The content of this Newsletter does not constitute legal or tax advice and may not be relied upon as such. Should you seek advice with regard to your specific circumstances, please contact your Schellenberg Wittmer liaison or any of the following persons:

In Zurich:

Roland Mathys
Partner
roland.mathys@swlegal.ch

Andrea Mondini
Partner
andrea.mondini@swlegal.ch

In Geneva:

Philippe Ducor
Partner
philippe.ducor@swlegal.ch

Virginie A. Rodieux
Associate
virginie.rodieux@swlegal.ch

SCHELLENBERG WITTMER LTD / Attorneys at Law

ZURICH / Löwenstrasse 19 / P. O. Box 1876 / 8021 Zurich / Switzerland / T +41 44 215 5252
GENEVA / 15bis, rue des Alpes / P. O. Box 2088 / 1211 Geneva 1 / Switzerland / T +41 22 707 8000
SINGAPORE / Schellenberg Wittmer Pte Ltd / 6 Battery Road, #37-02 / Singapore 049909 / www.swlegal.sg

www.swlegal.ch