Reichlin Hess
Rechtsanwälte
Steuerberater
Notare

Reichlin Hess AG
Hofstrasse 1a
6300 Zug
Schweiz

T + 41 (0) 41 729 10 70
F + 41 (0) 41 729 10 80
law@reichlinhess.ch
www.reichlinhess.ch

CHE-138.478.936 MWST
Eingetragen im
Anwaltsregister des
Kantons Zug

Data Protection:
Threatening EU Law: Swiss Companies Forced to Take Action

Well known: As of 25 May 2018 the European General Data Protection Regulation will become directly applicable in all EU member states. What you may not be aware of: The said Regulation will also apply to numerous Swiss companies. And breaches may be vigorously sanctioned.

1. Scope (Art. 3 GDPR)

According to Art. 3 of the EU General Data Protection Regulation (GDPR), such regulation will in particular apply to Swiss companies that process personal data of natural persons located in the EU if the Swiss company in question (i) is offering goods or services to such EU located data subjects, whether against payment or free of charge (e.g., through a national website on which the prices are not only listed in Swiss Francs or which includes delivery and payment terms for customers in the EU), or (ii) is processing data to monitor the behaviour of data subjects in the EU (e.g. analysis of the online surfing behaviour of EU citizens for marketing purposes). Swiss companies are well advised to check if and to what extent these new rules also apply to them. We would like to highlight in particular the following obligations Swiss companies may have to comply with going forward:

2. Obligation to Designate a Representative in the EU (Art. 27 GDPR)

Swiss companies within the scope of the GDPR are generally required to designate a representative in the EU. This obligation does not apply if data processing (i) takes place only occasionally, (ii) does not include special categories of data and (iii) is unlikely to result in a risk to the rights and freedoms of indiviudals.

3. Obligation to Keep Records (Art. 30 GDPR)

The obligation to keep records of all data processing activities will create substantial additional work. It will mean compiling a summary of every single data processing activity carried out by the company which will often be a cumbersome process.

4. Consent: Stringent Requirements (Art. 4 Para. 11 and 7 GDPR)

Consent must be given by an unambiguous, active action and the recipient must be able to provide evidence that such consent has been given. Checkboxes pre-populated with a tick may not be considered a declaration of consent. Declarations of consent contained in documents such as privacy policies must be displayed separately from the rest of the content. Furthermore, there is a limited restriction on tying arrangments: the conclusion of a contract may not be made conditional on the consent to processing of data that is not required for the performance of the contract in question.

Consents may be withdrawn at any time. The process for withdrawing consent must be just as easy as the process for giving consent.

5. Comprehensive Obligations to Provide Information at the Time Data is Acquired (Art. 13 et seq. GDPR)

Art. 13 and 14 GDPR stipulate comprehensive obligations to actively provide information at the time the data is acquired; in principle these obligations apply even if the data is not collected from the data subject. Going forward, whenever data is purchased from address dealers the data subjects will have to be informed.

The same obligations to inform will also apply in the event of any subsequent changes to the original purpose for which the data is collected.

6. Rights in Case of Automated Data Processing (Art. 22 GDPR)

The data subjects have the right not to be subject to automated decision-making processes if such decisions could have legal effects on them or be of similar significance. This does not apply if the automated decision-making process is necessary for the conclusion or performance of a contract, or if it is permitted by law, or if the data subject has given his/her express consent.

Consequently, the data subjects must be informed of any such automated processing of their data, and they have the right to access any data being processed this way.

7. Right to Data Portability (Art. 20 GDPR)

Where data is processed by means of automated processes based on a consent or a contract, the data subjects may request to receive their own personal data which they have provided to a data controller, in a structured, commonly used and machine-readable format.

8. Right to Erasure (Art. 17 GDPR)

In principle, the data subjects may at any time request that their personal data be erased. This right does not apply if the data processing is necessary for purposes of asserting legal claims or compliance with EU legislation.

If personal data acquired is disclosed to third parties, such third parties must also be informed of any requests for erasure, provided that such third party information does not involve a disproportionate effort.

9. Data Privacy by Design, and Data Privacy by Default (Art. 25 GDPR)

“Privacy by Design” and “Privacy by Default” are two catchphrases of the GDPR:

“Privacy by Design” means that data controllers must take into account the aspects of data protection law already when designing the data processing structure.

The principle of “Privacy by Default” requires that data controllers put in place suitable measures to ensure that, as a default, personal data is only collected if and to the extent such collection is necessary for the processing purpose in question.

10. Data Protection Impact Assessment (Art. 35 et seq. GDPR)

Art. 35 GDPR requires the performance of a “Data Protection Impact Assessment” if the data processing entails high risks to rights and freedoms of individuals due to its type, scope, context and purpose, and especially if the processing involves the use of new technologies or processing of a large scale of special categories of data. The assessment must include, as a minimum, a systematic description of the data processing operations, an assessment of the necessity and proportionality of the data processing, an assessment of the risks for the data subjects and an overview of the measures undertaken to reduce these risks.

If the result of this assessment indicates that the data processing, without any measures, constitutes a high risk, the supervisory authority must be consulted prior to the data processing.

11. Obligation to Notify Data Protection Breaches (Art. 33 et seq. GDPR)

Going forward, all personal data breaches must be documented and reported to the supervisory authority without delay, if possible within 72 hours. This reporting obligation does not apply if the breach does not represent any foreseeable risk with respect to the rights and freedoms of the data subjects. In many cases, the data subjects must be notified as well.

12. Internal Data Protection Officer (Art. 37 et seq. GDPR)

Going forward, certain data processors will be obliged to appoint an internal data protection officer. This will be compulsory if the data processor’s main activity involves extensive, regular and systematic monitoring of people, or if a large amount of particularly sensitive data is being processed.

13. Breaches Punished with Extremely Severe Penalties (Art. 83 GDPR)

Breaches of the GDPR may be punished with extremely severe penalties. For certain breaches, the regulation stipulates a fine of up to 20 million Euros, or up to 4 percent of a company’s worldwide annual turnover.

14. Implementation / Required Action

The implementation of this regulation requires substantial efforts: first of all, companies must gain a reliable overview of all their data processing operations, and use this as the basis for a gap analysis. They must then formulate implementation strategies and responsibilities, adapt internal processes where necessary, implement internal auditing, draw up guidelines, amend privacy policies and contracts with customers, suppliers, etc., generate reporting forms and other templates, obtain consents and, where necessary, carry out internal training.

We are confident, however, that by tackling these legal issues together with you we will be able to minimize the actions required on your end to comply with the new law. We would be pleased to help you determine your legal needs and obligations. If you have any questions or would like to receive further information, please do not hesitate to contact us.

The content of this article does not constitute legal or tax advice, and may not be used as such. If you wish to obtain advice regarding particular circumstances, please get in touch with your contact person at Reichlin Hess or with the authors of this newsletter.

Version of 29 September 2017

Andrea Hauser, LL.M. – andrea.hauser@reichlinhess.ch
Matthias Lerch, LL.M. – matthias.lerch@reichlinhess.ch

Reichlin Hess
Attorneys at Law
Tax Advisors
Notaries

Reichlin Hess AG
Hofstrasse 1a
6300 Zug
Schweiz
T +41 (0)41 729 10 70
F +41 (0)41 729 10 80
www.reichlinhess.ch