STSA SWISS TRADING & SHIPPING ASSOCIATION

N° 9

STSA INSIGHT

May 2018

General Data Protection Regulation for Swiss-based commodity trading firms

The EU's General Data Protection regulation (GDPR) will enter into force on 25 May 2018. Swiss-based companies holding data on EU nationals will have to comply.

Introduction to GDPR

The primary objective of the GDPR is to give citizens back control of their personal data. From an economic standpoint, the GDPR aims to simplify the regulatory environment for international business by unifying the regulation within the EU.

It imposes new rules on companies, government agencies, non-profits, and other organizations that offer goods and services to people in the EU, or that collect and analyze data tied to EU residents. Even organizations outside Europe need to be compliant, or otherwise face significant penalties. At the most basic level this requires organisations to determine the legal basis under which data is collected and, if not included in employment and contractual relationships, to collect consent from individuals for the holding and use of their personal data.

GDPR confers individuals the following rights:

- to be informed,
- to access,
- to rectification,
- to erasure,
- to restrict processing,
- to data portability,
- to object, and
- rights in relation to automated decision making and profiling.

Swiss position

Switzerland is required to adopt into its national law rules to the same effect as GDPR as these have a bearing on the Schengen agreements.

Switzerland is updating its national data protection rules that date back to 1992. A new federal legislative proposal (P-LPD) was approved by the Federal Council on 15 September 2017 and is currently going through Parliament. The Law is expected to enter into force in 2019 and should not only align Swiss rules with GDPR but also offer a brand new framework for data protection in Switzerland.

Timeline

Because the GDPR is a regulation and not a directive, it means that it is directly applicable in all EU member states from May 2018.

With the GDPR set to come into force on **25 May**, many companies face a race against time to achieve compliance. Many tasks are likely to be time-consuming, so firms need to make sure they are allocating the right resources and time to those activities. **Past 25 May, should full compliance not have been reached, companies should be in a position to show that GDPR implementation is under way.**

Main steps to be undertaken at corporate level

GDPR implementation can be broken down in 4 key steps:

1. Nomination of a **Data Protection Officer**.
2. **Awareness raising** and data protection infosessions and trainings for staff should be organised.
3. **Assessment** of data and data systems, including security aspects, and creation of data registries.
4. GDPR **data compliance mechanisms** –in particular consent recording- and policies such as "privacy notices".
5. **Documentation** of GDPR compliance and internal processes.

Companies should do an inventory of data held and cleanse this data, keeping only compliant data (i.e. contractual or for which consent has been recorded). This holds true for existing data and for new and on-going data.

Updated data policies and procedures need to be put in place or reviewed in accordance to GDPR. Companies shall categorise data based on the level of risk and secure it accordingly.

The Data Protection Officer is ultimately responsible for implementing the appropriate technical and organisational measures.

A **systematic approach** would require:

1. Listing the processing of personal data, the data processed (e.g.: contracts) and the media on which they rely.
2. Assessing the risks caused by each processing by:

- identifying the potential effects on the rights and freedoms of individuals concerned, the sources of risks (who or what could be the cause of each feared event?) and the possible threats (what could allow each feared event to occur?);
- Determining the existing or planned measures which allow for each risk to be dealt with (e.g.: controlling access, back-ups, traceability, security of the premises, encryption…).
- Evaluating the severity and likelihood of the risks, with regard to the previous elements (for example regarding a scale: negligible, moderate, significant, maximal).

3. Implementing and checking the planned measures.
4. Carrying out periodical security audits.

Links to useful resources

- CNIL security of personal data management guide (in EN)
- UK Information Commission 12-step Guide to GDPR (in EN)
- Swiss draft Bill on Data Protection ("avant-projet", in FR)
- Swiss Confederation – Press release of 13 April 2018 (in FR)
- FER online course Découvrir la protection des données (in FR)
- STSA member SGS also offers a "GDPROnline" app for SMEs.

STSA
Rue de Chantepoulet 11
P.O. Box 1565
1201 Geneva
Switzerland

Tel. +41 22 715 29 90
info@stsaswiss.ch

WWW.STSA.SWISS