THE GENERAL DATA PROTECTION REGULATION (GDPR)

WHAT YOU NEED TO KNOW FOR DOING BUSINESS WITH EUROPEAN COUNTRIES

WWW.SGS.COM

SGS

1 INTRODUCTION OF GDPR

The General Data Protection Regulation (GDPR) was published in the Official Journal of the European Union on 27 April 2016. After a probation period of two year, it shall apply on 25 May 2018[1]

GDPR differs from its predecessor, the Data Protection Directive 95/46/EC, in the way that it is a regulation. It means it is directly applying to all Member Bodies without transposition[2], hence shortening the implementation time and ensuring implementation consistency.

If your company is unable to compile with GDPR before 25 May 2018, it may face administrative fines of up to 4% of global turnover or €20m, whichever is higher.

The aim of GDPR is to:

- recognize protection of personal data as human rights
- define the principles and rules of the protection
- harmonize the protection in member states and allow free movement of personal data within

It is consisted of:

- organizational requirements (EU representative office, data protection officer, consent record retention, contract requirements, etc.)
- Seven data rights for individual
- certification scheme
- member states supervision
- EU Data Protection Board establishment
- other legal procedures

2 SEVEN DATA RIGHTS FOR INDIVIDUAL

The core content of the GDPR is to establish seven rights of an individual regarding the processing of his personal data. Any organization who are in processing of these data would need to ensure these rights are protected.

Processing is defined in the GDPR as any automatic or manual operations, such as collection, recording, organization, structuring, storage, adaption or alternation, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

DATA RIGHT	DESCRIPTION	EXAMPLES
Right of access	Allow an individual to request a copy of his personal information.	A bank customer has the right to request a copy of his personal data record, including address, phone, etc.
Right to rectification	Allow an individual to correct his personal information.	A broadband customer has the right to request the information held by the ISP so that he could update his contact number.
Right to erasure	Allow an individual to remove his personal information.	A beauty shop customer has the right to request his information be removed after he no longer is a member or customer of the shop so that he would not be called for latest promotion.
Right to restrict of processing	Allow an individual to prohibit his personal information from processing, except retention for legal purpose or similar.	An architect has the right to request his previous employer not to include his CV in bidding of tenders, but maintaining his name in historical won tenders is allowed, to keep track of legal accountability.
Right to data portability	Allow an individual to migrate his personal information from one party to another.	An insurance customer has the right to request his profile to be migrated to another insurance company. If there exist a common electronic format for the industry, the insurance company shall also provide the record in that common electronic format.
Right to object	Allow an individual to object for direct marketing or similar.	A marketing company using email to promote business shall provide an "unsubscribe" link.
Right not to be subject to automated individual decision-making, include profiling	Prohibit the controller or processor from assessing any individuals by automatic means without explicit consent.	A social networking company shall seek explicit consent from end users before performing behavior analysis to deliver targeted advertisements.

[1] *Article 99, EU GDPR, http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf*

[2] *Transposition requires each Member Body to adopt the Directive and transform its requirements into the Member Body's own regulation. As a result, additional implementation time and different interpretations of the Directive may occur.*

3 DOES GDPR MATTER TO YOUR BUSINESS

IF YOUR BUSINESS:		
CONDUCT BUSINESS IN EU	SELL PRODUCTS OR SERVICES TO EU	DESIGN PRODUCTS FOR EU MARKETS
HAVE OR PROCESS CONSUMER DATA OF BOTH EU CITIZENS AND NON-CITIZENS WHO IS INSIDE EU	CONDUCT MARKET RESEARCH USING PERSONAL DATA FROM EU	ETC.

YOUR BUSINESS IS LIKELY TO BE WITHIN THE SCOPE OF GDPR

Remarks: GDPR applies to any individual in European Union, regardless of his nationality or citizenships. And it applies to any related activities or transactions, regardless of the processing or store location.

4 A SAMPLE CASE STUDY

Assuming a Hong Kong retailer offering tailor-made designer-cloths in a shop in UK, and its customers could also join their membership scheme through its shop's website. The server of the website locates in Hong Kong.

Under GDPR, the personal data of the shop's customers (name, address, body size, etc.) should be stored within EU, and their website should be hosted in an EU server by default, unless the shop receives approval from UK Information Commissioner's Office, UK's authoritative body to enforce GDPR, as well as all appropriate safeguard stipulated in the GDPR shall be implemented.

Furthermore, if in the future, the retailer changes it business model and decides to close the UK retail shops and relies on UK local resellers to obtain tailor-made orders, the HK retailer is still not clear of its GDPR obligations because they would be processing personal data obtained from their UK reseller agents.

5 PREPARING TO BE GDPR-READY

To comply with the GDPR before the deadline 25 May 2018, you should immediately:

1. Appoint a data protection officer. (article 37)
2. Train your employee. (article 47)
3. Identify the personal data and related processing activities under your organization. (article 30)
4. Determine the handling of the 7 rights. (article 15 – 22)
5. Determine the main establishment in EU for your company, and thus determine the lead supervisory authority. (article 4)
6. If you do not have any establishment in EU, you would still need a representative in one of the EU member states. (article 27). However, under this situation, described in clarification document wp244 point 2.2 from EU Article 29 Data Protection Working Party, there would be no lead supervisory authority. Then the company would need to observe the regulations of all applicable supervisory authority.
7. Demonstrate compliance. (article 5.2, 24.3)

6 WHAT SGS IS OFFERING

- One-day GDPR awareness training
- Gap analysis against GDPR
- ISO 27001 Information Security Management System training and certification

WHY SGS

SGS is the world's leading inspection, verification, testing and certification company. SGS is recognised as the global benchmark for quality and integrity. With more than 90,000 employees, SGS operates a network of over 2,000 offices and laboratories around the world.

Enhancing processes, systems and skills is fundamental to your ongoing success and sustained growth. We enable you to continuously improve, transforming your services and value chain by increasing performance, managing risks, better meeting stakeholder requirements and managing sustainability.

With a global presence, we have a history of successfully executing large-scale, complex international projects. Our people speak the language and understand the culture of the local market and operate globally in a consistent, reliable and effective manner.

To learn how SGS can help you overcome the legal challenges, contact hk.cbe@sgs.com for more information.

WWW.SGS.COM

WHEN YOU NEED TO BE SURE

SGS