FIDAL ASIA ATTORNEYS

EUROCHAM Workshop:
"Keep Calm and Get GDPR Compliant"

Legal Perspective: Origin, Coverage, Compliance and Penalties

Regulation perspective & business outcomes

Practical steps to compliance

Ho Chi Minh City, 15th June 2018

Disclaimer

Since the **25th May 2018**, the new ***EU General Data Protection Regulation*** **(GDPR)** require all organisations doing business from/with Europe/holding data related to EU subjects, to **manage data** on their customers, employees, contacts and any other relevant persons **more securely and effectively.**

Compliance with the GDPR is to be **considered and designed on a case by case basis**, taking into account **the specific facts** of an organization's own business, operations and use of data.

This presentation provides a set of discussion points that may be useful in the development of an organization's GDPR compliance efforts, but is not intended to be a personal legal advice, guidance or sufficient recommendations per se.
An organization should consult with its own legal counsel about what obligations they may or may not need to meet. Thank you.

GDPR: What for ?

Because:

- **Technology developments & globalisation:** Need to **address the challenges, seize the opportunities** of the digital economy
- **Constitutionalisation** of the fundamental right to data protection (Lisbon Treaty)
- **Fragmentation of legislative framework** (different transpositions of Convention 108, Directive 95/46/EC into national laws)

Therefore: *« A modern European Data protection framework »*

- **Evolution** rather than revolution
- a **harmonised and simplified framework**, legal convergence
- an **updated** set of rights & obligations, enhanced protection
- a modern governance system, more effective law enforcement
- Protecting individual liberties of all EU citizens / Facilitating trade by protecting privacy

"Stronger rules on data protection mean people have more control over their personal data businesses benefit from a level playing field"

GDPR: Why is it important ?

- **Significant business impact** for organisations and how they manage data
- **Process impacts:** collect, storage, processing, access, transfer, and disclosure of an individual's data records
- **Potential heavy penalties** for violations – 4% of global revenues
- **Wide implementation:** these protections apply to **any organisation (anywhere in the world)** that processes the personal data of EU data subjects

Personal data
Any information that can identify a living person – directly or indirectly – or that relates to them

***Sensitive personal data** need particular care*

GDPR: What is it not ?

- It's not just a **security** issue
- It's not just a **legal** issue
- It's not just a **compliance** issue
- It's not just a **risk** issue
- It's not just a **data** issue

It's ALL of these, and more…

- It's also a **business development factor**
  - Stronger rights = more trust = facilitate business
  - Creating a level playing field: territorial scope
  - Cutting red tape: abolishment of prior notification and authorisation requirements
  - Risk based approach benefiting all your process
  - Opportunity to support your company's digital transformation

GDPR: What is it?

The **key principles of data privacy** still hold true, but have been **strengthened**

- **Increased Territorial Scope** (extra-territorial applicability): applies to all companies processing the personal data of data subjects residing in the EU, regardless of the company's location
- **Higher penalties** for non-compliance: up to 4% of annual global turnover or €20 Million (whichever is greater)
- **Consent** must be **clear and distinguishable** from other matters, provided in an intelligible and easily accessible form, using clear and plain language. Easy to withdraw.
- **Accountability, Breach reporting**, notification
- **Right to Access - Data Portability - Right to be Forgotten**
- **Privacy by Design**
- **Data Protection Officers - Data Protection Impact Assessments**

Don’t panic !

- **Bad news: the deadline was 25th May 2018**
- **Good news: it’s not the datapocalypse**

- Your company is not expected to be fully & perfectly compliant since that date

- Good faith, ongoing process, awareness are key
- Mostly, GDPR compliance steps are common sense, analysis, observance, effective linkage between departments

Where to start ?

- **Communication actions: Inform your team** of GDPR issues for the company, impacts on their daily life (awareness)

- **Information asset audit**
  - **What** information is being **collected**?
  - **Who** is collecting it?
  - **How** is it collected?
  - **Why** is it being collected?
  - **What legal basis** do we use?
  - **How** will it be *used*?
  - **Who** will it be **shared** with?

- **Diagnose compliance discrepancies**, formalize a remediation roadmap (main directions)
- Establish the **Register of Processing Activities**
- Appoint a **person in charge (DPO)**

And then

- Formalize / adapt the **Data Governance Charter**
  - Establish GDPR rights management processes (portability, rectification, forgetting, etc.)
  - Consolidate the Security Framework (SI Charter, Enabling Policy, ISSP, Incident Management Policy, PCA etc.)
  - Identify and train the actors involved
  - Consider a certification process: Governance label

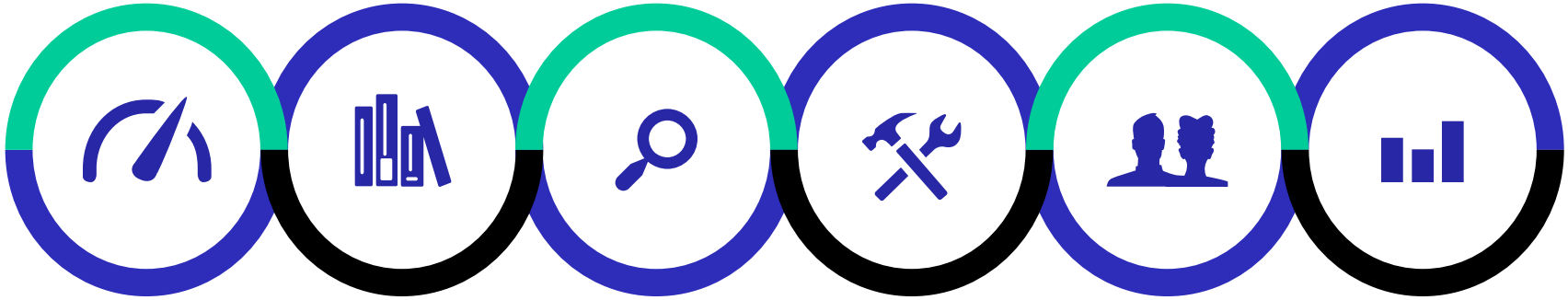
- Adapt the **Information System**
  - Modify applications to implement the principles of "Privacy by default" and "Privacy by design"
  - Automate regulatory treatments (purges, anonymization, portability, etc.)
  - Adapt / strengthen security systems

And then (continuing)

- **Validate the contractual frameworks used in your company**
  - Ensure the conformity **of commercial contracts** with customers, partners, service providers
  - Update the General Terms and Conditions / appendix for existing clients
  - Update your website with Privacy Policy, Cookie Policy.
  - Check your HR documentation

- **Communication & marketing**
  - Legal basis for processing (legitimate interest/LIA, c
  - Different rules for email/text, phone, print
  - Issue wih unsolicited direct marketing, not business
  - Clean your mailing list/ STOP bad practice
  - Ensure active consent proof (opt-in) + opt-out
  - Compliance for existing contacts

Support process



Diagnostic

- Differences vs. the regulation
- Recommendations for compliance

Budget of remediation program

Registry of Treatment Activities

PIA (Privacy Impact Assessment)

Transformation projects (systems and organization to achieve compliance)

Change management accompanying team members in the evolution of their responsibilities and their role

Measured Regular improvement of corporate compliance vs. GDPR

Constant monitoring

Next steps

- These **slides will be shared** after today's event
- **Speak with your IT, com & mkg, HR team** about the GDPR project
- Get **additional documentation:** Guides, checklists, quick prior diagnostic are available online, free (your national authority in charge)

- **If you have further concerns, specific questions, need support** with the process and/or legal framework update, **contact us !**

Contact

Caroline CHAZARD

chazard@asiattorneys.com

FIDAL AsiAttorneys

Saigon Trade Center - Suites 21.01-02

37 Ton Duc Thang , District 1

Ho Chi Minh Ville, VIETNAM

Tel : (84-8) 3910 22 84 - Fax : (84-8) 3910 22 85

Wwww,asiattorneys,com – wwww,fidal,com

http://www.fidal-donnees-personnelles.com/