General Data Protection Regulation (GDPR – EU 2016/679)

What impact on your company?
The Legal context and the key principles

The new European regulation on data protection is ambitioning to reinforce and standardize the protection of personal data of individuals.

Rules will apply to any company collecting or processing personal data regardless of the company size.

The regulation will apply from 25 May 2018.

GDPR applies to personal data processing:
- **Personal data** is any type of data allowing the identification of an individual (name, picture, email address, bank account, IP address, localisation information, ...).
- Data processing refers to any operation applied to personal data (collect, record, usage, storage, deletion, ...);

The key stakeholders are:
- Any **individuals** whom personal data are collected/processed.
- The **controller**, responsible of data processing, who must identify how and why data will be processed.
- The **processor**, as third-party, processing data on request of the responsible.
- Both data controller **AND** processor are deemed as jointly responsible of the data.

For more details on the regulation itself and its legal implications, contact: privacy@lex4u.com
For your organization, what challenges and impacts

Compliance to GDPR is mandatory for any organization processing personal data (e.g. employees, clients in a B2C relation)

5 major domains of compliance have been identified
- Data Governance
- Rights of individuals regarding their personal data
- Data security
- Data transfer
- Authorization (need to know and transparency)

Depending on individual set-up, companies will be sized to address this new game changer more or less smoothly. But all will be facing the same challenges:

- The measure is worldwide, it covers all data controllers, processors, and data subjects based in EU; it also applies to organizations, outside EU, processing personal data of EU residents.
- You first need to know where you stand, and translate the regulation into specific actions relevant for your organization (depending on data and system characteristics).
- You must always be in a position to demonstrate and communicate on your actions.
- Besides technical or legal parts, process and organizational axes must be considered. Addressing GDPR requires approach and knowledge combining these four dimensions.
- Comply with GDPR is a continuous process, not only a one-off effort.
- Many organizations are facing the difficulty to appoint an employee with appropriate profile (i.e. Data Protection Officer).
Anticipated financial sanctions are huge (up to 4% of annual turnover or EUR 20 millions)! However, this might not be the most important side of the downturn; have you also considered, e.g.

- GDPR has a strong legal constraint, especially regarding the joint responsibility between the data controller and the data processor.
- Reputation impact in case of breach and loss of goodwill.
- Operational damages caused by intrusion and higher costs to comply ‘after’ while the urgency is becoming critical.
- Loss of opportunities by not being able to meet customer/partners privacy security standards; or by not having developed this new competitive advantage.

- Be the first to inform your client on your actions for taking care of his personal information.
- Strengthen and review your processes leading to better data integrity and control.
- Control your data as a new valuable asset for your company.
- Cost reduction following ‘Privacy by Design’ allowing reduction of storage and processes.
- Even though some “wait and see” tendency could arise, keep in mind that the regulation will be enforced and that several requirements will last, are common-sense and to be considered as an added-value for organizations, so start now with these ones.

At first sight it may appear overwhelming, though a coolheaded and structured approach will show it might not be!
So remain pragmatic for your one-off preparation…

The assessment
  – Ensure you don’t make more complex what you must eventually do; identify stored and processed data (contracts review, review of communications to clients and employees, data flows and security assessment)

The recommendations
  – Come with pragmatic solutions aligned on your type of activity and industry benchmark; risk assess these storages and processes

The planning and the structuring of your remediation plan
  – Not everything can be done at the same time, but at the end everything must be documented and risk under control

The remediation itself
  – Get organized operationally, put the counter measures in place, communicate, communicate, communicate, …

…but it’s only the start of a new journey that will last!

Equip yourself
  – The regulation requires to document and be able to proof at any time your actions, as well as allow the individuals to claim for their rights … use a sized tool for this, and appoint a responsible

Keep training your teams
  – The culture and the mindset will be key moving forward, make it an asset; embed ‘privacy by design’ in all your projects

Stay tuned
  – The environment will still evolve, so keep yourself informed to better anticipate
Our commercial offer to support you throughout this new challenge

We conduct…

- a 1- or 2-hour meeting to allow scoping of the mission letter, based on your company set-up
- the assessment of the current situation, covering (1) inventory of stored and processed data, (2) contracts review, (3) review of communications to clients and employees, (4) clients data flow and (5) generic cyber security assessment
- the risk qualification and the detailing of the recommendations with practical remediation, we structure your GDPR compliance plan and put it on an actionable timeline

…you get

- A detailed offer, sized to your needs, with clear timeframe, deliverables and transparent pricing
- A report of the current situation, with recommendations and proposed optional offer for guiding you throughout the next steps
- Tailored GDPR compliance plan, detailing the measures to be taken and the workforce required to implement it successfully

Depending on your needs, we may also propose our services to implement part of your remediation plan…

In order to conduct these different steps, we leverage on different methods and tools, being complementary to ensure consistency and being exhaustive

**Our tools**

- Classical tools & methods
- ‘GDPR Compliant Documents’ generator
- ‘Integrated GDPR Data & Process Mapping’ tool
- GDPR Check-List
- SMART Decision Tree
- Live Heatmap

**LAWBOX**

smart law for smart people

**Market Practice**

**Insights Analysis**

**Interviews**

**Questionnaires**

**Internal Documents**
Why is UpQuest a strong partner to address your GDPR challenge?

Through its network of professionals, UpQuest brings together complementary experts taking care globally of your regulatory journey.

We combine under one umbrella:

- **Seasoned auditor** experience to facilitate the assessment exercise
- Organizing the assessment through **Client Journey and Agile** approaches while leveraging on practical common sense
- Leveraging on our **audit tool** to make it your **operational support** moving forward
- Experienced resources in **structuring and managing** strategic projects when need be
- Acquaintance in **data management**, through expertise on the field in different industries
- Dedicated **legal advice** on the GDPR consideration, together with off-the-shelf contractual solutions
- Bringing **collective intelligence** together with **communication strategy** to evolve to the expected Data Privacy mindset and culture
- Access to **cyber-security experts** when your remediation journey requires it
- To guide you throughout this journey, we will brought our certified **DPO competencies**

Not forgetting that your company could potentially be eligible to some financial help or **subsidies** to address this challenge, we will look at this for you.

... and to bring you the best of all we are partnering with Lex4U.
“We guide our clients on their transformation journey to make it a successful adventure”

www.upquest.be/gdpr.html