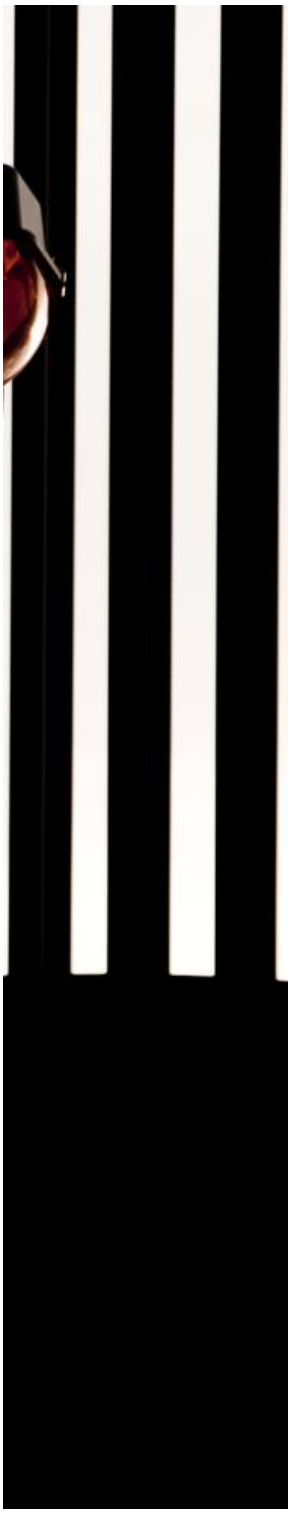


ARTICLE

M-12: OVERVIEW OF THE 12 KEY CHANGES BROUGHT BY THE GDPR

IT and Data Protection Competition, Retail and Consumer Law Commercial and International Contracts | 24/05/17 | Florence Chafiol

Less than a year from now, on 25 May 2018, the European General Data Protection Regulation 2016/679 ("GDPR") dated 27 April 2016 will become the backbone of EU personal data protection regulations. You will find below the most significant changes that will be brought by the GDPR:

1 RATERRITORIALITY OF THE GDPR

It will be difficult to avoid it as the GDPR applies to:

- ✓ Any data processing implemented by data controllers (DC) or data processors (DP) established on the EU territory regardless of whether the processing actually takes place within or outside the EU (establishment criterion);
- ✓ Any processing implemented by a DC or DP established outside the EU that offers goods or services within the EU territory or that monitors behaviours (profiling) within the EU (targeting criterion).

2 LAWFULNESS OF PROCESSING AND CONSENT

- ✓ The legal basis for processing (e.g. consent, performance of a contract or legitimate interest) must be clearly indicated to the data subjects at the time of the data collection;
- ✓ Enactment of the CNIL's doctrine in the definition and assessment of valid consent. The GDPR reinforces the requirements to be met for data processing based on consent – for instance, the acceptance of a privacy policy, or of T&Cs or ToUs can no longer be deemed as a valid legal basis for data processing;
- ✓ When the processing is based on the DC's legitimate interests, the DC will have to be in a position to demonstrate that a "balance of interests" was carried out, balancing the DC's interests against the preservation of the fundamental rights and freedom of the data subjects.

6 DATA PROTECTION IMPACT ASSESSMENT – DPIA

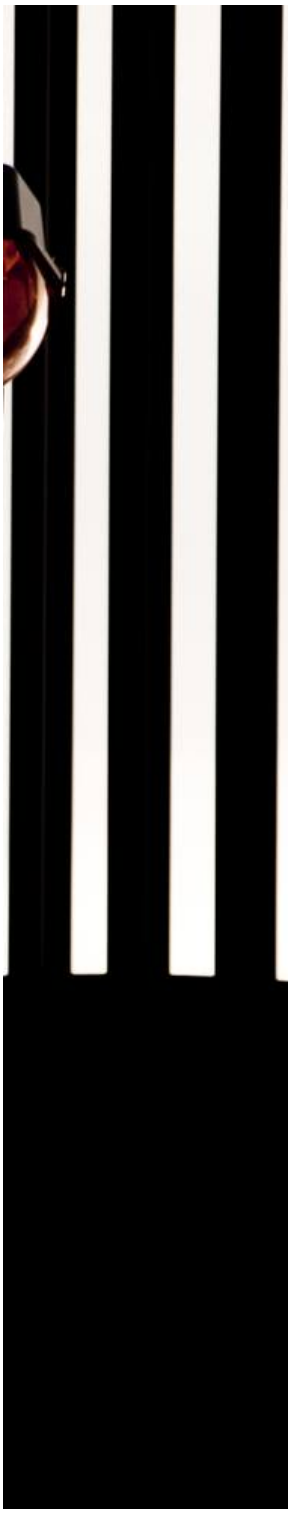
- ✓ Mandatory DPIA in some cases i.e. for all processing operations representing a high risk, the DC will be expected to perform a DPIA;
- ✓ In case of proven high risk, the DC will have to consult with the supervisory authority prior to the implementation of the processing.

7 SECURITY AND NOTIFICATION OF PERSONAL DATA BREACHES

- ✓ General obligation to notify personal data breaches to the supervisory authority;
- ✓ DC (no longer restricted to telecom providers) must notify the supervisory authority within 72 hours of the personal data breach;
- ✓ Obligation to inform the data subjects in case of high risk to their rights and freedoms;
- ✓ DP must notify the DC in case of personal data breach.

8 CERTIFICATIONS AND CODES OF CONDUCT

- ✓ Increased possibility of using certification and codes of conduct to prove data processing compliance;
- ✓ Codes of conduct will be drawn up by the representative stakeholders of business sectors then submitted to the supervisory authority for monitoring, approval and publication.



3 THE DATA PROTECTION OFFICER (DPO)

- ✓ Duty to appoint a DPO in certain cases: (i) the processing is carried out by a public authority or body; (ii) the core activities of the DC or the DP consist of large scale data processing: either for purposes of regular and systematic monitoring of data subjects (profiling); or of sensitive data or data pertaining to offences or criminal convictions;
- ✓ Possibility of using an external DPO without limitation;
- ✓ Duty of information and advice towards the DC/DP, of monitoring compliance with the legislation, of acting as point of contact for the supervisory authority, …;
- ✓ Must have relevant training and be afforded the necessary means to carry out the DPO's duties.

4 LEAD SUPERVISORY AUTHORITY AND EDPS

- ✓ Each national authority has jurisdiction to exercise its functions and powers in its own country.
- ✓ In the case of cross-border processing (e.g.: a company having subsidiaries in several EU member states) the lead supervisory authority of the DC will be the supervisory authority of the main establishment. However, there are some exceptions whereby several national supervisory authorities will be allowed to cooperate.
- ✓ The European Data Protection Supervisor (EDPS) will replace the Article 29 Working Party and, where needed, will decide disputes between the various supervisory authorities.

5 ACCOUNTABILITY AND DATA GOVERNANCE

- ✓ Removal of the "preliminary formalities" system (although certain formalities may remain, including the "authorization application" ("demande d'autorisation")), obligation to keep a register;
- ✓ Principle of compliance and accountability of stakeholders, implying they must be able to demonstrate at all times the implementation of appropriate protective measures and compliance with the GDPR (mechanisms, procedures, DPIA, etc…).

9 STATUS AND NEW OBLIGATIONS OF DATA PROCESSORS

- ✓ Some obligations apply directly to DP;
- ✓ DP will bear direct responsibility for some breaches and joint liability with the DC for indemnification of the data subjects;
- ✓ Obligation to keep a register of processing activities;
- ✓ May have to appoint a DPO;
- ✓ Obligation to provide support to the DC to achieve compliance with the GDPR (security, DPIA, destruction…).

10 INFORMATION OF THE DATA SUBJECT AND TRANSPARENCY

- ✓ Increased amount of information to be provided to the data subjects at the time of data collection;
- ✓ Duty of transparency in the communication (information provided in a readable, clear and comprehensible format).

11 DATA SUBJECTS' RIGHTS

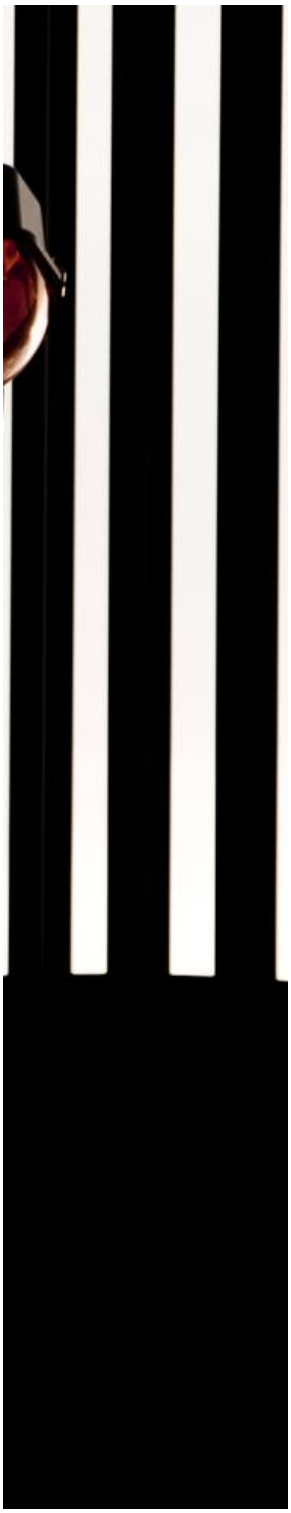
- ✓ Existing rights remain;
- ✓ Right to data portability (obtaining one's data in a readable format);
- ✓ Right to be forgotten;
- ✓ Right to restriction of processing;
- ✓ Right to lodge a complaint with the supervisory authority (already exists in practice although not mentioned as such);
- ✓ Right to an effective judicial remedy against the DC or the DP;
- ✓ Right to receive compensation for the material loss or moral injury resulting from a breach of the GDPR provisions (joint liability of the DC and DP).

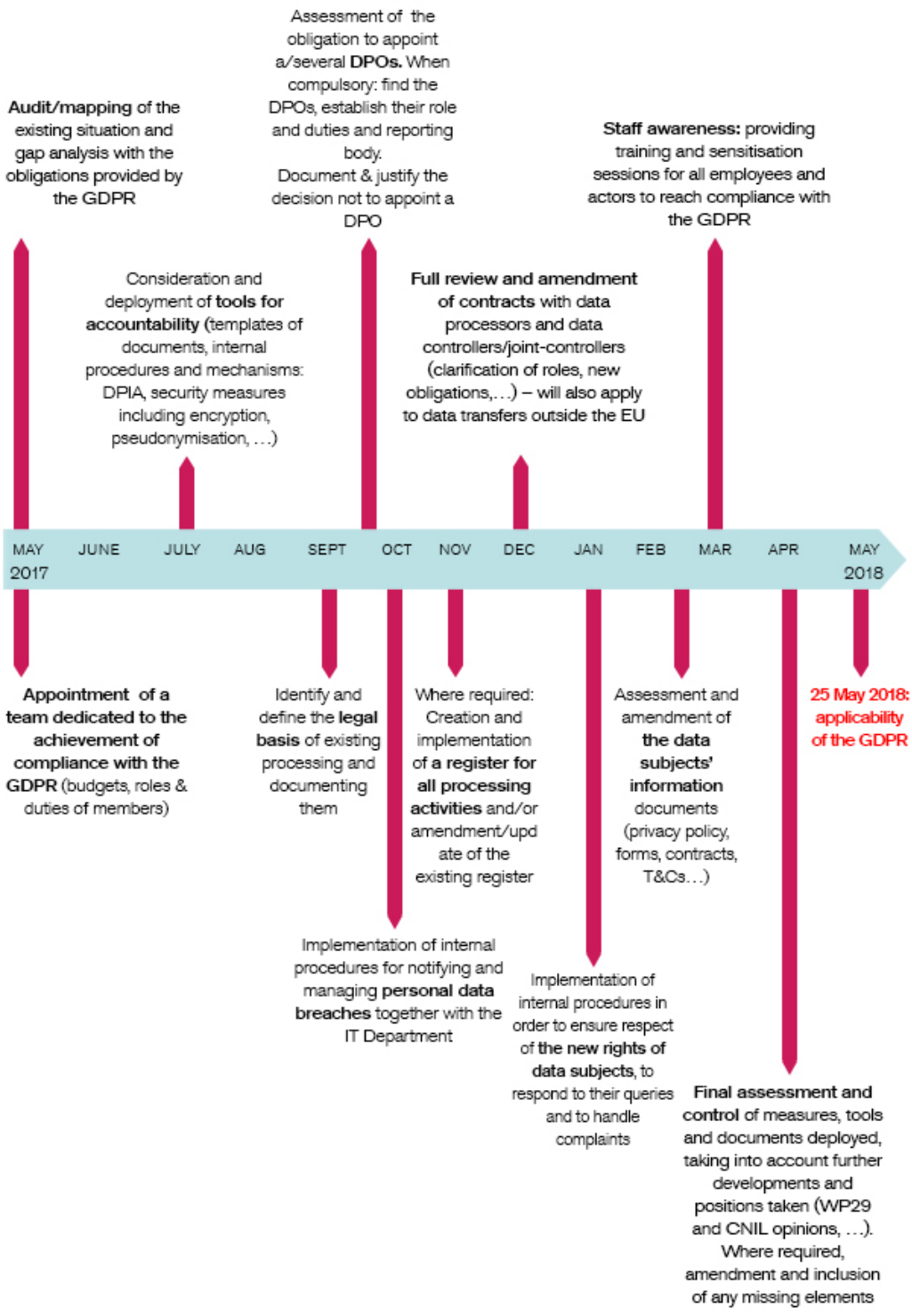
12 ADMINISTRATIVE FINES

- ✓ Increase of the amount of fines;
- ✓ 2 levels of fines, depending on the infringement;
- ✓ Up to Euro 10 million and 2% of the total worldwide annual turnover of the preceding financial year (whichever is higher): e.g. non appointment of a DPO, absence of register, personal data breach notification …
- ✓ Up to Euro 20 million and 4% of the total worldwide annual turnover of the preceding financial year (whichever is higher): e.g. non-compliance with data transfer obligations, lack of or faulty information of the data subjects …

These key changes will be dealt with in further detail in our coming newsletters as well as during our training sessions.

Linked to the above changes, you will find below a timeline for achieving compliance with the GDPR, which can be considered as a "suggested action plan" for the measures and actions to be taken until the Regulation becomes applicable (25 May 2018). These are long term measures and will need to be customised to the internal structure of each organisation as well as to the developments and positions taken by the competent authorities.




Audit/mapping of the existing situation and gap analysis with the obligations provided by the GDPR
Assessment of the obligation to appoint a/several DPOs. When compulsory: find the DPOs, establish their role and duties and reporting body.
Document & justify the decision not to appoint a DPO
Staff awareness: providing training and sensitisation sessions for all employees and actors to reach compliance with the GDPR
Consideration and deployment of tools for accountability (templates of documents, internal procedures and mechanisms: DPIA, security measures including encryption, pseudonymisation, …)
Full review and amendment of contracts with data processors and data controllers/joint-controllers (clarification of roles, new obligations,…) – will also apply to data transfers outside the EU
MAY 2017
JUNE
JULY
AUG
SEPT
OCT
NOV
DEC
JAN
FEB
MAR
APR
MAY 2018
Appointment of a team dedicated to the achievement of compliance with the GDPR (budgets, roles & duties of members)
Identify and define the legal basis of existing processing and documenting them
Where required: Creation and implementation of a register for all processing activities and/or amendment/update of the existing register
Assessment and amendment of the data subjects' information documents (privacy policy, forms, contracts, T&Cs…)
25 May 2018: applicability of the GDPR
Implementation of internal procedures for notifying and managing personal data breaches together with the IT Department
Implementation of internal procedures in order to ensure respect of the new rights of data subjects, to respond to their queries and to handle complaints
Final assessment and control of measures, tools and documents deployed, taking into account further developments and positions taken (WP29 and CNIL opinions, …). Where required, amendment and inclusion of any missing elements