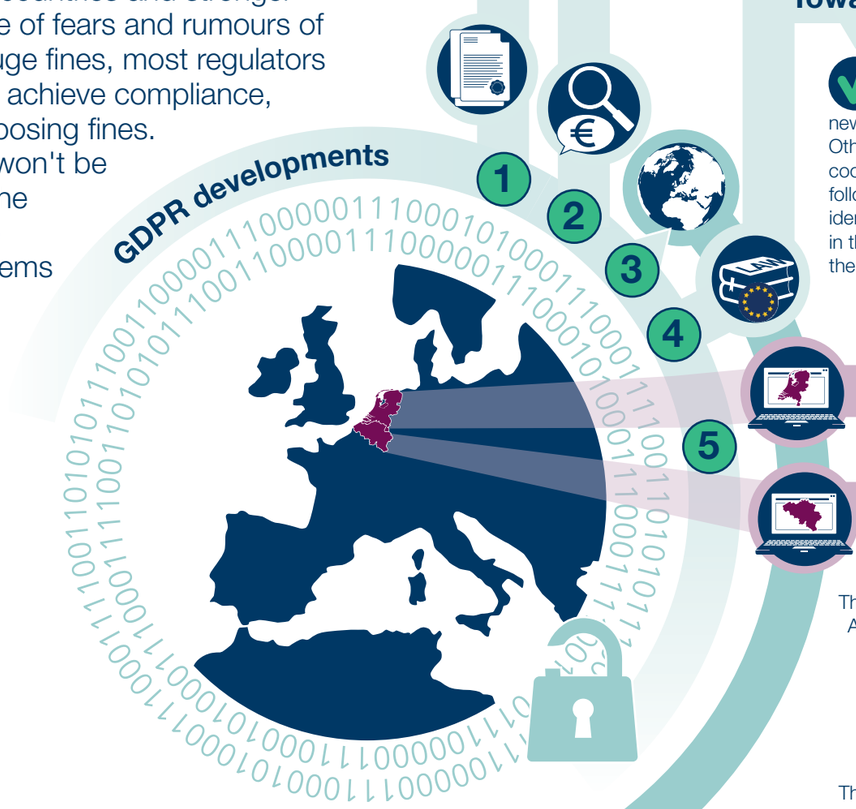
One year of GDPR

The regulatory warm-up

The first year of the General Data Protection Regulation (GDPR) is over. The data protection framework in Europe did not change substantially, other than an expansion of the territorial scope to non-EU countries and stronger powers of enforcement. In spite of fears and rumours of immediate enforcement and huge fines, most regulators focused on helping companies achieve compliance, or enforced without directly imposing fines. This does not mean that fines won't be imposed soon. At the start of the second year of the GDPR , the 'regulatory warm-up phase' seems finished. At the same time, the GDPR is becoming the world wide game-changer in the protection of personal data.

This visual gives an overview of the main GDPR developments in the first full year. More information is available in our extensive white paper, with particular attention for regulatory enforcement and expectations for the future.

Click here for the complete white paper



Regulators establish roles in guidance and enforcement

Data Protection Authorities (DPA)

Each EU country has appointed a DPA to be responsible for data protection enforcement.

European Data Protection Supervisor (EDPS)

Responsible for data protection compliance by EU institutions and acts as data protection consultant to the Council of Europe, European Parliament and European Commission.

European Data Protection Board (EDPB)

The EDPB provides further clarification to the GDPR by publishing draft guidelines and opinions, for example on the GDPR's territorial scope.

Court of Justice of the European Union (EJC)

As the highest court, the ECJ has the final say on data protection issues. Recent decisions include cases regarding the qualification as (joint) controller or processor, as well as the right to be forgotten in the context of search engines.

Enforcement activity expected to increase, including from other authorities

Towards a standardised definition of consent

Consent must be freely given, specific, informed and unambiguous. While this is not new, it is finally now being implemented broadly. Other consent requirements, such as those for cookies and access to payment information, will follow close behind, despite not necessarily being identical. Delimitation of regulatory powers was seen in the context of personal data processing, including the notion of consent, under PSD2.

First year in the Netherlands...

Enforcement
The Dutch DPA has used the first year to build up its resources and to inform and educate, rather than to impose fines. Recently, the Chair of the Dutch DPA stated that fines will be imposed later this year.

GDPR awareness
The GDPR has increased the general public's awareness of data protection rights. In combination with enhanced individual rights, companies now receive many more requests from data subjects to access or rectify their data, to which they must respond actively and in a timely manner.

... and in Belgium

Implementation
The Belgian Data Protection Act of 30 July 2018 slightly complements the GDPR, but focusses more on the implementation of the EU Directive 2016/680.

Enforcement
The Belgian Data Protection Authority, created by the Act of 3 December 2017, has not been very active since the entry into force of the GDPR, but its brand new Committee has recently announced that it will start taking actions.

Click here for Stibbe contact persons

More severe enforcement from national DPA's is to be expected in the months to come. The first significant fine, of EUR 50 million, has been imposed on Google ( ). Furthermore, there is increased enforcement activity in data protection-related matters from other regulatory authorities ( ). In relation to this, more cooperation is seen between regulatory authorities.

The Dutch DPA has entered into a cooperation protocol with De Nederlandsche Bank (Dutch Central Bank) regarding the enforcement of the Second Payment Services Directive (PSD2).

The most striking enforcement action by a DPA so far is the French DPA's imposition of a EUR 50 million fine imposed on Google. The fine amount is not the only striking element about this enforcement action; the French DPA also discussed Google's corporate governance.

The German Bundeskartellamt (Federal Cartel Office) issued a decision prohibiting Facebook from combining user data from different sources under German competition law. The decision illustrates that violations of data protection law can constitute violations of other substantive laws.

The Italian Autorità Garante della Concorrenza e del Mercato (Competition Authority) imposed a EUR 10 million fine on Facebook for misleading and aggressive commercial practices, illustrating the interplay between data protection law and consumer protection law.

The British Financial Conduct Authority imposed a GBP 16.4 million fine on Tesco Bank for failing to exercise "due skill, care and diligence" against a cyber-attack in November 2016. This enforcement action shows the common ground between data protection law and financial law.

Third country data transfer standards still being tested

After Brexit, the UK will be classed as a third country, and, consequently, personal data streams from the EU to the UK may no longer flow as freely as they did before. As it stands, companies that transfer personal data from EU countries to the UK after Brexit will have to take additional measures to ensure lawful data processing.

The Privacy Shield allows for the free flow of personal data from the EU to self-certified entities in the US. The previous Safe Harbour regime was declared invalid by the ECJ in the Schrems case.

The Privacy Shield is not without criticism. At the same time, the alternative standard solution for data transfers to non-EU countries, known as the Standard Contractual Clauses, is also still being tested by the European Court of Justice.

Stibbe