GDPR COMPLIANCE PRIMER

Working Paper 01/2017

IAB Europe
GDPR Implementation Working Group

Version 1.0
22 May 2017

About IAB Europe

IAB Europe is the voice of digital business and the leading European-level industry association for the interactive advertising ecosystem. Its mission is to promote the development of this innovative sector by shaping the regulatory environment, investing in research and education, and developing and facilitating the uptake of business standards.

About the GDPR Implementation Group

IAB Europe's GDPR Implementation Working Group brings together leading experts from across the digital advertising industry to discuss the European Union's new data protection law, share best practices, and agree on common interpretations and industry positioning on the most important issues for the digital advertising sector. The GDPR Implementation Working Group is a member-driven forum for discussion and thought leadership, its important contribution to the digital advertising industry's GDPR compliance efforts is only possible thanks to the work and leadership of its many participating members.

Acknowledgements

The GDPR Compliance Primer has been prepared by the members of the IAB Europe GDPR Implementation Group under the leadership of ***Improve Digital***.

Contacts

Matthias Matthiesen (matthiesen@iabeurope.eu)
Senior Manager – Privacy & Public Policy, IAB Europe

Chris Hartsuiker (hartsuiker@iabeurope.eu)
Public Policy Officer, IAB Europe

Contents

Overview

On 27 April 2016, the European Union has adopted the General Data Protection Regulation ("GDPR").[1] The GDPR will become directly applicable law in the European Union ("EU") and European Economic Area ("EEA") on 25 May 2018, superseding national data protection laws currently in place.

The GDPR will not only apply to companies based in the EU but also to companies all over the globe offering goods and services to people based in the territory of the Union, or monitor the behaviour of individuals located within it. Data protection law regulates the processing of personal data, defined broadly as any information that relates to an identified or identifiable natural person, which may include amongst others online identifiers that can be used to single out a natural person, for example for digital advertising purposes.

The GDPR grants data protection authorities the power to levy significant administrative fines against businesses found in breach of the law. Depending on the severity of the infringement fines can go up to € 20,000,000 or 4 per cent of a company's annual global turnover – whichever is higher.

This document has been prepared by members of the IAB Europe GDPR Implementation Group to provide guidance to companies across the globe on how to start thinking about legal compliance with the GDPR.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), available at http://eur-lex.europa.eu/eli/reg/2016/679/oj/.

The Road to GDPR Compliance

Review and Document Data Processing Activities and Security Measures

Accountability is a central theme that runs throughout the GDPR. Reviewing and documenting all your data processing and security activities is a good first step towards this goal.

As part of this process, you should also identify why and how you are processing the personal data you hold. Getting this basic understanding of data processing activities may require you to pay attention to special considerations – especially whether you are processing sensitive personal data. Additionally, the review process may reveal that your processing activities require special safeguards, so that, depending on the nature of the data processing taking place, the security processes in place at your company may also need to undergo a reassessment. This is a necessary step, considering the much higher fines that companies might be subject to in the event of a breach or other events which could have been prevented or mitigated with more appropriate safeguards.

A good way to approach this exercise is to bring together different departments of your company. You should avoid a situation where GDPR compliance is left solely to your legal teams, a Data Protection Officer (DPO), or IT. Interviews and questionnaires with employees from all departments – and potentially with key suppliers and partners – will allow you to identify what type of data processing occurs in each area of your company's work. Understanding *all* these processes is key. This allows you as a company to record every type of processing based on their purpose, which provides an incredibly valuable data processing map to ensure compliance with the GDPR.

Things to Document

As you go through reviewing and documenting your data processing activities you should consider each on the basis of 'what, where, when, why' as well as the expected consequences of the process, and conduct a risk analysis for each process. Keep in mind this also includes any employee data you are processing. The following questions may help you in this process:

- What information is given before collecting and processing of data?
- Whose data are you processing, what is it, where is it processed, when is it processed and why is it processed? (Do you have a legal basis; do you process in accordance with the data processing principles)?
- What data is anonymised, what data is pseudonymised?
- For how long are you storing such data?
- Who do you share such data with?
- What is the risk level for each process?

- In which cases is your business a controller, a processor, or a joint controller?[2]
- Are you processing what ANY member state would consider personal data (ex: IP address, cookie, any online identifier)?
- Is your process for security reasons? If so document specifics on that.
- Consider that any 'personal' data that is stored or sent outside of the EU needs to follow Cross Border Transfer Rules (Chapter 13 GDPR).
- Are you currently receiving and sending consent along to your processors and other third parties? Is consent received just for you or also your third parties?
- Review and document security processes.
- How do you and any company that acts as a processor, sub-processor or joint controller for your data keep the data secure? As per the GDPR, data breaches must be reported to the DPA within 72 hours of the breach.[3] If you don't already have a plan for this, you should create one. Consider creating a template for sending this information.

Create and Execute a GDPR Compliance Roadmap

The above assessment should help you identify activities which – in part or as a whole – could create conflicts with the GDPR and therefore require changes. The following questions should be considered during this process:

- In what way do your current processes conflict with the GDPR, and are there changes you can introduce to solve this?
- How long will it take to make the necessary changes?
- Do you process data on the basis of users' consent? Do you use a standardised method to receive and pass on consent to third parties and processors?
- Do you need to build additional logs?
    - For example, if data is processed on the basis of users' consent, to record with a timestamp when consent was given, not given, or revoked (connected to an IP address, cookie and/or other identifier).
- How will you handle a user's "right to access" and other data subject rights (Chapter III of the GDPR, Articles 12-22) and maintain your proof of compliance?
- Work with your processors and sub-processors to create documented instructions on the handling of data (Data Processor Agreements).

[2] The GDPR defines these terms in Articles 4(7) and (8).
[3] GDPR, Article 33, recitals 73, 85-88.

Create Data Protection Impact Assessments[4]

The GDPR requires data controllers to carry out an Impact Assessment prior to any new data processing activity in the following cases:

- Where a new technology is used;
- When the processing is likely to have a high risk for data subjects. You can use a single Impact Assessment for multiple processing operations as long as they present similar risks;
- Where it involves a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
- When you process a large scale of sensitive personal data;[5]
- When you systematically monitor a publicly accessible area on a large scale.

Pay close attention to the work of supervisory authorities – they are tasked with establishing a public list of processing activities which require a data protection impact assessment. They may also choose to publish a 'whitelist' of processing activities which do *not* require a data protection impact assessment.

Review and Amend Existing Vendor Contracts and Privacy Policies

Reviewing and changing your internal processes where necessary is only one part of the compliance journey. Another important aspect is to ensure that these are reflected in the contracts you have with partners. In certain cases, the GDPR requires you to have specific agreements in place with the companies you work with, such as when your company and another company are considered 'joint controllers'. As a reminder, the data controller is the one which determines both the purposes and the means of processing of personal data.

At the very least, companies must review already existing vendor contracts and their own privacy policies.

We recommend that you:

- Review all vendor contracts, and amend where necessary.

[4] Draft Article 29 Working Party Guidelines on Data Protection Impact Assessments (WP 248), available at: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137.
[5] GDPR, Article 9, Recitals 51-56.

    - When dealing with multiple data processors, an 'arrangement' between the joint processors must be created to apportion data protection compliance responsibilities amongst themselves.[6]
- Review your Terms and Conditions.
- Review your Privacy Notices (external disclosure) and Privacy Policies (internal rules).
    - You should have rules and procedures in place for employees who work with personal data and document them in privacy policies.
    - Data subjects must be provided with certain information about the collection and further processing of their personal data. This information must be provided in a "concise, transparent, intelligible and easily accessible form, using clear and plain language […]" – usually in the form of a privacy notice.[7]
    - A summary of the arrangement of joint controllers needs to be made available for data subjects.

You could consider using tools or software to monitor that third parties act in compliance with the agreed upon contract and privacy policies. There is a wide range of market solutions to data leakage, including tag management solutions, privacy tools, data loss prevention tools, etc.

Appoint a Data Protection Officer (DPO)[8]

The GDPR requires companies to designate a data protection officer:

- If the law of the Member State requires it;
- If the company's core activities consist of processing which requires regular and systematic monitoring of data subjects on a large scale;
- If data processing is a core activity and involves regular and systematic monitoring of data subjects on a large scale; or the data processed is sensitive information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data or biometric data, and data concerning health or a natural person's sex life or sexual orientation.

A DPO is formally tasked with ensuring that an organisation is aware of and complies with its data protection responsibilities. DPOs should have expert knowledge of data protection law and practice and should be able to perform the following functions:

- Informing and advising the relevant controller or processor (and any employees who process personal data) about their obligations under the GDPR;

[6] GDPR, Article 4(7), Article 26(1), Recital 79.
[7] GDPR, Article 5(1)(a), Article 12-14, Recitals 39, 58, 60.
[8] Article 29 Working Party Guidelines on Data Protection Officers ('DPOs') (WP243 rev.01), available at http://ec.europa.eu/newsroom/document.cfm?doc_id=44100.

- Monitoring compliance with the GDPR by a controller or a processor;
- Advising on impact assessments and engaging in prior consultations with DPAs;
- Cooperating with DPAs and acting as the point of contact;
- Dealing with all data protection matters affecting the controller or processor properly in a timely manner. The controller or processor must provide the DPO with necessary resources and support to do this.

The DPO can be an employee or an outside consultant; the GDPR provides that groups of companies may appoint one DPO if the DPO can fulfil their function for each of those companies. The DPO is bound by a confidentiality obligation in relation to his or her work, and the DPO also has special protection from their employer**.** The organisation cannot instruct the DPO in the performance of his or her duties and cannot terminate the DPO's employment nor take any other disciplinary action resulting from the performance of their duties.

Establish a One Stop Shop with your DPA[9]

One of the potential benefits that the GDPR may provide for companies is the concept of the One Stop Shop. This applies to organisations with multiple establishments across the EU as it allows them to designate a 'lead supervisory authority'. Therefore, organisations operating in multiple member states will need to carefully consider their options in relation to the establishment of a One Stop Shop.

Under the GDPR, the DPA of the EU country where the organisation has its 'main establishment' will be its 'lead authority'. The lead authority has the power to regulate that organisation across all member states. To qualify for a One Stop Shop the organization needs a 'place of main establishment' within the EU. The main establishment is usually the company's European headquarters, but as a matter of EU company law this could be different in certain situations.

Having a One Stop Shop and a lead DPA as a single point of contact (as opposed to having to deal with DPAs in multiple member states) will allow for a more uniform application of compliance across EU markets.[10]

Inform, Stay Informed and Enforce

You should inform and train your employees about the implications of the GDPR and your new privacy policies on their work and make sure that respecting your privacies is enforced through appropriate disciplinary actions where necessary.

[9] Article 29 Working Party Guidelines on The Lead Supervisory Authority (WP244 rev.01), available at: http://ec.europa.eu/newsroom/document.cfm?doc_id=44102.

[10] A full list of data protection authorities in Europe can be found here: http://ec.europa.eu/justice/data-protection/article-29/structure/data-protection-authorities/index_en.htm.

Stay on top of industry initiatives and standards by joining and engaging with IAB Europe and IABs in the markets in which you are active, as well as following the work of the Article 29 Working Party (the future European Data Protection Board) and data protection authorities in the markets in which you are active.

It is also important to inform your business partners in a timely manner of any changes you make to your products or services as a result of your efforts to comply with the GDPR. In case your organisation is consumer-facing, they also need to be informed of updated privacy policies. Particularly, when it comes to using consent as a legal basis for personal data processing, it is extremely vital that new processes in place are communicated to all parties involved.

- Inform Employees, Processors, Users, Clients (well ahead of May 25, 2018) of changes to your terms and conditions and privacy policies.
- Inform Vendors, processors, sub-processors, joint controllers of necessary contract changes.

About the IAB Europe GDPR Implementation Working Group

IAB Europe's GDPR Implementation Working Group brings together leading experts from across the digital advertising industry to discuss the European Union's new data protection law, share best practices, and agree on common interpretations and industry positioning on the most important issues for the digital advertising sector.

The GDPR Implementation Working Group is a member-driven forum for discussion and thought leadership, its important contribution to the digital advertising industry's GDPR compliance efforts is only possible thanks to the work and leadership of its many participating members.

For more information please contact:

Matthias Matthiesen (matthiesen@iabeurope.eu)
Senior Manager – Privacy & Public Policy
IAB Europe

Chris Hartsuiker (hartsuiker@iabeurope.eu)
Public Policy Officer
IAB Europe