World Federation of Advertisers

Hunton & Williams

GDPR Guide for Marketers

Five things every brand owner should know about the General Data Protection Regulation

Executive Summary

As of May 2018, the General Data Protection Regulation (GDPR) will require all companies to make major changes to the way they collect and process consumer data. This is likely to have a significant impact on marketers who use consumer data to drive targeted and effective marketing campaigns.

GDPR applies to any company which offers goods or services to consumers in the European Union or monitors[1] the behaviour of people in Europe. This means that most global companies will be affected, even if their global headquarters are not based in Europe.

Companies could be faced with big fines if they don't comply. These fines could reach up to 4% of a company's annual global turnover, which for Global 500 companies could mean fines ranging from $800 million to as high as $19.2 billion.

In a 2017 survey of WFA members, 94% of companies representing more than US $20 billion of global ad spend said that GDPR was important for their organisation. However, 70% said that marketers in their organisation were not fully aware of the implications of the GDPR for future marketing campaigns.

This guide, developed with the support of Hunton & Williams LLP, aims to help address this gap by highlighting five key areas of GDPR which marketers should be aware of in order to prepare.

"GDPR is critically important for our company as it will impact our global operations across the world. Philips is investing significant resources to meet the requirements of GDPR and help marketers understand the implications for their day to day work"

Blake Cahill, SVP of Global Digital Marketing & Media, PHILIPS

Contents

About this Paper

The General Data Protection Regulation (GDPR) is a major piece of privacy regulation. It will apply from 25 May 2018. It is likely to have a significant impact on almost all large multinationals, as it applies to any company which offers goods or services to consumers in the EU or monitors the behaviour of people in Europe. These companies could be required to substantially change the way they collect and use consumer data. From a brand owner's perspective, GDPR will require a greater focus on how brands communicate with consumers about their privacy and could limit the way some consumer data can be used to develop personalised marketing.

WFA's GDPR Guide for Marketers highlights some of the key elements of GDPR that are likely to have an impact on brand owners and provides concrete suggestions for how marketers should think about their approach to privacy in the context of GDPR. Whilst this guide is not exhaustive, the objective is to highlight a few areas where marketers can start thinking about new approaches and start discussions with the relevant technical experts in their organisations (e.g. legal, compliance and digital governance) to find out more about their company's approach to GDPR. **This guide is intended to complement rather than substitute or constitute legal advice.**

Why is GDPR important for marketers?

1. GDPR will significantly change how and when companies can use consumer data

Europe is often seen as a region with some of the strictest data protection rules in the world and GDPR confirms that image by strengthening existing privacy protections for consumers. This includes a much stronger focus on getting meaningful consent from consumers to use their personal data, including stringent requirements for companies to improve the way they explain to consumers how their data will be used.

2. GDPR will affect almost all large multinational companies.

GDPR applies to any company which offers goods or services to consumers in the EU or monitors the behaviour of people in Europe. This means that most global companies will be affected, even if their global headquarters are not in Europe.

3. Companies run the risk of paying huge fines for non-compliance

Sanctions for not complying with GDPR include fines that could reach up to 4% of a company's annual global turnover. For Global 500 companies, this could mean fines ranging from $836 million to as high as $19.2 billion. As well as regulatory fines, GDPR also opens up the possibility of consumers and not-for-profit organisations launching legal proceedings for compensation in the event of data processing in violation of GDPR.

01

Consent

GDPR puts a strong focus on empowering consumers to decide how their personal data is used by companies. Consent is already one of several legal grounds which companies can rely on to justify the processing of personal data. However, GDPR sets out new and extensive conditions for consent to be valid.

This is likely to mean that in many cases consumers will need to be asked for their consent **more often,** because consent will be needed for each purpose for which a company wants to process personal data. In addition, consumers will need to be given the possibility of withdrawing consent at any time. These requirements may disrupt the consumer's online experience and lead to irritation or, in some cases, refusal to provide consent.

In many cases, however, it may no longer be enough to rely on a general permission given by ticking a box when signing up to a service. Under the new rules, consent must be **freely given, specific, informed and unambiguous,** provided either by a statement or a clear affirmative action.

Freely given	Consumers cannot be forced to provide consent to their data being collected and processed in order to sign up to a service, unless the data is necessary for the service to work.
Specific	In many cases, it will no longer be enough to rely on permission given by ticking a box linked to a privacy policy that covers a wide range of data uses. Consumers will also need to specifically agree to certain uses of their data.
Informed	Companies will need to provide consumers with large amounts of information about how their data will be used. For more information about what information to provide, see Chapter 3: Transparency.
Unambiguous	Consent must be a clear indication that a consumer is agreeing to their data being used. It is unlikely that some 'passive' methods of consent (e.g. continuing to use a website without reading the privacy notice) would be considered unambiguous and sufficient.

Brand owners will need to be able to demonstrate that consent was provided in a way that meets these conditions even if the data was collected by a third party. This means that brand marketers and their legal teams will need to work with agency partners and other third parties to ensure this is possible.

In most cases, **explicit consent** will be necessary to carry out any kind of detailed customer profiling. Explicit consent means that consumers must have the possibility to agree or disagree to a particular use of their personal data by making a clear affirmative statement (written or oral).

Explicit consent will also be required for processing what GDPR calls 'special categories' of data, which are deemed to be particularly sensitive. This includes:

- Personal data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, on a large scale.
- Genetic[2] or biometric[3] data which uniquely identifies a person.
- Data related to health[4], sex life or sexual orientation.
- Data relating to criminal convictions and offences.

Next steps

- Review digital assets with legal and, where necessary, update all consumer touchpoints to reflect the new rules on consent.
- Review data collection practices of agencies and other third parties to assess compliance with GDPR.

02

What if consent isn't an option?

Consent is not the only legal grounds that companies can rely on for the processing of personal data. GDPR also allows personal data to be processed, where necessary, for the 'legitimate interests' of the company without needing to get consent.

This may be particularly relevant in cases where getting consent from a consumer would not be a viable option e.g. because the company doesn't have a direct link to the consumer to ask for consent.

For example, in some cases a company may be able to argue they have a legitimate interest in processing the data of a client, as long as there is a relevant and appropriate relationship between them.

However, in order to rely on 'legitimate interest', marketers would need to work with their legal teams to carry out a legal risk assessment that takes into account:

- The balance between the company's legitimate interest and the consumer's right to privacy (or other fundamental rights).
- Whether a consumer would reasonably expect their personal data to be processed in this situation, based on their relationship with the company.

Where companies process data based on 'legitimate interest', they will have to explain those interests to consumers (for example, in the company's privacy policy).

Marketers should work with their legal teams to explore whether legitimate interest could be possible legal grounds to rely on for data processing in certain situations.[5]

Next steps

- Review on a case-by-case basis with legal teams whether consent is needed to use data collected through marketing campaigns.

03

Transparency

Transparency is one of the key principles of EU data protection law and GDPR introduces additional transparency obligations for companies. It requires companies to provide information to consumers about many elements of how they are using (or are planning to use) their personal data. GDPR also states that information about data processing must be provided in a concise and intelligible form, using clear and plain language.

These requirements create a difficult balancing act for marketers. On the one hand, more information needs to be provided to consumers but it must be done in a way that isn't overwhelming or difficult to understand. Marketers will need to explore creative ways to build this into data-driven digital campaigns.

In February 2017, WFA led a Digital Governance Exchange (DGX) workshop for members to share ideas and best practice about how, where and when consent should be gathered in order to create the best conditions for consumers to have transparency, choice and control over their personal data. Six key principles emerged during the session, which may be useful when thinking about how to implement this element of GDPR.

MAKE IT VISUAL	• The 'emoji' idea - use easy-to-understand symbols to explain privacy policies e.g. seals, trustmarks, icons • Tell me a story - short videos instead of text
KEEP IT SHORT AND SIMPLE	• Only use language a 13-year old child could understand • Keep it relevant • Highlight what is remarkable, and enable users to click through to read more
DON'T ANNOY ME	• Only ask for consent when it's required • Be non-intrusive - don't get in the way of the user experience
LET ME CHANGE MY MIND	• Take back control - create easy-to-use systems to let users control all their privacy settings in one place e.g. dashboards, notification centres, task bars • 'I regret' button - give users the chance to easily opt back in/out whenever they want
MAKE IT EASY	• Make getting out of the situation easier and faster than getting in • Easy gestures to opt in or out e.g. swipe instead of click
TELL ME WHAT YOU'RE GOING TO DO	• Explain to users why you want their information when you ask them for it • Explain consequences/implications of saying yes or no • Clearly explain value exchange e.g. 1 music video = 10 second advert

Next steps

- ☑ Explore creative ways to build information about privacy into online marketing campaigns and digital assets.

04

Processing children's data

In order to process personal data related to children, parental consent will be required[6]. GDPR sets the age of a child at 'below 16 years old', although national regulators in EU countries can opt to lower this age to anywhere between 13 and 16 years old.

This means that companies will need to put in place mechanisms to ask for and verify parental consent. Although national regulators in some EU countries may decide to lower the age at which parental consent is needed, companies should be prepared to implement these mechanisms for children up to the age of 16.

GDPR doesn't lay out specific details on how to verify that parental consent is valid. Initially, companies which have services or products that appeal primarily to children may wish to mobilise their legal or public affairs departments to engage with the data protection authority in their jurisdiction to ask for guidance on how to implement these measures.

Next steps

- ☑ Review all campaigns and/or digital assets that may involve the use of children's data (under 16 years old) as parental consent may be required.

05

Re-using data for other purposes

In many cases, personal data is collected with a specific purpose in mind e.g. signing up to receive a newsletter. However, marketers might be interested in using this data to develop insights that could be used in other marketing campaigns or for targeting similar messages about other products or services. GDPR only allows this under specific circumstances.

If it is not possible (or appropriate) to ask the consumer for consent again, marketers will need to work with their legal teams to carry out an assessment of whether the data can be used for other purposes without consent.

This assessment will need to take into account:

- Any link between the purposes for which the data was originally collected and what marketers would like to use the data for in the future.
- The context in which the data was originally collected.
- The reasonable expectations of consumers, based on their relationship with the company.
- Whether the data is 'sensitive'.
- The possible consequences of using this data for new purposes.
- Whether the data has been anonymised, encrypted or protected in other ways.

Next steps

- ☑ When looking to re-use data collected from historical campaigns, discuss with your legal team to check if this is still possible.

Checklist

When GDPR is applied in all EU countries on 25 May 2018, marketers will need to be prepared for the changes highlighted in this guide. In order to prepare, marketers should consider taking at least the following steps:

- Explore creative ways to build information about privacy into online marketing campaigns and digital assets.
- Review digital assets with legal and, where necessary, update all consumer touchpoints to reflect the new rules on consent.
- Review all campaigns and/or digital assets that may involve the use of children's data (under 16 years old) as parental consent may be required.
- Review on a case-by-case basis with legal teams whether consent is needed to use data collected through marketing campaigns.
- When looking to re-use data collected from historical campaigns, discuss with your legal team to check if this is still possible.
- Review data collection practices of agencies and other third parties to assess compliance with GDPR.

Additional considerations

The following section looks at a number of other elements of GDPR which, although they are likely to have less of a direct impact on marketers, are useful to be aware of from a company perspective. For more information about how your organisation is preparing to implement the following requirements, we suggest you reach out to your legal teams.

Accountability

GDPR requires companies to implement a number of measures to be able to demonstrate compliance, including the following:

Some companies will be required to appoint a dedicated Data Protection Officer (DPO) to oversee all data processing activities. This requirement only applies to companies whose core activities involve:

- Regularly monitoring people in a systematic way 'on a large scale'.
  OR
- Processing personal data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, 'on a large scale'.
  OR
- Processing genetic[7] or biometric[8] data in order to uniquely identify a person, 'on a large scale'.
  OR
- Processing data related to health[9], sex life or sexual orientation, 'on a large scale'.
  OR
- Processing data relating to criminal convictions and offences, 'on a large scale'.

Companies will need to assess whether they fit into any of the above categories in order to decide if they are legally obliged to appoint a Data Protection Officer[10].

Companies will need to set up an internal system to carry out data protection impact assessments before doing any data processing which is likely to result in a high privacy risk for individuals[11]. Marketers should work with their legal teams to understand how and when to trigger a data protection impact assessment for upcoming projects.

Companies will have to maintain internal records of their processing activities in writing, although companies with less than 250 employees may be exempt (under certain conditions). GDPR provides a list of the information which would need to be included in these records.

Companies without an EU base will be required to appoint an EU representative in a single EU country who will act as a contact point for data protection authorities.

Consumer rights

Companies will need to ensure that systems are put in place to respond to requests from consumers about their personal data. Consumers will have the right to ask companies to give them access to their data, and make requests for it to be deleted, amended or given to them (subject to certain conditions). Consumers will also be entitled, under certain conditions, to object to the processing of their personal data and to have their personal data returned to them. They can also request to have their data transferred to another company. Companies will need to be prepared to respond to these requests 'without undue delay' and update their IT systems accordingly.

Data breach notifications

Any security incidents related to personal data (such as a hack or a leak)[12] will need to be notified within 72 hours to the relevant data protection authority. In some cases, it will also be necessary to notify consumers directly.

The short notification deadline will require companies to respond very quickly to any suspected security incidents related to personal data and could have implications for a brand's reputation.

Marketers should consider working with legal, IT and other parts of the business to develop a standard communication strategy to respond to security incidents related to personal data. This could involve developing techniques and ideas on how to notify consumers directly with minimal damage to the brand's reputation.

Sanctions

Companies will face fines of up to 4% of global annual turnover[13] or €20 million[14] for non-compliance with GDPR, whichever is higher.

Consumers, non-profit organisations and associations representing consumers will also be able to launch legal proceedings against companies for non-compliance with GDPR.

Contact information

Please contact **Catherine Armitage, Senior Public Affairs Manager**, for further information (c.armitage@wfanet.org, +32 470 367677).

[1]"Monitoring" refers to, for example, the tracking of individuals online.

[2]Genetic data is defined in GDPR as "all personal data relating to the genetic characteristics of an individual [...] which give unique information about the physiology or health of that individual".

[3]Biometric data is defined in GDPR as "any personal data ... relating to the physical, physiological or behavioural characteristics of an individual which allows or confirms the unique identification of that individual" e.g. facial images or dactyloscopic (fingerprints) data.

[4]Data concerning health is defined in GDPR as "personal data related to the physical or mental health of an individual which reveal information about his or her health status". This includes information about the provision of health services.

[5]For more information about the concept of 'legitimate interest', see Article 29 Data Protection Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller

[6]Unless other legal grounds can be used, see Chapter 2: What if consent isn't an option?

[7]Genetic data is defined in GDPR as "all personal data relating to the genetic characteristics of an individual [...] which give unique information about the physiology or health of that individual".

[8]Biometric data is defined in GDPR as "any personal data ... relating to the physical, physiological or behavioural characteristics of an individual which allows or confirms the unique identification of that individual" e.g. facial images or dactyloscopic (fingerprints) data.

[9]Data concerning health is defined in GDPR as "personal data related to the physical or mental health of an individual which reveal information about his or her health status". This includes information about the provision of health services.

[10]In addition, companies will also need to assess specific DPO requirements that (continue to) apply at EU Member State level. Companies that do not fall into the criteria outlined in this paper are not obliged to appoint a DPO under GDPR, but may still want to appoint a DPO on a voluntary basis in order to facilitate compliance with GDPR's requirements. This type of 'voluntary' DPO will be subject to the same requirements in GDPR that apply when designating a DPO is mandatory.

[11]Data protection impact assessments will be required for any data processing which is likely to result in a high risk for individuals' rights and freedoms.

[12]GDPR defines security incidents related to personal data as 'data breaches' i.e. breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure or, or access to, personal data, transmitted, stored or otherwise processed.

[13]Of the preceding year.

[14]Approximately equivalent to USD 22.5 million.

World Federation of Advertisers
London, Brussels, Singapore

wfanet.org
info@wfanet.org
+32 2 502 57 40

twitter @wfamarketers
youtube.com/wfamarketers
linkedin.com/company/wfa