qualifio

2 years of GDPR

How has it affected marketers?

www.qualifio.com

Table of content

Introduction

Introduction

May 2020 is the second anniversary of GDPR, a time to stop and have a think about what has been achieved so far. What challenges are marketing professionals still facing? What are their most common questions?

The GDPR has changed the way we collect and process data over the past two years. Sanctions have been made against companies that aren't compliant enough. Brexit has happened, so we're waiting to see what's going to happen to data protection in the UK. And much more is happening in the field.

In this ebook, we're talking about the changes that the GDPR has brought this year and we're also looking at the three main challenges facing marketers nowadays:

- The average level of knowledge of the GDPR;
- The concept of consent;
- And the fact that GDPR isn't just about consent.

So keep reading!

Two years: what has changed?

Enforcing the GDPR in marketing has made waves. In the past two years, we've seen:

- In France, the French Data Protection Authority (CNIL) has fined Goggle for its lack of transparency and information. It was considered that the information provided by the company was not easily accessible to users and was not systematically clear and understandable. Users were not able to understand the processing of their personal data (**€50 million**).
- Again in France, the CNIL has also fined Grand Optical France **€250,000** for failing to sufficiently secure the data of its customers placing an order online from its website.
- In the Netherlands, a tennis association, the KNLTB, was fined **€525,000** for illegally selling its members data to two sponsors.

Sanctions are being made against companies that aren't complying with the GDPR but, according to GDPR's advocates, it's still not enough. Experts think that the fines will need to be much higher for the largest companies like Google, Facebook or Whatsapp, to take data protection seriously. So there might be some changes coming related to sanctions in the future.

On the topic of **national laws**, not every country of the EU is in accordance with the GDPR yet. Greece, Slovenia and Portugal, for example, still have to bring it into their laws. And other countries are only hiring and training teams, which means the GDPR has not yet been fully enforced across the European Union.

What about **Brexit**? Marketers from all over the world have heard about Brexit. Starting on January 31st 2020, the UK has exited the EU. However, **according to GDPR officials**, the Regulation should still be implemented in the UK for at least a year before changing.

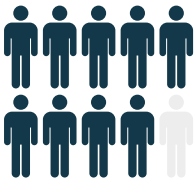
On the topic of **cookies**, the ePrivacy Directive, which will be replaced by the **ePrivacy Regulation**[1], seems to have fallen behind schedule. The EU rejected the proposal in November 2019, which means it won't come into effect for another year at least. It doesn't mean you shouldn't take care of your cookies policy and your privacy policy. Make sure they're as up to date as possible.

And last but not least: **other countries have adopted a data protection policy**. Maybe you've heard of the **LGPD** or the **CCPA**, which are Brazil and California's new laws on data protection? If you have a business in these areas, you might want to have a look.

But let's get back to GDPR...

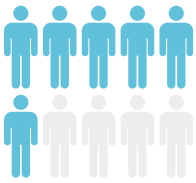
[1] Little reminder: a directive needs to be incorporated into national laws, while a regulation is applied throughout the E.U. as soon as it comes into effect.

Marketers: what are your challenges?



According to a study from **TRUSTe/NCSA**,

92% of online customers cite data security and privacy as a concern.



In another report, the **Chartered Institute of Marketing** discovered that

57% of consumers don't trust brands to use their data responsibly.

Digging a bit deeper, a report from **Symantec** stated that

90% of businesses believe it's too difficult to delete customer data

and that

60% don't have a system in place to help them do so.

Alarming, isn't it?

On the bright side,

78% of companies have completed a GDPR assessment,

and

32% have increased their data protection budget.

However, only

31% of the companies asked believe they are in full compliance with the GDPR.

So what are the challenges encountered by marketing professionals?

Not every team is well equipped to face the GDPR.

A lot of questions about the Regulation are still hanging, and teams can't answer them. Having an expert within your marketing team is essential if you want your marketing actions to be 100% compliant.

Consent is trickier than it seems.

Not only will you need one's consent in regards to the processing of their data, whether they are clients or prospects, but you will also need it if you want to contact them by email or if you met them at an event, for example. So two consents are always better than one, one for every use that you may have.

GDPR is not just about consent.

There are six legal grounds for processing data. Each of them is suited to a particular situation. Yes, consent is important, but you don't need it for everything. Furthermore, there are a couple of rights you'll need to understand and take care of when you're collecting data.

Challenge #1:
Not every team is well equipped to face the GDPR

The purpose of the General Data Protection Regulation (GDPR) is to give EU citizens control over their personal data and change how companies are handling that data. Requirements under GDPR include requiring explicit user consent to collect and **process personal data**, as well as allowing users to request access to or deletion of that data.

However, not every team member understands what it means and what are the rules of the GDPR that every company should follow. Every member of your marketing team must be at the same level of knowledge regarding the GDPR.

Okay, but what does it mean concretely? **Here's the GDPR re-explained**.

What constitutes the "processing" of "personal data"?

The term "**personal data**" refers to any information that helps identify a natural person (or be identifiable), directly or indirectly. In practice, this means one or more specific element(s) making up the physical, physiological, economic, cultural or social identity of an individual such as an online handle, a name, a postal address, an email address, a phone number, etc.

Then there is what's known as "**sensitive data**", such as data that reveals political opinions, religious or philosophical beliefs, racial or ethnic origin, trade union membership, details of one's sex life or sexual orientation, medical information or biometric data (fingerprints, a photograph, etc.).

"**Data processing**" occurs when you perform one or more of the following operations upon personal data (whatever the process used): collection, recording, organisation, structuring, storage, adaptation or modification, extraction, consultation, usage, communication or supply, limitation and also deletion.

Who is the "data controller"?

The "**data controller**" is the person who determines, alone or together with others, the purposes (i.e. the objectives pursued) of the data processing and methods to be used (i.e. the methods used for collecting and processing).

This may be a natural person (e.g. a doctor), a legal person (e.g. a company), an association (e.g. a charity) or even a public body (e.g. a local council).

The identification of the data controller(s) is essential because they are the ones bound by data protection regulations, meaning the general data protection regulation applies to them directly!

If you need to be reminded...

Marketers **are not free** to collect data and process personal data as they wish.

In fact, in order to comply with the regulations, any processing of personal data must meet certain strict conditions. All personal data must be specifically:

- Processed in a lawful, loyal and transparent manner;
- Collected for purposes which are defined, legitimate and clear;
- Appropriate, relevant and necessary with regard to the objectives pursued;
- Precise and, where applicable, up to date;
- Stored in a form which allows for the identification of the person concerned for a limited period, i.e. solely for the period required for carrying out the processing's goals.

> **FOR EXAMPLE:**
> a company is allowed to store data about its customers for the duration of their agreement, but only on the condition that the retention of this data is actually necessary to fulfil the agreement.

- The retention period must be reasonable with regard to the goals pursued, depending on the circumstances and type of data. Each case must be evaluated individually.

> **FOR EXAMPLE:**
> the contact details of a potential customer who does not respond to any offers for three years must be deleted, while images captured by a CCTV system cannot be retained for more than one month

- Collected and processed in a manner which ensures its security.

Furthermore, **the processing of "sensitive data" is in principle prohibited**. In any case, the law strictly limits it. This type of data requires special protection due to the significant risks in regards to the fundamental rights and freedoms of the persons concerned. That's why such data can be processed solely in the scenarios stipulated by **law** (for instance, when the person concerned has given their explicit consent for the processing of this type of data or when the processing of this data is necessary in order to meet an obligation of employment law or social security law). When it comes to sensitive data, caution is very much the watchword.

Challenge #2:
Consent is trickier than it seems

" 'Consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."

(Article 4, paragraph 11)

Any personal data processing activity requires the data subject to give their consent before the processing can take place, providing, of course, that consent is the legal basis for processing personal data.

At the GDPR level, consent is not to be taken lightly. A simple checkbox may be appropriate in some cases, provided that it is specifically mentioned to which processing operation this consent is linked. For example, "I agree to receive commercial offers from Company X." It must also mention a link to the Privacy Policy so that the prospect knows what their personal data will be used for.

This consent must have several characteristics. It must be:

- **FREELY GIVEN**: consent must, of course, be given freely. No unreasonable pressure may be exerted on the person concerned. Therefore, consent will not be considered as "freely given" if there is an imbalance between the person and the data controller.

  Examples of imbalance: a citizen in relation to the authority or a worker in relation to their employer.

- **SPECIFIC**: If you wish to use the data collected for different purposes, all of them must be explained at the time of the consent request. It can also help when segmenting data. Your prospect could tell you how they would like to be contacted via a dropdown menu, for example, or choose which type of newsletter they would like to receive if you offer several.

- **INFORMED**: When you seek consent, it should be formulated in clear and simple terms and should express information that is understandable and accessible. It is therefore not advisable to use legal or technical jargon, which will often be incomprehensible to your prospect.

- **UNAMBIGUOUS**: the data subject must understand that their consent allows you to use their personal data.

ATTENTION

The collection of consent by the acceptance of the general conditions of use or sale is not valid. Be sure to create an additional opt-in that will help you collect this consent in due form because information related to personal data cannot be confused with other information.

PRO TIPS

- Avoid collecting email addresses of individuals on websites or discussion forums.
- Do not pre-tick the boxes when you ask someone to agree to receive commercial communications or communications from other partners.
- Do not make access to a service, the purchase of a good or the benefit of a discount conditional on the acceptance of receiving advertising messages electronically.

In which cases should consent not be collected?

There are two cases in which consent should not be collected:

1. If the commercial message is sent to the professional email address of a natural person and the subject of the message is related to their profession. We are then in a B2B framework. However, it is advisable to inform the person when collecting their email address.

2. The commercial message concerns products or services similar to those already acquired by the consumer from the same company. For example, if a person bought sunscreen from company A, you could send a product email about other sunscreens or similar products to that person.

   Again, this person **must be informed** that their contact information will be used for business prospecting purposes, but only for products or services similar to those already provided by the same company. It is also important that the person is able to object to the use of their data.

How to motivate consumers to consent to share their data?

The question of motivation is probably the most difficult of all. How to motivate them to share their personal data? Two examples:

Have a good Privacy Policy

In general, the establishment of a good Privacy Policy, clear and transparent information on how data are processed, creates confidence among consumers. Most consumers are afraid because they do not understand what they are committing to when they transmit their data.

They must, therefore, be given the opportunity to obtain prior information in a very transparent way, users must be able to understand the processing of their personal data. That's why it's also important to make sure your Privacy Policy is also easy to understand.

Want to know more about what makes a good Privacy Policy? **Click here**.

Towards the monetisation of data sharing

In Japan, it is possible to pay for your consumption in exchange for your personal data.

A Japanese channel offers students the opportunity to pay for their coffee by providing personal data. This data is then transmitted to partner companies. These "sponsor" companies pay for coffee in exchange for surveys or other solicitations.

In return, students will receive advertisements or surveys to complete.

Gamification as a way to collect first-party data

Interactive marketing, also called gamification, is a way for brands and media to collect first-party data about their audience and customers. In exchange for a prize or entertainment, most consumers are more likely to share their data. It's then up to the brand or media to add a consent box to be able to send them personalised emails afterwards.

"We have been able to develop a regular animation strategy with contests that provide us with safe and reliable feedback from subscribers, opt-ins and traffic, but also visibility and a better brand image. It is a whole that allows us to sell better and to be more competitive in the long term."

Tom Legeay

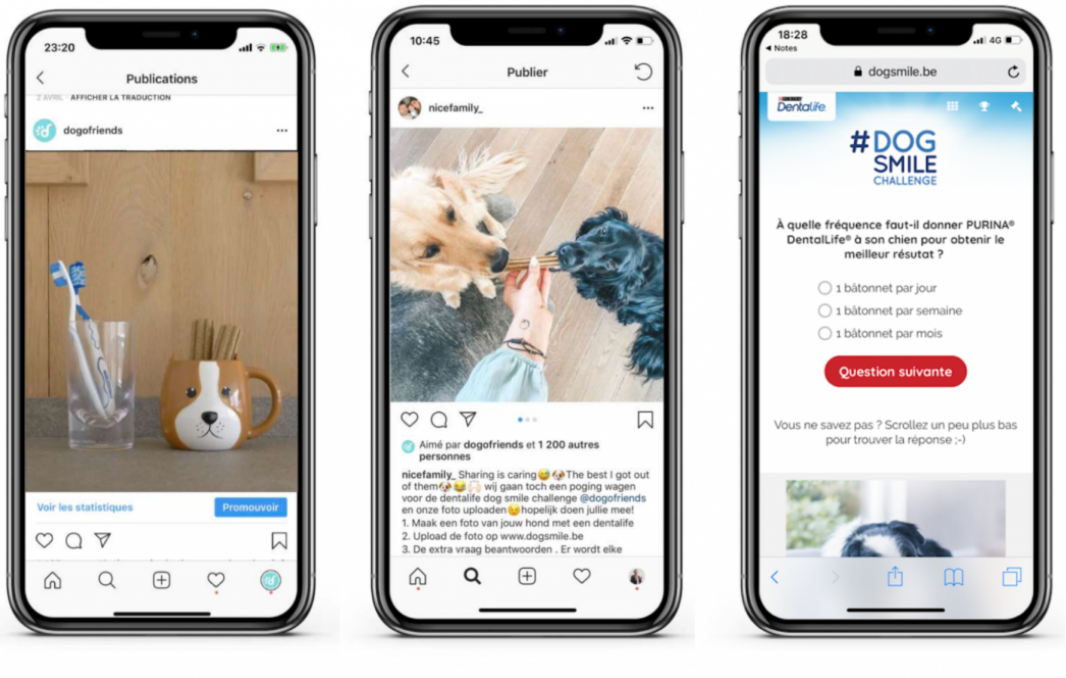
Digital Content & Marketing Campaigns Project Manager at ticketmaster®

Let us show you an example of how gamification can be GDPR compliant:

The marketing agency **Dogofriends** conducted a photo contest for the dog and cat food brand, **Purina**.

The objective was to promote the brand's new product, Purina Dentalife, a chewing stick for dogs.

For twelve weeks, dog owners could enter the photo contest by posting a photo of their dog with one of the brand's sticks and answering a short questionnaire. A question about the dog's name was asked in the form, in which two opt-ins were also present to collect consents for future communication. One opt-in to receive Purina's newsletter, and another opt-in to receive Dogofriends' newsletter.



The gamification campaign was promoted through online (Facebook ads, newsletters, influencers,...) and offline (flyers, samples, internal promotions) channels, ensuring greater visibility with consumers.

The data collected in the photo contest were used to personalise the commercial messages. Each email sent to the participants was personalised with the name of the dog in the subject, previously collected via a form. The brand found that, thanks to this customisation, the opening rate increases by 10% on average... while being GDPR compliant.

PRO TIP

To ensure the proper use of the data you collect through gamification actions, we recommend that **you integrate them into your data management tools**, such as your CRM.

Can you reuse the data collected for another purpose than the one for which they were originally collected?

Once and for all: the answer is no. It is not possible to reuse this data once it has been collected for a specific purpose.

FOR EXAMPLE:

Contact details collected during a recruitment operation may not be used to address advertising. The person who consented to provide information in the context of this recruitment did not give permission to receive commercial communications.

Can you forward the collected data to business partners?

It is possible to adapt the methods of obtaining consent in order to make this transmission legal, but this requires several conditions:

- The person must give their consent before any transmission to partners.

FOR EXAMPLE:

You could provide a checkbox when collecting data with the sentence "I agree to receive offers from business partners" and add a link to the list of partners. However, ideally, the data subject should be able to give consent for each of the partners separately, just like Dogofriends and Purina did in our example about gamification.

- A certain amount of information on the identity of the partners must be provided to the data subject.

FOR EXAMPLE:

For example, when collecting consent, a comprehensive list of trading partners must be easily accessible either via the form or via a link. Do not forget to refer the person concerned to the Privacy Policies of the various partners so that they are well informed of the processing of their data by your business partners.

- The person must be informed of changes and modifications to the list of partners, especially when it comes to the arrival of new partners.

  It can be done in several ways: when the company that collected the data sends a prospecting email, it can inform the person of changes in the list of partners. And when the new partner wishes to communicate for the first time with the prospected person, they inform the data subject, within one month, of the processing they are doing of the data subject's data.

IMPORTANT

The consent that the company has obtained to collect data on behalf of its partners is only valid for those partners. These partners will need to obtain the person's consent if they wish to send the data received to their own partners. In other words, there is no transmission of this consent.

- Partners must ensure, from the first communication with the data subject, that they inform them of the source from which they obtained their data and how the person can exercise their rights. Finally, partners must comply with the information obligations set out in **Article 14 of the GDPR**.
- The right of opposition is exercised either with the partner or with the company that initially collected the data. Attention that in the latter case, the company at the source of the collection will have to pass on the effects of this right of opposition to its partners who are also recipients of these data.

FOR EXAMPLE:

A person expresses their wish to oppose the processing of this data for the purpose of commercial prospecting, directly with the company that initially collected their data. This company will then have to inform its partners to whom the data of the data subject have been transmitted. There is, therefore, a communication work to be done on the company's side at the source of the data collection in order to pass on the information.

Challenge #3:
GDPR is not just about consent

What's the right of objection in the GDPR?

The GDPR gives the individual the right to object to the processing of their personal data, in particular when the data are processed for the purpose of prospecting. Therefore, any commercial communication by electronic means must offer the consumer a way to stop receiving this type of message in a simple, free and easily accessible way.

FOR EXAMPLE:

In an advertising email, you will need a direct link to unsubscribe from the mailing list, clearly and separately from any other information.

It is important to note that this right to object to commercial prospecting must be explicitly brought to the attention of the person concerned. Once the person has exercised their right to object, the controller must put in place the necessary measures to stop the processing.

What is the right to be informed in GDPR?

The GDPR also means the end of incomprehensible terms and conditions written in technical jargon and small print. Information is to be provided in a concise and accessible format. The data controller is held by a duty of transparency that requires them to provide straight and simple answers to the user regarding the identity of the data controller, the purpose of the processing for which the personal data are intended, the exercise of their rights, as well as other items stated in **Article 13**.

WHICH FORMATS SHOULD YOU USE?

Focus on formats that make information more accessible. For example, this is the case for question-answer formats used by a number of companies such as Renault and L'Oréal for their privacy policies. Using everyday language, these companies answer questions that may arise in relation to the processing of personal data: what data are collected (L'Oréal lists them in an exhaustive way), for what purposes, where they are stored, etc.

How about data storage & retention?

It is important to adopt logical behaviours when it comes to storing and retaining data, and especially when it comes to security.

Physical security

A common example is the unlocked cabinets.

Imagine: you work in an accounting office. You welcome a customer into your office and move to another room, leaving them alone in front of an open cupboard. In this cabinet are files of other customers, containing personal data. There is a risk that your client, left alone, may access this data.

It is, of course, important to keep your files secure in all circumstances. Be sure to lock your cabinets.

IT security

The same is true when it comes to digital information. One of the best IT security practices is to set up access codes to your company's server, as well as a unique identifier per person.

ATTENTION

Computer security is the preferred field of activity of the **CNIL** (French Data Protection Authority). So think about good security to protect yourself from sanctions.

Example: Grand Optical

The CNIL has fined Grand Optical France €250,000 for failing to sufficiently secure the data of its customers placing an order online from its website.

It was indeed possible to access hundreds of invoices from the company's customers via the Grand Optical France website. These invoices contained data such as first names, last names, postal addresses and health data (ophthalmological correction) or, in some cases, the social security numbers of the persons concerned.

The CNIL found a safety defect. Indeed, the www.opticalcenter.fr site did not include any functionality to verify that a customer is connected to their personal space ("customer space") before displaying their invoices.

Conclusion

Through the massive use of data to segment and qualify their audiences, marketing professionals are still facing many challenges in understanding and complying with the rules of the GDPR. After two years of application, not all companies are complying with it, and it's more than ever necessary to do so in order to avoid severe penalties in the future.

In this ebook, we have tried to give you some answers to the many questions marketers are still asking about consent, processing of personal data, security and retention of that same data. We hope you have learned a few things and that you have now a couple of ideas to put into practice regarding your own compliancy.

Looking for a compliant way to collect customer data? Qualifio can help you

What is Qualifio?

Qualifio is the leading SaaS in Europe for interactive marketing & data collection. It allows you to easily create and publish interactive content (quizzes, personality tests, polls, and 50+ other innovative formats) on all your digital channels, and to collect data on your audiences to better engage, qualify, segment and monetise them.

How does it work?

Create

Choose your interactive campaign and customise it without any extra development

Publish

Easily publish your campaign on your websites, mobile apps, social networks or on a dedicated minisite

Collect data

Run GDPR-compliant data collection campaigns thanks to a set of dedicated features

Get results

Visualise and extract profiles collected and campaigns statistics in real time

Segment & monetise

Connect the platform to your marketing & data tools (CRM, DMP, SSO, email, automation, Analytics, etc.)

Interested?

REQUEST A DEMO

Need more info?

CONTACT US

Resources

QUALIFIO, *"Marketing & GDPR: 15 questions one year after"*, 2019

QUALIFIO, *"GDPR: 15 examples of best practices for obtaining marketing consent from users"*, 2018

QUALIFIO, *"Everything you need to know about the new General Data Protection Regulation (GDPR)"*, 2017

DIGITALEUROPE, *"Almost two years of GDPR: celebrating and improving the application of Europe's data protection framework"*, 2020

GDPR.EU, *"How the GDPR could change in 2020"*, 2020