Marketing & GDPR

15 questions, one year after

qualifio

Introduction

How to obtain **consent**? What about the data collected via **social networks**? Under which conditions can marketers send commercial solicitations? Lex4U's lawyers answer the most frequently asked questions from marketing professionals, one year after the implementation of the GDPR.

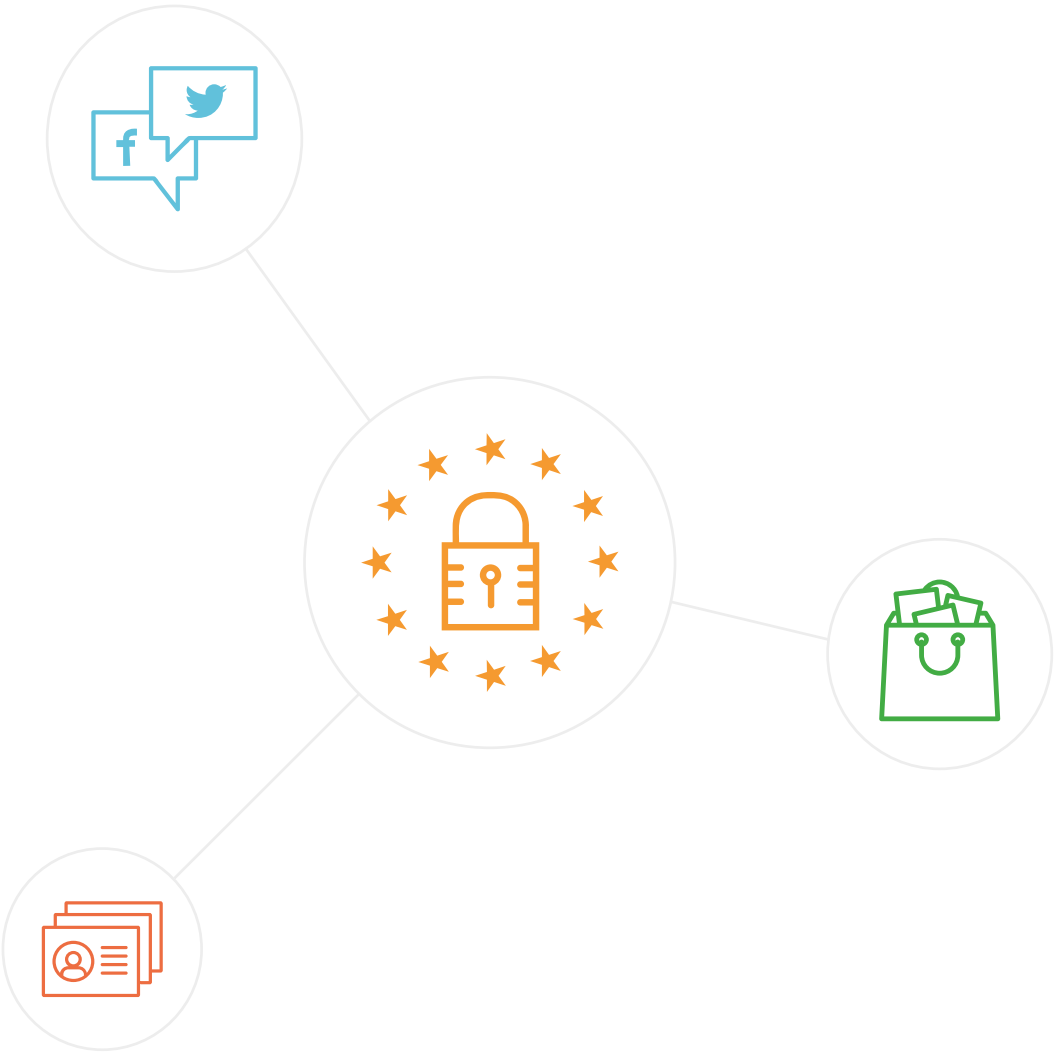


Table of content

1 How to obtain consent?

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 drop-down 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.

2 How to send commercial solicitations electronically, without violating privacy rights, in a B2C relationship?

Before answering this question, it is worth recalling the difference between postal, telephone and digital marketing.

The main difference is that it is **not necessary to obtain consent in the context of a telephone call with human intervention** (as opposed to an automated electronic communication system) **or the sending of postal mail**, provided that the person contacted has been properly informed and has not exercised their right of objection.

In addition, it is possible to send a commercial prospecting email to an individual without their prior consent if the prospecting concerns a similar product or service and that person has been informed of the use of their data for commercial prospecting purposes.

However, it is **essential to obtain this consent in the context of digital communication** (via email, fax or text message) and to enable the recipient to exercise their right of opposition in a simple way.

In all cases, according to the rules of the GDPR, the data controller must provide the clearest possible information on the use of the data for commercial and charitable solicitations of direct marketing campaigns.

In order to obtain this consent, we recommend that you use an **opt-in**, i.e. a checkbox explaining the purpose for which you wish to collect the person's data.

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.

3 How to send commercial solicitations electronically, without violating privacy rights, in a B2B relationship?

As in B2C, at the time of data collection, the person must be **informed** that their email address will be used for commercial prospecting purposes. They must also **be able to oppose** this type of use simply and free of charge at any time.

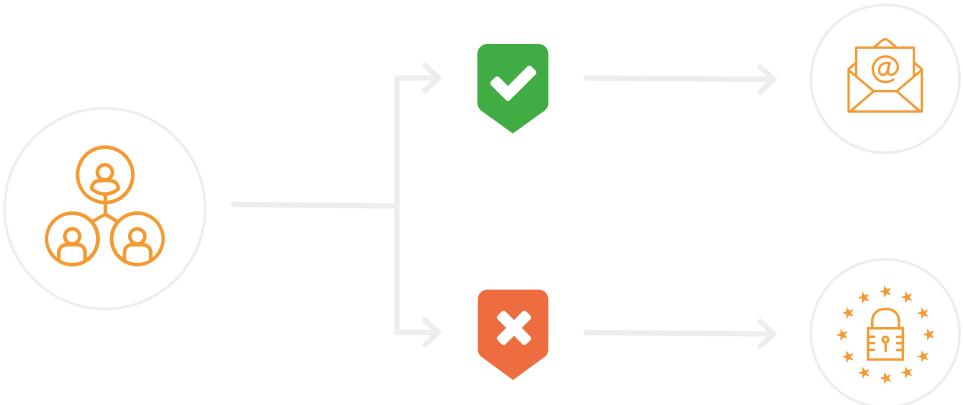
ATTENTION

The object of the solicitation must be related to the person's job.

Can we send emails to info@ or contact@ addresses?

Generic business addresses, i.e. info@example.com or contact@example.com, are not subject to the principles of consent and opposition because they are not personal data.

The question becomes debatable as soon as the email address contains the person's first and last name. In this case, the email address contains personal data. The principles of consent and opposition therefore apply.



4 In which cases should consent not be collected? What are the exceptions?

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. As we saw in the previous question, 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.

5 What is 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/ listing, 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.

6 Is it allowed to reuse the collected data for purposes other than those for which they were originally collected?

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.

7 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.

➔ 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.

In summary, when transmitting data to business partners, it is essential to inform about:

- the name of the company that transmitted the data to the partners (the company that initiated the collection);
- the identity of the partners and an updated list of them;
- the purposes for which the partners will process the data;
- the rights of the persons concerned, and in particular the right to oppose commercial prospecting by the partner(s).

8 What about countries outside the European Union?

It should be recalled that the central point of the GDPR is the **individual**, the European citizen. The objective is to **protect** people from the abusive use that companies can make of their data. Therefore, the GDPR also applies beyond the EU.

It must therefore be understood that the GDPR applies even to companies established in countries outside the EU **when the processing of personal data concerns an EU resident**. Indeed, whether or not the processing takes place in the Union, the GDPR has a global scope.

The case of Switzerland

In the case of Switzerland, the European Commission has adopted an "adequacy decision". This is a decision by which the Commission recognises that a country outside the EU offers a level of personal data protection comparable to that guaranteed in the EU. Thanks to this "decision", personal data can circulate between the EU and the third country concerned.

As a result, Europeans citizens benefit from an increased level of protection, in line with EU privacy standards, when their data are transferred to Switzerland.

LIST OF COUNTRIES THAT HAVE BEEN THE SUBJECT OF AN ADEQUACY DECISION

Andorra, Argentina, Canada, Guernsey, Faroe Islands, Isle of Man, Israel, Japan, Jersey, New Zealand, Switzerland and Uruguay.

The case of the United States

There is no general data protection law in the United States. However, a self-certification mechanism, better known as Privacy Shield, has been put in place. The European Commission has recognised this as providing an adequate level of protection for personal data transferred to the United States.

IN A NUTSHELL

Privacy Shield is a "partial" adequacy decision, because data transfer is only made easier for companies that are committed to its principles.

However, in July 2018, the European Parliament disavowed this system by considering that "*the current Data Protection Shield does not offer the adequate level of protection required by EU data protection law and the Charter of Fundamental Rights of the European Union*".

HOW CAN WE ENSURE THAT DATA TRANSMITTED TO THE UNITED STATES ENJOYS AN ADEQUATE LEVEL OF PROTECTION?

If a company is self-certified with Privacy Shield, a data transfer to it can, at least for the time being, be made. However, taking into account the European Parliament's disavowal, it may be appropriate to take additional precautions and organise transfers to the USA on the basis of one of the other possibilities offered by the GDPR.

In practice, we are thinking directly of a contract containing the standard contractual clauses that have been put in place by the European Commission.

Other mechanisms exist in the Regulation but should be used sparingly, either because of their restrictive nature (list of derogations) or because of the complexity of their implementation (codes of conduct or binding corporate rules).

What about Brexit?

The impact that Brexit will have on the application of the GDPR in the United Kingdom depends on political negotiations before the official Brexit date of 31 October 2019.

There are therefore two possibilities:

EITHER THE AGREEMENT WITH THE EU IS APPROVED

In this case, there will be a two-year transition period during which the GDPR will remain in effect. Nothing will therefore change during the 2 years following Brexit with regard to the transfer of data to the United Kingdom.

EITHER THE AGREEMENT WITH THE EU IS NOT APPROVED

Without an agreement, the United Kingdom will be considered a third country from 1 November 2019. It will then be necessary to compensate for the absence of an agreement by using one of the tools allowing the supervision of these transfers (an adequacy decision for example).

9 What about the data collected via social networks?

The use of data collected via social networks is a complicated issue. Care must therefore be taken: just because the data are public does not mean that they can be used freely.

The LinkedIn case

Let's take a simple example: you are looking for a way to contact a person on LinkedIn and find their email address, published on their profile. This one is accessible to you because you are part of this person's professional network.

According to the principles of the GDPR, you need a **legal basis** for the use of this personal data. In the context of direct marketing, whether in B2C or B2B, the data subject must be informed about the use of their personal data. In this case, even on the basis of the application of **Article 14 of the GDPR**, which mentions the possibility of processing data that you have not collected yourself, it will be complicated for you to explain that the data subject was clearly informed at the time of collection.

On the other hand, it will be easier to justify contact with a person in the context of a professional solicitation, given the objectives of the LinkedIn social network. You just have to mention that you have found the email address on LinkedIn when contacting the person.

The case of Facebook contests

Example: You are launching **an Easter contest** in which you invite your audience to find an egg hidden in one of the publications on your Facebook page.

Since the **Wirtschaftakademie decision**, Facebook page managers have been considered as co-responsible for this page.

In order to reuse the information collected in these competitions, you will need to inform participants about the processing of their data properly. This explanation can take place within the framework of your Privacy Policy, accessible via a link to be found in the data collection form, for example.

Finally, the principle of "**purpose limitation**" must be respected and the data of these persons must not be reused for any other purpose, unless it is compatible with the original one, as envisaged in **Article 6 (point 4) of the GDPR**.

10 What is the impact of the GDPR on audience targeting on social networks?

Regarding audience targeting, the first question to ask is obviously "does this processing make it possible to identify a natural person or to make them identifiable?"

If we are talking about a general targeting (typically an age group in a defined territory), it is impossible to precisely identify a natural person on the basis of this targeting alone.

If, on the other hand, targeting concerns a behavioural analysis based on the pages visited/seen/etc. by the individual, this targeting is directly linked to their own behaviour. The third party company wishing to market using this behavioural data will then have to ensure that Facebook has obtained the consent of the individual.

Obviously, in the case mentioned above, it will be necessary to give fundamental importance to the information provided to the individual, both on the part of Facebook and the company processing this data.

In view of the various decisions on Facebook taken by the European authorities, it will be necessary to be extremely cautious.

Concerning tracers and retargeting, the subject is in vogue. Indeed, Advocate General Michal Bobek delivered general conclusions in the **FASHION ID** case which, schematically, could lead to the conclusion that the manager of a website is co-responsible for the processing of the company that installed the plug-in.

11 What about data storage and 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.

12 Where are we on sanctions?

Sanctions and controls have already been put in place in several countries, including France. The French Data Protection Authority (CNIL) sanctions both large companies, such as Google, and smaller ones.

The Google example

Google was fined €50 million for its **lack of transparency and information**. It was considered that the information provided by Google 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.

The example of a real estate company

The French Data Protection Authority also imposed a financial sanction against a real estate company that had solicited, by text message and **without their consent**, owners of real estate properties for sale.

It is therefore not only large companies that are subject to control by the authorities and sanctions.

And in Belgium?

On the Belgian side, the Belgian Data Protection Authority has also started its first meetings, and therefore its first controls. Therefore, **you should not skimp on your data protection compliance** because the consequences of non-compliance can be serious.

13 How to process information retrieved during events?

1st case: the speaker retrieves the data

The speaker of a conference obtains the list of attendees and their email addresses, via which they have registered.

It would be good practice for the data subjects to be informed at the time of registration that the list has been forwarded to the speaker and the purposes for which they will process the personal data.

But what is the legal basis applied?

- ➔ At the time of registration, a specific opt-in is provided and the purposes clearly defined in the opt-in message. This allows the data to be processed on the basis of consent.
- ➔ Legal basis of the legitimate interest: in this case, the persons concerned must be properly informed in advance. You must also give them the opportunity, on the same day and afterwards, to object to the processing of their personal data for marketing purposes.

2nd case: the data is recovered via an application

Imagine: you are present at a car show. The exhibition has set up an application in which attendees can enter personal data such as their last names, first names, dates of birth and email addresses. This data creates a **unique QR code** that is linked to the email address of the data subject.

As an exhibitor you also have access to the application and you have a feature to scan the QR code in order to obtain the email address, last name and first name of the person who passes through your stand.

HOW TO PROCESS THE DATA?

- It is necessary to **verify that the organising fair that has set up a privacy document** accessible via the application and that explains the ins and outs of the data processing it carries out. In addition, it should be verified that this information document clearly explains that scanning the QR code will transfer the data to a given exponent.
- As an exhibitor, you will be able to contact the person who came to your booth - in the event that the person presented you with their phone with the QR code voluntarily. To do this, you must comply with the requirements of **Article 14 of the GDPR** if you have not collected the data subject's information yourself.
- **Contextualise your first contact** with a simple and clear sentence, such as "We met at Salon X."
- At the level of the **legal basis**, it is possible to justify these processing operations on the basis of legitimate interest. The person did seem interested in your services or else they would not have shown you their QR code to scan. That is why it is extremely important to check the legal documents that are used by this type of application in order to verify that the data subject has been properly informed of the use you intend to make of them.

3rd case: the example of Batibouw

Imagine: you meet a prospect at the Batibouw show, the biggest Belgian trade fair for Construction, Renovation and Home Improvement for professionals and the general public. Your company, specialised in bathrooms and kitchens, makes a first estimate based on the explanations and requests of this prospect.

Following this first contact, you contact them the following week. You are therefore using the legal basis of necessity for the performance of a contract, and more precisely for pre-contractual measures.

Finally, after a complete quotation, the person concerned does not wish to follow up on this quotation.

What can you do with this personal data? **Nothing**.

Indeed, the person has given you their data for a specific purpose: the construction of a kitchen. They have not given you permission to use their data for any other purpose.

A good practice would be to provide quotation forms with opt-in checkboxes allowing the consent of the data subject to be obtained for purposes other than those related to the sale, in particular the sending of documentation relating to commercial prospecting.

14 What will happen to GDPR and e-Privacy in the future?

The future is, in principle, uncertain. It is not easy to predict what will happen. However, here are some ideas for reflection:

- ➔ It can of course be expected that **other sanctions will fall**, in particular in Belgium where the Data Protection Authority recently held its first meetings, which will therefore probably follow on from the first controls.
- ➔ The recent **adequacy decision** concerning Japan leads us to believe that the Commission will try to extend international trade with new agreements of the same type, which of course favour trade.
- ➔ And finally, still with a view to strengthening the single digital market, a **proposal for an e-Privacy regulation** on privacy and the protection of personal data in **electronic communications** has not yet been adopted. It was originally intended to come into force at the same time as the GDPR.
- ➔ This Regulation complements and clarifies the GDPR: it reinforces the obligations of privacy and confidentiality of communications in the electronic communications sector. It will harmonise all national laws in the EU concerning this type of communication and will have a direct impact on the digital marketing market.

15 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, c**lear 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.

Towards the monetisation of data sharing

In Japan, for example, 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. It is these “sponsor” companies that pay for coffee in exchange for surveys or other solicitations.

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

Focus on interactive content and first-party data collection

If you are a marketing professional, collecting consent is now part of your daily life, whether it is to collect data for personalisation purposes, do advertising targeting, increase your contact base through opt-ins, etc. As we have seen, the GDPR more formally sets out the conditions that must be met for such consent to be considered consistent with the GDPR.

Some marketing formats encourage opt-ins and the collection of GDPR-compliant data more than others. This is the case with interactive formats such as quizzes, contests, personality tests and surveys, which many major brands and media use. By immersing visitors completely in the advertiser's universe, these formats mechanically increase the conversion rates observed.

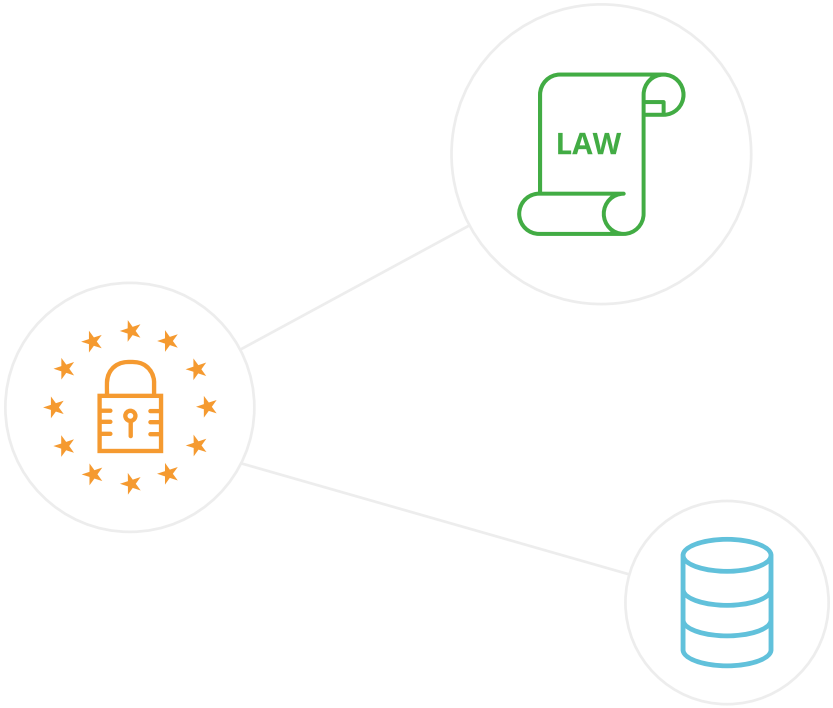
But these formats have another advantage in a post-GDPR context: they are used to collect "first-party" data (i.e. obtained directly from the data subject), via the forms they contain. The GDPR obviously reinforces the importance of first-party data as opposed to second-party and third-party data, since the former is often based on the legal basis of consent.

Qualifio allows you to create this type of interactive content easily and without technical skills. Qualifio's "**GDPR toolbox**", a set of features dedicated to GDPR, allows you to ensure the compliance of all your marketing and collection actions in Qualifio.

Conclusion

Through the massive use of data to segment and qualify their audiences, marketing professionals face many challenges in **understanding and complying with the rules of the GDPR and e-Privacy**. It is now more than necessary to comply, otherwise severe penalties will be imposed.

We have seen it in this ebook: whether on social networks or your own website, the collection of **consent**, the responsibility for the **processing of personal data**, the security and retention of the same data,... all of this is important in order to engage consumers and customers legally.



About the authors

Nathan Vanhelleputte is a member of the Brussels Bar since February 2018. He obtained his Master's degree in Law from the ULB in June 2015 with the mention cum laude (with Honors) and directly joined the insurance company AIG.

He left the American company after two years to participate in the founding of a consulting firm specializing in Compliance and Regulatory.

After this experience he decided to join **Lex4u** to work on topics such as commercial law, contract law, personal data protection regulations and information technology law.

Nathan obtained the Data Protection Certification from the Solvay Brussels School.

He is still involved in projects of the University where he holds the position of President of the Association of Former Students of the Faculty of Law.

Adeline Balza is passionate about new technologies and all issues related to Intellectual Property rights. Therefore, after completing her Master's degree in Law at Université Libre de Bruxelles in June 2017, she decided to pursue her studies in English at Katholieke Universiteit Leuven in order to specialise in Intellectual Property Law and Information and Communication Technology Law.

After obtaining her Master of Laws in July 2018, Adeline joined Lex4u in October 2018 to practice mainly Privacy and Data Protection Law and New Technology Law.

Mehdi Benallal is Head of Marketing at Qualifio, the leading platform for interactive marketing and data collection. He is a member of the GDPR committee at Qualifio and regularly speaks at conferences on the impact of the GDPR on companies' marketing activities.

About 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?

BOOK YOUR DEMO WITH LIVE CUSTOM EXAMPLES

Need more info?

CONTACT US