

IAB Europe Webinar

GDPR One Year On. Lessons Learned

Thank you for joining! We will begin momentarily.

iab.^{europe}  iubenda

Welcome



**Matthias Matthiesen,
Director, Privacy & Public
Policy, IAB Europe**

Agenda

- GDPR Overview & Key Aspects
- GDPR Common pitfalls
- Q&A



GDPR Overview & Key Aspects



**Philip M. Weiss,
Director of Marketing,
iubenda**

Overview



At its most basic, **the General Data Protection Regulation** specifies how and when personal data should be lawfully processed.

- It became fully enforceable on May 25th, 2018
- It's intended to strengthen data protection for all people whose personal information fall within its scope, giving them greater control of their personal data.

At its most basic, **the General Data Protection Regulation** specifies how and when personal data should be lawfully processed.

- **Personal data under the GDPR refers to any data that relates to an identified or identifiable person.** *This includes pieces of information that, when collected together, can lead to the identification of a person.*
- Under the GDPR personal data may only be processed if there's at least one **legal basis** for doing so.

The Consequences of Non-compliance include

- fines up to EUR 20 million (€20m) or 4% of the annual worldwide turnover;
- sanctions such as official reprimands, periodic data protection audits; and
- liability damages.

GDPR Key Aspects



**Abbie Clement,
Head of Content,
iubenda**



**Philip M. Weiss,
Director of Marketing,
iubenda**

Key Aspects



The Legal Bases of Processing Data

- **Consent.** The user has given consent for one or more specific purposes;
- **Contractual requirements.** The processing is necessary for the performance of a contract in which the user is a participant or necessary in order to take steps (requested by the user) prior to entering the contract;
- **Legal obligation.** The processing is necessary for fulfilling a legal obligation to which the data controller is subject;
- **Vital interests.** The processing is necessary for protecting the vital interests of the user or of another person;
- **Public interest.** The processing is necessary for performing a task carried out in the interest of the public or as contained under the official authority given to the data controller;
- **Legitimate interest.** The processing is necessary for the legitimate interests of the data controller or third party, except where overridden by the interests, rights and freedoms of the user, in particular where the user is a child.

Note: Legal bases shouldn't be “picked” at random, as they **must legitimately apply to your situation**.

When it comes to evaluating whether or not a legal basis (outside of consent) can apply, we suggest working with a legal professional as determining the correct legal basis is critical and can be difficult.

Furthermore, there will always be data processing activities where consent is the safest, best or only option.

Consent

- **Consent must be affirmative, informed and freely given in order to be considered valid.** The mechanism for acquiring consent should be unambiguous and involve a clear “opt-in” action (the regulation specifically forbids pre-ticked boxes and similar “opt-out” mechanisms).
- The regulation also gives users a specific right to withdraw consent. It must, therefore, be as easy to withdraw consent as it is to give it.
- Where the processing based on consent, you must also be able to demonstrate that valid consent was collected.

Users' rights

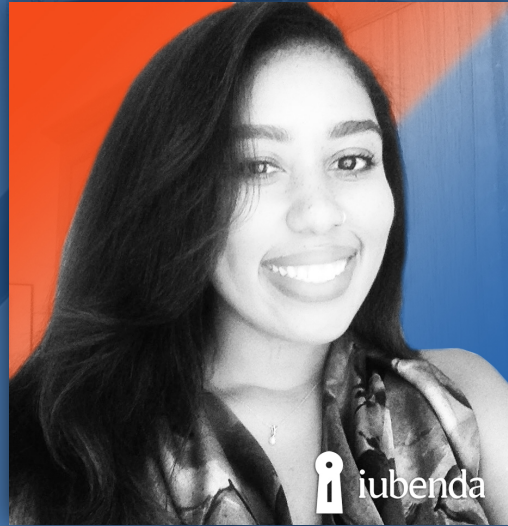
- **The right to be informed.** Organizations must provide users with information about the data processing activities they carry out.
- **The right to access.** Users have the right to request and access their personal data and information about how their personal data is being processed.
- **The right to rectification.** Users have the right to have their personal data rectified if it is inaccurate or incomplete.
- **The right to erasure.** When data is no longer relevant to its original purpose or where users have withdrawn consent or where the personal data have been unlawfully processed, users have the right to request that their data be erased and all dissemination ceased.

Users' rights

- **The right to object.** Users have the right to object to certain processing activities carried out on their personal data. In a nutshell, the user can object to the processing of their data whenever the processing is based on the controller's legitimate interest, or the performance of a task in the public interest/exercise of official authority, or for purposes of scientific/historical research and statistics.

The user has to state a motivation for their objection, unless the processing is carried out for direct marketing purposes, in which case no motivation is needed to exercise this right.

GDPR Common Pitfalls



**Abbie Clement,
Head of Content,
iubenda**

1 Assuming that the GDPR does not apply to you because you're based outside of the EU or do not have EU-based users.

The GDPR can apply in any one of three scenarios:

- where your base of operations is in the EU;
- where you're not established in the EU but you offer goods or services (even if the offer is for free) to people in the EU; or
- where you're not established in the EU, but monitor the behaviour of people who are in the EU (as long as that behaviour takes place in the EU).

This scope is quite wide-reaching and, therefore, means that the GDPR can apply to you whether you're based in the EU or not.

2 Failing to maintain proofs of consent / not being able to demonstrate that valid consent was collected.

Because consent under the GDPR is such an important issue, it's vital that you keep clear records and that you're able to show that you've acquired valid consent.

Should problems arise, the burden of proof lies with you, the data controller, so keeping demonstrable proof is both vital and required.

2 Failing to maintain proofs of consent / not being able to demonstrate that valid consent was collected.

The records should at least include:

- who provided the consent;
- when and how consent was acquired from the individual user;
- the consent collection form they were presented with at the time of the collection;
- which conditions and legal documents were applicable at the time that the consent was acquired.

*Ref: Article 29 Working Party, Guidelines on consent under Regulation 2016/679, Guide to the General Data Protection Regulation (GDPR), Information Commissioner's Office, <http://www.ico.org.uk>

3 Confusing the roles and responsibilities of the data controller and the data processor.

- The term “**data controller**” means any person or legal entity involved in determining the purpose and ways of processing the personal data.
- The term “**data processor**” means any person or legal entity involved in processing personal data on behalf of the controller.

Ultimately, **the data controller bears the responsibility** for the user data processed, and therefore, knowing which role applies to you is vital.

Note: These roles are not based on choice, but rather, on an objective assessment. Getting this wrong can lead to severe fines if found in breach.

3 Confusing the roles and responsibilities of the data controller and the data processor.

For example

An e-commerce company collects users' personal data and stores it using a 3rd party cloud service.

In this scenario, the e-commerce company is the data controller and the organization running the cloud service is the data processor.

4 Failing to create and maintain records of your processing activities.

The GDPR requires that both data controllers and data processors keep and maintain “full and extensive” up-to-date records of their data processing activities.

The records of processing activities must be in writing. While both paper and electronic forms are acceptable, **it is best practice to use an electronic method of record-keeping so as to facilitate easy amendments.**

4 Failing to create and maintain records of your processing activities.

Full and extensive records of processing are **expressly required** in cases where the data processing activities:

- are ***not occasional***; or
- could result in a risk to the rights and freedoms of others; or
- involve the handling of “special categories of data”; or
- is carried out by an organization that has more than 250 employees.

This effectively covers almost all data controllers and processors.

5 Failing to collect separate consents for separate purposes.

Example scenario: A website owner uses a sign-up form that allows users to consent to receiving emails for both product updates and third-party offers using a single opt-in mechanism like a checkbox.

In this scenario, the website owner / data controller is failing to comply with requirements as the consent acquired must be specific to a singular purpose.

5 Failing to collect separate consents for separate purposes.

In cases where you want to send more than one type of email to your users, you're required to get additional consent specific to those uses, **as you must have multiple consents for multiple purposes.**

This doesn't necessarily mean that you must use a separate form for each purpose, it simply means that you should give the user the opportunity to actively consent to each *purpose* (see the *following example*).

5 Failing to collect separate consents for separate purposes.

Terms and conditions

☐ I agree to the [terms and conditions](#)

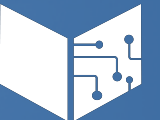
Contact permission

☐ Yes, I would like to receive a weekly digest of content posted to this blog (optional)

☐ I agree to receive product information and offers from this blog (optional)



Q&A




Get in touch

communication@iabeurope.eu

info@iubenda.com

 [@iabeurope](https://twitter.com/iabeurope)

 [/iab-europe](https://www.linkedin.com/company/iab-europe)

www.iabeurope.eu