

everything you  
need to know  
about



GDPR



what**counts**

## General Data Protection Regulation (GDPR)

### overview

GDPR is essentially a new regulation put in place by the European Parliament, the Council of the European Union, and the European Commission to help unify the data protection for all individuals within the European Union. This regulation was adopted on April 27th, 2016 and will become enforceable on May 25th, 2018. The GDPR will replace the EU Protection Directive which contains current recommended guidelines regarding personal privacy.

### in short:

- GDPR applies to organizations that are in EU or collect and distribute personal data from EU users.
- GDPR includes new regulations on how consent is displayed and acknowledged
- Any lists acquired prior to the GDPR must have traceable consent and be in adherence to updated procedures
- Data storage and elimination requirements should be reviewed to assure compliance

### scope

This regulation applies if the data controller (organization that collects data from EU residents) or processor (organization that processes data on behalf of data controller e.g. cloud service providers) or the data subject (person) is based in the EU.

Regulation also applies to organizations based outside the European Union if they collect or process personal data of EU residents. In the case of an Email Service Provider, or Email Marketer sending to a subscriber based within the European Union, these regulations will be applicable.

According to the European Commission “personal data is any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a home address, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer’s IP address.”



## consent

Article 32 of the GDPR states specifics around acceptable consent:

“Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject’s agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. **This could include ticking a box when visiting an internet website**, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject’s acceptance of the proposed processing of his or her personal data. **Silence, pre-ticked boxes or inactivity should not therefore constitute consent.** Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject’s consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.”

Valid consent must be explicit for data collected and the purposes data is used for. Data controllers must be able to prove “consent” (opt-in) and consent may be withdrawn.

This aligns with the explicit consents we require for email communication, as stated within our Anti-spam policy, <http://www.whatcounts.com/company/whatcounts-anti-spam-policy/>.

Starting in May 2018, brands have to collect affirmative consent that is “freely given, specific, informed and unambiguous” to be compliant with GDPR.

Many practices that marketers previously used to opt-in email subscribers would not be compliant under GDPR. Strategies such as requiring an email address to download a whitepaper or providing contact information to enter a contest will no longer be compliant if you didn’t tell them you’d use their personal data to send marketing messages. A subscriber must actively agree that it is okay to use their data for that specific reason; otherwise, it won’t be legal to add those email addresses to their mailing list.

## who does the GDPR impact?

The GDPR not only applies to organizations located within the EU but it will also apply to organizations located outside of the EU if they offer goods or services to, or monitor the behavior of, EU data subjects. It applies to all companies processing and holding the personal data of data subjects residing in the European Union, regardless of the company's location.

**If you're collecting email addresses and send email to subscribers in the EU, you'll have to comply with GDPR—no matter where you're based.**

## privacy policies

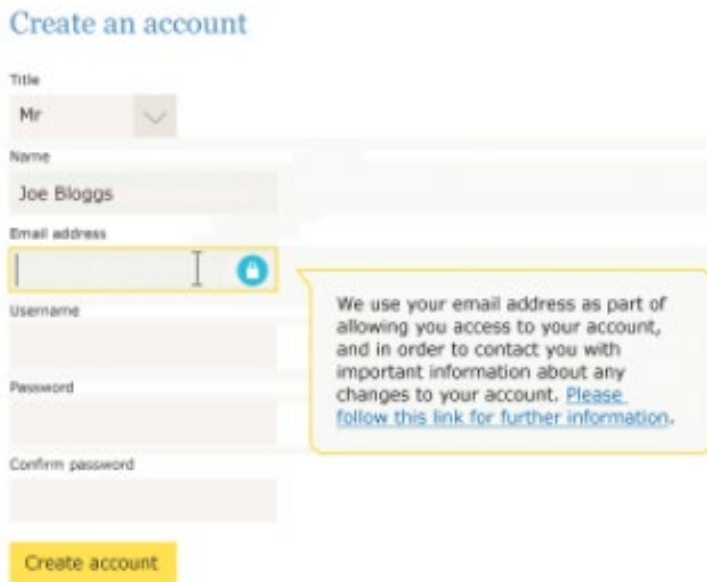
Requirements through the GDPR will also bring changes into how marketers/companies provide their Privacy Policy information.

Here are the requirements expressed through GDPR:

- Concise, transparent, intelligible and easily accessible;
- Written in clear and plain language, particularly if addressed to a child; and
- Free of charge.

This means that a simple link to an extremely long Privacy Policy will no longer be acceptable when alerting subscribers that their data will be collected for other uses.

A creative option that will work with many sign-up forms within our industry is a “Just-In-Time” privacy notice. In these cases, when the user engages with a data field, relevant information is displayed at that time with a pop-up style hint. Here’s an example:



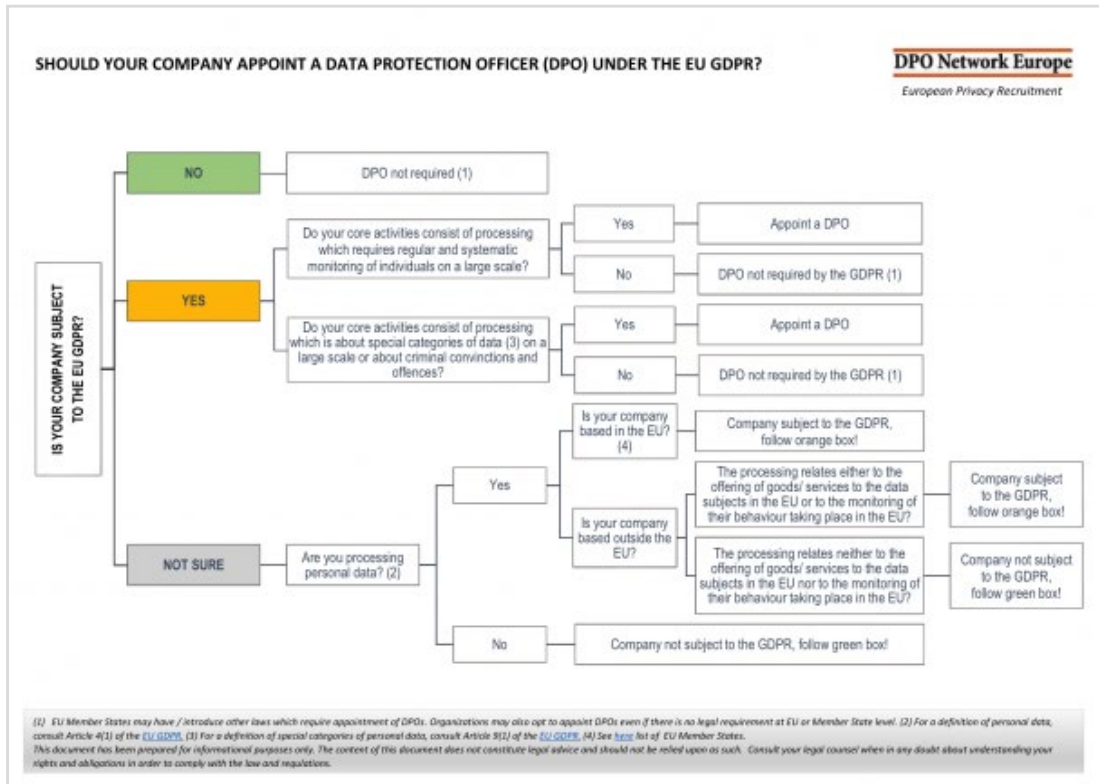
The screenshot shows a 'Create an account' form with the following fields: Title (Mr), Name (Joe Bloggs), Email address (highlighted with a yellow border and a blue speech bubble icon), Username, Password, and Confirm password. A yellow 'Create account' button is at the bottom. A pop-up notice is displayed over the email field, stating: 'We use your email address as part of allowing you access to your account, and in order to contact you with important information about any changes to your account. Please follow this link for further information.'

Here you can see when a subscriber highlights the email field to enter their information, they are provided with a notice explaining what their email address will be used for, and also a link to their current privacy policy for additional information.

## storing personal data

The GDPR emphasizes the secure storage of personal data and the right to have that data removed upon request. Complying with GDPR guidelines may significantly change your current procedure for storing and eliminating data. In the future, you will need to handle data accordingly:

- Proof of consent to use an email address or other personal data must be documented and stored. Records of the agreement will need to be reproduced when called upon.
- The ability to withdraw consent (unsubscribe) of the use of an email address needs to be easily accessible. No hunting for an unsubscribe button; it should be in plain view.
- Individuals also have the right to ask for the permanent elimination of any personal data. The GDPR explains this as the “right to be forgotten”. When requested, personal data must be scrubbed from the system with no remaining trace of the information.
- Should a breach in security occur, it must be reported to the data protection officer or a supervisory authority within 72 hours of its discovery. The nature of the breach, the number of those who are potentially harmed, and the “likely consequences,” will need to be provided.
- Some companies, mainly those that are considered data controllers, may be required to obtain a Data Protection Officer.



## preparing for the new regulation

- Determine whether or not you are using email addresses from the EU. If the email has a .eu or other European extensions at the end, that's a pretty good sign. If your company currently collects IP information for website submissions, you may also need to consider using this information to determine their country of origin.
- If your database includes subscribers whose permissions haven't been collected according to the GDPR's standards, or if you can't provide sufficient proof of consent for some of your contacts, you will need to solicit permission from them once again, abiding to the standards set forth by these new regulations.
- Review any requests for email addresses, including pop-up windows and sign-up forms, to make sure the language is clear and specific, and covers all the reasons for using that address.
- Keep a record of all individual permissions to use their email address and be prepared to present the consents if asked.
- Take steps to protect against potential breaches in security. Review your current data storage and security practices to see if additional measures should be added.

## must-read disclaimer

Please be advised that this resource includes our informed interpretation of the General Data Protection Regulation and its applications.

This document is for informational purposes only and is designed to help you, as marketers, better understand the law and how it might affect you.

We are not lawyers and nothing presented here is, or should be construed as, legal advice. It may be necessary to consult your legal or compliance department for specific guidance in regards to adherence with the law.