alto marketing
Life science and healthcare communications

GDPR

what it means and what you should do

Read on for our practical guide

Understand legal basis

Understand definition of consent, legitimate interest

Review your policies

Including data, privacy and cookie policies, and change if necessary

Review consent policy

Review how you seek, record and manage consent - do you need to make any changes?

Create a consent form

Use across all platforms explaining what consent is being given for

Create an inventory

What personal data do you hold? Does it comply? Why do you have it?

Include privacy rights

Include data deletion, portability and access rights

Address access requests

Plan how you will handle data access requests

Make customers aware

Create programme of communications about GDPR

Communicate with staff

Make staff aware of the changes and impact

Delete remaining data

Once GDPR is in force, delete all data that does not fall into 'consent' or 'legitimate interest' categories

GDPR – what it means and what you should do

With the implementation date for GDPR quickly approaching, we have devised a guide to help your business best prepare for the changes, along with tips for increasing opt-in rates before the cut-off date. GDPR affects all data held by a company on EU-based individuals, including employees. In this guide we consider how this might affect your marketing communications and offer recommendations that can be implemented straight away.

Summary

GDPR (General Data Protection Regulation) is a European privacy regulation that will come into effect on May 25th 2018 to protect the personal data of all individuals within the European Union. According to the European Commission, personal data can be *"anything relating to an individual in their private, personal or public life. It can be anything from a name, a home address, a photo, bank details, IP address and posts on social networking websites".* The penalty associated with non-compliance can be anything up to €20 million or 4% annual turnover (whichever is higher). Note: Although GDPR only applies to EU-based individuals, any company collecting personal data from individuals in the EU (no matter where it is based) will have to follow GDPR regulations.

The essentials

- You must get explicit consent from an individual to contact them or process their personal data. This means that prospects, customers, and partners need to explicitly confirm that they are happy to be contacted (pre-ticked boxes or assumption of consent are not permitted).
- The tracking of consent is mandatory - you must have evidence of each individuals' consent, including how and where the consent was gathered.
- All data you hold on EU-based individuals where consent has not been obtained must be deleted by May 25th.
- Organisations must be explicit about what will happen to the data, how they will use it, and why it is necessary to hold/obtain.
- People have the right to access, amend or delete any personal information collected about them.
- Businesses can also use the legal basis of 'legitimate interest' to hold/process data. Legitimate interest applies when necessary for your company's business, or those of a third party. Examples include:
    - Holding data on individuals and contacting them where there is a relevant and appropriate relationship (i.e. the individual is an existing client)
    - Maintaining a limited amount of personal data (i.e., just their email address) after someone has opted-out in order to ensure no more communications are sent to them

In order to use legitimate interest, you must be able to be able to prove why it was necessary to process and/or use the individuals' data, and explain the nature of the interests for doing so.

Continued…

Alto's recommendations

Without preparation, you may have to delete a significant number of EU contacts from your database, and so we recommend the following steps and series of communications to minimise this drop-off.

1. **Give people reasons to opt in to your database** – ensure that they know that you are/will be providing useful, informative content such as white papers, guides, infographics, videos, eBooks etc, which people can access and download in exchange for them opting-in.

2. **Create a consent form to be used across all platforms** so that all opt-ins are gathered in the same format and obtain the same information. You should provide a link to this form on all elements of your opt-in communications. You will need to include a short description of what the individual is consenting to, along with reference/link to your privacy policy. It is best to use the same explanation across all platforms (email, in person, on social media, and organic web visits) to ensure continuity in how you gather, process, and use data.

3. **Develop a series of communications specifically about GDPR** in the lead up to 25th May, using a positive message to encourage contacts to opt in to your database. Each contact opportunity is likely to encourage only a small percentage of your database to opt in, hence the need for multiple communications through different channels. Communications, such as those below, should have links to your opt-in form:
   - **Send out a series of emails about GDPR** - suggest a minimum of 2 weeks apart. Text should be changed so that the emails appear fresh
   - **Create a banner** to include at the top of all general marketing emails asking people to opt-in
   - **Upload posts to your social media accounts** about GDPR and the reasons for opting-in
   - **Add a pop-up or banner on your website** inviting visitors to add themselves to your database
   - **Include an opt in banner in your email signatures –** for customer-facing, and ideally for all, employees

4. **Face-to-face contacts** – you need to have evidence that people you have met in person have opted-in to your communications. Have a printed form or a smartphone/tablet form on your stand. Any other contacts should be followed up with an email asking them to opt in.

5. **Set up an automatic double opt-in email** – Every time someone responds to your communications and opts-in, have a process in place that sends out a follow on email asking them to confirm their consent and adjust/add to their preferences. This double opt-in is not mandatory but highly recommended. Ideally this should be done automatically.

Further practical tips

- **Start auditing your mailing list now** to review which EU-based individuals have already opted-in, who you still need to opt-in, and the proof to go with this, so that all your records are in place and up-to-date by May 25th
- **Ideally centralise all your data on a CRM system** and make sure users have access to view, change, and delete their data through a preference centre

Continued…

- **Update your privacy statement** to explain how data will be processed, provide instructions for opting-out, and how individuals can access their information and report any inconsistencies
- **Update your cookie policy** to ensure individuals give explicit consent for your site to store cookies – pre-ticked boxes or assumptions will no longer be valid
- **Check that third party tools and providers** are fully compliant with GDPR and that they have steps in place to store and process data appropriately, including evidence of an individual's consent to data being shared
- **Use social media more** to connect with prospects and share relevant content

We hope the information provided in this guide will be useful to understanding and implementing GDPR changes before the regulation comes into force on May 25th, bearing in mind that these changes only apply to EU-based individuals.

If you would like any further guidance or have any queries regarding GDPR then get in touch today.

Tel: +44 (0)1489 557672

Email: info@alto-marketing.com

Other helpful resources

- ICO's Guide to GDPR
- EU GDPR
- IT Governance guide to data protection and GDPR
- DMA's guide and webinars to GDPR