WHAT YOU NEED TO KNOW ABOUT GDPR
HOW TO STAY COMPLIANT

[WHITE PAPER]

Vuelio

WHAT IS GDPR?

Vuelio

The EU General Data Protection Regulation (GDPR) comes into force on 25 May 2018. Within this document we'll explore what GDPR means for you.

GDPR is an EU-wide regulation that will replace the current data protection laws in the UK. The new Regulation has been designed to provide greater protection for personal data in today's digital world, where we are all interacting more than ever before by email, social media and web applications.

In the UK, the Information Commissioner's Office (ICO) will be the 'Supervisory Authority' responsible for implementing and enforcing GDPR's requirements, as it does now under existing UK data protection legislation.

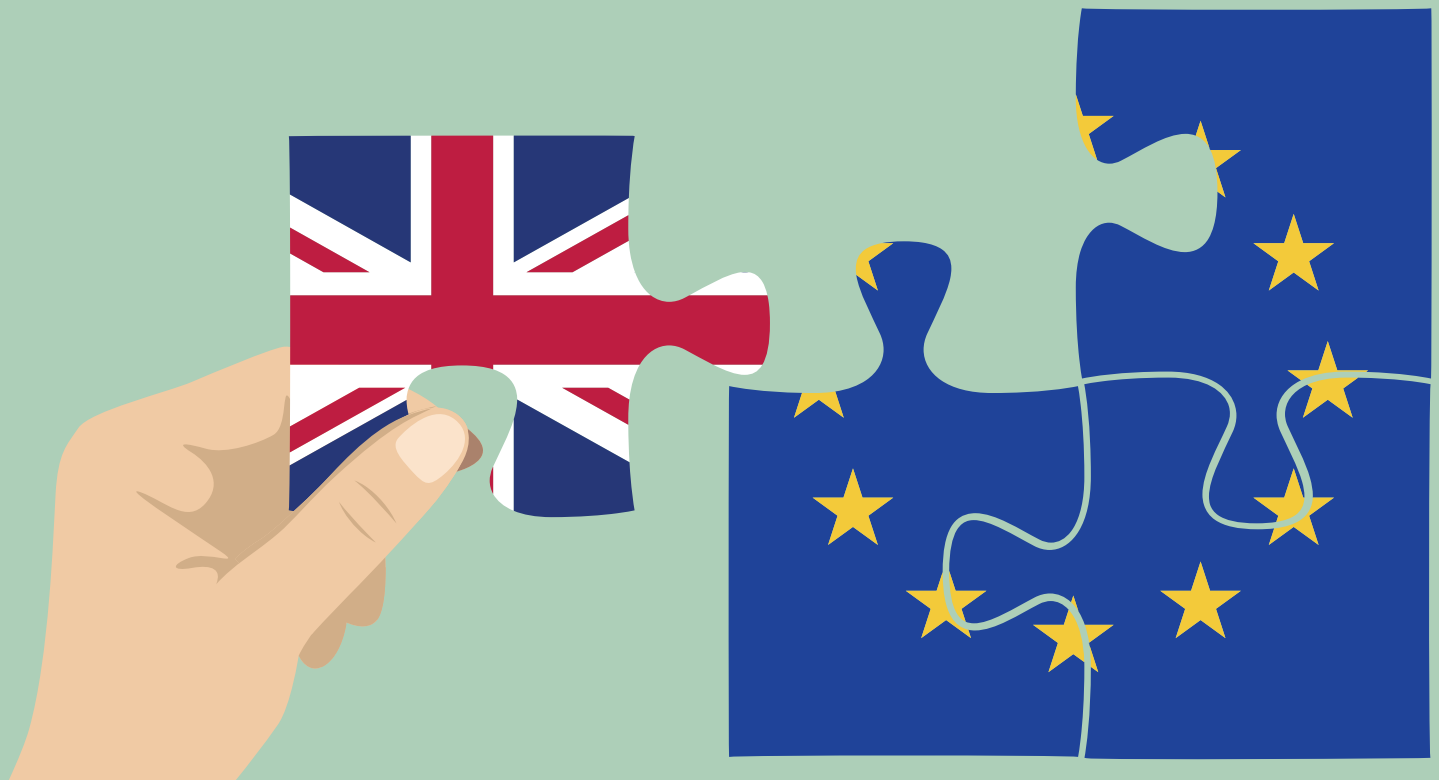
The ICO has a range of options available for investigating compliance, including requesting and reviewing supporting records from those that manage personal data, or physically visiting sites and inspecting premises. GDPR provides the ICO with significantly greater financial penalties for non-compliance or data breaches: maximum fines will rise from their current £500,000 limit to £17m (€20m), or 4% of global turnover – whichever is greater.

Getting GDPR wrong is not an option as these fines could bankrupt most businesses.

BUT WHAT ABOUT BREXIT?

Vuelio

Though plans for Brexit continue, the UK Government has made it clear that GDPR will become part of UK law from 25 May 2018, and equivalent data protection requirements will remain in force once the UK has exited the European Union. This is necessary to ensure consistency throughout Europe, where the Government has expressed wishes to retain strong trading links. GDPR also applies to organisations who interact with citizens of other EU countries, so even post-Brexit, GDPR's requirements will need to be understood and complied with.



WHAT DOES GDPR AFFECT?

GDPR applies to the handling and storing of any personal data, that could be used to directly or indirectly identify a person.

GDPR provides a wider definition of personal data than previously, which includes:

- Name
- Photo
- Email address
- Bank details
- Posts on social networking sites
- Medical information
- Computer IP address

Even data that has been 'pseudonymised' (which temporarily removes personal identifiers) remains in scope of the new regulation depending upon how easily the process can be reversed.

Like existing Data Protection regulation, GDPR refers to 'data controllers' and 'data processors'.

Controllers: You are a controller if you decide how data is collected, managed, stored, used and/or deleted. You have legal responsibility for the personal data you manage and you determine how it is to be lawfully processed.

Processors: You are a processor if you manage the data on behalf of controllers but do not determine its uses, purpose, collection or deletion. You are only complying with (legal) instruction from controllers.

If controllers need to use a data processor for part of their activities, they are required to choose carefully to ensure that such processors are 'demonstrably compliant' with GDPR. They will also need to provide such processors with written instructions relating to the data processing which is to be undertaken, and the processor is obliged to follow these.

Controllers

If you are a data controller, you are not relieved of your obligations under GDPR where you have engaged a data processor. You have obligations to ensure the data processor is GDPR compliant, and contractual clauses will need to be in place to record their responsibility to follow your data processing instructions.

Processors

If you are a data processor, acting on behalf of a data controller, be aware that GDPR places specific legal obligations on you. For example, you need to maintain full compliance with GDPR for your own organisation, with records that support the processing of personal data that you are undertaking. You will also have legal liability if you are responsible for a breach.

DOES THIS APPLY TO MY ORGANISATION?

Vuelio

If your organisation collects, manages, processes or stores personal data about individuals, then you will be responsible for complying with GDPR. Those who do not process personally identifiable information will be exempt, but as most companies process their employees' data for HR purposes, GDPR applies to nearly every organisation.

Personal information includes:

- Personal data contained within email messages (and attachments) and calendar invitations
- CRM systems, including lists of contacts and sales activities exported to other systems
- Marketing databases used for advertising your services and attracting new customers
- Customer correspondence, including enquiries, complaints and financial information
- Registration forms and delegate lists associated with events
- Most uses of social media (e.g. Facebook, Instagram, LinkedIn and Twitter)

INDIVIDUALS' RIGHTS UNDER GDPR

Vuelio

Data processing organisations need to be aware of several new and expanded rights that individuals have under GDPR:

- **Right of Access**: the right of an individual to request details of any of their personal data that is being processed or stored by an organisation
- **Right to Rectification**: the right of an individual to request the correction or completion of any personal data that is found not to be accurate
- **Right to Erasure**: the right of an individual to have their personal data deleted when it is no longer required, and there is no other legal basis for it to be retained
- **Right to Restriction of Processing**: the right of an individual to request a restriction of the continued processing of their personal data in specific circumstances
- **Right to Object**: the right of an individual to object to the processing of their personal data for specific activities, including direct marketing and automated profiling
- **Right to Data Portability**: the right of an individual to request that their personal data is extracted and sent to an alternative data processor, under certain circumstances

For each of these, it will be important to:

- Operate effective processes for each right, ensuring responses within 30 days
- Provide full training for your employees in managing rights requests
- Ensure that your supply chain is contractually obliged to support you in responding to requests
- Maintain full records to show the ICO that you are responding to requests

LEGAL BASIS FOR PROCESSING

GDPR mandates that the processing of personal data can only be undertaken when at least one of six criteria has been met. The most obvious choice for businesses already working with data is legitimate interests. It is not only the most flexible option – as it depends to some degree on a sound argument – but is also considerate of commercial needs.

The legitimate interests basis has three elements: identify a legitimate interest; show that processing is necessary to achieve it; and balance it against the individual's interests, rights and freedoms. Interests could be yours or those of a third party, and can benefit commercial needs, individuals or society more broadly.

Be warned though, the legitimate interest criteria, if used, requires you to take on extra responsibility for considering and protecting people's rights and interests (flexibility works both ways).

Other criteria include the fulfilment of a contract with a data subject, the organisation's need to report certain personal information for legislative and regulatory purposes (e.g. providing tax and welfare data to the relevant authorities), or explicit consent. GDPR has significantly enhanced the consent requirements that need to be met.

CONSENT CHECKLIST

Vuelio

If you choose to use consent as your basis for processing data, remember the following:

- Make the request for consent prominent and separate from terms and conditions
- Ask people to positively opt in
- Don't use pre-ticked boxes or any other type of default consent
- Use clear, plain language that is easy to understand
- Specify why you want the data and what you're going to do with it
- Give individual ('granular') options to consent separately to different purposes and types of processing
- Name the organisation and any third-party controllers who will be relying on the consent
- Tell individuals they can withdraw their consent
- Ensure that individuals can refuse to consent without detriment
- Avoid making consent a precondition of a service
- Ensure you're aware of vulnerable individuals, and take extra steps where necessary

Recording consent:

- Keep a record of when and how you got consent from the individual
- Keep a record of exactly what they were told at the time

Managing consent:

- Regularly review consents to check that neither the use of data nor relationship with the individual has changed
- Regularly refresh consent at appropriate intervals, including any parental consents
- Use privacy dashboards or other preference-management tools as a matter of good practice
- Make it easy for individuals to withdraw their consent at any time, and publicise how to do so
- Act on withdrawals of consent as soon as possible
- Don't penalise individuals who wish to withdraw consent

CONSENT CHECKLIST

Vuelio

Consent must be confirmed in words, to avoid ambiguity, rather than any other positive action (so no thumbs-up emojis). Once that consent is given, there is no time limit on how long it lasts – that depends on the reasons the data was collected. If something changes or the nature of the consent implies a limited use, then you'll have to ask for consent again.

Sometimes consent isn't possible, or fair, if the organisation will process the individual's data anyway. This may be in the case of an employer collecting their employee's data or a government agency carrying out their normal duties. In these situations, consent should not be sought as it would be misleading to think the individual had a choice.

Once consent is part of your processes then it should be easy for individuals to withdraw consent at any time. Preference-management tools, like simple forms that show people what they're signed up for and allow them to make changes, are an easy option for this.

WHAT ISN'T COVERED BY GDPR?

Vuelio

Not everything needs to abide by GDPR's rules. Exemptions are allowed when data processing is safeguarding:

- National or public security and defence
- The prevention, investigation, detection or prosecution of criminal offences
- Public interests, in particular economic or financial interests, including budgetary and taxation matters, public health, civil law and security
- The protection of judicial independence and proceedings
- Against breaches of ethics in regulated professions
- Monitoring and inspection of regulatory functions connected to the exercise of official authority regarding security, defence and other important public interests
- The protection of the individual, or the rights and freedoms of others

These exemptions also cover whistle-blowers and journalists who are protected so they can continue to hold organisations and governmental authorities to account.

Compliant comms software?

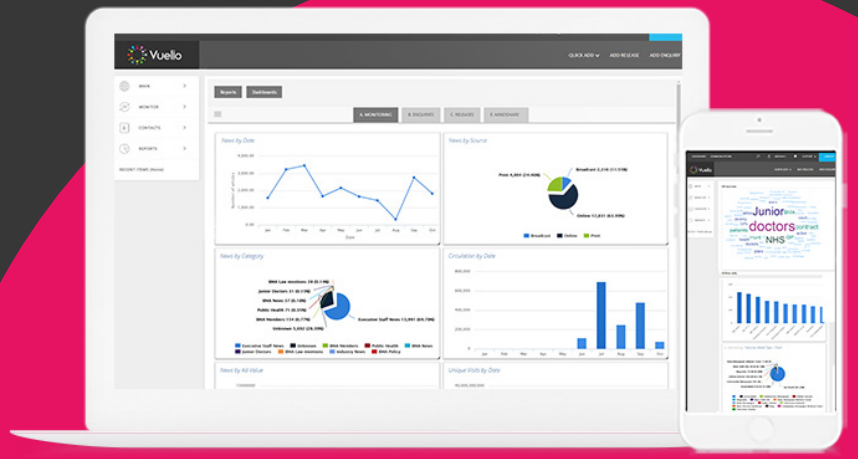
CONTROL YOUR COMMUNICATIONS WITH VUELIO

Make all your communications and data GDPR compliant with the Vuelio Integrated Communications Suite.

Log all your stakeholder interactions, access the world's largest media database, optimise press release distribution, monitor all your media, track parliament and political developments and measure your communications to understand the effectiveness of your campaigns, the strength of your brand, and the ROI of everything you do.

VUELIO INTEGRATED COMMS SOFTWARE ALLOWS YOU TO:

- Centralise all your engagements and stakeholder data to log, share and report stakeholder engagement activities, ensuring consistent communications that help maintain and improve crucial relationships and GDPR compliance
- Access the largest UK database of journalists, editors, bloggers and other media contacts, full of the information you need to succeed: names, numbers, profiles, pitching preferences, and pet hates - all in a GDPR compliant database
- Listen to what people are saying about your brand across millions of social, broadcast, print and online sources and track all of those conversations in one place



GET FREE DEMO

Or call us on

020 3426 4125

Vuelio