GDPR: What does it mean for business?

Brought to you by the Lead Forensics Knowledge Base

Compliance by design

LEAD FORENSICS

UK: 0207 206 7293
www.leadforensics.com

This guide will help you to:

- Understand how changes to GDPR will affect your business
- Ensure your business is fully compliant with new regulations
- Put processes in place to manage change and remain compliant
- Create a Sales and Marketing strategy that takes new laws into account

Contents

The new General Data Protection Regulation (GDPR) comes into force on 25th May 2018.

GDPR affects any business that holds or processes information about residents in the European Union. This is true, even if the business itself is based outside the EU.

About Lead Forensics

Lead Forensics is an example of marketing and sales enablement software trailblazing in a GDPR compliant environment. Lead Forensics identifies the visitors to an organisation's website, fueling marketing and sales team with the business related contact details of people actively interested in the products and services of their organisation.

Take a look for yourself with a free, no obligation trial:

GET STARTED

Introduction

GDPR – which stands for General Data Protection Regulation – was developed by the European Parliament, with the aim to strengthen data protection laws for individuals within the European Union. It is designed to simplify and unify data protection laws across all countries in the EU.

The regulation is enforceable from **25 May 2018**, at which point businesses need to ensure they are fully compliant, or they risk incurring hefty financial penalties. Far from being simply a tick box exercise, being compliant with GDPR may require a fundamental shift in business processes to adopt a compliance first mindset with well documented processes and structured reviews in place.

How does GDPR Affect Business?

GDPR affects any business that holds or processes personal information about residents of the European Union. This is true, even if the business itself is based outside the EU.

Following Brexit, the rules will still apply in the UK, with the government planning to introduce a data protection bill that will closely mirror GDPR and its requirements.

At the heart of GDPR is personal information, which is defined as any information that can be used to identify a person (directly or indirectly), including: name, identification number, address and personal IP address.

It also covers sensitive personal information, such as: genetic data, health, sex life, sexual orientation, religious & political views, mental, physiological, economic, cultural or social identities. Basically, anything that could put someone at risk of unlawful discrimination.

GDPR is likely to bring about a big change in the way some businesses collect, store and process information about individuals. When processing personal information, businesses must ensure:

- It is processed lawfully, fairly and in a transparent manner
- That data is only processed for a specified, explicit and legitimate purpose
- Any information held must be relevant to the specified purpose
- All data must be accurate and up to date
- No data is kept for longer than necessary
- Information is handled and processed in a way that maintains security
- There must be a 'lawful basis' for processing the data

Lawful Basis for Processing

A common misconception around GDPR is that it doesn't permit businesses to process personal data, or you may have heard that specifically you need 'consent' to process personal data. This is not strictly correct. The GDPR is there to protect and control the use of personal data, but it is not intended to hinder business or industry, the intention is to ensure businesses consider and protect the rights and freedoms of their data subjects.

Example: Consider the police force, they have a necessary requirement to process personal data in the interest of public safety, they of course could not seek consent from their data subjects before collecting and processing the data, otherwise it could compromise the case! GDPR applies across all industries and therefore, it is logical that there are actually six lawful basis that an organisation can collect, process and store data.

Under GDPR there are six lawful basis for processing:

- **Legitimate interests**
- **Consent for a specific purpose**
- **Contractual necessity**
- **Controller bound by legal obligation**
- **To protect vital interests**
- **Public interest or official duty**

The most relevant of these in a B2B sales and marketing environment is 'consent' and 'legitimate interests', we'll explore those a bit further, however, more information regarding all six lawful basis can be found at the ICO website.

1. Legitimate Interests

Legitimate interests is perhaps the most flexible lawful basis on which you may process personal data, and is likely to be the lawful basis that most marketing and sales teams will look to use in a B2B environment. With legitimate interests you may collect, process and store personal data, as long as you have considered and can prove that there is a legitimate interests (basically a good reason why). It is also important to show that you've balanced the use of 'legitimate interests' against the individual's rights and freedoms. You must also include full details of your legitimate interests in your public-facing privacy policy.

The ICO specifically mentions direct marketing as an area in which it could be deemed necessary to leverage legitimate interests, it mentions that the processing must be in a targeted and proportionate way of achieving your purpose, and the organisation should also consider whether there is another reasonable and less intrusive way to achieve the same result.

The ICO recommends conducting and documenting three tests when looking to leverage Legitimate Interests:

1. **Purpose test:** are you pursuing a legitimate interests?
2. **Necessity test**: is the processing necessary for that purpose?
3. **Balancing test:** do the individual's interests override the legitimate interests?

(source: ICO's Guide to General Data Protection Regulation)

Of the six lawful basis specified under GDPR, 'legitimate interests' is the most flexible. However, there are still some strict guidelines around its use.

Data can be processed in the legitimate interests of the data controller (or a third party) and that can include the personal or business interests of yourself or a third party. The key exception is where such interests are overridden by the interests or fundamental rights and freedoms of the data subject - especially if that subject is a child.

The process of direct marketing is detailed as a potential use of legitimate interests under GDPR, but this shouldn't mean it is taken as a free pass to do whatever you want. Processing under this basis places additional responsibility on the organisation to consider and protect each individual's rights and interests. Data processing must be proportionate, targeted, have the smallest possible impact on the individual and not require consent under the Privacy and Electronic Communications Regulations (PECR) which focuses on additional protection for consumers.

Here is a basic checklist of the type of questions that need to be considered:

- Have you identified a legitimate interests?
- What are you trying to achieve? Is this method necessary to get these results, or are there less intrusive methods available?
- What is the benefit of the data processing and what would be the impact if it didn't go ahead?
- Are the data subjects' rights being balanced correctly against your own?
- Is the data you are looking to process sensitive or private? Are you processing the data of children or vulnerable individuals?
- Have you included suitable safeguards to ensure the data is protected? (if not, what can you put in place to minimize impact and risk?)

In a nutshell, legitimate interests only applies if the processing you wish to carry out is deemed necessary. By this meaning it is proportionate, targeted and that the same result couldn't be achieved through any other, less intrusive means.

What is a Legitimate Interests Assessment?

If you decide to use legitimate interests as a lawful basis, then a Legitimate Interests Assessment (LIA) must be completed in all cases. A LIA is basically a risk assessment that aims to ensure you've gone through a comprehensive decision-making process and have balanced your own interests against those of the data subject. There isn't a standard format that you must follow, however you must clearly show that you have considered everything and can justify the outcome reached.

Your LIA must be constantly reviewed and updated whenever there are any significant changes in the nature, purpose or context of the processing you are undertaking, to ensure your new purpose still complies. If there is a conflict, it is still possible for your interests to prevail, as long as there is clear justification.

Remember to keep a record of all LIAs you complete, as you'll need to demonstrate compliance and to prove that you have fully weighed up personal interests and potential effects. This will be vital evidence, especially if a data subject is to complain or raise a query.

Your privacy policy must also include full details of the legitimate interests you wish to use. This must be written in clear, unambiguous language and explain exactly what your interests are.

2. Consent for a Specific Purpose

For consent to be used as the lawful basis, individuals must give their explicit consent (not assumed through a pre-ticked box etc) and positively opt-in for their data to be held and used. Here, you must always offer very specific options, so that you get separate consent for separate actions.

If services are being offered to children, then parental consent will be a requirement. In any cases where consent is difficult to obtain, you must look for a different lawful basis for your data processing.

If consent has been selected as the most appropriate lawful basis for processing data based upon a specific business requirement, the business must only leverage consent moving forward, it cannot revert to legitimate interests after seeking consent (if for example the business is not happy with the consent response rate). Once consent has been sought, consent must be the lawful basis for processing for that specific process on an ongoing basis. However, different lawful bases for processing can be deemed suitable for different business processes – specific to the business requirement and the differing data subjects.

Let's Get Specific – What is Personal Data?

Offering greater protection for personal data lies at the heart of the new regulation, so you need to understand what constitutes personal data under GDPR. As the processing of any personal data falls under its remit, organisations operating a B2B, B2C or business-to-employee models will all have the same obligations.

What is classed as personal data?

- **Identifying information** - This includes any information that can be used to identify a person (either directly or indirectly), including name, identification number, email address, bank details and an IP address, etc.
- **Sensitive personal information** - This includes genetic data, or information around health, sex life, sexual orientation, religious & political views, mental, physiological, economic, cultural or social identities. Basically, anything that could put someone at risk of unlawful discrimination.

GDPR and its Impact on Sales & Marketing

The good news is that operating a successful sales and marketing function is absolutely still possible under GDPR. The key is to ensure that data processes are fully considered with a compliance first mind set. To help, we've listed below some of the main considerations sales and marketing teams will need to comply with:

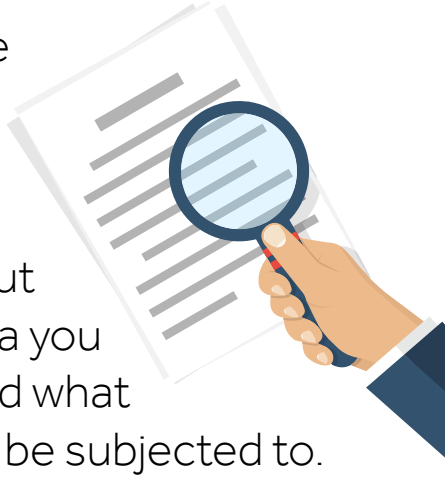
1. The right to be informed

Every business should publish a clear privacy policy, which is written in plain and simple language that can be easily understood. You must ensure you provide individuals with detailed information about exactly what data you are gathering and what processing it will be subjected to. You also need to be able to answer direct questions from individuals, as to exactly how you are using this data and what you hold. Under GDPR, you must never use jargon to confuse people over issues of intent. Any information provided must be unambiguous, clear and simple.

2. The right of access

Data subjects can request a full copy of the information your business holds about them at any time. You are obliged to provide this in a commonly used electronic format and this must be provided within 30 days of receiving the request. Whilst you have the right to refuse any requests that are deemed deliberately unfounded or excessive (particularly if they're repetitive or in quick succession), you must tell them you are doing so within one month, and at the same time informing them of their right to complain to the supervisory authority or take legal action.

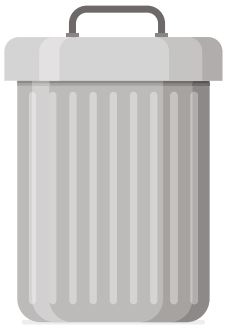
You must ensure you provide individuals with detailed information about exactly what data you are gathering and what processing it will be subjected to.



3. The right of rectification

If at any point an individual finds the information you hold on them is incomplete or incorrect, then they can request that you rectify it. These changes must be made within one month.

4. The right to erasure



The individual has a right to have their personally identifiable information deleted completely from your system on request. This is also known as the 'right to be forgotten'. It is important to know the difference between erasure and opt out. In order to opt out, your organisation will need to retain some personally identifiable information. For example in email marketing, to ensure suppression of opt outs organisations will have to keep a database of all email addresses that do not wish to receive email communication. If a request for erasure is received, the data subject is effectively asking for all data that is held to be removed - including any data held on suppression files. This means that in the future, erased data could potentially be gathered again if appropriate, however if the customer requests contact to be suppressed, the business should ensure they're in a position to do so and ensure no future correspondence is received. Organisations should look to manage the expectations of requests to ensure that the data subjects understand the difference between erasure and suppression.

5. The right to restrict processing

An individual can object to you processing their data for any task they wish. While you must abide by their wishes, you can continue to hold data that does not conflict with their request. An example of this would be in email marketing when a person requests to opt out.

6. The right to data portability

If someone has willingly provided their information to you, they also have the right to request that you transfer this data to another organisation, in a standard electronic format. If this service is requested, you must comply within one month, free of charge.

7. The right to object

Individuals have the right to object to any form of data processing and marketing, at any point, including to retract consent they have previously given.

8. Right to object to automated decision making

To protect individuals from potentially damaging decisions being made by automated systems, users can request the manual intervention of a human. Any systems you currently have need to be updated, to allow cases to be referred to decision makers that can speak to the user directly in the case of a dispute.

In summary, individuals are being given far greater control over their data and the onus is on organisations to ensure these rights are met in a timely manner (typically being one calendar month from the date of a request).

Individuals are being given far greater control over their data and the onus is on organisations to ensure these rights are met in a timely manner

GDPR Compliant Email Marketing

In the B2B world, marketers will be able to leverage 'consent' or 'legitimate interest' as a lawful basis for processing. Emails that target a B2B audience and which leverage a segmented target database are likely to be able to leverage 'legitimate interests' as the reason for collecting and processing data.

For example, if an organisation sells HR Software, and sends an email about the HR software to HR Managers at their business email address, it could be feasible that the recipient would be interested in the software based upon their current job role, which could be deemed as a legitimate interest.

Never conceal your identity, always clearly display the contents of the message and provide information to withdraw consent easily.

If however, that same HR Manager becomes the Sales Manager, the individual is unlikely to still be interested in HR software and therefore the need for businesses to keep data up-to date and current is critical.

Regardless of who you're sending your email to, you must never conceal your identity and must always clearly identify the marketing context of the message itself. Each email or message needs to provide clear information about how to withdraw consent, which must be simple to do.

The Opportunity Presented by GDPR

At first glance, these new rules may seem like a headache for marketers, but it's not all doom and gloom. The reality is, marketing will adopt a data first mentality, and the importance of safeguarding the interests of the data subjects will be front of mind - which can only be a good thing!

Adopting a more segmented, relevant approach to marketing will produce better results, whilst protecting the people's data at the same time.

Marketers will be encouraged to think about how they are handling data, what they are using it for and why they are using it. And, should look to document their thought processes and rationale in extensive policy documentation to show effective due diligence. It is right that marketers adopt a more segmented, relevant approach to marketing - which should in turn actually yield a better overall result for the business whilst protecting the rights and freedoms of the data subjects at the same time. A double bonus.

Will GDPR Kill Off Sales?

GDPR doesn't mean the end of sales!

Like marketing teams, sales team should be looking to take a highly targeted, segmented approach contacting only those that have either consented to receive sales correspondence or those that are likely to have a well thought out legitimate interest in the product or services being sold.

Sales professionals need to take heed of the right to withdraw consent, and therefore an effective CRM system is a must to ensure that sales professionals can centrally log a withdraw request from a data subject.

Sales professionals need to take heed of the right to withdraw consent, and therefore an effective CRM system is a must to ensure that sales professionals can centrally log a withdraw request from a data subject.

A New Sales and Marketing Strategy

Under GDPR control is put even more so into the hands of the individual - and rightly so. Therefore, organisations looking to overhaul their Sales and Marketing strategies as a result of GDPR should be considering:

- An effective CRM system
- How leads are procured

Lead Forensics is an example of marketing and sales enablement software trailblazing in a GDPR compliant environment. Lead Forensics identifies the visitors to an organisation's website, fuelling marketing and sales teams with the business related contact details of people actively interested in the products and services of their organisation. Businesses can operate a marketing and sales function safe in the knowledge that their leads have proactively visited the business website - how much more of a legitimate interest could there be, than someone perusing a company website?

Lead Forensics is currently offering a complimentary trial of the market leading software - request your demonstration and complimentary trial here.

While it's true that GDPR is likely to impact many businesses and how they currently operate, it also presents a great opportunity to bolster inbound marketing campaigns – a strategy that can bring new customers to you in a manner which complies perfectly with the new regulations.

Disclaimer: The information contained within this guide is not intended to be legal advice and should not be seen as a recommendation of any particular legal understanding in relation to GDPR compliance. It is simply an overview of the EU data privacy laws and some of the key issues that certain businesses may need to address. It should not be thought of or relied upon as legal advice. If you are at all unsure, then always seek the advice of an experienced legal team, who will be able to advise you in detail about your individual circumstances.

Further information with regard to GDPR, including the full GDPR regulation can be found on the ICO website.

GDPR Compliant Lead Generation. Take the free demo and trial today...

Uncover who your anonymous website visitors are, identify when they're ready to buy and access the contact details you need whilst being GDPR compliant.

By being your efficient central hub for website visitor intelligence, lead generation and marketing insight, LeadForensics will give you all the data you need to convert high quality leads faster. Imagine if you could take control of your lead generation activity, then nurture and convert your prospects before your competitors even get close.

Experience turbo-charged GDPR compliant lead generation with a free demo and trial today.

Experience turbo-charged lead generation with a free demo and trial today:

GET STARTED

020 7206 7293

www.leadforensics.com