KashFlow

The Small Business Guide to GDPR

On 25 May 2018, the General Data Protection Regulations will replace the Data Protection Act 1998. If you handle any form of personal data, then this will affect your business. It's therefore essential that you effectively prepare.

5 things you need to know

1. The General Data Protection Regulation (GDPR) is replacing the Data Protection Act 1998 from **25th May 2018**.

2. The GDPR's main aims are to **simplify and unify data protection laws** across the EU and UK, and to give citizens and UK/EU residents more control over their **personal data**.

3. The Regulation will **apply to any company processing the personal data of individuals in the EU** in relation to offering goods and services, or else to monitor their behaviour.

5. Significant penalties can be imposed on employers who breach the GDPR, including **fines of up to €20 million or 4% of the businesses annual turnover**, whichever is greater.

6. The level of fine will depend upon the type of breach and any mitigating factors, but they are designed to strongly penalise anyone who shows a disregard for the GDPR.

Will Brexit affect GDPR?

The short answer is: no.

The GDPR will continue to apply to UK businesses for now, regardless of Brexit. The Government has signalled that even if it did drop the GDPR, it'd replace with legislation that mirrored it anyway. The UK was one of the key driving forces behind the creation of GDPR - it's therefore unlikely that it'll be replaced with something drastically different even if the UK does change it.

Any business dealing with EU citizens will legally still have to comply with the GDPR regardless of where they are based in the world.

Gathering data under the GDPR

Under the GDPR, there'll be a few changes to the way you can collect data from individuals...

What types of data are there?

There are two main types of data specified in the GDPR. For each, you'll have to demonstrate an understanding of what they are, what you hold, where this information is coming from, what it's being used for and where it's going.

Personal

Names

Addresses

Emails

Bank details

Photos

IP addresses

Sensitive

Health details

Religious views

Marital status

Sexuality

Trade union activities

Details of criminal offences

With sensitive data, the consent given must be more explicit and the reasons for collecting it in the first place must be clearer.

Securing consent

GDPR clearly states that you need "specific, informed and unambiguous" consent to hold data on individuals. This likely means any proof of consent you currently have will need rewriting to ensure it clearly states what data is being collected and why.

Fair processing

To ensure data is fairly processed, you'll need to give people clear information about what you're doing with that data. Following these steps will help keep you compliant:

1. ***Tell them why you're processing their personal data and the legal basis you have for doing so (e.g. they've given their consent).***

2. ***Describe the type of recipients you may be sharing this information with, such as customers, employees, subcontractors or suppliers.***

3. ***Say how long you'll be holding this data (called the retention period).***

Handling data under the GDPR

The way you handle and use data will also change, for example...

You can only use data for its intended purpose

Under the GDPR, you can process data if it's compliant with the original reason for collection – e.g. emailing a customer on your mailing list. But you won't be allowed to use this data for any other purpose, such as providing their details to third parties or using it for additional purposes.

Individuals have the right to be forgotten

Individuals will have more say in how your business uses their data. They'll now have the "right to be forgotten" where you'll have to delete all record of them if there's no contradicting legal grounds (for example, they're no longer a customer so your contract doesn't give you the legal right to keep their data).

You can't keep data forever

The GDPR state that you should only hold on to data for as long as is necessary. So if you're still keeping the contact details of customers that don't have existing contracts with you anymore, you'll need to sort through your records.

Note that consent might not be required for pre-existing data if you have a legal basis for keeping it that's compliant with the existing Data Protection Act. E.g. keeping the contact details of existing customers so that they can be invoiced for goods and services rendered.

Similarly if you want to keep their data – say it's a subcontractor you want stay in touch with about future work opportunities – then you'll need their specific consent. Again, look at HR software or other management systems if your current setup doesn't allow you to recall and permanently delete data.

You'll have to respond to access requests

Individuals will be able to request a free copy of the data you have on them, correct any inaccuracies, object to how it is processed in certain circumstances or ask for it to be completely delated. These demands must be dealt with **within a month** of the request date.

10 steps your business can take to prepare for GDPR

1. Read as much as you can on the subject. You and your team will need to fully understand the terms of GDPR, how it will affect policies and procedures for recruitment, the course of employment and the way in which contracts are terminated.

2. Make note of all the personal data you have, where it came from and who it is currently shared with. In order to do this, you may need to perform an information audit.

3. Review your current privacy policy and make sure it fits the GDPR. This will include making sure you have a lawful reason for processing personal data and that this is reflected in your policy.

4. Make sure your current system covers all of the rights individuals will have under the GDPR. You should also communicate these rights, and any changes to your system, with every employee.

5. When dealing with Subject Access Requests, make sure your employees can freely access their data and update it where necessary.

6. Your current system will need updating if it doesn't offer individuals to the chance to look up, record and manage consent to any changes in their personal data. This is covered by the **Read & Accept** feature in KashFlow HR Plus.

7. Ensure you IT systems are all up to date and include a way to comprehensively delete data. This will be essential once individuals have the "right to be forgotten".

8. Familiarise yourself with ICO's code of practice on Privacy Impact Assessments. You should also look at Article 29 Working Party's latest guidance. These cover Data Protection by Design and Data Protection Impact Assessments, as specified by GDPR.

9. You'll need to assign a Data Protection Officer, who will take responsibility for data protection compliance. Whether this become a formal role, and where it sits within your company, is a decision you will have to make.

10. Make sure you have the right measures in place to deal with data breaches. You will need to detect them, report on them and carry out further investigation where necessary.

What if you're an employer?

Under the Data Protection Act 1998, employers are required to provide employees and job applicants with a privacy notice, setting out certain information. Under the terms of the GDPR, employers might now need to provide more detailed information.

1. Employers might now need to provide more detailed information, such as how long personal data will be stored for
2. Should data potentially be transferred to different countries, employees will need to be informed
3. Subject access requests (SAR), where individuals request their personal data, are changing. It'll be free to make a request, and any info should be available electronically
4. All employees will have the right to have personal data deleted or rectified in specific circumstances The GDPR will also impose a mandatory breach reporting requirement. This means employers will have to notify and provide key information to the data protection authority within 72 hours of any breach.

Note: the standard consent clause in most contracts may not be specific enough for the GDPR, so you may have to provide new contracts with updating wording.

How KashFlow HR can help

Secure Access Requests GDPR aims to give the individual better control over their personal data. With KashFlow HR, controlling your employee's data couldn't be easier. The software includes employee self-service, which grant employees 24/7 access to their personal data; and other supplementary information. KashFlow HR gives employees access to all their data. It also allows you to set permissions so they can update, or just view, based on their needs.

Securing consent KashFlow HR Plus includes "Read & Accept" which, it can also be accessed from anywhere - meaning employees can check their personal information and make approvals even when they're not in the office.

Secure storage While not part of GDPR law, it's important that all personal data is securely stored. Using cloud software means you're not relying on a potential insecure cabinet in the corner of your office. Everything is kept online and accessible from anywhere.

How have KashFlow been preparing?

In recognition of the level of work needed to align our current practices and policies with the new rules and requirements, KashFlow have been preparing for the anticipated changes for some time. We have the highest confidence in our ability to support all customers in meeting their new responsibilities under the terms of GDPR.

During the last few months, KashFlow has been carrying out a full GDPR product compliance analysis and risk-assessment. All data processing documentation that will be relevant to the new Regulation will also be fully updated in advance. We are taking three key steps to achieve this:

1. Documenting all current processes and data flows, and analysing any potential areas of weakness or vulnerability across our whole cloud product portfolio. This enables us, to pinpoint areas ripe for improvement in advance of the GDPR deadline, and to take swift and positive action to make improvements.

2. Carrying out a detailed 'gap analysis.' This is extremely helpful in identifying our overall level of compliancy ahead of the introduction of the Regulation, as well as allowing us to detect areas needing improvement in our product offering.

3. Conducting risk assessments to identify where any additional security measures may need to be implemented within the KashFlow software, and whether any other key GDPR compliance requirements are necessary prior to the Regulation's introduction.

The KashFlow promise to you

Any extra product functionality required by GDPR will be fully implemented into KashFlow software prior to the 25th May 2018 commencement date. All customers will be kept fully informed of any significant changes that may be necessary to your software's service provision due to the new legal requirements.

How KashFlow can help you prepare

The GDPR will affect businesses of all size, therefore it's essential that you're compliant – even if you're a sole trader.

Fortunately, using business software like the Accounting, Payroll and HR software provided by KashFlow, means that you're adopting technology that can help make compliancy easier to achieve.

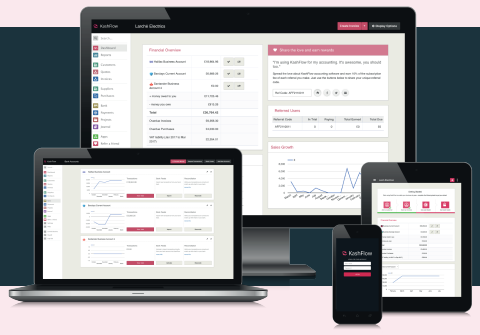
It's easy to edit ✓

It's your responsibility to make sure data is accurate and, where possible, up-to-date. With our cloud software, any amends you make are synced using Real Time Information (RTI) so you're always working with the most up-to-date data, even if you're working across multiple devices.

It's secure ✓

Data security is central to GDPR-compliance, so it's essential that you take all necessary steps to keep your data safe. Data encryption is a highly-recommended way of keeping your data safe,

KashFlow's cloud software offers the same level of security as internet banking, with data stored on a central server and supported with secure backup servers. This leaves no trace of financial data on company computers, so if your device gets misplaced or stolen, your data remains safe.



Our software also offers:

- ***Multi-factor authentication options***
- ***HTTPS on all app pages***
- ***Encryption of sensitive data at rest***
- ***Certification to PCI DSS***

It includes an audit trail ✓

We've recently introduced Additional User functions to KashFlow, which includes an Audit Trial that helps you track who's done what and when. This can help with the "integrity and confidentiality" section of the GDPR, which state that "appropriate technical and organisational measures against unauthorised or unlawful processing, loss damage or destruction" are made.

It keeps everything at your fingertips ✓

Meeting the one-month timeframe on access requests will be easier when your customer or employee data is stored in one digital space. With KashFlow Payroll and HR, employees can access their payslips and other data through 24/7 Self-Service – lowering the administrative burden on you.

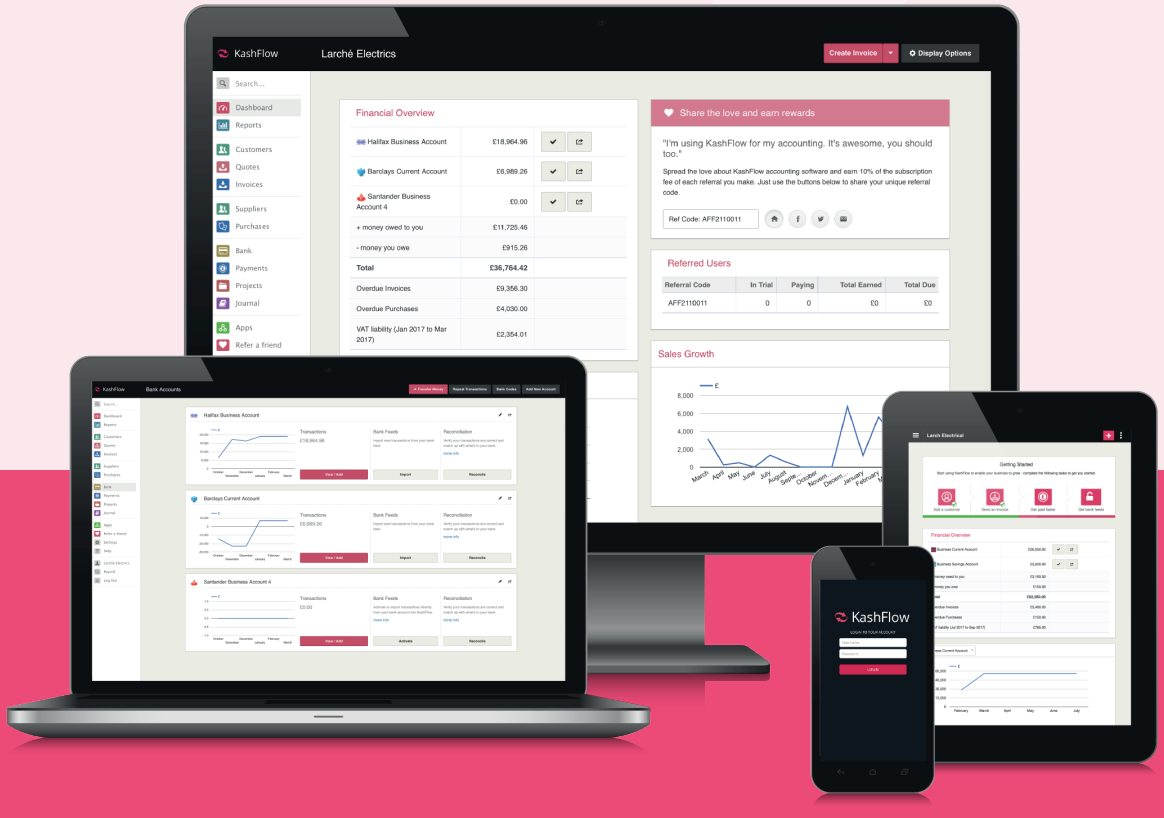
About KashFlow

This guide to getting paid faster was brought to you by KashFlow – specialists in straightforward accounting software for sole traders, contractors & small business owners across the UK.

Over **57,000** time-strapped business owner-operators use our **Accounting software** to stay in control of their accounts, get paid faster and make sure they're tax compliant. And as a small business takes on its first employees, KashFlow **Payroll** and **HR** are there to support too.

Started, grown and still based in the UK, we experience the same changes, challenges and legal compliance UK businesses face first-hand – and from that, we've built software that makes it all easy.

Want to try us out for free? Sign up for trial today to see where we can take you.



Take a FREE trial