GDPR explained

what does it mean for benefits?

summary

- GDPR is the updated data protection law coming into force in May 2018
- All organisations (including sole traders, public services and charities) have obligations
- There are stricter penalties in place for non-compliance
- 'Data' means any number, email address, IP address or other information that can signify an individual
- Data subjects have enhanced rights.

Read our blog for more background on GDPR
https://caboodle-technology.co.uk/gdpr-mean-benefits/

responsibility for benefits data

Under GDPR, there are two types of responsibility for data: data **controller** and/or data **processor**.

The Information Commissioners Office (ICO) describes these:

- Controller determines the purposes and means of processing personal data
- A processor is responsible for processing personal data on behalf of a controller.

Your organisation is likely to be controller of certain activities (such as benefits data) but could also be a processor if your business provides services for another organisation. You will need to establish which activities you perform and whether you are controller or processor of these.

Both controllers and processors have obligations under GDPR. Controllers must make sure processors only act on their written instructions in the 'purposes and means' of processing the personal data. Processors must also demonstrate that they are compliant with the new law.

To offer your workforce benefits, you will act as data controller when you process their data for benefit applications and to administer payroll. This means that GDPR applies to benefits as well as any other data processing activities.

changes to current law

GDPR enhances what's in place already, but there are changes you must be aware of.

The main points are:

- **Accountability**

  You need to demonstrate your compliance with GDPR in a tangible way. Contracts for services where third parties ('processors') process personal information (including for processing your benefits), documenting your data processing activities and completing Privacy Impact Assessments when using new technologies or where the risk of disclosure of personal information is high are a must.

  You must maintain records of data processing, assess the impact of your processing and make sure any online systems you use to process personal information are secure.

  Identifying and documenting the who, what, why, where and how of your data processing activities is a really good way to start.

  Once you've documented your data processing activities, get rid of any that aren't essential and put a written policy in place to show you've identified the data you use and how you use it.

  In short, documented evidence is key to achieving compliance.

- **Lawful reason**

  You must have a lawful reason for processing personal information if you're a data controller. The time to decide on your lawful reason for processing is now.

  Once you've completed your list of data processing activities, decide your legal basis for processing for each activity.

  One of the following must apply:

  - **You've received explicit consent**

    Auto-selected tick-boxes, or opt-out messages, are a big no-no. If you currently use these mechanisms to market to your customers, be aware that data subjects must proactively and unambiguously opt-in to receive any marketing information and that you must only send them information about what they've agreed to receive.

    Under the ePrivacy Regulations, users must explicitly sign up to the use of their data including receiving marketing and the use of third-party software such as Google Analytics.

    You will need to decide if using consent as the lawful reason for processing employee benefits information is the right basis for you.

- **Necessary for the performance of a contract**

  The ICO say this basis applies where:

  > *You have a contract with the individual and you need to process their personal data to comply with your obligations under the contract*
  >
  > *You haven't yet got a contract with the individual, but they have asked you to do something as a first step (eg provide a quote) and you need to process their personal data to do what they ask*

  Guidance published by the ICO states you can process data under this legal basis to fulfill your obligations under an employment contract.

- **Necessary for legal obligation**

  You will be obliged to process some personal information according to additional legislation in employment, social security and social protection.

- **Three other lawful bases are:**

  - **Necessary to protect vital interests**

    Where processing is necessary to protect someone's life

  - **Task carried out in the public interest**

    This will mostly apply to UK public authorities

  - **Legitimate interests -The ICO say:**

    > *"If you are a private-sector organisation, you can process personal data without consent if you have a genuine and legitimate reason (including commercial benefit), unless this is outweighed by harm to the individual's rights and interests.*
    >
    > *Legitimate interests is the most flexible lawful basis, but you cannot assume it will always be appropriate for all of your processing.*
    >
    > *If you choose to rely on legitimate interests, you take on extra responsibility for ensuring people's rights and interests are fully considered and protected.*
    >
    > *Legitimate interests is most likely to be an appropriate basis where you use data in ways that people would reasonably expect and that have a minimal privacy impact. Where there is an impact on individuals, it may still apply if you can show there is an even more compelling benefit to the processing and the impact is justified."*

There are other things to consider for processing according to legitimate interests. You must prove that this basis applies and conduct a legitimate interests assessment (similar to a risk assessment) for each data processing activity to prove it's the most appropriate basis for your processing. There are templates to complete this assessment online, and the ICO provide full guidance on their website.

deciding your legal reason for processing benefits data

You may decide that if you offer Employee Benefits as part of your contract terms, then your lawful basis for processing information is 'necessary for the performance of a contract'.

Some argue that the legal basis for processing benefits data is performance of the contract of employment under which employee benefits are a term, other articles say that this is no longer valid under GDPR because of its heavy weighting in favour of employers and that another legal basis should be considered instead.

myth: I must rely on consent to process data

There are five other legal bases for processing data. What's important is that you select the right basis for you.

The Information Commissioner's Office (ICO) have published guidance on consent. This explains the other rights people will have when processing is based on consent.

Examples:

The ability to withdraw their consent at any time, the right to erasure (also known as 'the right to be forgotten'). Where an individual can request the deletion or removal of personal data where there is no compelling reason for its continued processing.

The right to data portability, which allows individuals to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, "without hindrance to usability" (such as an Excel spreadsheet that the data subject can download themselves or that can be sent to them in a secure manner).

The ICO advise that:

"Consent is one lawful basis for processing, but there are alternatives. If consent is difficult, you should consider using an alternative basis."

If you are not sure which lawful basis to proceed with, seek legal guidance or call the ICO helpline.

being clear about benefits data

Transparency

You must tell data subjects exactly what you do with their information.

Ask yourself:

- Why is personal data processed?
- Whose personal data is processed?
- What personal data is processed?
- When is personal data processed?
- Where is personal data processed?
- Who will it be shared with, and why?

Once you've identified these scenarios, decide which are the highest risk and which you may need to put extra protection in place for. You'll then need to write a statement that explains your processing activities and include it somewhere it can easily be seen – your online privacy statement is the perfect place, but make sure it's not hidden in the footer. You can also set this information out in a letter, fair processing notice or contract appendix. Make sure the information is clear, easy to understand and include contact details for someone at your organisation data subjects can use to obtain information about how their data is processed.

You also need to ensure you keep all your personal information up to date, and data subjects have a right to correct any information being processed that's inaccurate. If you're sending information to a third party to provide your benefits, they will need to receive any updated information, too.

Data subjects can ask for information on how you obtain, process, store or otherwise use their data. This is called a Subject Access Request. You must respond to these within one month with the requested information.

myth: I need a data protection officer

The ICO tell us that all public sector organisations processing personal data, any carrying out large scale systematic monitoring of individuals (for example, online behaviour tracking) or any completing large scale processing of special categories of data or data relating to criminal convictions and offences must appoint a Data Protection Officer (DPO).
There is no requirement to appoint a DPO for other processing activities.

However, you may wish to consider assigning resource to deal with data protection administration, but this doesn't have to be a designated DPO. It may be appropriate to assign these responsibilities to each team leader, or to an administration department.

data transfer

You can't transfer data outside of the EU unless the organisation you're transferring to are complaint with GDPR - and that includes hosting firms. Some non-EU organisations have looked ahead to put additional approved certificates in place like Privacy Shield. Always carry out your own checks for compliance on a case-by-case basis.

You also can't share data with other organisations (such as suppliers) without first making sure they are compliant with GDPR. Standard contract terms should be updated to include the right to audit and to help monitor supplier compliance. There's a checklist on the ICO website here that shows what to include. Always make sure you obtain professional advice for contracts if you are not sure.

breach notification

Do you have a system in place to recognise and analyse data breaches?

It's a requirement under GDPR to report certain breaches within 72 hours of them happening to the ICO, and if you think the breach will have a significantly detrimental impact on individuals, you must also inform those who have been affected.

First of all, you need to easily work out which types of breaches the ICO need to hear about. Having a system where you can categorise and risk assess breaches will help you in deciding which breaches have "adversely affect[ed] individuals' rights and freedoms" that you need to report immediately to the ICO.

You must retain records of all breaches, regardless of the level of detriment to the data subject.

myth: It won't matter after Brexit

After Brexit, GDPR is effective if you deal with businesses with data subjects in the EU, and here in the UK, GDPR will be copied into UK domestic law under the EU Withdrawal Bill and be known as the UK Data Protection Bill. Whichever way you look at it, GDPR applies to your business if you process personal information.

Caboodle and GDPR

Salary Extras from caboodle is a safe, secure, online solution for your employee benefits. We're proud of our ISO27001 certification, which demonstrates excellence in Information Security standards.

Security isn't just about applying the latest security technology to our expertly built and tested benefits and engagement platform. Being certified requires rigorous review and maintenance of all working practices, from data transfer to call handling, to ensure they are secure and robust.

We've implemented processes and procedures so that we know caboodle employees are working to the highest security and data protection standards. Our processes and procedures are defined by risk assessment, delivered with training, monitored for effectiveness and externally audited by experts.

As well as ensuring compliance with our security system, the dedicated caboodle security team make sure the company are compliant with laws and regulations. Of course, being ISO27001 certified means we're already practicing the best data protection model for our business. By May 2018, we'll have attended and delivered training, mapped data and updated our processes and contracts to ensure we're compliant.

For more information on Salary Extras, get in touch with one of the friendly caboodle team today.

This whitepaper uses information from the ICO, the independent regulatory body of data protection and privacy laws in the UK. See ico.org.uk for more information.
The information in this paper is for guidance only and is not and shall not constitute legal advice. Consult a professional adviser or solicitor for advice on your responsibilities.