GDPR FAQs

Section 1: Introducing GDPR

What is GDPR?

GDPR stands for General Data Protection Regulation. It replaces, but builds on the current Data Protection Act and means we'll have to act even more carefully when it comes to collecting, using, storing, deleting and sharing personal data belonging to our colleagues, members and customers.

When does it come into force?

25 May 2018

Who does it affect?

Every organisation that processes Personal Data.

Why did the Data Protection Act need to be replaced?

The 'Data Protection Act' is the law used in the UK, but it's based on a European Law called the 'Data Protection Directive'. The Directive is being replaced by the GDPR, and therefore our own law has to fall in line with that. The aims of bringing GDPR in are:

- Create a consistent law across Europe, so that it's easier for the countries within Europe to exchange information with each other and so that non-European countries find it easier to deal with European Countries.
- Modernise the law - Many changes (especially changes in technology) have happened since the Data Protection Act was introduced in 1998, and the Law needed to be updated the reflect this.
- Give individuals stronger rights in relation to their personal information. This will help to build trust between individuals and organisations.

But we're going to leave Europe, why do we need to use their law?

As the UK will still be part of the EU in May 2018, the changes to the law will apply to us and we must be ready. Also, at Co-op, we've already said publically that we want to be 'trusted with data', so we want to process personal information in the best way possible, and GDPR will help us to do this.

The UK Government has also made a commitment to reach and maintain the high standards introduced by the GDPR, and currently has a bill before Parliament that will mean we'll adopt the requirements of GDPR.

What are the key changes?

Area of change	What the change means
Fines	This is a big change. Under the Data Protection Act, companies can be fined up to £500,000 for a significant breach of the Act. Under GDPR, companies can receive fines of up to 4% (dependent on the type of breach) of annual worldwide turnover. For Co-op, 4% would be £377 million!
Definitions	'Personal data' now also covers IP addresses, cookies and location information. 'Sensitive personal data' (called 'Special Categories' under GDPR) will now also include biometric and genetic data. The definition of a child has now been changed to mean anyone under the age of 13 - so we must check our processes for anywhere that we may capture children's information.

Individuals Rights	Subject Access Requests: Under DPA if an individual wants copies of information we hold about them, we have 40 calendar days to respond and can charge a £10 fee. Under GDPR we'll have 1 month to respond and there'll be no fee. Right to Erasure: This means individuals can ask for information held about them to be deleted. If we won't delete it, we'd need a good reason why not. Again, our systems must be set up to delete information where a decision is made to do this. Right to portability: This means individuals can ask us to extract their information electronically so that it can be given to another organisation. We need our systems to be set up in a way so that this can easily be done.
Consent	Under GDPR, there is an explicit requirement that organisations must be able to provide evidence of consent. Our processes and systems must be set up to collect and record this consent clearly. There's also a clearer definition of consent in GDPR, with a very high standard, so we must check that the ways we currently collect consent reflect this. Consent means offering individuals real choice and control. Genuine consent should put individuals in charge, build trust and engagement, and enhance our reputation.
Privacy by Design	At the point of introducing new processes or systems where personal information is involved, we'll need to think carefully about how they're designed so that the information being processed is appropriate, and doesn't intrude on the privacy of the individuals whose information is involved. For 'risky processing' (risky means: high volumes of information, sensitive information, or information which will have a big impact on the individuals involved), it will be mandatory to complete a 'Data Protection Impact Assessment' (DPIA). A DPIA is a process to help us identify and minimise the data protection risks of a project, process or system.
Data Breach notification	Under GDPR, all organisations must report data breaches to the Information Commissioner's Office (ICO) within 72 hours or 'without undue delay' unless we are satisfied that there is little risk to individuals' rights and freedoms. So we need everyone to know what to do if they spot a data breach. We have already updated our processes to investigate incidents quickly (including notifying the ICO where required). If you suspect something is wrong call the Information Incident hotline on **0844 262 9990.**
Data Processors	Data Processors are other companies that we use to process personal information for us e.g. a third party company who mails out member promotions for us will need access to some of the personal data we hold. Under GDPR, if the loss/misuse is their fault, then they may be found responsible and action taken against them instead. So we must make sure the contracts and agreements we have with these third parties reflect that.
Accountability	GDPR places more accountability onto organisations. We need to understand what information we hold, why we hold it, who we share it with, how we store it etc. To do this, we must have comprehensive documentation evidencing our processes.

What is classed as personal data? Where can I find a full comprehensive list?

Personal data is any information that relates to or identifies a person or lets you pick that person out of a crowd, even if you don't know their name. This could include a name, address, date of birth – literally anything that allows an individual to be potentially identified.

Is there a time limit on how long we can hold personal data for?

Not as such. What the law says is that you have to know the reason you have personal data, and when you no longer need it, you must delete or destroy it. Each part of the business has retention schedules to help us comply with the law.

What happens if we get GDPR wrong?

Under the Data Protection Act, Co-op can be fined up to £500,000 for a breach of the Act. Under GDPR, the Co-op could be fined up to 4% of our annual turnover (almost £400m) – a massive increase!

- Depending on the information lost, our customers/Members/colleagues could suffer financial loss or distress, and lose trust in us.
- Others could claim compensation from us.
- Our reputation could be damaged, resulting in less people buying products/services from us.
- The regulator can also force us to stop handling personal data in a particular way, which could have a really serious impact on the business

Any of these would affect our ability to deliver our Stronger Co-op, Stronger Communities ambition.

Section 2: Co-op and GDPR

How are Co-op protecting our customers' colleagues' and members' information?

Each areas area of our business is reviewing and developing ways to protect personal information:

- Technical measures, like firewalls and good anti-virus software;
- Physical measures, like locking filing cabinets;
- Procedural measures, like policies about who's allowed to access information and who it can be shared with.
- Training for all Co-op colleagues so they understand the basics of protecting information.
- More in depth role specific training for colleagues that are involved with high risk information handling or for the ones that deal with requests.

What does GDPR mean for me?

It depends who you are:

Exec/Senior Manager	• It's your responsibility to ensure your team know about GDPR and how they comply with the new regulation • Be clear on the way that data protection matters can be raised at board level
Customer-facing	• How we manage our customer and member data has always being important to us. GDPR just means we'll have to recognise requests from individual and complete them a little quicker, ensure we report anything that isn't quite right as soon as possible and know where to go to ask if you are not quite sure. The Data Protection team are always on hand to answer any queries.

Change delivery	• It's really important you consider GDPR right from the outset of any change programme. • We'll need to consider things such as: seeing if you need to do a Data Protection Impact Assessment, and embedding data protection and privacy in to any projects.
Transformation team	• It's really important you consider GDPR right from the outset of any transformation programme. • We'll need to consider things such: as building data protection and privacy in to changes, and considering the impacts. You may have to complete Data Protection Impact Assessments.
Colleague	You must handle personal information even more carefully than previously. For example: • We must be clearer with people about how we use their information. • We need to understand our data flows better, to make sure personal information is being collected/used/shared/stored properly and securely. • We must be appropriately trained. • People have more rights in relation to their information. They can ask for copies of it (either for themselves, or to be transferred to another organisation of their choosing), ask for it to be deleted or claim compensation where it's been lost/mishandled. We have to be able to recognise requests, even where people don't mention the law or their rights, and our systems and processes need to be able to handle these requests. • Help is always available, so if you're not sure, ask your data lead or the data protection team.

Are the GDPR rules different if you're sharing personal data with agencies/public compared to sharing with a colleague?

The principle of making sure that only those who have a need to access personal data are the same whether that's with a third party or a colleague within Co-op. Where sharing with a third party it's really important that we do so only in line with the procedures put in place by Co-op. We would not share personal data with an outside organisation without following the procedures because we have to be satisfied that they are allowed access to the personal data and that they have appropriate measures in place to protect the personal information. We have a detailed Procurement policy to ensure our third parties can be trusted.

Section 3: How do I…??

How do I protect personal information?

This is a very open and broad question depending on your role however, the GDPR provides a set of rules for letting different parts of Co-op, and different organisations, access, store, and use personal data. They'll normally have different reasons for doing so.

So we don't make you sit here all day reading this, briefly, you must be very careful about the personal information you hold and in particular who you pass it on to. Think about what you are using personal information for and whether this is what the individual concerned would expect you to be using it for. Have a look at policies and standards around Information Security, which have been designed to ensure we protect personal information.

We have just launched the new GDPR training which gives you a better understanding of how you protect personal information. You can access the training anytime so you can go back in a refresh at any time.

How do I find the GDPR-relevant Policies and Procedures?

Have a look at the policies, standards and guidance on intranet and for store colleagues: How Do I. Typing GDPR in the search bar on the intranet will also provide some good information.

What parts of GDPR should I consider when starting a project?

If your project is going to use personal information, then you'll start off with a Data protection Impact Assessment (DIPA) screener questionnaire. This will tell you whether you need to complete a full DIPA or not. We've got a full process for completing a DIPA as part of our project management process (P4CM). If you're not sure what to do please contact the Data Protection or Data Governance teams.

What do I need to do if I want to take a photo of a colleague for a newsletter/social media?

There's a privacy consideration to using pictures of real people who work for us. If you must use a colleague's photo its good practice to minimise privacy concern. One example is not to put the colleague's names on the picture. It is also prudent to ask the colleague to sign release forms stating that they agree to have their photo to be used for the intended purpose.

Am I allowed to put things on a colleague noticeboard about my team?

If what you intend to put on the noticeboard is related to work activities then it will, in most cases, be OK to put things on a colleague noticeboard about your team. However, you must follow information handling procedures. Consider what sort of personal information you're putting on the noticeboard. For instance, it will be excessive or a misuse of personal information if you were to put a colleague's name, home address, telephone number and mother's maiden name on a noticeboard. If in doubt ask the Data Protection team.

Do I need to ask my team for permission to hold their birthday in a team birthday list?

Personal information used for domestic use like keeping a birthday list is covered by an exemption under the regulation. However, it is good practise to seek colleagues' permission to keep their birthdays in this way and make sure it's then used in line with other personal information i.e. kept securely, not distributed wider than is necessary and updated to be kept accurate.

What do I do if I misplace a printed document that I'm working on?

Report it to your line manager or data lead. If information been lost or misplaced, you will must act immediately to make sure that any possible problems can be handled effectively. Report all incidents to the Information Incident Hotline on **0844 262 9990**.

Can I get fined personally or will it be Co-op that gets fined?

Co-op could get fined for breaching the GDPR. If you've not followed the policies and procedures that are there to manage information well, then you might be disciplined.

Plus, nobody wants to be the one that got Co-op a big fine.

Do I have to delete all documents/images I have that include a name, photo?

This comes down to assessing necessity. Look at your local processes and procedures and think about why you have that information in the first place. Is it still needed for that particular reason? If it is, then it's okay to keep it. If it isn't, then talk to your data lead – it might have to go!

How do I get permission to use people's data?

You won't always need permission to handle someone's personal information. If you do, then you should be really clear about what it is you're asking permission to do, and what that means for the individual. Make sure that consent is **separate** from any other terms and conditions. The Data Protection team can help you, and the Information Commissioner's Office has published guidance.

Am I allowed to email a colleague's personal email address/phone number for work purposes if they've given me it?

It depends why they gave it to you, but it's not normally a good idea. If they gave you their email address because you're friends, you shouldn't use it for another purpose, like work.

How do I raise a data protection incident?

If something has gone wrong – personal information has been lost, or used in the wrong way – you should speak to your line manager in the first instance but also call the Information Incident Hotline on 0844 262 9990.

If the incident is serious, a member of the Data Protection team will contact the Information Commissioners office on Co-op's behalf after following the GDPR Incident Management process.

Section 4: Further information

Who can I speak to or where do I go if I've got a question that's not answered in the FAQs?

We're aiming for each area of the business to have its own data lead, who has more in-depth knowledge about GDPR, who may be able to help you.

Co-op has a dedicated Data Protection team that can help answer questions or concerns and who can provide guidance on unclear or complicated areas. You can contact the team by email at dataprotection@coop.co.uk

The Information Commissioner's Office has lots of guidance and advice on its website, www.ico.org.uk. They also have a helpline where you can ask for advice, but they can't 'approve' procedures.