GDPR – an overview

What is GDPR?
The 'General Data Protection Regulation' (GDPR) is a new law which will completely replace the Data Protection Act in May 2018.

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 need to be ready. The Government has also committed to putting GDPR in to national law. Also, at The Co-op, we've already said publically that we want to be 'trusted with data', so we want to process people's personal information in the best way possible, and GDPR will help us to do this.

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 2% or up to 4% (dependent on the type of breach) of annual worldwide turnover. For the Co-op, 4% would be £377 million! So we need to prepare well.
Definitions	'Personal data' has a broader definition and now also explicitly covers IP addresses, cookies IDs 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'll need to check our processes for anywhere that we may capture children's data.
Individuals Rights	When individuals are making requests to exercise their rights under GDPR we'll have 1 month to respond and there'll be no fee. Below are a list of individuals rights under GDPR: - **Subject access**. People can ask for a copy of what an organisation has about them - **Rectification**. People can ask for something that's incorrect to be corrected - **Erasure**. People can have their information deleted under some circumstances - **Restriction**. People can make an organisation handle their data in a particular way - **Portability**. People can ask for their data to be sent to another organisation - **Objection**. People can object about how or why their information is handled. - **Automated decisions**. Where automated decisions have a substantial effect, people have the right to human intervention.
Consent	Under GDPR, organisations will need to evidence valid consent. Our processes and systems need to be set up to collect and record this consent clearly. There's also a clear definition of consent within GDPR so we need to check that the ways we currently collect consent reflect this.

Area of Change	What the change means
Privacy by Design	Under the GDPR we have an obligation to implement measures to ensure that we handle personal information in a way that puts privacy at the forefront of all our activities. There are a lot of ways that we can include data protection and privacy in what we do. One of the ways to do this is by conducting a Data Protection Impact Assessment (DPIA). A DPIA is a process that helps us identify and address privacy risks at an early stage by analysing how the proposed use of personal information will work in practice. A DPIA is mandatory in certain circumstances but in any case they are a very useful tool in making sure that we handle people's information correctly.
Data Breach notification	Under GDPR, it will be mandatory for all organisations to report significant data breaches to the Information Commissioner's Office within 72 hours or 'without undue delay'. So we need everyone to know what to do if they spot a data breach, and to have processes in place to investigate this quickly (including notify the ICO where required). If there's a serious risk to individuals' rights and freedoms, then we have to tell them, too.
Data Processors	Data processors are other companies that we ask to handle personal information on our behalf. For example a company printing payslips for us will need to have some colleague data to do that. While we clearly have to be careful about who we ask to operate on our behalf, the GDPR makes them directly accountable if they get something wrong. That's a change, as under the current law, we would be considered responsible, as they'd be acting on our behalf. We're looking at our contracts and how to update them to make sure that they reflect the changes to the law.
Accountability	The GDPR requires that we're accountable for how we're using personal information, and to be able to demonstrate we've met our obligations. That means that we need to know and to document what personal information we have, what we're doing with it, and what our justification is.

What has Co-op done about GDPR?

The Exec approved a mandatory programme for GDPR. A third party was engaged by the Programme to see where we needed to improve in readiness for GDPR. Workshops and 1-2-1 interviews were carried out, with around 300 processes and 100 IT systems being reviewed which involve the processing of personal information across The Co-op. The findings from this helped us to create a delivery plan to make sure we're prepared for GDPR, and representatives from each business/function are working to make sure that their areas are ready.