Data Protection – A Quick Guide

Here's a short guide to get you up to speed on the current law relating to Data Protection – no doubt you will have heard about the **General Data Protection Regulation (**"GDPR**")**, which became law in the UK in May 2018.

This is only a short guide to get you on the right track, but if you do need more information or have any specific questions that apply to your day-to-day job, see who to contact at the end of this Guide.

So, why is GDPR important?

GDPR is all about '**personal data**' – that's quite literally any piece of information about a living person. For example, someone's name and home address, email address, NI number, bank account details, where they go on holiday, what they buy in our stores, how much they spend on utility bills, membership details, what prescriptions they may take, CCTV images, notes or opinions written about them etc.

This of course includes us, as colleagues, so our personnel files, performance reviews or appraisals are also personal data. Certain types of personal data, such as medical information, ethnicity, religious and political beliefs etc., as well as criminal records are known as **special category data** and you need to take even more care when processing them. As you might imagine, the Society collects, stores, shares and uses a large amount of personal data relating to members, colleagues, agency workers, customers, contractors, suppliers, etc. – this is called processing. So, it's important to recognise when you are handling personal data and to understand how to treat it to make sure the Society is compliant with the law.

What's important to know?

A few basics you should know about:

- **We have to be very transparent in how we handle people's personal data** – when collecting it we must tell people exactly how we will use it, how long we will keep it for and what rights they have in relation to their personal data. We must also have a clear legal reason for using their personal data, and keep records of how we process it so that we can demonstrate compliance with the law in case something goes wrong and we need to justify it to the Information Commissioner's Office ("ICO"), the data protection supervisory authority in the UK.

- **We must keep people's personal data secure, accurate and up-to-date**, and record all the changes we make when we are asked to do so. If the data is wrong, people can ask us to put it right (this is called right to rectification). We can only use people's personal data for the reasons we collected it in the first place and not for anything else without letting them know in advance. There are also rules around the sharing of personal data with external third parties.

- **There are other rights people have in relation to their data and you need to be aware of them**. For example, people can ask us what personal data we hold about them and ask for copies of it - this is called making a **Subject Access Request**. People can also ask us to stop using their personal data (this is called right to object) if they no longer want to receive our direct marketing, for example. Or we may be asked to delete their personal data (this is called right to erasure, or to be forgotten), although we may not always have to comply with these requests if we have a lawful reason for retaining their data. There are other rights people have, but what's important is that if you receive any of these requests **you tell your business group's Data Protection Champions (DPCs) immediately** as we have to respond to requests within strict time limits to comply with the law.

- **If things go wrong**, for example if we lose someone's personal data, or it gets stolen or is sent to the wrong person by mistake, or say our IT systems are hacked, that's called a **data security breach**. Under the law, the Society must deal with these incidents very promptly as sometimes

they need to be reported to Regulators and, if that's the case, **we only have 72 hours to do so or risk a fine**. So, if you think something's gone wrong or you are told about it by a customer, a member, a colleague or anyone else, **you must tell your DPCs immediately**.

- **We must have a Data Protection Officer** ("DPO") in certain cases – the Society has appointed a DPO for Healthcare, Energy and Phone Co-op, based on the type, and volume, of personal data they process. Of course, the rest of the business groups must be monitored too, but the law doesn't need them to have a DPO, so we call it Data Protection Manager (DPM) instead. Both roles are carried out by the same colleague.

What about Brexit?

GDPR is an EU Regulation and, in principle, it will no longer apply to the UK if we leave the EU. However, we will need to comply with UK data protection law and the government intends to include similar requirements to GDPR into UK data protection law when we exit the EU – so in practice there will be little change to the core data protection principles, rights and obligations that we have to comply with. The Data Protection Act 2018 ("DPA 2018"), which currently supplements the GDPR within the UK, will continue to apply and will be amended accordingly.

Who needs to know about data protection?

Every colleague in the Society needs to know about it, because **we are all in it together and we are all accountable** as so many of us process personal data in some way as part of our day jobs.

What happens if we don't comply?

This is really important – **organisations that don't comply with the law could face fines of up to 4% of their global annual turnover**. That's a really significant amount for us – about £60m. There are other serious consequences too – like the damage to our reputation and the fact that our members and customers would no longer trust us and stop trading with us.

So, data protection is not just about rules and regulations. It's about doing the right thing and applying the same care in looking after someone else's personal data as you would your own. People expect, quite rightly, that we comply with the law, but also trust us to manage their personal data respectfully.

Where do I get more information?

You can find all data protection policies and procedures the Society has put in place on **Colleagues Connect**: https://colleaguesconnect.midcounties.coop/working-here/data-protection/.

A good starting point is our **Data Protection Policy**.

Who do I contact?

Your business group's DPC should be contacted in the first instance – you can find the contact list on Colleagues Connect: https://colleaguesconnect.midcounties.coop/working-here/data-protection/

For the reporting of issues and guidance and support contact the Data Protection team – Anna O'Leary, Governance Assistant (Co-operative House, Warwick) , 01926 516 385 and Sean McGovern, Senior Legal Counsel (Co-operative House, Warwick), 07548127154 Email: data-protection@midcounties.coop.

The Society's Data Protection Officer (Manager) is Andrew Stride, Head of Legal Services (Co-operative House, Warwick) Email: data-protection@midcounties.coop who oversees compliance.