coop midcounties

GDPR Refresher
SEPT 2019

Retail Group

What is GDPR?

The **General Data Protection Regulation** (EU) 2016/679 is a regulation in EU law on data protection and privacy for all individuals within the European Union. It addresses the export of personal data outside the EU.

The GDPR aims primarily to give control back to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.

It became enforceable in **May 2018**.

The fine for data breaches can be up to 4% of Group Turnover – circa £60m!

Personal Data

What is personal data?

- 4.1.Personal data is any information, held electronically or in organised paper filing systems, that relates to an identified or identifiable person by means of an identification number, or any other factor specific to that person's physical, physiological, mental, economic, cultural or social identity:

- 4.2.Under GDPR, the concept of personal data is extended further, to include also email addresses, IP addresses, satellite geo-location tracking, website tracking etc.

GDPR – Data Security

GDPR requires us to take appropriate steps to ensure that personal data that we use is kept secure against the risk of loss, destruction, unlawful disclosure, unauthorised access etc.

All personal data must be kept locked in a filing cabinet with access to the cabinet restricted (All stores should have a secure area, if your store doesn't please let your DM know)

As a Store Manager you and your Team Leaders will very likely come into contact with customer data, Hermes for instance and definitely will with Colleague data.

GDPR – Data Security

- ✓ Recruitment should be through E-ploy and not held on site
- ✓ FIT notes should be sent to the centre where they can be held securely
- ✓ Personal Records should be in a locked cabinet in store, with limited access
- ✓ All lost property will need to be logged and kept within a secure, restricted area, with the exception of bank cards which should be kept in the safe and should be destroyed if not collected within 24 hours
- ✓ The card should be cut up in the presence of a witness and signed off by both parties
- ✓ Any customer returning to collect belongings should bring appropriate ID and sign to say they have their goods
- ✓ Both forms will be available on the Intranet under Food Retail/Policies and Procedures/Security

Customer Impact

- You should not hold data on your customers unless they have consented to you using it and for a specific purpose (Home Delivery/Monthly Account/Customer notice boards) and should only be kept for the purpose it was gathered
- Membership - All variations of paper forms being used will not be GDPR compliant therefore membership applications will not be accepted by this method any longer.
- Future customers should join themselves by calling the membership team in person, or by using the society's main online membership application site

CCTV Access

- Only Store/Team managers who have received training on the correct use of CCTV should operate the equipment
- Government Bodies as well as Law Enforcement agencies should be given access to CCTV via USB/CD on request and with the correct forms
- No member of the public should be shown CCTV under any circumstance
- Anyone other than law enforcement requesting CCTV should apply to data.protection@Midcounties.coop
- If you are unsure about GDPR/CCTV you can contact ann.hudson@midcounties.coop

SAR Enquiries

Everyone has the right to ask for their personal information – Under the new guidelines it will be free to get a copy of any personal information an organisation holds about you. This is known as a **Subject Access Request**.

- If a request is made by a customer for an SAR they, not you, must send the detail through to the centre on the email below
- The Data Protection team will make a call on whether the request is valid and begin the process, you need do nothing further
- All Subject access requests must be sent to data-protection@Midcounties.coop, the team then have 30 days to comply with the request

Data Breaches

- In a working environment with colleagues it can be easy to breach the law without even realising it so it is important you are able to spot the signs of a data breach. If you become aware, or find yourself in any of the following situations, you must tell your DPC straight way
  - Someone's personal data has been sent to the wrong person or place
  - Allowing CCTV footage to be viewed by anyone other than trained colleagues
  - Someone has accessed personal data they shouldn't have

The Society then has 72 hours to notify the Information commissioners office or ICO of a data breach

Questions

GDPR Champion – Ann Hudson

Contact:
food.gdpr@Midcounties.coop

GDPR Deputy – Mark Williams