GDPR Guidance for Co-operatives

Data Protection and the GDPR: what do you need to know?

This toolkit has been produced in partnership with Anthony Collins Solicitors.

Anthony Collins solicitors

CO-OPERATIVES UK

GDPR Guidance for Co-operatives

Data Protection and the GDPR: what do you need to know?

The law which governs how businesses in the UK (including co-operatives) protect, use and store people's information is changing in 2018.

The introduction of the General Data Protection Regulation and the Data Protection Bill (which is currently before Parliament) will amend how we collect and use personal information about individuals.

This guidance is not intended to provide a comprehensive guide to the regulations but to help you understand the key elements of change and the aspects that are most likely to require action. It is intended to be read alongside the guidance from the Information Commissioner (the "ICO") and links to some key guidance are provided below.

What is the GDPR?

The General Data Protection Regulation 2016 ("GDPR") comes into force in the UK on 25th May 2018. It replaces the Data Protection Act 1998 and will harmonise data protection law throughout Europe.

The changes in the law are a result of the ever increasing volume of personal data held by organisations of all kinds. The data held is often a huge asset for an organisation, but if misused it breaches an individual's right for their personal data to be protected.

The GDPR seeks to uphold 6 principles when an individual's personal data is 'processed' (the term 'processing' is a wide term which covers most things which can be done with personal data, including collecting it, storing it and using it):

1. Personal data must be processed fairly and lawfully and in a transparent manner.
2. Personal information must be collected for specified, explicit and legitimate purposes.
3. Personal data must be adequate, relevant and limited to what is necessary for the purpose.
4. Personal data must be accurate and up to date.
5. Personal data must not be kept longer than is necessary.
6. Personal information must be processed in a manner which ensures security of the personal data against unlawful processing, accidental loss, destruction or damage.

When deciding to process personal data, the above principles should always be considered. Not only is the date when the new law comes in force fast approaching but people are becoming more concerned about how their personal information is collected and handled and the media is paying more attention to issues relating to personal data. Your members, staff, services users or customers (depending on what kind of work you do) may be concerned about how you are using their data, and so compliance with the principles is important for both legal reasons and to provide reassurance to your members. Where relevant, this document will refer primarily to members, recognising that many co-ops will collect membership information, but you should bear in mind the other categories of individual that might be affected by these rules.

Personal Data and Sensitive Personal Data

Personal data is any information that relates to an individual who is identified or who is identifiable. It is not necessary for the individual to be named in the data to be considered identifiable. An address which is associated with a membership number is personal data even if the individual member is not named in the same list. Personal Data includes information which describes an individual's physical or mental condition, economic situation, or an individual's cultural or social identity.

There are certain types of information ('special categories of data', commonly referred to as 'sensitive personal data') which are subject to stricter controls. These include a person's mental or physical heath, their trade union membership or religious belief. If your co-op processes sensitive personal data, there are much narrower permitted reasons for processing such data and so you should consult the ICO guidance before collecting or further processing it.

Sensitive personal data is information concerning:

- Racial or ethnic origin.
- Political opinions.
- Religious belief or similar including philosophical belief.
- Trade union membership.
- Physical/mental health or condition.
- Sexual life or sexual orientation.
- Commission or allegation of an offence.
- Proceedings of any offence, disposal of proceedings, sentences.
- Genetic data.
- Biometric data.

Legal Grounds

The GDPR sets out the following legal grounds under which an organisation may process personal data (non-sensitive):

- Necessity to protect the vital interests of the individual– e.g. disclosing an employee's heart condition to a paramedic.
- Necessity for the performance of a task carried out in the public interest.
- Necessity for the performance of a contract with the data subject.
- Necessity for compliance with a legal obligation.
- Necessity for the legitimate interests of the data controller.
- Consent.

This guidance will focus on the final four grounds as these are likely to be more relevant for co-ops.

The ground 'necessity for the performance of a contract with the data subject' may be relied upon when processing personal data of an employee, provided that the data which is collected and used is necessary for entering into or performing the employment contract. It may also be relevant when dealing with members. This means that you may collect information which is required to sign a valid contract and to carry out the contract.

The ground 'necessity for compliance with a legal obligation' will be relied on when secretaries collect and store information which must be held on registers. This is because the information on the registers of members and directors are required by law.

The ground of 'necessary for the legitimate interests of the data controller' may be relied on by membership officers when contacting members. Communicating with members involves processing the contact details of those members and therefore a legal ground is required. It is important to note that the ground of 'legitimate interests' cannot be relied on when sending promotional/marketing material by automated means such as email or SMS. In such case consent is required, and this is discussed in more detail later on in this document.

When using this ground, you must consider whether your legitimate interests are overridden by the need to protect the fundamental rights and freedoms of the individual. If this is the case the ground of 'legitimate interests' cannot be relied upon. This consideration is especially important where the person concerned is a child. This ground may be relied on to contact members where their information is required for the furtherance of an interest of the co-op e.g. notifying them of the AGM time, date and location or forwarding election details, unless the ground of 'necessary for performing a contract with the data subject' can be used instead.

The ground of consent is commonly used but often misused. The GDPR further restricts the use of consent as a ground due to its abuse in the past, by requiring a higher degree of consent.

Consent must be "freely given, specific, informed and unambiguous". It must be given by means of statement or a "clear affirmative action" which means that 'opt out' consent is not considered valid. The individual must be able to withdraw their consent at any time and withdrawing consent should be as easy as it is to give consent. It is also not enough to obtain consent but you must be able to "demonstrate" that you have obtained proper consent.

Consent to a form of data processing cannot be a pre-condition for entering into a contract. This is because consent would not be considered to be 'freely given'. A prospective member cannot be required to give consent to receive email marketing in order to become a member of a co-op because in such a scenario the new member isn't given a real choice on whether to accept to receive marketing, which is not necessary for membership.

It is crucial that the individual fully understands how and why their data will be used before giving consent. A blanket, open ended consent for the collection of data for many different reasons is not acceptable as the individuals cannot be certain how or why their data will be used. An example of an unacceptable consent clause is "*I consent to allowing X co-op to use my data for their records and to be used as X co-op deems fit for market research".* The consent given would not informed as it is too ambiguous.

Due to the strict nature of the consent ground, it is advisable to seek another ground for collecting and using data when possible.

Co-operatives, such as social care providers, who process sensitive personal data, must, when processing sensitive data, not only find a ground from the list above but most also, in addition, establish a ground from a second list of grounds which includes the following:

- Necessity to establish or defend legal proceedings.
- Necessity for statistical, scientific or historical research purposes.
- Necessity for reasons of substantial public interest on the basis of law.
- Consent.
- Necessity for the provision of health or social care or treatment or the management of health or social care systems and services on the basis of law or pursuant to contract with a health professional.
- Necessity to protect the vital interests of a data subject where the data subject is not capable of giving consent.

It is important to refer to the law and available guidance before relying on one of these grounds because a number of conditions apply to them, for example, the 'provision of health or social care' ground only applies when the data is collected or used (processed) under the responsibility of an individual who is subject to a legal obligation of secrecy such as a doctor.

Example

Your secretary must hold each member's information including the name, date of birth and residential address.

Is this personal data?

What is the legal ground for collecting and storing this data?

The data listed above is classed as personal data as it clearly relates to an individual. The information may be held by the co-op because it is required by statute which states that each co-op must hold a record of its members and directors. As this information is required by law, the legal ground 'necessary for compliance with a legal obligation' permits the collection. The information is not sensitive and therefore an additional ground is not required.

Communicating with people (data subjects) about how personal information will be held and demonstrating compliance with the law

The GDPR requires that you are able to demonstrate that you comply with the law so each co-op should have documentation which explains what data you hold, how you collect it and what you will do with it.

The key documents that will enable you to do this are:

- A Data Protection Policy.
- Privacy notices (also known as a Fair Processing Notices).
- A Website Privacy Policy (if relevant).

The **data protection policy** is the document which informs staff and others acting on behalf of your co-op how to handle personal data in compliance with the law. This can include how data should be used when carrying out marketing. Having a clear policy in place and making sure that all those who represent the co-op are aware of the policy and are trained on data protection helps show that your co-op takes the protection of personal data seriously. The policy is normally an internal document but you may choose to make it available to the public to further emphasize your commitment to data protection.

Privacy notices and website privacy policies are very similar documents. They are both communications to data subjects which explain why and how you process their personal data. Website privacy policies typically also cover information about how the website uses cookies (small files which store information on a user's computer). The GDPR clarifies what information must be given in privacy notices (including website privacy policies) and also requires that privacy notices are written using clear and plain language and are provided in a concise, transparent, intelligible and easily accessible form.

The **privacy notice** should not be a generalised document but should clearly describe how you handle and use personal data. It should be provided to individuals at the time you collect the data at the latest. The notice should include the following, among other information:

- The identity and contact details of your co-op and the officer responsible for data protection.
- The purposes and legal ground for processing data.
- The recipients of the personal data.
- If you are transferring data to any organisations situated outside the EU the notice should also include the legitimate interests pursued by that organisation and the safeguards in place to protect the data.
- The expected length of time the data will be stored.
- The individual's rights to access to, erasure or restriction of their personal data.
- The right to complain to the ICO.

If you collect data from third parties you need to provide a privacy notice to the data subjects concerned within a reasonable period after obtaining the data and not later than one month. If you use data collected from third parties to communicate with an individual you should, at the latest, provide the privacy notice at the time of your first communication, and if you disclose that data to another recipient, at the time when you disclose the data.

If you have a website, a **website privacy policy** should include specific information which explains which data is being collected, how and why. The information should also explain the website's use of cookies if applicable. It is prudent to include a prominent and clearly visible link to the website privacy policy on your website so that you are able to show that you have given the required information to visitors.

The ICO recommends you regularly review the policies/notices in order to ensure they are up to date with the co-op's practices.

Secretaries should provide privacy notices which explain to directors and members the reasons for holding their information (such as full name, address and date of birth), including that it is a legal requirement for a co-op is to keep statutory registers. All the other information listed above needs to be given, including that the members names will be publically available in the statutory books and can be accessed by anyone upon a valid request.

Privacy notices may be given in writing or by other means, including by electronic means. You may choose to adopt a layered approach by having a comprehensive privacy notice which is available on your website and which members can request a copy of (for example if they are unable to access the internet), and then providing more concise notices at the time specific data is collected, which signpost to the more comprehensive information. The method each co-op utilises to communicate with their members will vary depending on the size of the co-op, the type of work that you do, and the type and quantity of data that is processed.

Examples

If individuals can sign up to become members through your website, the privacy notice information can be given during the sign up process. You may, in addition, include it in a confirmation email to a new member so that they are able to access it at a later date. If the information is available on a webpage you may include a link to this page in the confirmation email instead of providing the whole text. You need to be able to show that you have provided the required information at the right time. It may be easier to do so if you ask new members to confirm that they have read and understood it.

If a member signs up in person, providing a printed link to a webpage containing the information may not be enough to satisfy this requirement unless the individual can easily access it when signing up. A printed privacy notice may be more appropriate.

When dealing with children, you could consider providing the information in an interactive manner.

If an employee of a social care co-operative wishes to notify a family member of the person who is cared for (the service user), of a change in the service user's care plan:

1. The information consists of personal data.
2. Parts of the information are also likely to constitute sensitive personal data as it relates to health.
3. Since the information is being given to someone other than the data subject, this constitutes 'sharing' of the personal data which is a form of 'processing'.
4. Legal grounds are required for processing data in this manner and a legal ground is required both from the first list and also from the second list of grounds described above for processing sensitive data.
5. The most appropriate legal ground in this case is consent. Consent is a legal ground under both lists of grounds, although for the purpose of processing sensitive data consent must be "explicit".
6. Since consent should always be 'specific' you should obtain consent to share the data with a specific family member so that the individual is given a wider choice with regard to who the information is shared with. You should also give the service user the option to choose what data is shared and what data isn't shared. You cannot presume consent.
7. When the information that is being shared is first obtained, the person who is cared for should have been informed that the data may be shared with family members for the purpose of keeping them informed about the service user's wellbeing provided that they give explicit GDPR-level consent for such sharing.

Direct Marketing

Direct marketing refers to sending promotional material to specific individuals, as opposed to, for example, sending generic, unaddressed promotional material to the occupants of properties in a certain area. Direct marketing can be used to offer the sales of goods or services, for fundraising, or be used to promote the organisation. Marketing by electronic means is more restricted than, for example, marketing by post.

Marketing by means of email, SMS or automated phone calls to individuals (as opposed to corporations) requires prior consent. Since 'consent' was not defined under the DPA, many organisations relied on 'opt out' mechanisms or pre-ticked consent boxes to obtain consent. Effectively, each individual had to 'opt out' if they did not want their information to be used for such marketing. The GDPR requires that consent is obtained by means of a "clear affirmative action" and therefore requires that consent is obtained by means of 'opt in' mechanisms. Many practitioners argue that since the GDPR seeks to clarify the existing law, GDPR-standard consent is required to send electronic marketing even before the GDPR comes in force.

Membership officers should ensure that any 'opt out' boxes are removed and replaced with boxes for individuals to 'opt in' when giving their clear and specific consent to receive direct marketing. If members gave consent through 'opt out' boxes until now, this will no longer be sufficient and fresh GDPR-level consent needs to be obtained. Co-ops should seek to gain consent for the activities through 'opt in' boxes before GDPR comes into force in May to ensure compliance or stop using and delete the data acquired through 'opt out' boxes.

Co-ops cannot send an email or text message asking for consent because such email or message would also constitute marketing. This applies even if only a small part of an email asks for consent and the rest of it isn't marketing.

If you are emailing a corporate entity such as another co-op or a company, or an individual using an email address which is owned by a corporate entity, you do not require consent to mail them and you may rely on the 'legitimate interests' condition for processing the data.

All marketing emails need to identify your co-op as the sender and give the recipient the option to opt out. Once an individual has opted out you must stop sending emails. This is regardless of whether a business address is used or not.

Sending marketing material by post and telephone (non-automated calls) is less restricted. You should cross reference the names and addresses against the Mail Preference Service or Telephone Preference Service to check whether the individuals have stated they do not want to receive marketing. Similarly to emails, the sender of the marketing by post must display their name and contact details to enable the recipient to opt out. Marketing by telephone should always display their telephone number to allow the recipient to reply.

Example

A retail co-op is organising an event to promote a new product. The officers in charge of organising the event wish to contact each member to advertise the event. The officers wish to use the email addresses of members to contact them and highlight the event.

Is this personal data?

What is the legal ground for collecting and storing this data?

An individual's email address is personal data and so you must only use the information on the basis of a legal ground. If the members have agreed to receive advertising from the co-op using an opt in system, you may use the email addresses to advertise.

The opt in system must be GDPR compliant and the email to advertise the event should allow the member to decline to receive more advertising if they no longer wish to receive it.

Third party contracts

Under the current law when you appoint a 'data processor' you are required to have a written contract in place which requires the processor to only process data on your instructions and to keep personal data secure. The GDPR lists a number of additional clauses which must be included in such contracts. The requirement does not only apply to contracts entered into after the GDPR comes in force on 25 May 2018 but also to contracts already in existence.

To ensure that your contracts with third parties are GDPR compliant, you should ensure that the contracts clearly stipulate the role of each party and the limits on the use of the data. The ICO has confirmed that there will be no grace period for preparing for the GDPR (https://iconewsblog.org.uk/2017/12/22/gdpr-is-not-y2k/) and therefore all contracts should be amended before 25 May 2018.

Examples of third parties who qualify as data processors are:

- IT service providers who provide cloud services where the membership list is held.
- Data analysts for market research.
- PR or advertising agents used to send marketing to the co-op's members.

The definitions of 'controller' and 'processor' are broadly:

- A data controller is the organisation which determines how and why the data should be collected and processed (the "purposes and means of the processing").
- A data processor processes personal data strictly on the instructions of a controller.

A cloud service provider will not decide what data is stored on the cloud and for what purpose but simply follows the instructions of the controller. Solicitors on

the other hand will determine how personal data you provide them with is to be used for the purpose of providing their legal services and you would not be able to tell them how to process the data for achieving that purpose.

It is possible that a single organisation can be both a data processor and a data controller in relation to different processing activities (it cannot be both a controller and a processor for the same processing activity). A cloud service provider will be a data processor when storing personal data for you, but will be a data controller of the data of its own employees. The distinction is not always easy to make but the ICO's guidance on 'data controllers and data processors' can help you make it: https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf

To ensure contracts with third parties will be GDPR compliant, we suggest you complete the following steps:

- Draw up a full list of contractors you deal with.
- Identify which ones are processors and which ones are controllers.
- Review contracts involving sensitive personal data or which deal with large volumes of data first as these involve a higher risk.
- Engage with the parties to agree amendments to the contracts to ensure GDPR compliance in a timely manner.

Many established processors have taken the initiative to start revising their terms and conditions already, and most processors should be aware of this new requirement.

Reporting Data Breaches

A data breach is defined as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".

Currently there is no legal requirement to report breaches to the ICO (although ICO guidance states that "the Information Commissioner believes serious breaches should be brought to the attention of his Office"). However, the GDPR places a duty on organisations to report the breach without delay. The GDPR requires that a personal data breach is reported within 72 hours after it is discovered where it poses a risk to any individual. Note that a breach can be discovered by a processor in which cases the clock starts to run immediately. It is therefore important that processors are required to notify you straight away.

When a breach poses a 'high risk' the data subject would also need to be notified of the breach. This can cover situations when the data breach might cause discrimination, identity theft, fraud, damage to their reputation or financial loss. For example, a retail co-op may have stored their member's credit card information. If this information is lost and can be accessed by someone who finds it, this would need to be reported to both the ICO and the individual concerned. This will allow the person to cancel their credit card and protect themselves.

It is important to note that the 72 hours begin to run from the time the breach is discovered and not when it is reported to the officer responsible for dealing with the breach, so it is crucial that breaches are escalated as soon as possible. All staff need to be made aware of your legal obligations.

When reporting to the ICO, you should explain the nature of the breach, and provide the contact details of the officer responsible for data protection so that the ICO may investigate the likely consequences of the breach and the measures you took and which propose to take to address it.

Examples of incidents that must be reported:

A CD containing personal data has been lost. It was subsequently found but as you cannot be 100% certain the data has not been accessed by another person, a notification to the ICO would be necessary unless it is unlikely to result in a breach to individuals. The breach should have been notified once the controller became aware the CD was lost.

Your IT systems have been infected by ransomware, malicious software which accesses your data and blocks all use until a ransom is paid. A notification to the ICO would be required as the attacker may have accessed personal data, which could be a potential risk to the rights and freedoms of the individuals.

The third party data processor has informed you of a breach which they have caused or suffered. You are considered to become aware of the breach when the processor becomes aware of the breach, since the processing is carried out by the processor on your behalf. You, as the data controller, are obliged to report this breach to the ICO and not the data processor. This is one practical reason why it is important to have the data processor clauses included in a contract with the processor.

Subject Access Requests

Data subjects (those whose data you hold) have the right to access their information. They have a right to request that you inform them of:

- The purposes of processing.
- The categories of personal data held.
- The recipients of the personal data.
- How long the organisation expects to hold their data before destruction.
- The right to lodge a complaint with a supervisory authority.
- If the data was not collected directly from the data subject, the source of the information.
- The envisaged consequences of such processing for the data subject.

In addition to being given the above information when an individual exercises this right they must be given a copy of their personal data that you process.

The information held by secretaries and membership officers may be requested at any time by individuals and it is imperative that you comply with the request. If you have reasonable doubts about the individual requesting the data, you are entitled to request they supply additional information so that you may determine their identity. This is to ensure the individual is only requesting their own personal data and prevent breaches. You need to be careful that when you are complying with such a request you do not inadvertently disclose personal data of a third party. Such third party personal data should be redacted.

The information should be supplied within 1 month of receiving the request. Where the request is particularly complex then the period may be extended to 2 months.

Data Protection Officer

The data protection officer is in charge of ensuring compliance and reporting breaches.

The GDPR only requires an organisation to appoint a data protection officer where its core activities involve regular and systematic monitoring on a large scale or consist of processing sensitive data on a large scale.

If you do not fall under this requirement, it may still be helpful to designate someone who can take ownership of data protection compliance although it should be made clear that the title, status, position and tasks of this officer are not those of a data protection officer, because the appointment of a data protection officer on a voluntary basis would attract all the legal requirements which apply to DPOs appointed on a mandatory basis. This can be done on a part time basis. Some useful guidance about data protection officers can be found here: http://ec.europa.eu/newsroom/document.cfm?doc_id=44100

Author:
Anthony Collins Solicitors
www.anthonycollins.com

Published by:
Co-operatives UK
Holyoake House
Hanover Street
Manchester
M60 0AS
www.uk.coop

Co-operatives UK is the network for Britain's thousands of co-operatives. Together we work to promote, develop and unite member-owned businesses across the economy. From high street retailers to community owned pubs, fan owned football clubs to farmer controlled businesses, co-operatives are everywhere and together are worth £36 billion to the British economy.

CO-OPERATIVES UK