General Data Protection Regulation

Employee data toolkit

November 2017

CO-OPERATIVES UK

www.uk.coop/gdprtoolkit

Contents

Introduction

From 25 May 2018, the General Data Protection Regulation ('GDPR') will change how businesses (including co-operatives) in the UK process, protect and store information identifying individuals. The GDPR significantly extends the current requirements of the Data Protection Act 1998 ('DPA 98') to reflect advances in technology and to create a unified approach to data protection across the EU. Significant breaches of the requirements could see a co-operative paying a levy of up to €20 million or 4% of the total worldwide annual turnover, whichever is greater.

The GDPR will become automatically effective on 25 May 2018. The GDPR will also be accompanied by a new Data Protection Bill ('DP Bill'), which will implement the GDPR standards across all data processing within the UK and will provide clarity on some part of the GDPR. The contents of the Bill have not been finalised.

This guide focuses on the GDPR's application to employers and explains how co-operatives will need to adopt new ways of working to become compliant, including reviewing current policies, procedures, employment contracts and privacy notices.

This guidance note will take you through some of the key changes, although it is advisable for each co-operative to read about the changes in detail and take their own legal advice. The Information Commissioner's Office (ICO) is also expected to update its Employment Practices Code before May 2018.

NOTE: The GDPR allows the UK to develop its own practices in a number of permitted areas. The Data Protection Bill is currently at the House of Lord's Committee stage.

Executive Summary

If your co-operative is already complying with the DPA 98, you are in a good place to comply with the GDPR and the DP Bill. Some of the requirements formalise existing current best practice.

Where the law is changing, it is important that preparations are made in sufficient time to ensure compliance by May 2018. For example, some co-operatives may find that they need to appoint a dedicated Data Protection Officer to comply with the new legal requirements.
In particular, your organisation will need to consider:

- The legal basis for processing different types of personal data belonging to colleagues
- Extended rights of colleagues as to how their data is processed
- The additional information that colleagues will need to be provided with
- How subject access requests will be processed.

Section 1: The Basics

1. What is the GDPR?

The GDPR is a European regulation intended to strengthen and unify data protection for all individuals within the European Union.

Will it apply to co-operatives?

Yes, the GDPR will apply to all UK businesses including co-operative businesses who are 'controllers' and 'processors' of data. We'll touch on these roles later.

What will happen to the Data Protection Act 1998 (DPA 98)?

The GDPR will replace the DPA 98, and a new Data Protection Act will sit alongside the requirements of the GDPR.

When will the new requirements start?

Businesses will need to start complying with the GDPR on 25 May 2018.

Will the GDPR apply before and after Brexit?

Yes, the UK Government has confirmed that the new GDPR regulation will apply from 25 May 2018 despite these negotiations. Even after the UK has left the EU, the UK will need to continue with the requirements to ensure that it qualifies under the GDPR to receive and process data relating to EU citizens.

What are data 'controllers' and 'processors'?

A 'controller' says how and why personal data is processed and the 'processor' acts on the controller's behalf. The definitions have not changed from those within the DPA, but there are now specific duties and obligations placed on processors. If you are a processor or controller (or both) of data or currently subject to the DPA 98, it is likely that you will also be subject to the GDPR.

In practice:

Sue gives her employer 'Big Co-operative' personal data (bank account details) during the recruitment process. Big-Co-operative uses an external payroll service 'Small Payroll' to pay Sue. Small Payroll receives personal data about Sue to process and pay her wages.

Small Payroll is a **processor** of the personal data received from Big Co-operative.
Big Co-operative is the **controller** of this data.

What activities are covered?

The broad activity covered by the GDPR is the 'processing' of personal data either manually or automatically which form part of a filing system or it is intended to form part of a filing system.

What does processing cover?

Processing generally covers any operation or series of operations you carry out on personal data:

- Collection
- Recording
- Organisation
- Structuring
- Storage
- Adaptation
- Alteration
- Retrieval
- Consultation
- Use
- Disclosure
- Dissemination

Section 2: What data is covered by the GDPR?

The DPA 98 and the GDPR apply to the processing of 'personal data' and 'sensitive personal data'. Any data the business holds where a colleague can be directly or indirectly identified, will need to be processed in accordance with the requirements of the GDPR.

What is personal data?

Both the GDPR and the DPA 98 direct how 'personal data' should be processed. The scope of 'personal data' has broadened under the GDPR.

Personal data is any information about an **identifiable** living person. In an employment context this could include employees, workers, contractors or agency staff, as well as information about job applicants and individuals who have left the company.

The person may be identified by name, an identification number, location data, an online identifier or by one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. Businesses will need to consider what methods could be reasonably used to identify the individual from the data.

The GDPR applies to both automated personal data and to manual filing systems where personal data is accessible according to specific criteria. This is wider than the DPA definition and could include chronologically ordered sets of manual records containing personal data.

Important:

Previously, the information had to have the individual as its focus i.e. being named on an email address list would not be sufficient. Now, information may relate to an individual even if it does not focus on him/her.

Since 2007, the EC Working Party has indicated that one of the three elements below are needed to be 'personal data':

1. The information is about an individual regardless of the purpose.
2. The data has been used or will be used to evaluate, treat in a certain way or influence the status or behaviour of an individual.
3. Use of the data is likely to have an impact on an individual's rights or interests.

Examples of personal data include CCTV film, lift or floor access information, computer log on data, data on websites visited, phone calls made and emails sent or received.

What about sensitive personal data?

Businesses will need to continue to take additional care when processing sensitive personal data.

- The definition of sensitive personal data has not changed and continues to include:
- Racial or ethnic origin
- Political opinions
- Religious and philosophical beliefs
- Trade union membership
- Health, sex life or sexual orientation
- Genetic and biometric data

Section 3: The Data Protection Principles

Your organisation will already be familiar with the data protection principles in place under the DPA 1998. The GDPR updates these principles. The purpose of the principles is to protect individuals against infringements of their privacy that cause harm.

The GDPR introduces a new transparency requirement, more robust data minimisation concept, allowance for data to be stored for longer for statistical research and controller accountability.

1.	**Lawfulness, fairness & transparency**	Personal data must be processed lawfully, fairly and in a transparent manner.
2.	**Limited lawful purpose**	Personal data must be only collected for specified, explicit and legitimate purposes.
3.	**Data minimisation**	Personal data must be adequate, relevant and limited to what is necessary in relation to the intended purpose.
4.	**Accuracy**	Personal data must be accurate and, where necessary, kept up to date.
5.	**Storage limitation**	Personal data must not be kept in a form which permits identification for any longer than necessary for the given purpose.
6.	**Integration & confidentiality**	Personal data must be processed in a manner which ensures its appropriate security
7.	**Accountability**	The data controller is responsible for, and must be able to demonstrate, compliance with the other data protection principles.

Section 4: Fair and transparent processing – privacy notices

Under the DPA 98, organisations have to provide individuals with information about how their data will be used (or 'processed') to ensure transparency. These are sometimes referred to as 'privacy notices', 'fair processing information' or 'notice of data processing'. The GDPR broadens those existing obligations.

Who should the information be provided to?

You must inform individuals that you have collected data from them whether that data has been collected directly, or received through a third party (unless providing the information would involve disproportionate effort). For example, personal data obtained from a job applicant who applies through your website or a candidate who has been sourced by a recruitment agent.

When should the information be provided?

When the personal data is collected from the individual, before or at the same time that the data is collected. Where the data is collected from a third party - as soon as possible and no later than a month after collection.

Where the reason for processing the data changes, you will need to update the information provided to the individual.

What language should you use?

The information must be conveyed in a concise, transparent, intelligent and easily accessible format using clear and plain language. Where you process data relating to children - it should be simple enough for a child to understand.

It must be provided in writing unless someone asks for the information orally.

What information do you need to provide?

Where personal data is directly collected from the individual:

- The identity and contact details of the data controller or its representative.
- The contact details of the data protection officer (where applicable).
- The purpose/s and legal basis for the processing of the personal data.
- Where 'legitimate interest' is relied upon - details of that interest.
- Who will receive the personal data (if anyone)?
- Whether you intend to transfer personal data to a non-EEA country or an international organisation - the safeguards in place.
- How long you will store the personal data (where unknown - the criteria for determining that period).
- That the individual has the following rights: right of access, rectification, erasure, restriction of processing, objection and data portability.
- Where you are processing data based on the individual's consent, their right to withdraw consent at any time.
- The right to lodge a complaint with the Information Commissioners' Office.
- Whether providing the data is a statutory or contractual requirement, or a requirement necessary to enter into a contract. Also, any obligation for the individual to provide the personal data and of the consequences if they fail to do so.

- The existence of automated decision-making (including profiling), meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
- Where you intend to further process the data for a purpose other than for which the data was collected you should firstly provide the individual(s) with information on the new purpose and any other relevant information.

Where personal data have not been obtained from the data subject:

The same as above with the addition of:

- The categories of personal data concerned.

Next steps: HR departments should review their existing privacy notices and incorporate the greater level of detail required by the GDPR.

Section 5: Limited lawful purposes and consent

What is lawful processing?

Before processing personal data, you must make sure that you have a legitimate ground for carrying out that activity.

This was already a requirement of the DPA, but the GDPR does make some significant changes in this area.

As a reminder, the following are the possible legal grounds for processing personal data:

1. The individual has given their consent (see below).
2. It is necessary for entering into or performing a contract with the individual (including an employment contract) e.g. obtaining bank details to pay the individual.
3. It is necessary due to a legal obligation (e.g. you need personal data to deduct tax or provide Employee Liability Information where a TUPE transfer applies).
4. It is necessary to protect the vital interests of the data subject (i.e. medical history provided to the hospital in the event of a life-threatening accident at work) or of another individual.
5. It is necessary for the purposes of the legitimate interests pursued by the data controller or a third party (except where this is overridden by the interests of the individual) and what that interest is.
6. It is necessary for preventing fraud and direct marketing.
7. It is necessary for the performance of a task carried out in the public interest in the exercise of official authority vested in the controller.

Once your co-operative has confirmed what legal ground it is relying upon, your organisation will be bound to use the data for that explicit purpose. Further processing of the data will only be permitted as long as the new processing activity is not incompatible with the original purpose. Where the new purpose is incompatible, consent from the individual must be obtained.

Can you rely upon consent as the grounds for processing?

The concept of consent in the GDPR is stricter than in the DPA.

The GDPR states that consent must be: "*freely given, specific, informed and unambiguous*". Consent can be provided verbally, but it advisable to get the consent in writing.

Where there is an imbalance in power between the individual and the data controller, consent will not be '*freely given*'. It is unlikely that consent given by an employee within an employment contract will be freely given. On this basis, it will be risky to rely upon 'consent' as the legal basis for processing all employee data, although it may be used for specific processing purposes such as in occupational health referrals.

Consider if your organisation could rely upon the ground that the processing of personal data is necessary for legitimate business interests, or it is necessary for performing the employment contract. In many cases, these grounds will be appropriate given the duties of the employer. The legitimate interests ground has not changed from its previous format within the DPA, although your organisation should consider 1) whether the processing is necessary or could be carried out in a reduced format and 2) whether the employee would expect their data to be processed in that way. In some contexts, your organisation will continue to rely upon consent as a legitimate ground for processing or will have this ground listed as one of the applicable legitimate grounds. If you continue to rely upon the ground of consent, here are some requirements to remember:

- The individual must be informed of the identity of the data controller and the purposes of processing the data.
- Pre-formulated forms or templates should be provided in an intelligible and easily accessible form using clear and plain language and should not contain unfair terms.
- The request for an employee to give consent must be separate from the remainder of the document and the employer must provide a separate signature box.
- It must be made clear that the employee is not obliged to provide consent and has the right to withdraw their consent at any time.
- It must be as easy for the employee to withdraw their consent as to give it.
- If different processing operations are envisaged separate consents should be sought.

NOTE: The ICO is due to publish guidance in December 2017 on the issue of consent.

Historic consents

Previously obtained consents will only be valid if they meet the new requirements of the GDPR. If your co-operative can only justify the processing of personal data on the basis of consent, you will need to check whether your existing declarations of consent comply with the GDPR. If they don't comply, you will need to re-seek consent from the individuals.

Consider:

1. Blanket consent clauses are likely to be ineffective.
2. Consent must be given for different personal data processing operations.
3. Is consent necessary for the contract to be performed?
4. Have individuals been informed of their right to withdraw their consent at any time and has this process been made easy?
5. Consent cannot be indicated by opt-out boxes.
6. Consent by inactivity (i.e. continuing to use a website) will not amount to consent.

Processing of Sensitive Personal Data

Sensitive Personal Data is only permitted to be processed under one of the following conditions:

1. The individual has given explicit consent for one or more specific legitimate purposes.
2. It is necessary for the purposes of carrying out the obligations and exercising the specific rights of the organisation as an employer and social security as authorised by the UK.
3. Processing is carried out in the course of its legitimate activities by a foundation association or any other not for profit with a political, religious, trade union aim and on condition that the processing relates solely to the members or former members or to person who have regular contact with it.
4. Processing is necessary to protect the vital interests of the data subject where the individual is physically or legally incapable of giving consent.
5. Processing relates to data which has been manifestly made public.
6. It is necessary for establishing or defending legal proceedings.
7. It is necessary for the purposes of occupational medicine for the assessment of the working capacity of the employee. It must be carried out on the basis of UK law or pursuant to a contract with a health professional.
8. Processing is necessary for statistical, scientific, historical research purposes on the basis of EU or UK law.
9. Processing is necessary for reasons of substantial public interest on the basis of EU or UK law.

Section 6: Rights of Individuals under GDPR

Individuals will have the following rights:

1. Right to be informed
2. Right of rectification
3. Right to object
4. Right to restrict processing
5. Right to data portability
6. Right to erasure
7. Right to notify
8. Right of access
9. The right not to be subjected to automated decision-making including profiling

1. Right to be informed

This information is dealt with by providing a privacy notice described earlier.

2. Right to rectification

The GDPR includes a right for individuals to have their data rectified without undue delay and this includes having incomplete data completed. For example, you may be asked to update an incomplete performance record.

3. Right to object

If your organisation has relied upon the 'legitimate interest' ground for processing data, individuals have the right to object to the processing of their data. As discussed previously, the legitimate interest ground will now be heavily relied upon by employers instead of consent.

You will also need to tell individuals that they can object to the processing of their data no later than the first communication. In practice, your organisation is likely to want to notify individuals at the point of data collection or at the time the privacy notice is provided.

4. Right to restrict processing

Individuals will have the right to restrict processing in the following circumstances:

- They contest the accuracy of the personal data (the controller can then verify the accuracy of the personal data).
- The processing is unlawful, but the individual doesn't want the data erasing.
- the organisation no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal proceedings.

When data is subject to a restriction, you will continue to be able to store the data, but may only process the data in the following circumstances:

- With the individual's consent.
- For the purpose of establishing or defending legal proceedings.
- For the protection of the rights of another person.
- For reasons of important public interest.

5. Right to data portability

GDPR includes a right for individuals to data portability where data has been processed by automated means. This is targeted at online service providers and allows data to be moved from one service to another. It could apply both in an automated recruitment process, on-boarding but also time and attendance records collected automatically.

The GDPR gives the individual the right to receive the personal data concerning themselves in a structured, commonly used and machine readable format (e.g. CSV, XML or JSON) and have that data transferred to another controller without hindrance. This should take place without undue delay and in any event within one month of receipt of the request although the period may be extended, by two further months where necessary, taking into account the complexity and number of the requests (provided the individual has been advised of the extension within the first month and been given reasons for the delay).

It will be interesting to see how much this right is used within an employment context.

6. The right to erasure (or "the right to be forgotten")

GDPR includes a right for employees to have their personal data erased without undue delay.

The right to erasure of data will apply to employees:

- Where their data is no longer necessary for the purpose it was collected, or processed, or if it was unlawfully processed.
- Where the employee has withdrawn their consent or objects to the processing of their data.

However, your co-operative will have the right to retain the personal data to:

- Comply with another legal obligation.
- Establish, exercise or defend a legal claim e.g. tribunal proceedings.

7. Right to notify

If you have shared the relevant data with a third party (i.e. a payroll provider or a training provider), your organisation must take reasonable steps to inform that party of the individual's wish for their data to be erased, rectified or restricted unless this will involve disproportionate effort.

8. Right of access

GDPR brings in further rights of access (above that currently in the DPA 98) for individuals in relation to their data and these rights to information to be provided to an individual include:

- The categories of personal data concerned.
- Whether their data has been or will be disclosed in third countries or international organisations.
- Where possible, the expected period for which the personal data will be stored, or, if not possible, the criteria used to determine that period.
- The existence of the right to request from the employer rectification or erasure of their personal data or restriction of processing of personal data concerning the data subject or to object to such processing.
- The right to lodge a complaint with a supervisory authority.
- The existence of automated decision-making, including profiling and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

9. Right to object to automated decision making including profiling

Under the GDPR individuals have the right not to be subject to a decision based solely on automated processing including profiling which produces legal effects on the individual or significantly affects them.

This does not apply where:

- The decision is necessary for entering into or performance of a contract between the individual and the controller.
- The decision is based on EU or UK law
- The decision is based on the individual's explicit consent.

Where profiling involves sensitive personal data, there are specific restrictions. However, automated decisions on these grounds in an employment context could amount to discrimination and are to be avoided.

Section 7: Business Obligations

Unlike the DPA 98, the GDPR imposes a significant burden for demonstrating compliance with the data protection regime on both data controllers and data processors. This contributes to the overall principle of accountability.

Subject Access Requests

GDPR brings in specific changes to subject access requests (SARs) and these are summarised in the table below.

SARs can often be a labour intensive and time consuming process. It will be important for HR departments to make themselves aware of the changes and make preparations for processing SARs in compliance with the GDPR.

This will include updating policies and procedures and reviewing what resource may be needed to complete the requests.

	DPA 98 (Before May 2018)	GDPR (After May 2018)
Timing of delivery of information following receipt of request	Within 40 days from receipt of the request.	**Without undue delay and at latest within 1 month of receiving the request.** The period **may be extended by 2 months** taking into account the complexity and number of the requests. You must inform the individual of any extension within 1 month of receiving the request, together with the reasons for the delay.
Fees	Fees can be charged up to £10.	No fee for a single copy of the requested data. Reasonable administrative charges for further copies. Where requests are manifestly unfounded or excessive, a reasonable fee is allowed taking into account the administrative costs involved.
Format of request	In writing.	No requirement for request to be made in writing and could be made verbally.

Format of delivery of data	Data to be provided in an intelligible form	Where the data is requested electronically, where possible the data should be provided electronically. In all other cases, the data should be provided in a "concise, transparent, intelligible and easily accessible form, using clear and plain language". If requested by the data subject, the data may be provided orally provided identity has been proven.

If following a request you do not take action on the request you should inform the individual as soon as possible and at the latest within 1 month of receipt of the request of the reasons for not taking action. You should also inform the individual of the possibility of lodging a complaint with a supervisory authority and to seek judicial remedy.

Relationship with Data Processors

Any contract put in place with a data processor (e.g. a training provider or payroll provider etc) must impose certain obligations on that processor. You will need to ensure that colleagues managing the procurement process understand the requirements. You can find a full list of the requirements on the ICO website.

Data Protection Officer

As currently drafted, under GDPR your organisation will only be required to appoint a data protection officer (DPO) where your organisation's core activities require regular and systematic monitoring of data subjects on a large scale or consist of processing data relating to criminal convictions and offences on a large scale. However, the Data Protection Bill (currently under debate) suggests that all data controllers may have to put in place a data protection officer.

Many organisations are waiting for guidance from the ICO whether this requirement will be applicable to them.

The DPO will be required to abide by strict confidentiality obligations and must ensure their independence.

Demonstration of compliance

The GDPR refers to a number of ways in which an organisation can help demonstrate compliance with the regulations including:

- Adherence to an approved code of conduct or an approved certification mechanism.
- Documenting of all personal data breaches.
- Adopt internal policies and implement measures which meet the principles of data protection by design, and data protection by default. Examples given by GDPR include minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features.

In order to demonstrate compliance, the controller or processor should maintain records of processing activities under its responsibility. Each controller and processor should be obliged to cooperate with the supervisory authority and make those records, on request, available to it, so that it might serve for monitoring those processing operations.

Privacy by design

Organisations must implement appropriate technical and organisational measures to ensure compliance with the Data Protection Principles. The GDPR states that organisations can obtain a certificate from an approved body to evidence compliance.

Your organisation must also implement appropriate measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be processed. These may include:

- Pseudonymisation and encryption.
- Ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems.
- Ability to restore the availability and access to personal data in a timely fashion in the event of a physical or technical incident.
- Process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of processing.

Maintain records of data processing

Under the GDPR organisations with more than 250 employees have a duty to keep records of their data processing and for this purpose organisations should keep accurate written (hard copy or computer based) records of the following:

- The name and contact details of the controller and their representative.
- Name and contact details of the DPO (where applicable).
- The purposes of the processing.
- A description of the categories of data subjects and of the categories of personal data.
- The categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations.
- Where applicable the transfer of personal data to a non-EEA third country or an international organisation –including the identity of the third country or international organisation and where applicable documentation of suitable safeguards.
- Where possible, the envisaged time limits for erasure of the different categories of data.
- Where possible, a general description of the technical and organisational security measures in place.

There are similar requirements for data processors.

Organisations will not have to comply where they have less than 250 employees, unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data or personal data relating to criminal convictions and offences. The definition of 'rights and freedoms' is the same as other parts of the regulations.

Data Protection Impact Assessment (DPIA)

Where processing is likely to result in a high risk to individuals rights and freedoms in particular where a new technology is being used (e.g. use of new software) a data protection impact assessment should be carried out.

A DPIA must also be carried out where there is:

1. A systematic and extensive evaluation of personal aspects relating to individuals based on automated processing and on which decisions that legally affect or significantly affect the individual are based.
2. Processing is carried out on a large scale of special categories of data
3. A systematic monitoring of a publicly accessible area on a large scale

Section 8: Data Protection Breaches – Notification and Recording

Currently there is no requirements for an organisation (unless a telecoms or internet provider) to inform data subjects or the Information Commissioners Office ('ICO') where there has been a breach of data security.

This changes with the introduction of the GDPR, when obligations are placed on organisations to notify certain types of personal data breaches to the individual/data subject and the ICO. Your organisation will also need to keep a log of all breaches.

1. Reporting

When will you need to report a data protection breach?

Notification to regulator: Employers have a duty to inform the ICO without delay, and where feasible, **within 72 hours** of becoming aware that an individual's personal data has been 'breached' unless the breach is unlikely to affect the rights and freedoms of the employee.

Notification to employee: There is no need to notify a breach to an employee unless the breach is likely to result in a high risk to the rights and freedoms of the employee.

Similarly, if technical measures have been put in place that make the data unintelligible (e.g. encryption) or subsequent measures have been taken to mitigate the risk to the individual's rights or freedoms, there is no need to notify the data subject. If the duty to notify would involve disproportionate effort, a public communication or similar step may be suitable.

What is a personal data breach?

GDPR defines a personal data breach 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."

What does is meant by the phrase 'rights and freedoms' of the employee?

This definition was already included with the DPA but is set out within the GDPR as:

- Processing that could give rise to discrimination, identity theft, fraud, financial loss, reputational damage, reversal of pseydonymisation, significant economic or social disadvantage.
- Processing that could reveal sensitive personal data.

What do you have to report?

Where notification is required this should include the following information:

1. The nature of the personal data breach including (if possible), the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned.
2. The name and contact details of the data protection officer or other contact point where the regulator can obtain more information.
3. The likely consequences of the personal data breach.

4. Measures (or proposed measures) taken to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

2. Records

How will my co-operative keep a record of breaches that have taken place?

Your co-operative will need to keep a record of all breaches (whether notifiable or not) and the record should contain:

1. The facts of the data breach
2. The effects of the data breach
3. The action taken

The record will enable the regulator to check compliance with the regulations.

Steps to take now:

- Ensure your staff understand what constitutes a data breach, and that this is more than a loss of personal data.
- Ensure that you have an internal reporting procedure in place, this could also be incorporated into the whistleblowing policy. This will facilitate decision-making about whether you need to notify the relevant supervisory authority or the public.
- In light of the tight timescales for reporting a breach - it is important to have robust breach detection, investigation and internal reporting procedures in place.

Section 9: Penalties

The penalties have increased under the GDPR. Where a serious breach has taken place, your organisation could be fined up to £18 million, or 4% total worldwide annual turnover (whichever is the higher).

Clearly the size of the fines could severely impact non-compliant businesses. Previously fines were set at a maximum of £500,000. The ICO has said that it will take a fair and reasonable approach to enforcement.

Appendix 1: Useful resources

ICO – Overview of the General Data Protection Regulation
https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/

ICO – Preparing for GDPR
https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

GDPR Regulation
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

ICO Employment Guidance
https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf

EU GDPR
http://www.eugdpr.org

UK Government press release
https://www.gov.uk/government/news/government-to-strengthen-uk-data-protection-law

Appendix 2: Checklist and Audit Tool

STEPS TO TAKE		✓ COMPLETED
AWARENESS		
1.	Are decision makers and key people in the business aware that the law around data protection is changing?	
2.	Does the business understand and appreciate the impact GDPR is likely to have?	
3.	Has the business highlighted areas which could cause compliance issues under GDPR?	
4.	Has the organisation raised awareness across the whole business that the GDPR could impact business practices from May 2018?	
5.	Is the business aware of the potential resource implications of GDPR?	
STRATEGY		
6.	Have you set out a strategy of the steps you will take to implement GDPR?	
7.	How will you measure how you are performing against your objectives?	
POLICIES, PROCEDURES AND PROCESSES		
8.	Have you checked your existing data protection policy and related policies to ensure they are up to date with the requirements of GDPR?	
AUDIT		
9.	Do you have a system in place that monitors compliance with the data protection policy?	
10.	Do you regularly review the effectiveness of data handling/processing activities and security controls?	
AWARENESS		
11.	Do you have data protection training in place for staff?	
INFORMATION YOU HOLD		
12.	Have you documented what personal data you hold, where the data has come from and who you share the data with?	
13.	Have you considered an information audit to help you understand the types of data you hold?	
14.	Have you identified where you may be operating as a 'data processor' as well as a 'data controller'?	

LAWFUL BASIS FOR PROCESSING DATA		
15.	Have you identified what types of processing you undertake and the reason for the processing?	
16.	Having identified the types of processing you carry out have you identified and documented the lawful basis on which you are processing data?	
17.	Have you explained the lawful basis in your privacy notices?	
PRIVACY NOTICES		
18.	Have you reviewed and updated privacy notices in line with the requirements of GDPR in advance of the commencement of GDPR?	
CONSENT		
19.	Have you checked how you seek, record and manage consent?	
20.	Can you confirm the following statements when considering the issue of consent as a legitimate reason for processing personal data? Asking for consent a. We have checked that consent is the most appropriate lawful basis for processing. b. We have made the request for consent prominent and separate from our terms and conditions. c. We ask people to positively opt in. d. We don't use pre-ticked boxes, or any other type of consent by default. e. We use clear, plain language that is easy to understand. f. We specify why we want the data and what we're going to do with it. g. We give individual options to consent to independent processing operations. h. We have named our organisation and any third parties. i. We tell individuals they can withdraw their consent. j. We ensure that the individual can refuse to consent without detriment. k. We don't make consent a precondition of a service. l. If we offer online services directly to children (i.e. work experience placements or recruitment), we only seek consent if we have age-verification and parental-consent measures in place.	

	Recording consent a. We keep a record of when and how we obtain consent from the individual. b. We keep a record of exactly what they were told at the time. **Managing consent** a. We regularly review consents to check that the relationship, the processing and the purposes have not changed. b. We have processes in place to refresh consent at appropriate intervals, including any parental consents. c. We consider using privacy dashboards or other preference management tools as a matter of good practice. d. We make it easy for individuals to withdraw their consent at any time, and publicise how to do so. e. We act on withdrawals of consent as soon as we can. f. We don't penalise individuals who wish to withdraw consent. g. Post May 2015 we do not intend to rely on any consents that do not meet the requirements of the GDPR.	
THE RIGHTS OF INDIVIDUALS		
21.	Have you checked and where necessary updated your procedures to ensure you can deliver the rights of individuals under the GDPR in relation to:- a. Right to be informed b. Right of access c. Right to rectification d. Right to erasure e. Right to restrict processing f. Right to data portability g. Right to object h. Right not to be subject to automated decision making including profiling	

SUBJECT ACCESS REQUESTS		
22.	Have you reviewed your procedures and processes to handle SARs under the new timescales?	
23.	Are business stakeholders appropriately trained on the changes to SARs and able to apply the new processes?	
24.	If your department currently handles a large number of SARs, have plans/resource been put in place to deal with the reduced timescale?	
DATA BREACHES		
25.	Do you have procedures in place to detect and investigate personal data breaches?	
26.	Do you have procedures in place to report a data breach (if necessary under GDPR) to the ICO and (if necessary) to the individual(s) concerned?	
27.	Are colleagues appropriately trained on identifying when a data breach should be reported to the ICO and or the individual(s) concerned?	
28.	Do you have a procedure in place to keep a record of all data breaches (whether notifiable or not) containing: 1. The facts of the data breach 2. The effects of the data breach 3. The action taken	
COMPLIANCE		
29.	Is there someone within the HR team with responsibility for data protection?	
30.	Have you assessed under the GDPR whether you are formally required to appoint a data protection officer? 1. Do you carry out large scale systematic monitoring? 2. Do you carry out large scale processing of special categories of data or data relating to criminal convictions and offences?	
CHILDREN		
31.	Do you have systems in place to verify age?	
32.	Do you have a procedure in place to obtain parental or guardian consent for any child under 16?	
INTERNATIONAL ACTIVITIES		
33.	If you operate in more than one EU member state have you determined who your lead data protection supervisory authority is and documented this?	

RECORDS OF PROCESSING ACTIVITIES		
34.	If you have more than 250 employees have you been keeping suitable records of your processing activities including- a. The name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection office. b. The purposes of the processing. c. A description of the categories of data subjects and of the categories of personal data. d. The categories of recipients to whom the personal data have been or will be disclosed including recipients in non-EEA countries or international organisations. e. Where applicable, transfers of personal data to a non-EEA country or an international organisation, including the identification of that country or international organisation and, in the case of transfers, the documentation of suitable safeguards. f. Where possible, the envisaged time limits for erasure of the different categories of data. g. Where possible, a general description of the technical and organisational security measures taken. If you have less than 250 employees you do not need to keep the records above unless: ▪ The processing you carry out is likely to result in a risk to the rights and freedoms of data subjects. ▪ The processing is not occasional. ▪ The processing which you carry out includes special categories of data or personal data relating to criminal convictions and offences.	
DATA PROTECTION BY DESIGN AND DEFAULT		
35.	Have you implemented appropriate technical and organisational measures to show you have considered and integrated data protection into your processing activities?	
DATA PROTECTION IMPACT ASSESMENTS		
36.	Have you established whether your processing activities fall under the requirement in the GDPR for you to have to undertake data protection impact assessments? a. Will you be using a new technology, and taking into account the nature, scope, context and purposes of the processing, is it likely to result in a high risk to the rights and freedoms of individuals?	

	OR b. Do you use systematic and extensive evaluation of personal aspects relating to individuals which is based on automated processing, including profiling, and on which decisions are based that produce legal effects or significantly affect individuals? OR c. Do you process on a large scale, special categories of data or of personal data relating to criminal convictions and offences? OR d. Do you undertake systematic monitoring of a publicly accessible area on a large scale?	
37.	Do you have an individual appointed with responsibility to determine whether a DPIA is required?	
38.	If a DPIA is required, do you have a suitably experienced individual to carry out the DPIA?	
39.	If a DPIA indicates there is high risk, who in the organisation can help address these risks?	
40.	If any risks cannot be sufficiently addressed to the requirements of GDPR, is there a procedure in place to consult the ICO and who in the organisation will do this?	

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

www.uk.coop/hrservices

Contact our advice team to discuss how it could benefit your co-op.

T: **0161 214 1750** E: **advice@uk.coop**

CO-OPERATIVES UK

www.uk.coop/gdprtoolkit