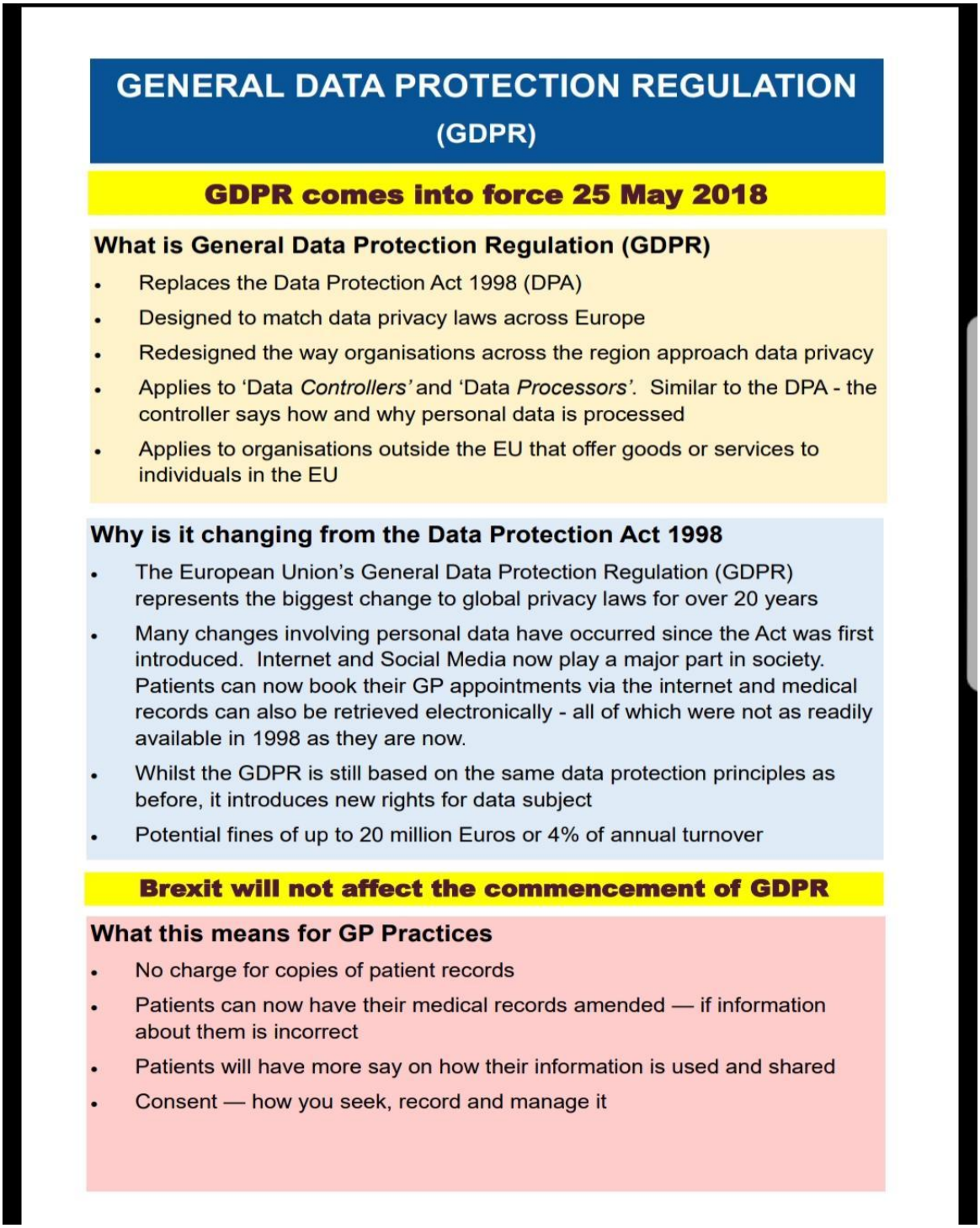
PELC
Partnership of East London Co-operatives Ltd

PELC GENERAL DATA PROTECTION REGULATION (GDPR) 2018 GUIDANCE

What is the GDPR?

The **General Data Protection Regulation** (GDPR)) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU).



Information Commissioner's Office —12 Steps to GDPR

1. ***Awareness*** – You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.

2. ***Information you hold*** – You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit

3. ***Communicating privacy information*** – You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

4. ***Individuals' rights –*** You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

5. ***Subject access requests*** – You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

6. ***Lawful basis for processing personal data –*** You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.

7. ***Consent –*** You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.

8. ***Children –*** You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.

9. ***Data breaches –*** You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

10. ***Data Protection by Design and Data Protection Impact Assessments –*** You should familiarise yourself now with the ICO's code of practice on Privacy Impact Assessments as well as the latest guidance from the Article 29 Working Party, and work out how and when to implement them in your organisation.

11. ***Data Protection Officers –*** You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements. You should consider whether you are required to formally designate a Data Protection Officer.

12. ***International –*** If your organisation operates in more than one EU member state (ie you carry out cross-border processing), you should determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you do this.

Who does the GDPR apply to?

The GDPR applies to ‘controllers’ and ‘processors’.

The definitions are broadly the same as under the DPA – i.e. the controller says how and why personal data is processed and the processor acts on the controller’s behalf. Further reading in the GDPR (See Articles 3, 28-31 and Recitals 22-25, 81-82

What information does the GDPR apply to?

Personal data

Like the DPA, the GDPR applies to ‘personal data’. However, the GDPR’s definition is more detailed and makes it clear that information such as an online identifier e.g. an IP address – can be personal data.

Sensitive personal data

The GDPR refers to sensitive personal data as 'special categories' of personal data. These categories are broadly the same as those in the DPA, but there are some minor changes, e.g. the special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual. Further reading in the GDPR (See Articles 2, 4, 9, 10 and Recitals 1, 2, 26, 51)

Key areas to consider:

Lawful processing

For processing to be lawful under the GDPR, you need to identify a lawful basis before you can process personal data. Referred to as the “conditions for processing” under the DPA. Further reading in the GDPR (See Articles 6-10 and Recitals 38, 40-50, 59)

Consent

Consent under the GDPR must be a freely given, specific, informed and unambiguous indication of the individual’s wishes.

There must be some form of clear affirmative action – or in other words, a positive opt-in – consent cannot be inferred from silence, pre-ticked boxes or inactivity. Further reading in the GDPR (See Articles 4(11), 6(1)(a), 7, 8, 9(2)(a) and Recitals 32, 38, 40, 42, 43, 51, 59, 171)

Children's Personal Data

The GDPR contains new provisions intended to enhance the protection of children’s personal data

The GDPR states that, if consent is your basis for processing the child’s personal data, a child under the age of 16 can’t give that consent themselves and instead consent is required from a person holding ‘parental responsibility’ – but note that it does permit member states to provide for a lower age in law, as long as it is not below 13. Further reading in the GDPR (See Article 8 and Recitals 38, 58, 71)

ICO Draft Guidance on Children and the GDPR

Individual's rights

The GDPR creates some new rights for individuals and strengthens some of the rights that currently exist under the DPA.

The GDPR provides the following rights for Individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

1. **The right to be informed**

The right to be informed encompasses your obligation to provide 'fair processing information', typically through a privacy notice. It emphasises the need for transparency over how you use personal data. Further reading in the GDPR (See Articles 12(1), 12(5), 12(7), 13, 14 and Recitals 58-62)

2. **The right of access (Subject Access Requests)**

The GDPR clarifies that the reason for allowing individuals to access their personal data is so that they are aware of and can verify the lawfulness of the processing.

A copy of the information must be provided free of charge. The removal of the £10 subject access fee is a significant change from the existing rules under the DPA.

There will be less time in which to comply with a subject access request under the GDPR. Information must be provided without delay and at the latest within one month of receipt. Further reading in the GDPR (See Articles 12, 15 and Recital 63)

3. **The right to rectification**

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete.

If you have disclosed the personal data in question to third parties, you must inform them of the rectification where possible. You must also inform the individuals about the third parties to whom the data has been disclosed where appropriate. Further reading in the GDPR (See Articles 12, 16 and 19)

4. **The right to erasure (the right to be forgotten)**

The right to erasure is also known as 'the right to be forgotten'. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing. Further reading in the GDPR (See Articles 17, 19 and Recitals 65 and 66)

5. **The right to restrict processing**

Under the DPA, individuals have a right to 'block' or suppress processing of personal data. The restriction of processing under the GDPR is similar. When processing is restricted, you are permitted to store the personal data, but not further process it. You can retain just enough information about the individual to ensure that the restriction is respected in future. Further reading in the GDPR (See Articles 18, 19 and Recital 67)

6. **The right to data portability**

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. Further reading in the GDPR (See Articles 12, 20 and Recital 68)

7. **The right to object**

Individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

Further reading in the GDPR (See Articles 12, 21 and Recitals 69, 70)

8. **Rights related to automated decision making and profiling**

The GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention. These rights work in a similar way to existing rights under the DPA. Identify whether any of your processing operations constitute automated decision making and consider whether you need to update your procedures to deal with the requirements of the GDPR. Further reading in the GDPR (See Articles 4(4), 9, 222 and Recitals 71, 72)

Accountability and Governance

The GDPR includes provisions that promote accountability and governance. These complement the GDPR's transparency requirements. While the principles of accountability and transparency have previously been implicit requirements of data protection law, the GDPR's emphasis elevates their significance. Further reading in the GDPR (See Article 30, Recital 82)

Data Protection by Design and by Default

Under the GDPR, you have a general obligation to implement technical and organisational measures to show that you have considered and integrated data protection into your processing activities. Further reading in the GDPR (See Article 25 and Recital 78)

Data Protection Impact Assessments

Data protection impact assessments (DPIAs) (also known as privacy impact assessments or PIAs) are a tool which can help organisations identify the most

effective way to comply with their data protection obligations and meet individuals' expectations of privacy. An effective DPIA will allow organisations to identify and fix problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur. While not a legal requirement under the DPA, the ICO has promoted the use of DPIAs as an integral part of taking a privacy by design approach. See the ICO's Conducting privacy impact assessments code of practice for good practice advice. Further reading in the GDPR (See Articles 35, 36, 83 and Recitals 84, 89-96)

PELC Data Protection by Design and Data Protection Impact Assessment Guidance Note

Data Protection Officer **(Michaelene Holder-March)**

Under the GDPR, you **must** appoint a data protection officer (DPO) if you:

- are a public authority (except for courts acting in their judicial capacity);
- carry out large scale systematic monitoring of individuals (for example, online behaviour tracking); or
- carry out large scale processing of special categories of data or data relating to criminal convictions and offences.

Further reading in the GDPR (See Articles 37-39, 83 and Recital 97)

Data Breach Notification

The GDPR will introduce a duty on all organisations to report certain types of data breach to the relevant supervisory authority, and in some cases to the individuals affected. Further reading in the GDPR (See Articles 33, 34, 83 and Recitals 85, 87, 88)

Transfers of Data to Third Countries or International Organisations

The GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations, in order to ensure that the level of protection of individuals afforded by the GDPR is not undermined

Further reading

Link Policies