eastlaw
efficiency, economy, expertise

An introduction to GDPR

The General Data Protection Regulations ("**GDPR**") come into force on 25 May 2018 and will overhaul the current system of data protection as set out by the Data Protection Act 1998. The GDPR goes into far more depth than the current legislation and means that local government and members alike need to reassess the way in which the public's data is collected, stored and processed.

Before looking at some of the key provisions of the GDPR in more detail below, it is a good idea to look at the rationale behind the changes and why they have come about.

The precursor to the GDPR is the Data Protection Act 1998, which until the 25 May 2018 is still the current data protection legislation in UK law. One of the main calls for an updated system was due to the age of the current legislation. The law came into force 20 years ago and since that time the way in which data is received, processed and stored has changed dramatically.

Whilst computers would have been a fairly common site in offices in 1998, since then we have seen an explosion of portable devices that are capable of carrying out the same tasks, such as smart phones and tablets. Data can be accessed instantly almost anywhere and at any time and this was simply not a consideration in 1998.

Equally, the GDPR provides identical protection and governance to all those living the European Economic Area, ensuring consistency across the board, something that was previously lacking with the old legislation.

Whilst members do not generally process large amounts of personal data, there is nonetheless a need to be aware of the key changes under the new legislation.

Some of the main salient points that need to be considered prior to implementation are as follows:

1. Consent

Consent is one of the ways in which data may be processed under GDPR. This may be particularly important for members, more so than for the Council, as you may not be able to rely on a legal basis (i.e. legislation that provides you with powers to process personal data), for the data that is processed.

The way in which members deal with consent surrounding the information that is received by members of the public is perhaps the biggest point to consider.

Under the GDPR anyone that you hold personal information on must give their explicit 'informed' consent for their data to be retained for a set period of time and processed, **unless there is another legitimate basis for processing that data.** This means that the individual **must** be made aware of how their information is protected, what it is used for etc.

2. New Privacy Policy Agreements

The GDPR makes it clear that all privacy policies need to provide specific details as to how data is treated and more importantly protected. The GDPR promotes user-friendly plain English policies that are easy to understand and clearly set out the way in which data is collected and processed by councils.

3. The Right to be forgotten (right to erasure)

This is perhaps one of the most popularised changes to come out of the GDPR legislation and has been much talked about both in professional circles and within the press.

The premise of the right to be forgotten under the GDPR, is that individuals have more power to withdraw their consent and to have their personal data amended, rectified or deleted. The right to be forgotten is a principle that has become more and more prevalent and has had quite a lot of press attention particularly surrounding online search engines such as Google. The issue that could potentially arise here is that some IT systems do not actually allow the right to be forgotten, this is the case even from some leading software vendors.

This is something that members should consider when working on iPads and other electronic devices as although data me have been deleted, there will often remain a trace of it somewhere.

4. Subject Access Requests

GDPR gives individuals the right to make a subject access request at any time and get a response within 1 month, whereby the timescale under current legislation is 40 days.

The council needs to ensure that it has processes in place to be able to meet the deadlines as if not it runs the risk of incurring substantial financial penalties. The council has reviewed and updated its policy on dealing with SARs to ensure that we remain compliant under the GDPR and this is available on the BCKLWN website if members wish to familiarise themselves with the changes.

5. Appointment of a Data Protection Officer ("DPO")

Whilst BCKLWN already has a designated DPO, it is important to emphasise that under the GDPR, DPOs are responsible for monitoring compliance, educating staff on their role and responsibilities under the GDPR etc.

Under the GDPR, a number of data breaches which were previously not reportable, will now be reportable and on top of this, the timescales are much stricter.

Where a member is concerned that a potential data breach has occurred, **they should notify the DPO as soon as they become aware of the potential breach** so that steps can be taken to firstly determine whether a breach has occurred and secondly to minimise the impact of a determined breach.

6. Need for Parish Councils to appoint a Data Protection Officer

Under the Data Protection Act, Parish Councils are not required to have a DPO, but under the GDPR, this is going to become a legal requirement.

All Parish Councils, irrespective of size will need to appoint a DPO who will have overall responsibility for the handling of the personal data of parishioners.

This is not exclusive to Parish Councils and in fact, under the GDPR, all schools as well as a large number of other public bodies will be required to appoint a DPO.

The legislation takes it one step further and states that the DPO must have in-depth knowledge of data protection systems and processes. Furthermore, Parish Councils will also have to adhere to the new rules surrounding Freedom of Information and Subject Access Requests.

Key Points for members to consider

- Have a think about the personal data you receive, what kind of information are you provided with and what are the most common reasons for being provided with this data;
- What do you do with the personal data you receive, how is it processed and treated;
- Familiarise yourself with the updated processes for Freedom of Information requests and Subject Access Requests ahead of 25 May 2018;
- Attend training session run by Eastlaw in May 2018 (date to be confirmed), to gain a more in-depth knowledge of GDPR.

Who to contact if you have any questions:

The GDPR is a vast piece of legislation and we recognise that members will likely have questions in relation to the new rules, both prior to the 25th May 2018 and even once GDPR has come into force.

If you have any specific queries or wish to discuss GDPR generally, then please feel free to contact a member of the Eastlaw team.

The best person to contact in the first instance is Jake Currier, Trainee Solicitor, who can be reached via the following details:

Email: jake.currier@eastlaw.org.uk
Tel: 01263 516416