Report to Cabinet

Subject: Introduction of the General Data Protection Regulation and the forthcoming Data Protection Act 2018

Date: 3rd May 2018

Author: Craig Allcock – Legal Advisor

Wards Affected

Not applicable.

Purpose of the Report

To advise Members in relation to the implications of the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 which will replace the Data Protection Act 1998 (DPA 1998); .

To update Members as to the steps being taken to ensure the Council is able to comply with the legislative changes and seek approval for amendments to policy and delegated powers.

Key Decision

This is not a Key Decision.

Background

1.1 The legislation governing data protection in the UK is changing. The Data Protection Act 1998 is being repealed and replaced by the GDPR and the Data Protection Act 2018, which is currently being considered by parliament. Whilst the Act is not yet in force, the GDPR will come into force in the UK with effect from 25 May 2018 at which point the Council is expected to be compliant. This report sets out the work already carried out to ensure compliance with the GDPR, however Members are to note that further legislation is awaited and ICO guidance has not been issued on all aspects of the new legislative framework. Whilst excellent progress has been made there is still work to do. Despite the UK's vote to leave the EU, the UK will still be a member of the EU when the GDPR comes into force in May. Following the UK's withdrawal from the EU, the Government has already confirmed that the GDPR will continue to govern data protection in the UK to ensure that the country's data protection framework is "*suitable for our new digital age, allowing citizens to better control their data".* Further to this, the Information Commissioner's Office (ICO) have also confirmed that the UK will mirror the GDPR as deviation from it could deem the UK as an inadequate country for data protection purposes and affect any post Brexit trade with the EU.

1.3 The GDPR has a much greater focus on individuals and what rights they have over their personal data. It places a greater emphasis on transparency and requires the Council to have and maintain clear documentation and records to demonstrate accountability. From a practical perspective, this means that it is not sufficient for the Council to have processes in place to comply; the Council has to have documentation in place to be able to evidence that it complies with the GDPR. Much of the work carried out so far has been behind the scenes to document the personal data the Council holds and amending and creating a number of documents.

Summary of additional requirements under the new legislation

1.4 There are a number of additional requirements that the Council must be able to meet to be able to demonstrate compliance with the new legislation. The Council is expected to have implemented technical and organisational measures to demonstrate that data protection compliance has been considered and integrated into all its day-to-day tasks. The Council must also appoint a Data Protection Officer, a statutory role, who will be responsible for ensuring on going data protection compliance.

1.5 The Council must be transparent in the way it handles personal data and must supply detailed information to individuals about how their information is being used. We must keep and publish records to show how we process information, where we receive it from, who we share it with, the basis for processing, how long we retain the information, categories of information and any international transfers of information.

1.6 Where personal information is lost or compromised the GDPR introduces a new duty on all organisations to report all significant breaches to the ICO within 72 hours. Significant breaches occur when personal data is lost or compromised and where the loss of that data is likely to result in a risk to the rights and freedoms of individuals or any harm to the individual. Minor breaches which do not put an individual at risk will not need to be reported to the ICO but will still need to be documented by the Council.

1.7 Data Protection Impact Assessments (DPIA) are now mandatory for certain types of processing such as when new technologies and processes are being used. They are also compulsory if the processing of personal data is likely to result in a high risk to the rights of individuals. A DPIA as in assessment of a process or procedure where personal data is being processed. The DPIA will help to identify and minimise any data protections risks associated with the processing.

Where the Council currently processes personal data on the basis that the individual has given their consent for the Council to have and use their data, the threshold for what constitutes valid consent will be a lot higher. The Council must be able to demonstrate that an individual has given informed consent for their data to be used. Currently under the DPA 1998 it is sufficient to ask individuals to tick a box if they do not want the Council to contact them for certain purposes such as newsletters, if not ticked it is implied that the individual gives their consent. Under the GDPR this will no longer be acceptable, the Council must be able to demonstrate that the individual has actively and freely given their consent. This does away with the implied consent and individuals must now actively tick a box if they do want to be contacted by the Council for some purposes. The individual

must also be able to withdraw their consent at any time. In some circumstances individuals have the right to request that their information is erased, they also have the right to restrict the processing of their information. Based on the current guidance, the Council's reliance on consent as a basis for processing will be limited in the future. This is because the imbalance of power between the Council and an individual means that we will need to take extra care to show that consent is freely given and that refusal to give consent will not restrict the individual's right to access services.

1.9 The 'legitimate interest' condition is currently relied on by the Council as a basis for processing and is often used by private companies once a sale has taken place to contact customers to attempt to sell further goods. As a Public Authority the Council can no longer rely on legitimate interest as a legal basis for processing personal information for the normal day-to-day tasks of the Council. Although the Data Protection Bill in its current form does allow for legitimate interest to be used as a basis for processing for commercial activities.

1.10 Individuals can make a request for copies of the information the Council holds about them, this is known as a Subject Access Request. Under the current legislation the individual must pay a £10.00 fee to receive their information, under the DPA 1998, the Council has 40 calendar days to respond to the request. The GDPR removes the £10.00 fee and reduces the 40 days to one month. There is also an emphasis on providing the information to the individual in an electronic format, where possible. The number of Subject Access Requests received fluctuates each year, but is not significant: 12 were received in 2017 and 6 in 2016 and it is worth noting that a number of requests are closed because the individual did not pay the £10 fee. The removal of the fee could result in a significant increase in Subject Access Requests and place an additional burden on staffing resources, which will need to be monitored.

1.11 The GDPR acknowledges the vulnerabilities of children and their personal information. When dealing with information from children the minimum age for giving consent to the processing of that information will be 13 years, parental consent will be required for anyone under the age of 13. Any privacy information or policies used by the Council to communicate how we process personal data should be written in a way that can be understood by children.

1.12 Any contractors processing personal data on behalf of the Council are expected to have implemented similar technical and organisational measures to protect the personal information given to them by the Council. Contractors will be expected to inform the Council of any data breaches without undue delay to allow the Council enough time to notify the ICO if necessary.

1.13 The maximum fine for breaches and non-compliance under the current legislation is £500,000.00. Under the GDPR the maximum fine will be significantly higher, €20 million or 4% annual turnover, whichever is highest sum.

1.14 The Council as a data controller and processor is required to register with the ICO annually. The current registration fee for the Council is £500.00 but the Digital Economy Act 2017 allows the ICO to change their fee structure. As of 25 May 2018 the ICO will implement a new fee structure which increases the ICO registration fee for the Council from £500 to up to £2900. This higher fee is payable by all organisations with more than 250 employees. The new Data Protection fee to be paid by councillors at the next annual renewal will be £40.

Steps taken to prepare for the introduction of the GDPR

1.15 In 2016 the Information Commissioner's Office (ICO) published guidance for organisations titled 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'. The guidance outlines 12 steps all organisations should be taking to ensure compliance on 25th May 2018. The Council is a member of the Nottinghamshire Information Officers Group (NIOG) alongside colleagues from all district councils across the county, the County Council, City Council, Fire authority and Police. NIOG has been working together sharing knowledge and documentation based around the ICO's guidance to ensure a similar approach is being taken across the county and that all districts and partner agencies are able to comply with the GDPR. NIOG has been meeting bimonthly to discuss and action any work required. Over the past 12 months the Council's Legal team has spent significant amounts of time and effort ensuring that the Council are able to comply with the GDPR and demonstrate that action has been taken for each of the 12 steps recommended by the ICO.

1.16 **Step 1 - Raise awareness** An introduction to the GDPR has been included in the mandatory data protection training for all officers, in total nine sessions were held between October 2017 and February 2018. Members were given an introduction to the GDPR as part of the ICO registration session in November. The Legal team circulated a briefing note, outlining the changes and what the Council needs to do to ensure compliance, to SLT and all Service Managers in December 2017. Further detailed training will be delivered and all officers will be briefed on the changes and new requirements. Training for Members will also be provided. 1.17 **Step 2 - Review the information you hold** A data audit of all the personal information held by the Council took place between November 2017 and March 2018. All service areas have produced a spreadsheet identifying all activities which involve the processing of personal data. The combination of these spreadsheets forms the Council's Information Asset Register (IAR) a document which identifies and records what personal data we have, where it is stored, where we receive the data, who we share it with and how long we will keep it for. Moving forward the IAR will be reviewed on an annual basis and kept up to date. 1.18 **Step 3 - Communicating privacy information** The GDPR requires certain information to be provided to individuals at the point of collecting personal data through a privacy notice. A privacy notice specifies information such as the Council's reason for processing the data, how long the data is held for, who the data is shared with and the individuals rights over their personal data. The GDPR doesn't state exactly how this information should be communicated to individuals, but the Council has worked with other councils in Nottinghamshire to agree templates to ensure that there is some consistency locally. All privacy notices currently being used are under review, a short form privacy notice template has been designed to be provided at the point of collecting personal data with longer more detailed privacy notices being added to the Council's website for each service area.

1.19 **Step 4 - Review procedures and be able to comply with individual rights** Where individuals wish to exercise the 'right to be forgotten' and ask for their personal data to be deleted the individual will send their request to legal services, who will then check the IAR to identify where we hold the personal data and whether the basis for processing is consent and then inform each service area accordingly to delete that individuals records. 1.20 **Step 5 - Update Subject Access Request procedures** Legal services have updated all template letters, applications, policies and procedures to ensure that requests can be handled

within the shorter one month timescale. All Freedom of Information representatives across the Council have been informed of the new shorter timescale and are aware that responses need to be sent out within this time. The GDPR also requires additional information about how individual's data is held and used by the Council be available to individuals. To comply with this, a shortened public version of the IAR, which includes this information, will be published on the Council's website. The request response will refer individuals to this.

1.21 **Step 6 - Legal Basis for Processing Personal Data**

In order for the Council to process personal data there must be a lawful basis for doing so. There are six legal basis's for processing personal data under the GDPR. These are that the individual has given their consent, that the data is needed for the performance a contract, that the data is needed to comply with a legal obligation, that the data is needed to protect the vital interest of the individual or another person, that the data is needed for the performance of a public task vested in the Council, or that the data is needed for the purpose of legitimate interest. As mentioned above, the Council's reliance on consent and legitimate interests will be limited in future and in the main, we will rely on public task and contract. The legal basis for processing personal information has been identified for all activities and recorded on the Information Asset Register.

1.22 **Step 7 - Review how consent is captured and recorded**

If the Council is currently processing information through implied consent, then processing will continue after 25 May 2018 if the Council can rely on public task or contract. However if this is not available, the processing will cease unless freely given consent has been recaptured and a positive indication of consent has been given. The process for capturing consent across the council has been reviewed and any tick boxes have been amended and replaced.

1.23 **Step 8 - Children**

As best practice the Council will treat the age of consent as 16. Any information obtained from an individual under the age of 16 will require parental consent where possible. The IAR identifies the activities where we are obtaining information from children and appropriate steps will be put in place to ensure that GDPR compliant consent will be obtained in future.

1.24 **Step 9 - Procedure for reporting Data Breaches**

The current breach reporting process has been reviewed. The Information Security Incident Management section of the Information Security Policy will need amending and updating to reflect the 72 hour reporting timeline to the ICO in the event of a serious breach where the loss or compromise of data may affecting the freedoms of individuals or lead to a risk of harm. The breach reporting procedure will be communicated to staff during the data protection training sessions/briefings.

1.25 **Step 10 - Data Protection by Design and Privacy Impact Assessments**

The idea of data protection by design is that data protection is at the forefront of every activity of the Council. This is done by raising awareness of data protection legislation and issues throughout the Council. Officer interaction with Legal Services on data protection issues has increased since the data protection training showing that officers are thinking about data protection in their day to day tasks. The Council will maintain this through ongoing officer training.

With regards to Privacy Impact Assessments, the Council are still awaiting some clarification from the ICO as to what is meant by 'high risk' technologies and processes. However NIOG has produced a template Data Protection Impact Assessment to be used whenever new technology or processing of personal data

is being considered. These assessments will help to identify and minimise any risks arising from the processing of personal data. Where ever high risk processing is identified and the risks to individuals are more than minimal, the Council will consult the ICO for advice and guidance on the processing.

1.26 **Step 11 - Data Protection Officer**

The GDPR requires the Council to designate an officer as its Data Protection Officer ("DPO") and sets out the tasks the DPO must perform. In summary, the role of the DPO is to assist the Council to monitor internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the ICO. The DPO is not personally responsible for data protection compliance but plays a crucial role in ensuring the Council complies. The GDPR also specifies a number of requirements in relation to the role – the DPO must be independent, be appointed on the basis of their professional qualities, and in particular, experience and expert knowledge of data protection law, be adequately resourced, not hold certain positions which would conflict with the role and report to the highest management level.

1.27 **Step 12 - International**

Personal data cannot be transferred out side of the European Economic Area unless the third Country has been approved by the European Commission. The Information Assets Register identifies if any personal data held by the Council is stored or transferred outside the EEA. Where this is the case appropriate checks have been carried out and measures have been put in place to protect it.

In addition to the 12 step guidance the Council is also reviewing all contracts, external processing and data sharing agreements that will still be live after 25 May 2018. All contractors and partners are being contacted and asked to agree to additional contract and agreement clauses to reflect the new GDPR requirements. All new contracts being entered into will include GDPR clauses.

1.29 A requirement of Schedule 1 of the Data Protection Bill is to have an 'appropriate policy document' in place where certain processing is carried out. The Council's Data Protection Policy will need to be amended to include additional information and to reflect the changes in order to be deemed an 'appropriate policy document'. Once the Act is in force and we have clarity about what the Policy needs to include, it will be redrafted and referred to Members for approval.

1.30 Any Council policies which refer to the Data Protection Act 1998 will also need amending to refer to the new legislation.

Proposal

2.1 It is proposed that Members note the implications of the GDPR and forthcoming Data Protection Act 2018 and the steps that have been taken to ensure the Council is compliant.

2.2 Whilst the Council is required to designate a Data Protection Officer, it is not clear at this stage what the workload for the DPO will be. As a temporary measure, for up to 12 months, it is proposed that the Council's Data Protection Officer will be the Service Manager for Legal Services with two deputy DPO's: the Information and Practice Manager and a Legal Advisor (litigation and Licensing). These individuals are suitable for appointment, having knowledge and experience of

dealing with data protection matters, but it is recognised that additional training will be required to ensure that they have expert knowledge in the new legislation. Given the fact that certain data breaches will need to be reported to the ICO within 72 hours, it is crucial that deputising arrangements are in place to ensure cover at all times (potentially including weekends and bank holidays). The temporary arrangements will enable a proper assessment of the workload to be made so that an informed decision can be made about permanent arrangements to be put in place. An honorarium payment will be made to the two post holders designated as Deputy DPO recognising the additional responsibility and at a level to reflect frequency. This will be at a rate of £100 per month per employee (pro rata).

2.2 The Information Security Incident Management section of the Information Security Policy has been amended, in particular to reflect the 72 hour reporting requirement under GDPR. It is proposed that the revised version which appears at Appendix 1 be approved.

2.3 Members will appreciate that there will be a number of existing policies which make reference to the Data Protection Act 1998, which will need to be amended to refer to the new legislation. In order to avoid the need to refer such amendments to Cabinet for approval, it is proposed that the Director of Organisational Development & Democratic Services be authorised to amend all of the Council's policies falling within the remit of the Executive which currently reference the Data Protection Act 1998 to reflect the new legislation.

2.4 The DPO functions specifically listed in the GDPR will be exercised by the DPO or deputy, however in order to enable operational decisions to be made, it is proposed that Members delegate authority to carry out all other functions under the GDPR and DPA 2018 (with specific reference to use of exemptions) to the Director of Organisational Development and Democratic Services.

Alternative Options

3.1 An alternative option is that Members do not grant approval to amend the Information Security policy and the Data Protection Policy. This would mean that the Council's policies and procedures would not be compliant with the legislation changes and could leave the council open to fines of up to €20 million.

3.2 Members could choose not to grant approval to amend the Data Protection Policy and all Executive policies which refer to the DPA 1998. However, this would mean that all policies including DPA 1998 would be out of date and refer to old legislation.

3.3 Members could not appoint a Data Protection Officer but this is a statutory post which must be in place on 25th May 2018, Members could approve another individual within the organisation or externally to take on the role, however at this time, after consideration of the post it is in considered that the Service Manager for Legal Services has the necessary expertise and sits at the appropriate level within the organisation to carry out the role.

3.4 Members could decide not to delegate responsibility for the GDPR implementation, training and compliance to officer level, however, this would place an operational burden on the Executive.

Financial Implications

4.1 There will be minimal financial implications for implementation of the GDPR and DPA 2018 as costs for implementation have been met through current budgets.

4.2 There will be a slight loss of income to the Council with the removal of the £10.00 fee for subject access requests, however this is estimated to be in the region of £100 annually, therefore this is not significant. There could also be an implication on staff time if there is a significant increase in the number of requests to the council. It is unclear at this stage what the loss of income and the impact on resources in both the legal department will be.

4.3 If the council are found to be non-compliant or have a major data breach the ICO can issue fines of up to €20 million.

4.4 If the Service Manager of Legal Services is appointed as the DPO, there will be no financial implications in the first instance as this will be absorbed into the postholder's current responsibilities. There will however be additional remuneration for the Deputy DPOs on a temporary basis as an honorarium. The cost of this for 2018/19 is expected to be approximately £2,300.

4.5 The annual ICO registration will increase from £500 to £2,900. In addition, the fee for individual Councillors to register will increase from £35, to £40 per year, which will require a maximum additional resource of £205 each year.

4.6 The costs of the temporary arrangements for the Deputy DPOs and the increase in the registration fees for 2018/19 will have to be met from savings. Savings have been identified within the Democratic Services Department and subject to portfolio approval a virement will be completed to transfer the budgets. For future years consideration will need to be given as to how this is funded. A develop bid may need to be submitted once we have a better indication of how this will be dealt with and what the more permanent arrangements will be.

Appendices

Appendix 1 – Information Security Incident Management section of the Information Security Policy.

Background Papers

None identified.

Recommendations

THAT Cabinet:

(a) notes the contents of the report and the steps taken to ensure the Council complies with the GDPR and forthcoming Data Protection Act.

(b) designates the Service Manager - Legal Services as the Data Protection Officer from 25 May 2018 and approves the establishment of two Deputy DPO roles as detailed in the report.

(c) approves the amendments to the Information Security Incident Management section of the Information Security Policy at Appendix 1 to the report to take effect from 25 May 2018.

(d) authorises the Director of Organisational Development & Democratic Services to approve amendments to all of the Council's policies falling within the remit of the Executive which reference the Data Protection Act 1998 to refer to the GDPR and/or Data Protection Act 2018.

(e) delegates authority to the DPO or deputy to exercise all the DPO functions listed in the GDPR and delegates all other functions under the GDPR and DPA 2018, with specific reference to use of exemptions, to the Director of Organisation Development and Democratic Services.

Reasons for Recommendation

To ensure the Executive is updated in respect of the Changes in Data Protection legislation and what the Council has done to ensure compliance. To ensure the Council is compliant with the GDPR when it comes into force on 25th May 2018 and the DPA 2018 in due course and to ensure the Executive is not overburdened with operational matters in relation to GDPR implementation and compliance.