**North Yorkshire County Council**
**Corporate and Partnerships Overview and Scrutiny Committee**
**12 March 2018**
**Data protection reform and GDPR**

**Purpose of Report**

To inform the Committee about the forthcoming reform of data protection law, and the measures being taken by the County Council to prepare for it

## Background

The European Union's General Data Protection Regulation (GDPR) will come into force in May 2018. The UK government has introduced a Bill to incorporate it into UK law in advance of "Brexit". The Bill includes aspects of GDPR left to member states to decide, and also incorporates the Law Enforcement Directive.

All the main features of the current regime will remain; but it is no longer enough to comply, it will be necessary to be able demonstrate compliance. It follows that all the good practice being done now should continue, but the governance arrangements must be reviewed and relevant documentation revised and extended.

## Overview of key issues

### Notification and fees

While the requirement to "notify" (register with) the Information Commissioner will go, the Council must still pay a fee and have a written record of all its processing of personal data. It may be that the level of detail required will be similar to that included in the current notification, but it is possible that additional or more extensive information will be necessary.

The fee will increase from the current £500 pa to £2,900. The fee for individual councillors will increase from £35 pa to £40 (both subject to the Bill being passed unamended)

### Consent and Privacy Notices

More information and explanation must be included in the Privacy Notices which must be given to customers, clients and other individuals. In particular they must include the "legal basis" for processing, of which the most relevant to the Council are

- fulfilment of a legal duty (such as safeguarding, or education)
- tasks done in the public interest (including discretionary services)
- performance of a contract (including the contract of employment)

If none of these is available, it may be necessary to rely on the individual's consent. However, in a significant change to current understanding, public authorities will not, in most circumstances, be able rely on consent, because of the supposed imbalance of power. Only if the individual has genuine choice and control will consent be valid. Where it is available, there must be evidence of that consent, which must be fully informed, freely given, and positively signified.

It follows that in many cases the terms of the forms signed by customers and clients will have to be revised so that they take the form of a Privacy Notice explaining what will happen, rather than a request for consent.

An imbalance of power also exists between employer and employee, which means that the Council may not be able to rely on consent to process employees' data.

However most such processing is done in performance of the employment contract, so this is not likely to affect current practice.

**Data Protection Impact Assessments**

Data Protection Impact Assessments (DPIAs) have long been good practice, but will be mandatory if a project poses risks "to the rights and freedoms of data subjects". Examples would include proposals for large scale processing of special category data such as ethnicity, sexuality or health, or extensive CCTV monitoring.

All DPIAs will need to be signed off by the Data Protection Officer. Projects which will involve high-risk data processing may even need approval by the Information Commissioner.

**Data Protection Officer**

All public authorities, as defined in the Freedom of Information Act, must appoint a Data Protection Officer (DPO). This role will be fulfilled for the Council by Veritau Ltd, under the terms of its existing contract.

**Reporting data breaches**

The Council will be obliged to notify the ICO of serious data security incidents without undue delay, and at the latest within 72 hours. Time starts to run from the moment the Council becomes aware of the breach. "Serious" means that there is a risk to the rights and freedoms of individuals. This will probably be decided on the sensitivity of the data, the number of people involved, and the possible consequences to them.

The individuals concerned must be notified as well, if the breach is likely to result in a high risk to their rights and freedoms.

In the event of a breach the following sanctions can be imposed by ICO:

- a written warning in cases of first and non-intentional non-compliance;
- regular periodic data protection audits;
- a fine of up to £17m (ie €20m) (an increase from the current £500k)

The Information Commissioner has said that she does not expect to amend her methodology for assessing the level of each fine so as to increase them significantly; it is simply that a higher maximum is available to her in extreme cases. There is therefore no significant increase in risk to the council here, only the continuing risk of actually suffering a significant data breach and being held culpable.

**Data Processors**

A "Data Processor" is a contractor employed to process personal data. All of the privacy risks fall on the Council as the client of such a contractor, so the contract must ensure the contractor protects privacy properly. This principle is unchanged under GDPR.

Such contractors will in future however have to have their own DPO, if they fulfil the relevant criteria. They will also have to report incidents to ICO as well as the Council. They may not employ subcontractors without Council consent.

Data processing contracts must therefore be identified and reviewed, to ensure these risks are properly provided for. Standard clauses have been suggested by the Crown Commercial Service.

**Data Subjects' rights**

Subject access requests must be answered within one month (reduced from forty days) although for complex or bulky requests the Council may notify the requester of an extension of a further two months. No charge may be made.

The so-called right to be forgotten: a data subject may require erasure of some or all of his or her personal data, on any of a number of grounds, unless there are legitimate grounds for it to be kept. The Regulation reverses the burden of proof so that the Council must demonstrate that it must retain the data, rather than the data subject showing how the processing is causing him or her harm.

**Preparation and risk mitigation**

The Corporate Information Governance Group, chaired by the Corporate Director, Strategic Resources, has agreed an activity plan based on the ICO's 12 Step Plan for preparing for the GDPR, which will lead to compliance within the "grace period" of twelve months permitted by the Commissioner (ie by May 2019).

The 12 steps for GDPR readiness as stated by the Information Commissioners Office are:

1. Creating Organisation Awareness
2. Auditing Information Assets
3. Communicating Privacy Information
4. Enforcing Individuals Rights
5. Responding to Subject Access Requests
6. Identifying the Legal Basis for Processing Personal Information
7. Reviewing how Consent is Obtained and Used
8. Enforcing Children's Rights
9. Implementing Effective Data Breach processes
10. Implementing Data Protection By Design
11. Appointing a Data Protection Officer
12. Identifying if International Data Processing is Occurring

The Data Governance Team and Veritau update the group of progress against this activity plan on a routine basis.

**Recommendations**

That the committee notes the changes outlined above and the risks they introduce; and also the measures taken to respond to them

Report author and contact:

Robert Beane, Information Governance Manager, Veritau Limited
Telephone: 01609 533219
E-mail: robert.beane@veritau.co.uk