STROUD DISTRICT COUNCIL

AUDIT & STANDARDS COMMITTEE

19 NOVEMBER 2019

AGENDA ITEM NO

10

Report Title	**GDPR UPDATE**
Purpose of Report	To provide an update on data protection and the process for dealing with potential data breaches
Decision(s)	**The Audit & Standards Committee RESOLVES to note the report**
Consultation and Feedback	None
Financial Implications and Risk Assessment	There are no financial implications arising from this report. Andrew Cummings, Strategic Director of Resources Tel: 01453 754115 Email: Andrew.cummings@stroud.gov.uk No risk assessment has been carried out at this stage due to the nature of the report which is principally informative
Legal Implications	There are no legal implications arising specifically from this report. Patrick Arran, Interim Head of Legal Services and Monitoring Officer Tel: 01453 754369 Email: patrick.arran@stroud.gov.uk
Report Author	Patrick Arran – Interim Head of Legal Services and Monitoring Officer Tel: 01453 754369 Email: patrick.arran@stroud.gov.uk
Options	The options are that the Committee can note the report and provide instructions to officers to carry out further work if necessary. Alternatively, the Committee can note the report and take no action.
Performance Management Follow Up	If the Committee instructs officers to carry out further work, a report will be taken to a future meeting of this Committee.
Background Papers/ Appendices	None

1. INTRODUCTION

On the 25th July 2019, the Committee received the annual report on Internal Audit Activity 2018/19. As a result of the questions arising from recommendations made as part of a recent successful GDPR Audit, members requested a further report to Committee regarding breaches of GDPR, the number of cases referred to the Information Commissioner's Office and the outcomes.

1.1 This report will provide a summary of the information requested, but as this is a public report, specific details will not be made available in case the data subjects can be identified by the information relevant to them. Members of the Committee have a need to know as part of their role and as such, more detail can be provided in private session if required.

1.2 It will be useful for members to be provided with a brief background to GDPR followed by an outline of the reporting requirements in the event of a breach. This will provide a context to the data breaches recorded since GDPR was brought into effect in May 2018. On the basis that no significant changes are anticipated as a consequence of Brexit, no consideration has been given to it in this report.

2. GDPR Background

Until 24 May 2018, the EU data protection regime was based on the Data Protection Directive (95/46/EC) introduced in 1995. However, the last 23 years has seen significant advances in information technology, and fundamental changes to the ways in which individuals and organisations communicate and share information.

2.1 The General Data Protection Regulation (GDPR), which was brought into effect in the UK by the Data Protection Act 2018, is an ambitious, complex and strict regulation designed to harmonise data protection law across the EU, and transform the way in which personal data is collected, shared and used globally. Most processing of personal data is subject to the GDPR.

2.2 The GDPR introduced a number of new features into the data protection regime, such as accountability, mandatory personal data breach notification, data portability and new obligations on processors.

2.3 Similarly to the DPA 1998, the GDPR applies to the processing of personal data:

- Wholly or partly by automated means.
- Other than by automated means, if the data forms part, or is intended to form part, of a filing system (in other words, manual structured personal data).

2.4 The GDPR defines personal data as "*any information relating to an identified or identifiable natural person (data subject)*". A person is identifiable if they "*can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*".

2.5 To determine whether a person is identifiable, a number of factors must be taken into account. It is important to be aware that information held (or obtained from another source) may indirectly identify an individual and could therefore constitute personal data (A car number plate for example).

2.6 Examples of personal data include:

- Personal information, such as name and address.
- Family details.
- Lifestyle and hobbies.
- Education and training.
- Health-related information.
- Employment data.
- Financial information.
- Contractual information (for example, goods and services provided to or by the data subject).

2.7 The GDPR requires that personal data should be processed in accordance with the principles in Article 5 of the GDPR which are very similar to those in the DPA 1998. However, there are now six data principles, rather than eight.

2.8 Responsibility for complying with the principles remains with the controller. The most important practical change is the addition of the accountability principle, which requires controllers to show how they comply with the six principles in Article 5(1), for example by documenting the decisions they take about a processing activity.

2.9 The GDPR aims to strengthen the rights of individuals. It does so by retaining rights that already exist under the Data Protection Directive and introducing the new rights of data portability, the right to be forgotten, and certain rights in relation to profiling.

2.10 Many of the core concepts under the Data Protection Directive remain unchanged under the GDPR. For example, the concepts of personal data, data controllers, and data processors (now respectively referred to as controllers and processors) are broadly similar.

2.11 In terms of the legal basis for processing, controllers must make sure that, under the first data protection principle, in addition to processing data fairly, lawfully and in a transparent manner, they have a legal basis for processing data. This is a fundamental feature of EU data protection law.

2.12 For public authorities The GDPR imposed a new obligation on both controllers and processors to appoint an independent data protection officer (DPO). For the purposes of this report, the DPO (The report author) is responsible for considering data breaches and reporting to the ICO when required.

3. Data Breaches

The Committee requested information regarding breaches of GDPR and the number of cases referred to the Information Commissioners Office together with the outcomes. Before setting out a summary of this information, it would be useful to outline the legal requirements in the case of a personal data breach.

3.1 What is a personal data breach? This occurs where there is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or

access to, personal data (*section 33(3), DPA 2018*). It can broadly be defined as a security incident that has affected the confidentiality, integrity or availability of personal data.

3.2 In summary, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed, if someone accesses the data or passes it on without proper authorisation, or if the data is made unavailable.

3.3 Personal data which is even temporarily unavailable will be considered a breach and may require notification if the unavailability has a significant negative effect on individuals. This would be the case where data is lost or miscommunicated but then retrieved. The ICO GDPR Guide states that "*a breach is more than just about losing personal data*". It includes breaches that have occurred both deliberately or accidentally through human error, for instance. Examples include:

- Sending personal data to the wrong recipient via email.
- Lost laptops or other mobile devices which hold personal data.
- Hacking of passwords, email accounts, networks and systems.
- Loss or theft of hard copies which include personal data.

3.4 The GDPR requires notification to the ICO of all data breaches without undue delay and where feasible within 72 hours. However, this does not apply if the data breach is unlikely to result in a risk to the individuals concerned. If it is not possible to report within the deadline, the controller will have to justify the delay to the ICO by way of a reasoned justification.

3.5 If the breach is *likely to result in high risk to the individuals*, the GDPR, requires the controller to inform data subjects "*without undue delay*", unless an exception applies.

3.6 As part of its extensive preparations for GDPR, the Council put in place a clear process for dealing with data breaches. This included designating specific roles and responsibilities, training employees, and preparing a notifications template. Consequently, the Council is able to, and does, react promptly in the event of a data breach.

3.7 All personal data breaches must be recorded by the relevant controller (including breaches which it decides against reporting), including the facts relating to the personal data breach, the effects of the breach and any remedial action taken in response. The ICO may demand the right to inspect these records.

3.8 This was an issue identified during the recent GDPR audit in that the Council only kept a record of breaches reported to the ICO. This has now been rectified and all breaches, regardless of whether they are notified to the ICO are recorded in a table.

3.9 Whilst the nature and outcomes of breaches reported to the ICO can be made available to members, unfortunately not all breaches which were reported to the DPO but not reported to the ICO prior to the audit will be recorded.

3.10 What breaches have to be reported to the ICO? Only certain personal data breaches must be proactively notified to the ICO and individuals. Notification to the ICO is triggered where

a breach is likely to result in a "***risk to individuals' rights and freedoms"*** (Section 67(1), DPA 2018). The obligation falls on the controller, i.e. the Council.

3.11 When assessing the risk to individuals, organisations will need to consider the specific circumstances of the breach, including the likelihood, severity and potential impact of the risk. The following factors will need to be taken into account when assessing risk:

- Type of breach.
- Nature, sensitivity and volume of personal data.
- Ease of identification of individuals.
- Severity of consequences for individuals.
- Special characteristics of the individual (for example, children or other vulnerable individuals may be at greater risk).
- Number of individuals affected.

3.12 An example of where a breach is unlikely to result in such a risk may be where personal data are already publicly available and therefore disclosure of the data does not, of itself, constitute a further risk to the individual.

3.13 When the DPO decides against reporting a breach, the decision is documented and any relevant evidence (where available) in support of the decision that the breach does not pose any risk to individuals' rights and freedoms is retained.

3.14 When is notification to individuals required? The requirement to communicate a breach to individuals is triggered where a breach is likely to result in a high risk to their rights and freedoms. Again, the obligation falls on the controller.

3.15 Whether individuals should be notified will depend on the circumstances of the breach. For example, a loss of data which can be confirmed as encrypted and where the key has not been compromised, may represent a very low risk, and would not require notification to individuals (or indeed ICO). However, even where data is encrypted, if there are no comprehensive backups of the data, then this could have negative consequences for individuals which could require notification.

3.16 The following information should be included in a breach notification to the ICO:

- A description of the nature of the personal data breach including, where possible, the categories and approximate number of individuals concerned and the categories and approximate number of personal data records concerned.
- The name and contact details of the data protection officer (DPO) (if applicable) or other contact point where more information can be obtained.
- A description of the likely consequences of the personal data breach.
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, actions taken to mitigate any possible adverse effects.

3.17 Due to the potential complexities of personal data breaches, it is possible that an organisation may not have all the necessary information within 72 hours of when they become aware of the breach. Therefore, it is possible to provide this information in phases, if further information is provided to the ICO without undue further delay.

3.18 The ICO has established two processes for reporting personal data breaches under the GDPR and DPA 2018. There is a self-assessment option to determine if the breach should be reported. If the breach is reportable, there is a personal breach notification reporting form available. If the incident may result in a heightened risk of individuals being affected by fraud, organisations should consider reporting the incident to Action Fraud.

3.19 The following information should be included in a breach notification to individuals:

- The name and contact details of the DPO (if applicable) or other contact point where more information can be obtained.
- A description of the likely consequences of the personal data breach.
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, actions taken to mitigate any possible adverse effects.

3.19 As stated above, a controller must notify a data breach to the ICO without undue delay and, where feasible, not later than 72 hours after having become aware of it. A controller is deemed to become aware of a data breach when it has "*a reasonable degree of certainty*" that the incident affects personal data. In practice, the threshold of a reasonable degree of certainty is not always clear-cut. There are two different scenarios.

3.20 Firstly, where a reasonable degree of certainty that the breach has occurred is self-evident. For example, an unencrypted removable device such as a USB with personal data has been stolen. In such instance, the 72-hour countdown starts as soon as the controller discovers the breach or is informed about the breach.

3.21 Secondly, where the controller needs to gather some evidence to establish with a reasonable degree of certainty that the suspected data breach has occurred. The 72-hour deadline begins only when the controller acquires a reasonable degree of certainty that the breach has occurred. Although there is not a set deadline for this preliminary investigation and assessment, actions to investigate should be carried out as soon as the controller finds out about a suspect breach. While organisations will be given some leeway to investigate incidents to determine whether they are in fact breaches, it is unlikely to be long.

3.22 There is no set deadline for notifications to individuals; however, this must be done without undue delay. The exact timeline will depend on the circumstances. For example, the need to mitigate an immediate risk of damage would call for immediate communication whereas the need to implement appropriate measures against continuing or similar personal data breaches may justify more time for communication.

4. GDPR Breaches post May 2018

Subject to what is said above about the fact that no record was kept of data breaches that

were not reported to the ICO, the records held by the DPO record 11 data breaches since May 2018. Of the 10 reported to the DPO, 7 were reported to the ICO.

4.1 Given the low level of risk posed by the breach, the effective action and mitigation immediately taken to nullify any risk, the ICO has not taken any formal action on any of the reportable breaches.

4.2 In terms of general themes, the data breaches arose in the following circumstances:

- Documents left by tenants who had been evicted were left / disposed of improperly during a house clearance by contractors.
- Email inadvertently sent to a third party
- Marketing database may have been accessible due to human error
- Customer details available on website (Planning consultees)
- Documents left on roof of a car
- Documents sent to Court and served on 3rd party in error

4.3 In all cases, the theme is to learn from the experience. Any recommendations made by the ICO are passed on to the relevant department by the DPO with a request to confirm receipt and evidence process changes where necessary.

CONCLUSION

5. There are clear and established processes in place to deal with any data breaches. The breaches outlined are, in the main, relatively low level. The ICO has not taken any formal action in any of the 7 cases referred and has been satisfied by the processes put in place to retrieve the situation and that the authority has implemented any learning.