Purpose: Noted

Date **5 DECEMBER 2017**

Title **UPDATE ON THE GENERAL DATA PROTECTION REGULATION AND SUBJECT ACCESS AND FREEDOM OF INFORMATION REQUESTS RECEIVED**

Report of Chief Officer

EXECUTIVE SUMMARY

1. This report provides:

- An overview of the requirements of the new General Data Protection Regulation (GDPR), which will come into effect on the 25 May 2018 replacing the Data Protection directive.
- A summary of our plans to ensure we will be compliant.
- A summary of the number and response times to Subject Access (Data Protection) and Freedom of Information Requests received into the Service.

THE GENERAL DATA PROTECTION REGULATION (GDPR) – AN OVERVIEW

2. The GDPR aims primarily to give control back to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. When the GDPR takes effect, it will replace the Data Protection directive. Below is a summary of the main differences between the GDPR and the Data Protection Act.

3. Many of the concepts and principles of the new regulation are much the same as those in the current Data Protection Act. The overall theme for the GDPR is privacy by design and data minimisation. It is designed to help individuals better control their data. Organisations must demonstrate that they only collect the minimum data required to meet the purpose and that purpose should be considered in the first instance. There is more emphasis on the documentation that data controllers keep to demonstrate their accountability.

4. The current eight Data Protection principles have been reduced to six. In summary, these are that data belonging to individuals must be:

- Processed fairly, lawfully and in a transparent manner.

- Collected/used for specified, explicit and legitimate purposes and not further processed for other purposes incompatible with the original purpose.
- Adequate, relevant and limited to what is necessary in relation to that purpose.
- Accurate and kept up to date, rectified without delay.
- Retained in a form that permits identification no longer than necessary.
- Appropriate technical and organisational data (processed in a way that ensures appropriate security of the personal data).

5. Like the Data Protection Act, the GDPR applies to 'personal data'. However, the GDPR's definition is more detailed. The more expansive definition provides for a wide range of personal identifiers to constitute personal data, reflecting changes in technology and the way organisations collect information about people.

6. A lawful basis is required for the processing of data under GDPR and it will require a high standard for consent. This is required for processing any individual's data unless the organisation has a legitimate reason or legal obligation to do so. If consent is required then the organisation must demonstrate that it has received clear and unambiguous consent. The purpose for which the consent is gained needs to be "collected for specified, explicit and legitimate purposes. In other words, it needs to be obvious to the data subject what their data is going to be used for at the point of data collection. If the individual is under 16 years old, then consent must be obtained by a parent. The requirement for consent includes both external customers and internal employees. In all cases, individuals must be informed of the data collection and potential use of, through Data Privacy Notices at point of collection.

7. The rights of data subjects have been widened and organisations must ensure they have clear, transparent and electronic methods for the data subject exercising their rights.

8. Organisations will be expected to include data protection controls at the design stage of any new technology that looks to collect personal data. They must:

    - routinely include data protection questions within projects and new initiatives
    - implement measures to demonstrate they have considered data protection into processing activities; and
    - Data Privacy Impact Assessments must be kept to evidence due diligence.

9. The GDPR will introduce a duty on all organisations to report certain types of data breach to the relevant supervisory authority. Organisations will have 72 hours to report a breach to the Information Commissioners Office and to those individuals whose data has been compromised. If a breach is not reported, an organisation can be fined for not reporting the breach as well as the breach itself. The fines will be significant – up to 10 million euros.

10. The GDPR places a duty on HFRA, as a public authority, to have in place by 25 May 2018 a suitable Data Protection Officer. This post should report directly to the highest level of management with their support in performing the tasks by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

ACTIONS BEING TAKEN TO ACHIEVE COMPLIANCE

11. The Knowledge Management Team have a plan to achieve compliance. We are working with colleagues in the ICT team. The plan includes the following key areas:

    - The recruitment of an Information Governance Manager (to include the role of Data Protection Officer). This provides us with a resource dedicated to information governance who will work closely with the ICT team.
    - To enable HFRA to achieve the highest levels of compliance as well as make best use of all its data and information assets as well as those that are shared with local and sector wide partners, we need to invest in a programme of organisation wide awareness building. At present training is being developed however we need to get to a position where every person who uses HFRS data is equipped with the knowledge and skills to do so in a compliant way. This is to be evidenced within a training log to show it has been completed.
    - The construction and maintenance of an Information Asset Register of all information processed within the Service.
    - An independent gap analysis.

SUBJECT ACCESS REQUESTS RECEIVED

12. In 2016/17, the Service received six subject access requests (individuals wishing to access personal information relating to them).

13. It is possible that the number of requests will rise as a result of the regulation coming into effect.

FREEDOM OF INFORMTION (FOI) REQUESTS RECEIVED

14. Although the legislation relating to FOIs remains largely unaffected by GDPR, much of the work to be undertaken will greatly improve our ability to quickly locate, access and where appropriate disclose the information to the requester. The information asset register will indicate the type of information, where it is held and who the Information Asset Owner is.

15. In 2016/17, we received 144 requests for information. 85% of these were completed within the 20-day limit.

16. We anticipate that the recent higher levels of requests are likely to resume or even increase with the introduction of GDPR.

COLLABORATION

17. The Knowledge Management team are exploring ways to collaborate with Hampshire County Council colleagues in terms of expertise and training in relation to Information governance.

RESOURCE IMPLICATIONS

18. Depending on the work required from the gap analysis, additional resources may be required but it is expected that this can be resourced from the current Knowledge Management budget.

LEGAL IMPLICATIONS

19. Legal implications are currently being assessed.

PEOPLE IMPACT ASSESSMENT

20. The proposals in this report are compatible with the provisions of equality and human rights legislation.

RISK ANALYSIS

21. Failure to comply with GDPR will put the Service at risk of incurring significant financial penalties, and reputational damage, both with our staff and the public. Furthermore, compensation can be given to those individuals whose information has been compromised or unlawfully released.

RECOMMENDATION

22. That the future obligations under the new General Data Protection Regulation are noted by Hampshire Fire and Rescue Authority.

BACKGROUND PAPERS

Guide to the General Data Protection Regulation (GDPR) – Information Commissioners Office
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr

Contact:

Sam Fairman, Performance Review Manager, Samuel.fairman@hantsfire.gov.uk, 07918 887502