REPORT TO: **Joint Management Board**

DATE: **21 February 2018**

AGENDA ITEM:

SUBJECT: **LANCASHIRE CONSTABULARY : DATA PROTECTION BILL/ GENERAL DATA PROTECTION REGULATION**

1. Decision Required

i. The Commissioner and Chief Constable are invited to note and comment upon the report as appropriate

2. Information

a. Background

i. In May 2018, the Data Protection Act 1998 will be replaced by the General Data Protection Regulation (GDPR) and a new Data Protection Act 2018. The Act will implement GDPR for ordinary processing operations and implement specific provisions that relate to law enforcement processing, in accordance with the Law Enforcement Directive.

ii. The Data Protection Bill has passed through the Lords and is due its second reading in the Commons. Royal assent will be received prior to May when the Act it has to take effect.

iii. The new legislation seeks to protect privacy rights in the digital age and ensure privacy by design concepts are embedded within operational activity. The most important aspect of the new legislation is the introduction of a new principle of accountability. Failure to comply could be costly. Chief Constables, as data controllers, are responsible and liable for compliance with data protection law where the potential financial penalty for non-compliance will increase significantly in May, 2018. The Information Commissioner has suggested that evidencing accountability is

pivotal to compliance. Potential maxim fines under the new legislation can be levied up to £18m. Fines for administrative failings, such as not appointing a DPO in accordance with the legislative requirements or failing to undertake data protection impact assessments can be issued up to £9m.

iv. The origins of the new legislation emanate from the ever evolving digital landscape and consequently the changing way in which organisations manage and process personal data, with different and increasing threats to privacy. Big data, artificial intelligence and machine learning are becoming more widespread in the public and private sectors. The Police Service is no different, and this is a particularly active period for the Service with national and local changes taking place with significant investment undertaken to replace out-dated systems and old technology. Data protection should not present a barrier to the use of such technology and innovation but help enable its introduction and implementation in a manner that is sustainable, with reduced risk, transparency and public confidence.
In addressing the new landscape in which information is collected, stored and used the new legislation places a greater onus on organisations to be more responsible for and to ensure that privacy considerations are embedded, monitored, and subject rights complied with. What was already recognised as being one of the most complicated pieces of legislation on the statute books will become even more complex, in particular for law enforcement bodies.
However, a number of the requirements of the new legislation can be broken down in to key themes.

v. The new principle of accountability will require Chief Constables' to ensure and demonstrate compliance with GDPR/ the DPA Bill. The Information Commissioner has suggested that evidencing accountability is perhaps the most important aspect of the new legislation.

vi. A strong theme, in addition to greater transparency, which runs through the legislation, is the enhanced requirement for records management. The Data Controller is required to 'maintain a record of all processing operations under its responsibility' and document the legal bases for processing and this has to be made available to the Information Commissioner upon request.

vii. The Data Protection Officer (DPO) is required to be involved in a timely manner in all issues which relate to the protection of personal data; so all new processing activities will require consultation with the DPO and where processing is to be undertaken on systems, a Data Protection Impact Assessment should be undertaken before a system is procured.

viii. There are further mandatory requirements; the new legislation provides stronger and enhanced rights for individuals. Subject access rights have to be complied with in a shorter time frame and without the need for a fee. Where a record is found to be inaccurate and amended there is a duty on the data controller to inform any recipients with whom that data might have been shared so that their records might be updated.

ix. Parties who process personal data on behalf of the data controller will also have additional responsibilities and liabilities. All contracts with third parties will need to be amended to include compulsory contract terms required by the legislation.

x. Where a data protection breach has occurred, the Information Commissioner may need to be notified and such notification has to occur within 72 hours.

b. The Regulator's Position

i. The Information Commissioner, Elizabeth Denham, has said her organisation is not planning to take a hard line on the 25 May implementation date for compliance with the GDPR. It is made clear that compliance should be an on-going effort with organisations demonstrating they are putting the key building blocks in place. Unlike planning for the Y2K deadline, GDPR preparation doesn't end on 25 May 2018 – it requires on-going effort. Although there is no 'grace' period and regulation will begin straight away, it is accepted that it will be an evolutionary process for organisations. They will be expected to continue to identify and address emerging privacy and security risks in the weeks, months and years beyond May 2018. Organisations who self-report and engage with the ICO to resolve issues and who can demonstrate effective accountability arrangements can expect this to be taken into account when any regulatory action is considered. Such commitment is likely to include:

- Organisational commitment – Preparation and compliance must be cross-organisational, starting with a commitment at board level. There needs to be a culture of transparency and accountability as to how personal data is used – recognising that the public has a right to know what's happening with their information.
- Understanding the information held – documenting what personal data is held, where it came from and who it is shared with. This will involve reviewing contracts with third party processors to ensure they are fit for GDPR.
- Implementing accountability measures – including appointing a data protection officer if necessary, considering lawfulness of processing, reviewing privacy notices, designing and testing a data breach incident procedures and considering the implications for new projects and completing Data Protection Impact Assessments.
- Ensuring appropriate security means continual rigour in identifying and taking appropriate steps to address security vulnerabilities and cyber risks
- Training Staff – Staff are the best defence and greatest potential weakness – regular and refresher training is required

ii. The ICO has also highlighted that compliance is conducive to operational effectiveness. Perhaps particularly relevant to the police service where information and personal data is, aside from our people, our most valuable asset.

Present Position - National Action

iii. Last summer, a national Data Protection Reform Group was established to assist the Service preparation for reform. The Group includes representatives from the Information Commissioner's Office and the Home Office, and the Force Information Assurance Manager (and Data Protection Officer) is a member of this Group. The Group has been able to engage upon and identify issues emerging in relation to the law enforcement provisions of the Bill.

iv. The Group also identified a number of work streams to address different issues and identify the new requirements within the new legislation in order to develop service guidance. These work streams are on-going and cover, for example a review of the wording on national forms (MG), implications for professional standards departments, human recourses, procurement, national training, position of the data protection officer within the police service etc.

c. Lancashire Action Plan

i. The potential impact of the legislation has been highlighted at various points over the past few years within various organisational reviews, and has informed some decisions, eg the establishment of a Records Manager. Preparation for the new legislation commenced in earnest last May, when a programme of work was identified.

ii. An essential part of that work was engagement with the information asset owners in order to identify the information held and how that information was being used and controlled. CPD events were arranged and attendance mandated by the Force Director of Resources, and SIRO. This work and direct engagement with individual departments to conduct information audits, is on-going with support from the Information Assurance staff. Staff vacancies and on-going business as usual has hindered progress.

iii. A Force DP Implementation Working Group has been established with various departmental representatives and audits are on-going in relation to Force polices and contracts. A media campaign will commence in March. The national training work stream is expected to deliver an updated training product for al staff prior to May.

iv. It is envisaged that Data Protection Officers' will be at the heart of the new legal framework, facilitating and monitoring compliance. On 21 December 2017, Ian Dyson, Commissioner for the City of London Police and Chair of the IMORCC wrote to all chief officers circulating a paper regarding the role and position of the DPO and highlighting the desirable and best practice elements of the business which organisationally should sit under the DPO. The content of the report was endorsed by the Information Commissioners' Office and consistent with the views of the Home Office.

v. The Report from Mr Dyson reflects upon the fact that a few forces already have robust structures in place with the DPO positioned at an appropriately senior level, reflecting the requirement of the legislation that they report to the highest management level. However, the report highlighted that for most Forces a change in philosophy, and understanding, will be required to adopt a pro-active approach to their self-regulatory framework and the management of risk associated with information. Such changes will require structural change, with the position of the DPO undertaking a more significant role within the organisation so as to be able to perform the statutory duties required of them, without interference or conflict. The report highlights that the DPO role includes the statutory functions and responsibilities including information access, compliance, audit, information security, and records management. Effectively, the DPO will be required to have a clear internal (organisational compliance) and external (contact point for individuals relating to the processing of their personal data) aspect to their role. A best practice model structure was provided. The report also suggested that Chief Constables' might wish to explore with their DPO undertaking he role for other public bodies.

vi. It is believed that HMIC will seek to include data protection within future HMIC inspections and that a thematic inspection may be likely in the foreseeable future.

3. Implications

a. Resource Implications

i. The legislation requires that the Data Controller has to support the DPO by providing the necessary resources to perform their tasks. To undertake the proactive engagement required by the legislation in order that the Chief Constable can demonstrate accountability and complete DPIAs, information sharing agreements, breach reporting, audit etc will require some additional resource. In addition, growth in demands from individuals' in relation to their rights might also have an impact on resources. This will require on-going monitoring and assessment.

ii. At an early stage it was recognised that there was an opportunity to explore mutual benefits with the OPCC relating to the role of the DPO. Last summer, it was provisionally agreed that the Force DPO would undertake the role on behalf of the OPCC, and that the PCC would provide financial support to a post, suitably senior in supporting the DPO in terms of their responsibilities. Other Forces are now also progressing in this manner.

iii. Some discussion has also taken place with LFRS regarding potential collaboration; however, whilst some support has been offered the LFRS is not as mature in terms of information governance and there remains a significant amount of work for the Force to undertake at this stage.

4. Background Papers

n/a

5. Report Author - Carl Melling,
Information Compliance Manager.