**Ref: GJF/2018/03/07**

# GJF Logo

# Board Meeting: 27 March 2018

**Subject:** General Data Protection Regulation   
(GDPR)

**Recommendation:** Board members are asked to note the requirement to comply with the new GDPR by 25 May 2018 and to support implementation of the action plan which will ensure compliance.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**1 Background**

The new General Data Protection Regulation (GDPR) will come in to force on 25 May 2018. The GDPR represents the most ambitious and comprehensive changes to data protection in the last 20 years and will improve upon the current the Data Protection legislation.

It has been confirmed that the UK’s decision to leave the EU will not affect the commencement of the GDPR and that all public and private authorities will have to be compliant with this new regulation by 25 May 2018. The requirement for compliance to GDPR will apply to all parts of the Board.

In terms of the GJF registered charity, further guidance will be sought from the Scottish Charity Regulator (OSCR) and the Charities Commission on the requirement that donors to the charity need to ‘opt-in’ to having their personal information held by the Board.

# The implementation of the GDPR will bring about some key changes to the current to data protection legislation which include:

# Increasing the rights for individuals

* + To be informed of data held by the Board
  + To have access to data held by the Board
  + To rectification where data held is inaccurate
  + To erasure of data (to be forgotten)
  + To restrict processing of data
  + To object to data being held
* Strengthening the obligations for organisations
  + To appoint a Data Protection Officer (DPO) for the Board
  + To ensure Privacy by Design – Data protection impact assessments must be completed prior to implementing new systems or processes
  + To mitigate risk when processing data by adopting measures
  + To implement an Information Asset Register detailing all information assets, including details of personal data held, where it came from and who it is shared with
  + To ensure contracts with Third parties who handle data on behalf of the Board, comply with GDPR regulations.
  + Strengthening the management of breaches
  + To notify any breach of GDPR regulations to the Information Commissioners’ Office within 72 hours
  + To notify data subjects, whose data has been affected, without undue delay
  + To introduce and maintain a Personal Data Breach Register within the Board

# Significantly increasing the sanctions where organisations are not compliant

* + The current maximum threshold for financial penalty which can be levied by the Information Commissioner’s Office is £500,000. However, this will increase to an upper limit of €20 million or 4% or annual global turnover, whichever is higher. Examples of the types of fines are listed below:

**Category A Fines**

This category focuses on issues with preparedness and administrative failures in implementing the Data Protection compliance programme. Fines for this category are capped at €10 million or 2% of worldwide annual turnover, whichever is greater. It includes, but is not limited to:

* Failure to execute a proper Privacy Impact Assessment
* Lacking designation of a Data Protection Officer, or issues with the roles and responsibilities of the DPO
* Issues with breach notifications, to Data Protection authorities or to Data Subjects
* Failure to implement Data Protection “by design and by default”.

**Category B Fines**

This category generally addresses actual breaches and major failures in compliance. Fines for this category can be up to €20 million or 4% of worldwide annual turnover, whichever is greater.

This includes, but is not limited to:

* Conditions for consent (in obtaining or processing data)
* Lawful processing of data
* Right of access by the Data Subject (Subject Access Request)
* Right of erasure (right to be forgotten)
* Right of rectification (accuracy of legally obtained personal data)

**2 Assessment**

A readiness assessment has been undertaken by the Information Governance Manager, which involved reviewing the requirements of the five key areas within the GDPR and assessing our current status.

1. Accountability and Governance
2. Individuals’ rights
3. Breach notification
4. International transfer of data
5. National derogations

This readiness assessment has resulted in the development of an action plan highlighting the required actions to ensure compliance along with action owners and timescales to complete.

It should be noted that there is only one element, 2.4, which is highlighted as red. Currently, the key clinical systems, used within NHSScotland, do not support the entire erasure of an individual’s data. This is an issue which affects all Boards across NHS Scotland and will require to be progressed collectively with the key systems suppliers.

The action plan, with Red, Amber, Green (RAG) status, is attached as Appendix A. Some of the key actions, which have already been carried out include:

* The introduction of an Information Asset Register for the Board. This register contains details of all Information Assets as well as details of Information Asset Owners who have responsibility for ensuring that the information asset is administered in line with the Board’s Information Governance policies.
* A review of all contracts with Third Parties, who handle data on behalf of the Board, to ensure compliance with GDPR regulations. A new contract template has been developed by Central Legal Office (CLO) which includes a fully GDPR compliant data protection clause and this will be issued to all Third Parties.
* Privacy Impact assessments have been undertaken for any new systems which have been introduced and, where appropriate, data processing agreements have been put in place.

The readiness assessment has also highlighted that consideration must be given to the appropriate governance structure which will ensure progress towards compliance with the GDPR. The governance and reporting of the action plan should reside with the Information Governance Group, chaired by Medical Director as Caldicott Guardian. The terms of reference of this group and membership will be reviewed and reprioritised to reflect the criticality of this work. An update will be provided to the Senior Management Team on progress against the action plans.

In addition, the Senior Management Team (SMT) has approved the recommendation that all Information Asset Owners attend training on GDPR and more specifically, on their role and responsibilities as an Information Asset Owner. This training will be scheduled in April 2018. Thereafter, each Information Asset Owner will be required to sign a declaration of acceptance of individual responsibility. This declaration will provide assurance that appropriate measures are in place within the respective departments to ensure compliance to GDPR. The declaration will also provide assurance that the requirements to ensure cyber resilience within their appropriate departments are met. A list of Information Asset Owners is attached as Appendix B.

**3 Recommendations**

Board Members are asked to note the requirement to comply with the new GDPR by 25 May 2018 and to support implementation of the action plan which will ensure compliance.

**Julie Carter**

**Director of Finance**

**March 2018**

**(Sally Smith, Head of eHealth)**

**Appendix A - GDPR Action Plan**

This plan indicates the actions to be progressed to ensure compliance of GDPR for 25 May 2017.

**1.0 Accountability and Governance**

Under the GDPR, the data protection principles set out the main responsibilities for organisations. The principles are similar to those in the DPA, with added detail at certain points and a new accountability requirement. The accountability principle in Article 5(2) requires us to demonstrate that we comply with the principles and states explicitly that this is our responsibility. See ICO guidance ‘what is the accountability principle?’

|  |  |  |  |
| --- | --- | --- | --- |
| * 1. **Awareness. Ensure decision makers and key people in the organisation are aware that the law is changing to the GDPR** | **RAG** | **Timeline** | **Owner** |
| Develop communications plan for all staff within the Board. | On track | March 2018 | IG Manager working with the Head of communications |

|  |  |  |  |
| --- | --- | --- | --- |
| * 1. **Document what personal data we hold, where it came from and who we share it with** | **RAG** | **Timeline** | **Owner** |
| Development of Information Asset Register | On track | December 2017 | IG Manager |

|  |  |  |  |
| --- | --- | --- | --- |
| * 1. **Implement appropriate technical and organisational measures that will ensure and demonstrate that we comply.** | **RAG** | **Timeline** | **Owner** |
| Full compliance with the Scottish Government Information Security Framework | On track | March 2018 | IG Manager |

|  |  |  |  |
| --- | --- | --- | --- |
| * 1. **Maintain relevant documentation on processing activities** | **RAG** | **Timeline** | **Owner** |
| Update relevant documentation, policies and legal notices | On Track | March 2018 | IG Manager |
| Development of Information Asset Register | On track | December 2017 | IG Manager |

|  |  |  |  |
| --- | --- | --- | --- |
| * 1. **Implement measures that meet the principles of data protection by design and data protection by default**. | **RAG** | **Timeline** | **Owner** |
| Development of Data Protection Impact Assessment and training for appropriate staff to complete assessments | On track | February 2018 | IG Manager |

|  |  |  |  |
| --- | --- | --- | --- |
| * 1. **Adhere to approved codes of conduct and/or certification schemes.** | **RAG** | **Timeline** | **Owner** |
| N/A | N/A | N/A | N/A |

|  |  |  |  |
| --- | --- | --- | --- |
| * 1. **Appoint a data protection officer.** | **RAG** | **Timeline** | **Owner** |
| Incorporate into IG Manager Job Description | On track | January 2018 | Head of eHealth |

**2.0 Individuals’ rights**

The GDPR creates some new rights for individuals and strengthens some of the rights that currently exist under the DPA.

|  |  |  |  |
| --- | --- | --- | --- |
| 2.1 **The right to be informed encompasses our obligation to provide ‘fair processing information’, typically through a privacy notice. It emphasises the need for transparency over how we use personal data.** | **RAG** | **Timeline** | **Owner** |
| Update information leaflets ensuring openness and transparency | On track | April 2018 | IG Manager |
| Update of current legal notices | On track | April 2018 | IG Manager |

|  |  |  |  |
| --- | --- | --- | --- |
| 2.2 **The right of access. Under the GDPR, individuals will have the right to obtain: confirmation that their data is being processed; access to their personal data; and other supplementary information.** | **RAG** | **Timeline** | **Owner** |
| Update policies and procedures to reflect changes to Subject Access Requests | On track | March 2018 | IG Manager |

|  |  |  |  |
| --- | --- | --- | --- |
| 2.3 **The right to rectification. Individuals are entitled to have personal data rectified if it is inaccurate or incomplete.** | **RAG** | **Timeline** | **Owner** |
| Develop process to support rectification of personal data held by organisation | On track | April 2018 | IG Manager |

|  |  |  |  |
| --- | --- | --- | --- |
| 2.4 **The right to erasure. This right enables an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.** | **RAG** | **Timeline** | **Owner** |
| Current systems used in NHS Scotland do not support this requirement | Red | TBC | Head of eHealth |

|  |  |  |  |
| --- | --- | --- | --- |
| 2.5 **The right to restrict processing.** **Under the DPA, individuals have a right to ‘block’ or suppress processing of personal data. The restriction of processing under the GDPR is similar.** | **RAG** | **Timeline** | **Owner** |
| Incorporate into the “Right to Rectification” process | On track | April 2018 | IG Manager |

|  |  |  |  |
| --- | --- | --- | --- |
| 2.6 **The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.** | **RAG** | **Timeline** | **Owner** |
| N/A | N/A | N/A | N/A |

|  |  |  |  |
| --- | --- | --- | --- |
| 2.7 **The right to object.** | **RAG** | **Timeline** | **Owner** |
| Review of research projects and legal basis for processing | On Track | March 2018 | IG Manager working with the Head of Research |

|  |  |  |  |
| --- | --- | --- | --- |
| 2.8 **Rights related to automated decision making and profiling. The GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention. These rights work in a similar way to existing rights under the DPA.** | **RAG** | **Timeline** | **Owner** |
| N/A | N/A | N/A | N/A |

**3.0 Breach notification**

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data. The GDPR introduces a duty on all orgs. to report certain types of data breach to the relevant supervisory authority, and in some cases to the individuals affected.’

|  |  |  |  |
| --- | --- | --- | --- |
| 3.1 **We have to notify the relevant supervisory authority of a breach where it is likely to result in a risk to the rights and freedoms of individuals**. | **RAG** | **Timeline** | **Owner** |
| Data Processing Agreements to be updated to reflect requirements of processor | On track | March 2018 | IG Manager |

|  |  |  |  |
| --- | --- | --- | --- |
| 3.2 **Where a breach is likely to result in a high risk to the rights and freedoms of individuals, we must notify those concerned directly without undue delay**. | **RAG** | **Timeline** | **Owner** |
| Already in place. | On track | Completed | IG Manager |

|  |  |  |  |
| --- | --- | --- | --- |
| 3.3. **Prepare for breach reporting** | **RAG** | **Timeline** | **Owner** |
| Already in place. | On track | Completed | IG Manager |

**4.0 International transfer of data**

The GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations, in order to ensure that the level of protection of individuals afforded by the GDPR is not undermined.

|  |  |  |  |
| --- | --- | --- | --- |
| 4.1 **Personal data may only be transferred outside of the EU in compliance with the conditions for transfer set out in Chapter V of the GDPR.** | **RAG** | **Timeline** | **Owner** |
| Already compliant. | On track | Completed | IG Manager |

**5.0 National derogations**

Article 23 enables Member States to introduce derogations to the GDPR in certain situations. These are similar to the existing exemptions from rights and duties in the DPA.

|  |  |  |  |
| --- | --- | --- | --- |
| 5.1 **Implementation of derogations similar to current exemptions** | **RAG** | **Timeline** | **Owner** |
| Further review required through NHS Scotland IG Forum | Amber | May 2018 | IG Manager |

**Appendix B – Information Asset Owners (IAOs)**

* Are directly accountable to the Senior Information Risk Owner (SIRO)
* Provide assurance that any risks to their information assets are managed effectively
* May “own” several information assets that include areas of overlap with other asset owners
* May own information assets that may be unstructured such as shared drive content
* Will appoint Information Asset Administrators who, in turn, will :
  + Ensure policies and procedures are followed
  + Recognise actual or potential security incidents
  + Consult their IAOs on incident management
  + Ensure that the information assets which are registered are maintained

|  |  |
| --- | --- |
| **Information Asset Owner** | **Number of Assets Registered** |
| Acting Chief Pharmacist | 7 |
| Assistant Director of Finance | 5 |
| Assistant Director of Finance (Governance) | 10 |
| Associate Director of Operations, Regional and National Medicine | 13 |
| Associate Director of Operations, Surgical Services | 12 |
| Associate Medical Director, Regional and National Medicine | 1 |
| Associate Nurse Director , Surgical Services | 2 |
| Associate Nurse Director (Education and Professional Development) | 4 |
| Business Services Manager | 7 |
| Clinical Perfusion Manager | 1 |
| Clinical Services Manager, Surgical Services | 1 |
| Clinical Services Manager, Regional & National Services | 3 |
| Consultant Anaesthetist | 1 |
| Consultant Anaesthetist | 2 |
| Consultant Anaesthetist | 1 |
| Director of Finance & SIRO | 1 (IAR) |
| General Manager, GJCH | 3 |
| Head of Clinical Governance | 4 |
| Head of eHealth | 14 |
| Head of Estates | 3 |
| Head of HR | 15 |
| Head of Laboratory Services | 2 |
| Head of Medical Physics | 1 |
| Head of Procurement | 7 |
| Head of Strategy and Performance | 2 |
| Head of Support Services | 2 |
| Learning and Development Manager | 2 |
| Medical Director | 1 |
| National eHealth Programme Office Manager | 1 |
| Nurse Director | 1 |
| Performance and Improvement Lead | 1 |
| Programme Director, Hospital Expansion | 1 |
| Radiology Services Manager | 2 |
| Research and Development Manager | 4 |
| Senior Manager, Prevention and Control of Infection | 3 |
| Spiritual Care and Diversity Lead | 1 |
| Telephonist/Receptionist Manager | 2 |
| Theatre Services Manager | 2 |