

## Audit and Assurance Committee Meeting

Date of Meeting	Tuesday 6 October 2020
Paper Title	Annual Review of GDPR
Agenda Item	18
Paper Number	AAC1-M
Responsible Officer	Jim Godfrey, Finance & Resources Director
Status	Disclosable
Action	For information

### 1. Report Purpose

1.1. Note the progress report re GDPR.

### 2. Recommendations

2.1 The Committee is invited to **note** the report.

### 3. Evaluation of GDPR

3.1. GDPR is an important issue for GCRB and all three colleges in Glasgow and for GCRB. Previous reports have outlined progress in respect of GDPR and the collaborative approach to Data Protection.

3.2. Members may recall that a report was provided to this Committee in October 2019. The report provided to this Committee meeting provides a review of progress

3.3. Under the guidance of Mairead Wood (Data Protection Officer), the Executive Team has been working to implement the agreed action plan.

### 4. Progress Against Agreed Actions

4.1. Mairead Wood has prepared an updated report which is appended.

### 5. Risk Analysis

5.1. The approach outlined above has enabled GCRB, and the Glasgow Region, to address the risks posed by the regulations in respect of Data Protection and GDPR. In particular, the risk that "There is a breach of legislation/guidance/code of practice and this results in a failure of governance".

### 6. Equalities Implications

6.1. There are no equalities implications as a direct result of this report.

## **7. Legal Implications**

- 7.1.** The duties and responsibilities in respect of GDPR are detailed in the relevant legislation. Failure to comply with the legislation, relating to GDPR, carries significant financial consequences.

## **8. Resource Implications**

- 8.1.** The primary cost associated with the implementation of the recommendations is the cost of staff time.

## **9. Strategic Plan Implications**

- 9.1.** Compliance with relevant legislation is clearly an obligation for GCRB. Whilst GDPR creates an additional administrative burden this is offset by some benefits that might contribute to the achievement of the region's ambitions. Such benefits may include; improved learner confidence and enhanced cyber security.

# Data Protection Update

GCRB BOARD REPORT 10/20  
DR MAIREAD WOOD

## Background

A data protection audit was undertaken in 2018 and an update provided to the Board in October 2019 on progress (see Annex A). All Tasks have been addressed. Only one task is outstanding; GCRB should use CoGC's IT Security Policy as the College provides the IT infrastructure to GCRB. It is unclear if this has been published yet (CoGC have a draft). Other tasks continue to be monitored and updated, specifically the IAR or Record of Processing Activity (ROPA/Article 30), retention schedule, new data sharing and processing agreements and compliance.

GCRB Board Meeting - October 2020			
TASK (from 2018 Audit)	UPDATE (2019)	UPDATE 2020	NOTES
Data Audit	Complete - approved by Board	√	
Privacy Notice	Complete - published on website - <a href="http://www.gcrb.ac.uk/sites/default/files">http://www.gcrb.ac.uk/sites/default/files</a>	√	
IAR (Article 30)	Record of Processing Activity (ROPA) in place - GCRB working through 'living document'	√	Living document
Retention Schedule	Schedule in place - GCRB working through	√	
Data Risk Register	Complete - update/manage as required (DPO review monthly)	√	
Training	Complete - annual training proposed going forward	√	Will schedule additional training in 2020
Review DSA's/DPA's	Ongoing - focus on getting formal agreements in place for 'in-kind' services	√	Concern re. 'in-kind' services (no contract)
DP Policy	Complete - GCRB to present to Audit and Assurance Committee	√	
Breach Policy	Complete	√	
SAR (& other requests)	In draft - scheduled to complete by Dec 2019	√	
FOISA	GCRB publishing FOI request handling procedure	√	DPO does not cover FOISA directly
DPIA	Complete - procedure/template	√	
IT Security Policy	GCRB will use CoGC Policy (in draft) as use CoGC IT Infrastructure	X	Requested from CoGC end 2020
Compliance	Ongoing	√	Suggest internal Audit for 2021

TABLE 1: List of tasks and updates from 2018 -2020

## Update

1. **ICO Registration:** As the only personal data being processed by GCRB is for HR purposes, GCRB are exempt from registering with the Information Commissioner's Office (ICO) and do not have to pay the associated fee. However, if GCRB were to start processing personal data as part of its reporting activity, this would have to be reviewed and would likely result in GCRB being required to register and pay an annual fee to the ICO.
2. **Data Protection Audit:** GCRB has all the data protection policies, procedures and documentation in place as identified in the initial audit in 2018. It is proposed that an internal data protection audit is undertaken by the HEFESTIS DPO (part of the role) during 2021.
3. **Data Processing 'in-kind':** GCRB staff and Board Members' personal data is processed by Glasgow Colleges in-kind. From a data protection (legal) perspective, GCRB is the Controller for this data and the Colleges are the Data Processor. This means the Colleges only process the data as directed by GCRB. However, the Glasgow Colleges are not set-up to act as a Data Processor and are likely to act as a separate, independent Controller. This means the College may make decisions on GCRB data and may be accountable for GCRB's data if there is a breach.
4. **Schrems II ruling:** Privacy Shield, which provides a safeguard for sending data to the US, is no longer valid. GCRB must consider if any of their data is currently processed under Privacy Shield (e.g. BoardPacks) and consider their options to ensure compliance.

## The year ahead

The Covid-19 pandemic, Schrems II ruling (regards Privacy Shield no longer being a valid mechanism to transfer data to the US) and upcoming Brexit in 2021 all impact data protection. These are being considered in relation to GCRB; data protection policies, procedures, privacy notices, ROPA, agreements and contracts should be reviewed and updated to reflect the changes these event have in relation to data protection law and regulation over the coming year. The proposed internal audit will identify where updates are required and identify any additional risks or changes required.