Government Actuary's Department

24 April 2018

General Data Protection Regulation Preparations

This letter provides an overview of GAD's readiness for the new General Data Protection Regulation (GDPR) which comes into force on 25 May 2018. Please speak to your usual contact if you have any specific questions in this regard.

It is the nature of our work at GAD that we process, for and on behalf of our clients, large sets of data. These data sets may, but will not always, contain personal data. It is the processing and retention of these data that we are focussing our preparations for GDPR, as well as (in common with all employers) the personal data we hold on our own staff in our HR systems.

Our preparations

As a data controller and processor of personal and other individual data, GAD takes its responsibilities seriously and we currently comply with the Data Protection Act.

We formed an internal GDPR Working Group last year, including representatives from all actuarial and central services teams across GAD, in order to ensure readiness for the introduction of the GDPR. The Working Group is chaired by an executive member of the GAD Management Board (Sue Vivian, Head of Public Service Pensions). It is supported on subject matter by our Data Protection Officer and by a specialist lawyer we have commissioned for additional advice and guidance. The Working Group report to the GAD Executive which collectively approves decisions of principle.

The Working Group is approaching the introduction of GDPR in a systematic way. Two research exercises were initially carried out:

- first a gap analysis to identify the areas where the introduction of GDPR would require a change in policy or practice

- secondly a data mapping exercise to identify the categories of data we hold and the reasons for holding it.

Using these exercises, an action plan was developed which includes both plans to change the mechanism by which we request, receive and process data which may include personal details, and some rectification work to proactively remove personal data that is no longer needed. In considering removal of existing personal data and retention of further personal data we are seeking to achieve an appropriate balance between business needs and risk.

Our related policy documents and procedures are being updated to reflect the operational changes identified, as well as to include the additional and variant requirements of GDPR.

Our ICT team is currently considering how best to ensure that any electronic systems we use to access or process personal data have "privacy by design" built in. Specific consideration is being given to our use of communication tools such as MS Outlook.

The Working Group has established the following key milestones.

Milestone 1 Complete data mapping exercise
The data mapping exercise is largely complete and scheduled to be fully complete by the end of April 2018.

Milestone 2: establish GDPR compliant systems, policies and procedures
Policies and procedures have been compiled and reviewed internally and are currently being reviewed by our lawyer. We have also asked the lawyer to review our client engagement letters and terms and conditions for GDPR compliance. We expect to have revised policies, terms of business, procedures and protocols in place (including being made generally available on our website and/or intranet) by the end of April 2018.

We are separately reviewing new protocols/processes to be adopted within our electronic systems (network and email) in consultation with the ICT team. Proposals will be put to the executive in April for implementation before GDPR comes into force.

We have established a portal for transmission of individual or personal data into GAD and identified and assigned responsibilities for managing the handling of that data in line with our intended policy. Your usual contact will explain how to use this portal.

Milestone 3: Communications and staff training
Achieving compliance with GDPR relies on all staff being fully aware of their responsibilities and implementing any required changes to the way they work. As part of our annual security awareness training, completed in March, all staff were given an introduction to GDPR. A further training session for all staff focused specifically on GDPR and led by our lawyer was held earlier this month.

Teams which are expected to adopt amended operational processes as a result of the changes to our policies and procedures will have training within team meetings during late April/early May. The Working Group includes representatives from all affected teams and the relevant group member will determine appropriate arrangements.

Key Mitigation strategies

GAD have identified some key risks as a result of GDPR and the following actions are being taken to mitigate these:

1. To mitigate the risk of non-compliance all of our proposed policies and procedures have been referred to an external (GDPR specialist) lawyer for review.

2. To mitigate the risks around personal data we receive from clients, our new protocols will seek to remove non-essential personal data on receipt and our ICT team are working closely with actuarial teams to ensure electronic systems limit the risk of personal data inadvertently being retained.

3. With regard to legacy data sets an exercise is planned to systematically remove personal data from historic data sets where there is no longer any justifiable reason for retaining that data.

This will not be completed by 25 May 2018 but any high risk areas will be identified and addressed as a priority.

GAD have also asked our internal auditor at the Government Internal Audit Agency to provide an independent assessment of our readiness plan and this internal audit work is well advanced, with recommendations received and being actioned.

We will be writing to you again in early May with further information including notification of the updates to our standard terms and conditions. Should you have further queries in the meantime, please feel free to contact your usual GAD contact.

Yours sincerely,

Mike Gerli
Data Protection Officer | Government Actuary's Department