A2 Scrutiny Working Group – 1st November 2017

Report to Cabinet on: General Data Protection Regulations Review – 9th January, 2018.

Observations made to: Cabinet

- The new General Data Protection Regulations (GDPR) would replace the Data Protection Act in May 2018. These new regulations apply to all of Europe from 25th May, 2018.
- The Westminster Government is proposing to introduce a new Data Protection Bill which will mirror the GDPR. The law needed to catch up with the technology and the amount and types of personal information that is used today.
- There is a new principle of "accountability" in the GDPR i.e. the Council will need to demonstrate how we are compliant with the regulations.
- Local authorities, are expected to rely upon the legislation that drives service delivery and make use of the provisions within Acts of Parliament which gives the Council powers to undertake public functions as their legal basis for the processing of personal information rather than the consent of the individual.
- With regard to contracts with 3rd parties who deliver services on our behalf, such as voluntary organisations, the Council will need to ensure that rules are set out in the contracts and agreements with those providers.
- Where data is provided to contractors, they should act on Council data in ways which they are authorised to do. Should there be a breach of the regulations this will still fall back on the Council, but the contractor could also be liable if they have not acted in line with the principles contained within the regulations.
- The GDPR contains provisions on the rights of individuals, such as being able to request that records held by the Council be deleted, that inaccurate information is corrected etc.
- The current Data Protection Act requires that when the Council receives a request as to what information the Council holds about the individual (Subject Access Requests), the Council can charge that individual £10 to provide that information and has 40 days to comply with the request. Under the new regulations the Council will not be able to charge for such requests and has 1 month to comply.
- It is likely that the numbers of subject access requests to the Council will double. Currently the Council only has 1 officer responding to such requests as well as Freedom of Information (FOI) and Environmental Information Regulations (EIR) requests.

- The maximum fine for failure to comply with the new regulations is €20m or £18m, where there has been a failure to facilitate the exercising of rights under the regulations. Additionally maximum monetary penalties for breaches of personal data could be levied up to €10 or nearly £9m.
- To comply with GDPR the Council will need to:
  - develop, introduce and undertake Data Protection Impact Assessments where required
  - appoint a Data Protection Officer.
  - for any breaches the Council will have 72 hours to notify the Information Commissioner's Office (ICO) of such breaches. This timescale includes periods including weekends and bank holidays.
  - Evidence its compliance with the principles of the regulations
- The Group asked if it would be possible for the Council to insure itself to cover the costs of any fines, and if the Council could not do this individually could it be done on an all Wales basis. *(Note – Insurance Section have confirmed that the Council cannot insure itself against a breach)*
- All services will need to undertake an Information Asset Audit and prepare Information Asset Registers, to ensure that the Council knows what data is being processed and where it is being stored.
- The Group asked whether Town and Community Councils were affected by the new regulations and whether they were aware that the new regulations were coming into force. The Scrutiny Manager was asked to contact One Voice Wales and raise this issue with them as the representative body for Town and Community Councils. *[Note – One Voice Wales has been contacted and they have advised Town and Community Councils and are preparing training]*
- The main differences between the Data Protection Act and GDPR as well as main concerns for the Council were as follows:
  - Services identifying the legal basis which is being relied upon to process the personal data, as currently the Council relies heavily on consent.
  - Accountability, and the need to evidence our compliance
  - Subject Access Requests, and the ability to exercise other rights under the regulations
- With regard to training for Members it was suggested that this would need to be mandatory and could be delivered by e-learning or by other methods. *[Note: Report considered by Member Development Working Group and to be considered by the Democratic Services Committee in November]*
- There were large pieces of work which the Council needed to undertake such as the Information Asset Audits, the assessments of the Information Risk., and the development of evidence of compliance
- Members expressed concern that there was a need to quantify the costs of implementing GDPR.
- There were some previous recommendations from the ICO when they undertook an audit into Powys County Council's compliance with the Data Protection Act a couple of years ago, which the Council still has included in its plan, such as what happens to data from schools that have closed and the need for an auditing system within the new Health and Social Care System (WCCIS).
- A detailed action plan will be developed from the Information Asset Audit responses, to identify and prioritise high risk areas requiring activity to deliver compliance where possible by 25th May 2018
- The position regarding additional resources was outstanding but Members recognised that this could be a risk in the delivering the plan if resources were not provided.

Scrutiny recommendations to Cabinet on the Council's preparation for GDPR:

- **Due to the high risk to the Council from the potential fines, and enforcement actions, officers be asked to consider whether it is possible for the Council to insure itself against the possibility of high fines under GDPR or whether this could be undertaken on an all Wales basis.**
- **One Voice Wales to be asked about whether information has been circulated to Town and Community Councils about GDPR.**
- **Services will need to have a clear understanding of the Legal Basis being relied upon for processing, rather than to rely on consent.**
- **There is concern that the numbers of subject access request will rise significantly with the implementation of GDPR, together with the loss of income to the Council.**
- **There is a high risk to the Council in being able to implement the plan for GDPR if additional staffing resources are not made available.**
- **The cost to the Council of implementing GDPR should be costed.**
- **Data sharing and disclosure rules need to be clear in contracts and agreements with 3rd parties, and partners.**
- **Compliance requirements from previous ICO reports need to be addressed.**

Membership of the A2 Scrutiny Working Group 1st November 2017
County Councillors G. Williams, K. Curry, S. Davies, J. Pugh.
Apologies form County Councillors E. Durrant and G. Jones.