Report of the Data Protection Officer

AUDIT COMMITTEE – 19th September 2018

GENERAL DATA PROTECTION REGULATIONS (GDPR)
DATA PROTECTION OFFICER UPDATE REPORT

1. Purpose of Report

1.1 This report provides the Audit Committee with an update from the perspective of the Council's Data Protection Officer (DPO) regarding the discharging of that role and the general approach to testing compliance with the requirements of the GDPR and Data Protection Act 2018.

2. Recommendations

2.1 It is recommended that the Committee:

i. Considers the report and satisfies itself that the Data Protection Officer role is being effectively planned and discharged to provide the Committee and the Council with the appropriate information and assurances with regards compliance with the GDPR;

ii. Receives formal 6-monthly DPO information / assurance reports; and

iii. Receives a further information / awareness session regarding GDPR and the role/work of the DPO.

3. Background

3.1 As the Committee is aware, the GDPR came into force on 25th May 2018 after a period of preparation of 2 years. What became more and more evident in the last few months before the implementation date, even with the period of preparation we had, was the huge amount of work needed.

3.2 Whilst the preparations were good and significant effort was put in by a lot of people across the Council, we like almost every organisation and sector I'm aware of cannot claim full and embedded compliance at this stage. What we do have however, and to give the Committee assurances, is a clear plan of what is needed and a governance structure to oversee and monitor this plan.

3.3 The Information Commissioner's Office (ICO) has acknowledged itself that many organisations will need time to fully implement all the necessary changes to working practices to meet all the GDPR requirements.

3.4 The process and work in preparing for the GDPR has been driven by the Information Governance Team, supported by other colleagues in IT, the Information Governance Board and senior management. The work undertaken already by the small IG Team is to be commended and the extent

of readiness and compliance thus far is testament to their expertise, drive and commitment.

3.5 Part of the GDPR requirements is to appoint a statutory Data Protection Officer (DPO). As the Committee is aware, this role has been added to that of the Head of Internal Audit and Corporate Anti-Fraud.

4. DPO Update

4.1 Since appointed, my focus has been to assist the IG Team and wider Authority to ensure there has been an effective plan and approach to being ready for and as far as possible, complying with the GDPR. This has involved reviewing revised policies and procedures, monitoring the project plan, advising on matters and issues as they arise, and more recently developing an 'audit-style' programme of activity to test compliance across the Authority. A revised and comprehensive general information governance risk register has also been reviewed.

4.2 Given the acknowledgement that full and embedded compliance has not yet been achieved, any compliance testing has, for the first part of the year, been deferred. What the Council has achieved however is a position of comprehensive awareness (almost 2,000 employees undertaking on-line training), significant change through revised policies and procedures, and not least the completion of 172 individual data process mapping exercises to review how Business Units manage personal information in their systems and services with regard to the GDPR requirements and general good practice.

4.3 This process mapping identified a number of actions that are now being followed up by the IG Team as Phase 2, to ensure that any areas where changes in service procedure were required have been completed. This will be further reviewed, on a risk basis, as part of my DPO assurance work.

4.4 Work is also continuing to ensure that all contracts the Council has contain the updated DPA 2018/GDPR clauses. In addition to this contract related work that's on-going is to also ensure that there is a written agreement between the Council as a data controller and any third party acting as a data processor on our behalf. The GDPR requires such relationships to be formally captured and agreed. Further meetings are planned over the next few weeks between Legal Services and Corporate Procurement, assisted by the IG Team and DPO, to complete this important phase of activity.

4.5 The Information Governance Board, chaired by Executive Director – Core Services as the Council's Senior Information Risk Officer (SIRO), receives detailed progress reports in relation to GDPR and all matters 'IG'. This is a well-established Board with all Directorates represented plus key technical officers from IT, the IG Team, Internal Audit and the DPO.

4.6 As mentioned above, I am developing an 'audit programme' of activity to ensure the DPO role is fully discharged. This audit programme will focus on the higher risk areas of data protection around children's' and vulnerable adults but also test awareness across all parts of the Council. As the

Committee will be aware the GDPR sets out 6 principles which in turn will guide compliance activity.

4.7 Compliance testing and assurance work will commence in a few weeks' time, also utilising specific days set aside in the main Internal Audit plan. The next report to the Committee will include the results of that work. I shall also report to the Senior Management Team, and as part of the responsibilities of the DPO, inform the Chief Executive directly should I need to raise a matter more urgently. The Committee should be assured that the DPO is afforded unfettered access to senior management and is required to undertake the role independently and without management direction. I can also assure the Committee that such arrangements are in place and accepted as part of the GDPR requirements.

4.8 The DPO role has also been offered to the Parish and Town Councils within the Borough and through a service level agreement to the South Yorkshire Pensions Authority. Two awareness sessions have been provided for Parish/Town Council Clerks and members. A programme of IG support and DPO provision has been discussed and substantially agreed with the Head of Pensions Administration. A series of training sessions and data process mapping workshops have also been planned for Pension's staff over the next couple of months.

4.9 As I have not undertaken any specific compliance testing work, I am not able to provide the Committee with an assurance opinion at this stage. I can however assure the Committee of the continued focus and work being driven by the IG Team particularly, to ensure full compliance is secured as soon as possible.

4.10 The Committee will be acutely aware of the spectre of the massively increased fines that the ICO can impose for information breaches and serious non-compliance issues. Whilst no guarantees can ever be made that the Council won't be subject to ICO fines or censure, the robust approach being taken to implement GDPR is minimising the risk.

5. Supporting Information

5.1 Should the Committee wish, the full GDPR programme action plan can be provided along with details of the IG Board for further assurance purposes. Any requests for further information should be directed to the DPO.

Contact Officer: Data Protection Officer
Email: DPO@barnsley.gov.uk