TONBRIDGE & MALLING BOROUGH COUNCIL

CABINET

20 March 2018

Report of the Director of Central Services & Director of Finance & Transformation

Part 1- Public

Matters for Recommendation to Council

1 GENERAL DATA PROTECTION REGULATION SOFTWARE

This report explores the use of software to enable the authority to comply with new data protection legislation.

1.1 Introduction

1.1.1 In May 2018 the General Data Protection Regulation (GDPR) will come into effect.

1.1.2 Under the GDPR, the Information Commissioners Office (ICO) can impose fines of up to 20 million Euros (circa £18 million) or 4% of group worldwide turnover (whichever is greater) for non-compliance.

1.1.3 The GDPR requires data protection by design and by default. In practice, this means that the protection of personal data and data security should be embedded into our processes, not as an afterthought. Importantly, one of the new requirements under GDPR is that the Council must be able to demonstrate compliance with the various data protection principles, which means keeping detailed records / documentation that may need to be presented to the regulator (the Information Commissioner) on request.

1.1.4 One of the requirements of GDPR is to understand what data you hold and who has access to it.

1.1.5 We should also, by default, limit the processing of personal data to that which is necessary for each specific processing purpose and not allow it to be accessible to an indefinite number of people.

1.1.6 Structured data (such as that which is found in databases) is the most straightforward to understand since there will be a database schema containing a description of what data is stored, along with access controls and audit logs maintained by the systems administrators within departments.

1.1.7 Updates to access controls in databases can be administered from a central location by the departmental system administrators using the tools within the relevant system (e.g. IDOX Uniform and Northgate iWorld).

1.1.8 Unstructured data (files and documents on network shares) prove more of a challenge. Locations such as the shared drives staff use in their day to day business contain folders that have various permutations of permissions allocated to them. Some can only be accessed by individuals, others by departmental teams, and some by the whole council.

1.1.9 There is no overview of what the files on these folders contain. Some may be benign whilst others may contain sensitive personal information. Without manually inspecting each file individually it is not possible to catalogue the files to determine whether they pose a risk with regard to GDPR or other regulatory compliance regimes such as PCI-DSS.

1.1.10 Using the standard tools available with Windows Server it is not possible to get an overview of access permissions across folders without manually inspecting each one. There are thousands of folders which would need to be inspected to obtain this information making manual inspection near to impossible.

1.1.11 Member training on data protection and the GDPR has been arranged for 27 March.

1.2 Software Solution

1.2.1 Automated software tools are available which can identify the contents of files, categorise them on sensitivity, audit access permissions, audit file access and be able to report on its findings in an easily digestible form which can then be used by the software to update permissions automatically.

1.2.2 Automated software can also assist with the management of users network accounts, identifying those that haven't been used for a long time, have expired passwords and those that have exceptions to the normal security profile / policy.

1.2.3 An automated software solution can meet a number of key business objectives, including:

- Alignment of GDPR compliance and data security policies.
- Mitigation of risk around data loss through preventative controls.
- Greater control and visibility of user access to data.
- Reduced storage costs through the identification of inactive data that can be removed.
- Improved efficiency gains within the helpdesk for maintaining user access controls.

1.2.4 A Capital Plan evaluation **[Annex 1]** has been conducted for the purchase of an automated software solution which can reduce the risks under GDPR in this area.

1.3 Legal Implications

1.3.1 The GDPR is implemented on 25 May 2018. The Council will need to demonstrate data governance processes and procedures in order to mitigate the risk of substantial fines by the ICO should a data breach occur.

1.4 Financial and Value for Money Considerations

1.4.1 The one-off purchase and implementation costs associated with an appropriate GDPR software package are estimated at £66,000 with on-going annual support and maintenance costs estimated at £23,000 per annum. The one-off costs can be met from the Invest to Save reserve. Use of the Council's resources implies a loss of investment income of £3,000 per annum. Revenue growth of £26,000 per annum (support and maintenance and loss of investment income) adding to the Council's savings target/s.

1.4.2 The market for this type of software is limited with only a small number of suppliers having a product which can provide the functionality required. Quotations will be obtained from the suppliers we are aware of who can meet the system requirements. If the number of quotes to be obtained is less than three a waiver will be sought in accordance with Contracts Procedure Rules.

1.5 Risk Assessment

1.5.1 Risks around compliance with the GDPR are detailed on the corporate Strategic Risk Register. Implementation of automated software in this report can help mitigate this risk.

1.6 Equality Impact Assessment

1.6.1 The decisions recommended through this paper have a remote or low relevance to the substance of the Equality Act. There is no perceived impact on end users.

1.7 Recommendations

1.7.1 Cabinet are asked to **recommend** to Council that an automated software solution for GDPR purposes be added to the Capital Plan funded from the Invest to Save reserve.

Background papers: contact: Darren Everden

Nil

Adrian Stanfield
Director of Central Services

Sharon Shelton
Director of Finance and Transformation