Walsall Council

MAZARS

Summary of Findings

Client: Walsall MBC

Audit Title: GDPR Review

Audit Date: September 2018

Audit Team: Sarah Knowles (Engagement Manager)
Vincent Rezzouk-Hammachi (Head of Data Privacy Services)
Kay Ejiwunmi (Auditor)
Liam McKenzie (Auditor)

Area of Scope	Finding	Management Response
Policies and Procedures		
GDPR policies and procedures are in place	Within the document "Information Governance Framework to include DP Policy", section 3.3.9 on 'Retention and Disposal of Records', makes reference to the 'Retention Schedule'. However, following a review of the Retention Schedule, there is reference to the Data Protection Act 1998. This Act has been replaced by the Data Protection Act 2018, which indicates that the document has not been updated. Furthermore the last review of Schedule is dated April 2016-17.	Appropriate measures are being taken to update such documents and that the required updates are due for publication by no later than the end of September as part of the GDPR project work plan. The requirements for records management actions had also been highlighted within the latest CMT and GDPR project update report ensuring that these areas of further action and work are recognised by the Council. Due Date: September 2018 Responsibility: GDPR Project team

Area of Scope	Finding	Management Response
Individual Rights		
Individual Rights are in place for all rights under the GDPR	Organisations are required to list all Individual Rights of data subject on their external privacy notice. We noted that the right not to be subjected to profiling or automated decision making had not been listed on Walsall's website under the tab 'Your Rights'.	The council is only required to publish information relating to the rights of individuals where required in line with any identified and or specified processing conditions. The Information Governance Team have ensured that the right to restrict automated decision making is recorded within the council Privacy Notice however this does not apply to current Council processes. The rights with regards to profiling, automated decision making and data portability all relate to processing which requires a data subject to input the data and in specific cases receives a decision as a result of said data input. For example online accounts, social media accounts, online banking or credit card applications. Due Date: Currently up to date Responsibility: N/A
Records of Processing Activities (ROPA)		
Lawful Basis of Processing – Legitimate Interest **Lawful Basis of Processing - Consent**	From discussions with the Data Protection Manager, it was asserted that, each directorate and service line was tasked with completing a Record of Processing Activities (ROPA) for the information assets within their remit. It was understood that the Information Asset Owner (IAO) was responsible for apportioning the lawful basis for processing for each of their information assets. From review, it was observed that Children's Services and Resource & Transformation directorates	The current Information Asset Register is a live document that is being processed by the directorate information asset champions and is being supported by the GDPR project lead. As part of this work the project lead undertakes further reviews and communications with the directorate leads to ensure they are applying appropriate processing conditions. It is the responsibility of the directorates to ensure they review, update and report on their directorate level compliance. The Information Governance Team have

Area of Scope	Finding	Management Response
	indicated they have chosen to rely upon legitimate interest or consent as a lawful basis for processing. The GDPR legislation states that a public authority cannot rely upon legitimate interest as a lawful basis for processing. In addition to this, relying upon consent as legal basis places further obligations on the Council to be able to demonstrate the data subject's consent, which is found under Article 7 and Recital 32.	placed a mandate with the ICT change board to align all current registers and records of processing activities into a single user friendly dashboard. Due Date: December 2018 Responsibility: Data Protection Manager
Records of Processing Activities timely review	At the time of the audit, the review of the Records of Processing Activities was performed manually. There is no long-term mechanism in place for the monitoring of the Council's Record of Processing Activities (ROPA).	All directorate leads and Information Asset Champions are informed of the requirement to ensure the registers and records are accurate and up to date with regular reviews. As part of this the IG team have placed a change mandate with ICT for the build of a single dashboard and or system to support the requirements and controls of records and information assets. Due Date: December 2018 Responsibility: Data Protection Manager