Civic Centre, Castle Street,
Merthyr Tydfil CF47 8AN

Main Tel: 01685 725000 www.merthyr.gov.uk

Cyngor Bwrdeistref Sirol
MERTHYR TUDFUL
MERTHYR TYDFIL
County Borough Council

SCRUTINY COMMITTEE REPORT

Date Written	8 November 2018
Report Author	Lisa Richards
Service Area	Information Governance Team
Committee Date	20 November 2018

To: Chair, Ladies and Gentlemen

DATA PROTECTION PROGRESS REPORT

1.0 SUMMARY OF THE REPORT

1.1 The purpose of this Report is to update the Committee on the Councils progress with implementing the General Data Protection Regulation that came into force on the 25 May 2018.

2.0 RECOMMENDATION(S)

2.1 That the Scrutiny Committee notes the contents of this Report.

3.0 INTRODUCTION AND BACKGROUND

3.1 The General Data Protection Regulation (GDPR) became effective on the 25 May 2018. The GDPR has brought considerable changes to data protection law in the UK and across the European Economic Area (EEA) more widely, and includes significantly greater fines for breaches of up to €20 million. The UK Data Protection Act 2018 (DPA 2018) has implemented and supplemented the GDPR in the UK. This Report summarises the Information Governance Team's programme for compliance with the GDPR and the DPA 2018 (DP laws).

3.2 An immense volume of personal data continues to proliferate and flow daily around the Council and between the Council and other external organisations. Examples concerning our Council have been mapped and are stored within our Register of Processing Activities which is held within the Information Governance Team. It has been identified that some of this personal data needs to be accessible beyond the Council's limits.

3.3 Information, including personal data, is a valuable Council asset. Hard facts and figures are essential to making decisions. Information assets must be used effectively to meet the Council's objectives. A failure by the Council to hit the right balance between risk and opportunity in our use of data could have serious consequences for us in the future.

3.4 There are many potential ramifications of failure to comply with DP laws, including:

- Prosecution of or regulatory enforcement action against the Council, resulting in substantial financial penalties of up to €20 million which is approximately £18 million.
- Adverse publicity, potentially leading to reputational damage and lost public trust.
- Missed opportunities and wasted resources.
- Increased scrutiny from data protection authorities whose remits and powers have increased substantially under the GDPR.
- Civil liability or punitive damages for employment-related breaches.
- Criminal liability for directors and senior managers resulting in imprisonment and substantial penalties.
- Critical system delays and failures.
- Orders issued by the Information Commissioner's Office in the UK that seriously impact the Council. Investigative powers include a power to carry out audits, as well as to require information to be provided, obtain access to premises and stop data processing.
- Business continuity issues.
- Becoming embroiled in litigation and its attendant time, effort and expense.

3.5 The aim of the Information Governance Team's programme for compliance is to ensure good information handling practice, provide accountability of those processing personal data and give rights to individuals. For example, identity theft, stolen credit cards and failure to comply with privacy policies may result in fraud, theft and deception. Abuse of health data, financial data or children's data can have an adverse impact on insurance, credit, jobs or parental control.

3.6 An individual has a fundamental right in the UK and across the EEA to have their personal data protected and their personal data may only be processed (that is, obtained, recorded, held, used or disclosed) under certain circumstances. This has a wide impact on Council's functions.

3.7 The implementation of the GDPR is an ongoing journey; as with all legislative changes the key focus of the Information Governance Team is to ensure the Council continues to be committed to the ever changing landscape of data protection.

4.0 WHERE WE WERE

4.1 Data protection compliance previously sat within a number of departments but was primarily considered the responsibility of the Freedom of Information Officer who was located within the Legal Department. Data protection was governed by the Data Protection Act 1998 and was not seen as a high priority or considered as a corporate risk until the Article 29 Working Party, which ceased to exist on the 25 May 2018 and has been replaced by the European Data Protection Board, announced in May 2016 that the GDPR would be coming into effect on the 25 May 2018.

4.2 The Freedom of Information Officer submitted a report to full Council on 28 September 2016 titled Data Protection Reform - The General Data Protection Regulation (GDPR) 2016 which detailed the potential areas of reform. The Information Governance Team was created at the end of November 2016 following the appointment of the Data Protection Officer and the Data Disclosure and Records Officer.

4.3 Prior to 25 May 2018 the Information Governance Team's objective was to develop the Councils compliance with data protection ensuring that adequate measures were implemented to achieve GDPR compliance. A fundamental obligation was to create an environment in which all Council departments that collect, share and use personal information do so responsibly, securely and fairly.

4.4 The Manager of the Information Commissioner's Office in Wales briefed the Council's Corporate Management Team in February 2018 which discussed the GDPR and the importance of the Information Governance Team's role in ensuring data protection compliance.

4.5 The Information Governance Team focused on improving compliance with DP Laws by creating a communications strategy which consisted of weekly updates detailing key points of the main focus areas, issuing a personal information survey which was used to identify the employees that processed special category data, the results of the survey enabled the Information Governance Team to develop a training programme which was rolled out to all relevant staff members. The training programme ran from March – September 2018 and was provided to members of staff including all senior officers, head teachers and school staff, Councillors and voluntary groups.

4.6 The Data Protection Officer submitted a further report to full Council on the 2 May 2018 titled Privacy Standards Policy and Supporting Policies which sought the approval of a number of GDPR compliant policies. These policies replaced the previous Data Protection Policy and would act as the foundation for the Council's GDPR compliance.

4.7 The commitment set out within the policies, in particular the Privacy Standard's Policy; provides a stepping stone for ensuring effective Regulation compliance across the Council. They also provided a means to ensure we can make the best use of our information and to provide a solid foundation to enable us to be open and transparent about what we do which is one of the main concepts of the GDPR.

5.0 WHERE WE ARE NOW

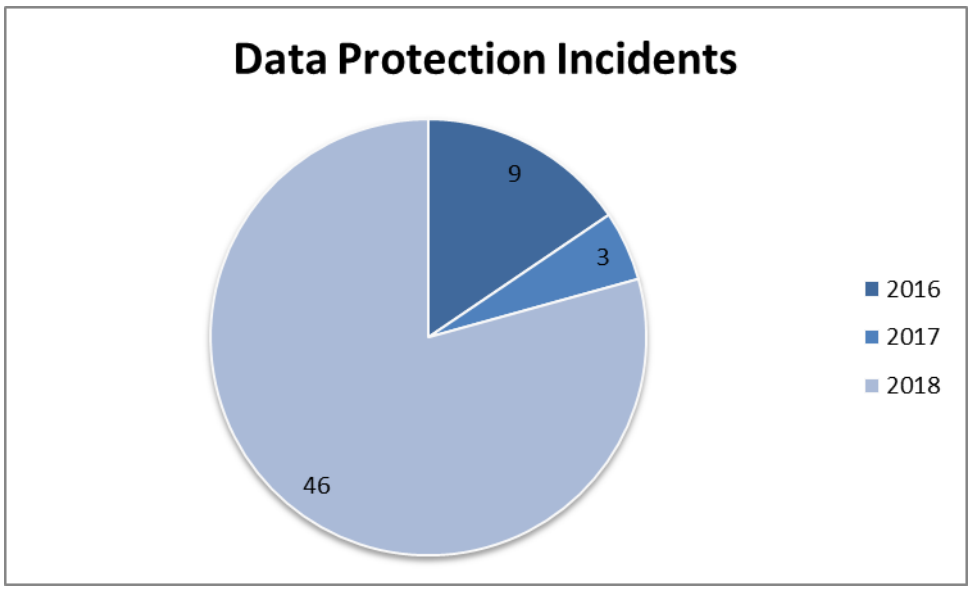
5.1 In addition to the GDPR training sessions that were delivered by the Data Protection Officer the Information Governance Team also launched 9 GDPR specific training modules within Bobs Business training platform. The GDPR training modules helps demonstrate important changes and highlight some of the new additions to the DP laws. The modules include:

- Why is the GDPR so important
- Key Definitions
- Key Changes Concepts & Data Processing Conditions
- Key Principles

- Privacy Impact Assessments & Security Measures
- Data Subjects additional rights and consent
- Data Protection Officer
- Fair Processing
- Data Breaches and non-compliance

5.2 The Information Governance Team has developed its programme for compliance in order to ensure that we are compliant with the DP laws. The introduction of the numerous policies and the effective communication strategy has given rise to a positive increase in staff awareness.

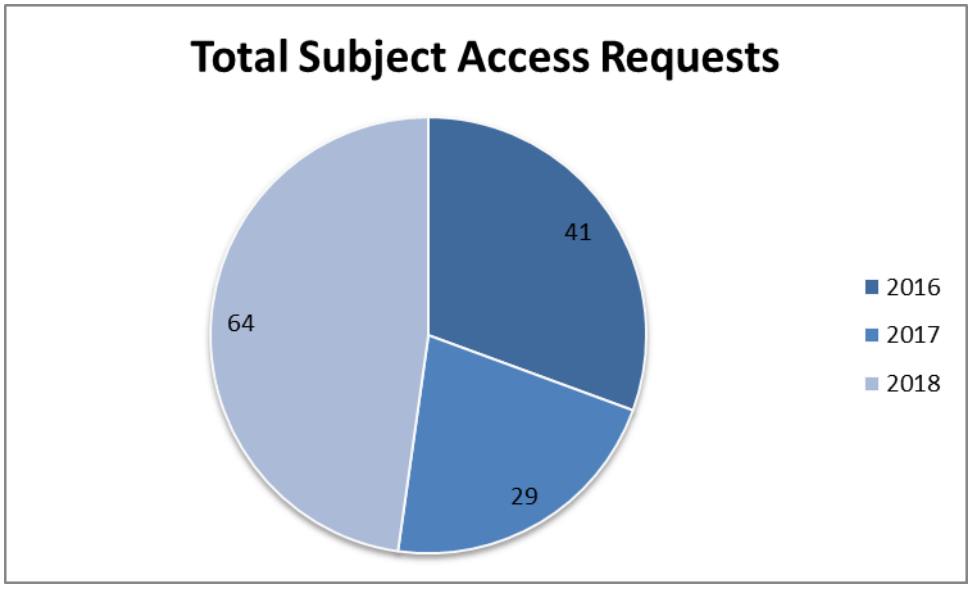
5.3 Since the implementation of the Data Protection Breach Policy the Information Governance Team has seen a significant increase in the number of data protection incidents that have being reported as detailed in the pie chart below. It is important to remember that the figures for 2016 and 2017 are complete calendar years whereas the data for this calendar year is not yet complete as such is not a true reflection of the figures for 2018:



5.4 In order to comply with the GDPR each incident must be investigated and if the incident results in a high risk to the rights and freedoms of the individuals it must be reported to the Information Commissioner's Office within 72 hours of first becoming aware of the incident. This increase has placed substantial pressure on the Information Governance Team as this significant increase was not anticipated.

5.5 The DP laws created new and strengthened the existing criminal penalties for individuals breaching data protection. Unfortunately since the 25 May the Information Governance Team has also seen an increase in investigating the number of criminal cases for breaching the DP Laws which have been included within the figures above.

5.6 The DP laws have given rise to a change in a number of the individual rights, the right to request your personal information, known as a subject access request, has changed considerably. The fundamental changes are the removal of the £10 fee and the decreased time limit for response. These changes have meant that the Information Governance Team has seen an increase in the number of requests we have dealt with as demonstrated in the pie chart below.



It is again important to remember that the figures for 2016 and 2017 are complete calendar years whereas the data for this calendar year is not yet complete as such is not a true reflection of the figures for 2018:

5.7 The right to be informed has also given rise to the number of privacy notices required. Each new project that is developed which uses personal information should have a privacy notice which details exactly how the Council is using the personal data and our lawful reason for doing so. The Data Protection Officer has been drafting these privacy notices on behalf of Council departments and The Information Governance Team's clients. Once a privacy notice has been translated into Welsh it is placed on our website for public inspection. Each privacy notice is unique and is a robust document which can be a number of pages in length. As such there are sometimes delays with translation, and therefore publishing as we do not wish for the Council to fall foul of our Welsh language obligations.

5.8 A principle concept of the DP law is to demonstrate compliance with the GDPR. This has meant that each service area must be aware of the reasons why they are using personal data and also what their legal justification is. This has caused a number of departments concern as their previous lawful reason was not compatible with the GDPR. This has meant that the Information Governance Team has been working closely with each service area to ensure that their processing activities are compliant and that they have the relevant documentation in place to demonstrate accountability.

5.9 All agreements relating to the processing of personal data have been updated and we are currently negotiating provisions with a number of data processors for internal department and external clients which the Data Protection Officer advises.

5.10 Following on from point 3.2 above as part of our GDPR compliance we were required to create a Register of Processing Activities (ROPA). A ROPA is a database which details how information flows through the Council and our legal justifications for processing the personal information. In order to develop the Council's ROPA the Information Governance Team identified key personel from each service area to be ROPA champions. These champions worked alongside each service area to set out

what they do, how they use, whether they share and how the store personal data. The ROPA is maintained by the Information Governance Team, when we are notified of a new processing activity it is reflected in our ROPA.

5.11 The Council also has a mandatory requirement to conduct a Data Protection Impact Assessment for certiain types of processing activities. These will include any processing which results in a high risk to the rights and freedoms of individuals, such as surveillance or when we are using technology to process a persons personal data. Departments, under the supervision of the Data Protection Officer are conducting such assessments for new projects and existing projects that are considered high risk. the Information Governance Team keeps a record of these assessments within our GDPR compliance system.

5.12 The Information Governance Team has successfully completed the GDPR practitioner training qualification. As such the Council now has there qualified practitioners and 3 training practitioners. This again demonstrates our commitment to GDPR compliance and helps demonstrate accountability.

6.0 WHERE WE WANT TO BE

6.1 The GDPR is still very new, it has had a global impact on data protection specifically relating to the way organisations process personal data. The guidance issued by the Information Commissioner details how we must comply; we are still awaiting guidance for some aspects of compliance which will be implemented on an ongoing basis. The DP laws have not yet been tested within the legal arena, in neither the Information Tribunal nor the Court arena; as such the way in which we are required to implement the DP law is subject to change. The Information Governance Team will strive to ensure that the Council remains compliant.

7.0 THE FUTURE OF DATA PROTECTION

7.1 In the UK, the GDPR was automatically incorporated into domestic law via the European Communities Act 1972 (ECA 1972). From 29 March 2019, the UK is expected to leave the EU (Brexit day), the European Union (Withdrawal) Act 2018 will repeal the ECA 1972 and simultaneously transpose the GDPR onto the statute book, making it domestic legislation in the UK. the current Government has said that repeal of the ECA 1972 will provide the legislature with an opportunity to scrutinise, amend, repeal or improve any aspect of EU law in the future; it is therefore possible that aspects of the GDPR could be amended at that point, or indeed any future point. At the same time, any changes to the GDPR would have to be carefully evaluated by the Government as it may adversely affect the UK's prospects of securing a formal Adequacy Decision from the European Commission for its domestic data protection law.

7.2 The DPA 2018 largely came into force in the UK on 25 May 2018 (a few provisions came into force on 23 July 2018). It serves several purposes including that it replaces the DPA 1998, supplements the GDPR and exercises some of the derogations in the GDPR which give EU member states discretion to legislate in certain areas. It extensively cross-refers to the GDPR and therefore the two must, be read together. It also aims to reassure the European Commission that on leaving the EU, the UK will provide an adequate data protection regime.

7.3 There is considerable uncertainty regarding the future relationship between the UK and the EU in relation to data protection, as in many other areas. Once the UK leaves the EU and any relevant transition or implementation period has expired, the UK will become a third country for the purposes of data protection law. This status has a number of significant practical consequences, in particular for international data transfers and enforcement of the GDPR.

7.4 The UK's status as a third country will have important consequences for incoming data flows from the EU. Under the GDPR, the transfer of personal data from a controller or processor organisation in an EU member state to a recipient located in a third country may only take place if specified conditions are met. It is essential that if we are trading or using the services of a company based abroad that we are making arrangements to either terminate those agreements or that we are complying with the specified conditions as per the GDPR.

7.5 The UK has indicated its willingness to start talks with the EU with regard to reaching an Adequacy Decision. However, the European Commission has not yet indicated a timetable for this and has stated that the decision on adequacy cannot be taken until the UK is a third country.

7.6 On Brexit day, the GDPR will be transposed onto the UK statute book, creating two distinct (albeit initially identical) legal regimes in the UK and the EU. As such our general processing activities will largely remain unchanged. The Information Governance Team will continue to keep abreast of any developments and changes to the landscape of data protection and will update the Council accordingly.

8.0 CONTRIBUTION TO WELLBEING OBJECTIVES

8.1 The implementation of the GDPR has had a significant impact upon how the Council is able to deliver its services. In order to deliver on any of the Wellbeing Objectives personal data must be used. The processing of personal data must be compliant with the DP Laws. As such the Information Governance Team has played a key role in ensuring other Council departments can achieve their wellbeing objectives by implementing appropriate procedures to ensure the Council is lawfully collecting, using and sharing personal data. The Information Governance Team has also been crucial for ensuring that the Council can demonstrate accountability by having appropriate evidence that supports the processing of personal data for our processing activities.

ELLIS COOPER
DEPUTY CHIEF EXECUTIVE / SENIOR INFORMATION RISK OWNER

COUNCILLOR ANDREW BARRY
CABINET MEMBER FOR GOVERNANCE AND CORPORATE SERVICES

BACKGROUND PAPERS		
Title of Document(s)	**Document(s) Date**	**Document Location**
List the Background documents which have been relied on in preparing the report. E.g. previous minutes of		

relevant committees			
Does the report contain any issue that may impact the Council's Constitution?			**No**