Taunton Deane Borough Council

Corporate Governance Committee – 26 March 2018

GDPR Action Plan Update

This matter is the responsibility of Executive Councillor Richard Parrish

Report Author: Richard Sealy, Assistant Director Corporate Services

1 Purpose of the Report

1.1 This report provides an update on the actions being taken by the Council in preparation for the implementation of the new (EU) General Data Protection Regulations (GDPR) which come into force on 25 May 2018 and the associated (UK) Data Protection Act, which is currently working its way through Parliament.

1.2 The report follows from the GDPR overview provided to the Members of the Committee at the December 2017 meeting.

2 Recommendations

2.1 To note the actions being taken in order to comply with GDPR.

3 Risk Assessment

3.1 GDPR compliance is recognised as a key corporate risk and is recorded on the Corporate Risk Register. The GDPR Compliance Action Plan and associated activities are the key mitigating actions for that risk.

3.2 Risk Matrix

Description	Likelihood	Impact	Overall
Risk - Failure to have adequate Data Protection Policies and procedures in place which are compliant with the new General Data Protection Regulation coming into force in May 2018 *Key Effects* Potential higher financial penalties imposed Potential reputational damage A lack of trust from the public regarding how we handle their personal data	4	4	16

The mitigations for this are the proposed changes as set out in the report	2	3	6

Risk Scoring Matrix

Likelihood	5	Almost Certain	Low (5)	Medium (10)	High (15)	Very High (20)	Very High (25)
	4	Likely	Low (4)	Medium (8)	Medium (12)	High (16)	Very High (20)
	3	Possible	Low (3)	Low (6)	Medium (9)	Medium (12)	High (15)
	2	Unlikely	Low (2)	Low (4)	Low (6)	Medium (8)	Medium (10)
	1	Rare	Low (1)	Low (2)	Low (3)	Low (4)	Low (5)
			1	2	3	4	5
			Negligible	Minor	Moderate	Major	Catastrophic
			Impact				

Likelihood of risk occurring	**Indicator**	**Description (chance of occurrence)**
1. Very Unlikely	May occur in exceptional circumstances	< 10%
2. Slight	Is unlikely to, but could occur at some time	10 – 25%
3. Feasible	Fairly likely to occur at same time	25 – 50%
4. Likely	Likely to occur within the next 1-2 years, or occurs occasionally	50 – 75%
5. Very Likely	Regular occurrence (daily / weekly / monthly)	> 75%

4 GDPR – Background and Key Changes

4.1 The General Data Protection Regulations (EU) 2016/679 were actually passed by the EU in 2016, but do not come into force until 25 May 2018. They will be accompanied by a new UK Data Protection Act, which is currently still going through Parliament. The latter piece of legislation covers the areas over which the GDPR provides for local discretion. We will have to ensure we comply with both pieces of legislation and this essentially replaces the current Data Protection Act (1998).

4.2 This new legislation covers virtually any organisation or individual who is collecting and processing personal data. So it applies to the Council, but also covers personal data that Elected Members collect as part of their role as a councillor.

4.3 The purpose behind the new GDPR Regulations is to provide a consistent approach

across the EU to data protection, to keep pace with technological changes and to attempt to redress the balance between the rights of the individual and the organisations that use and process their personal data. The technology and algorithms used for analysing and matching data provided by individuals in order to market services, make automated decisions etc. have become very sophisticated. Most of us provide data about ourselves without knowing what it is going to be used for, who is using it and how long it is going to be held for. Under the current legislative regime there is little that we can do about this. Consequently GDPR seeks to give back individuals control of their personal data.

4.4 GDPR provides individuals with a number of new rights and emphasises a number of existing rights. The key rights of individuals are summarised below:

- *The right to be informed* – of what, why and in what way their data is being processed – so we need to ensure we have clear Privacy Policies
- *The right of access* – individuals have the right to know what personal data of theirs we hold. They can continue to access their data via a Subject Access Request. However, these are free of charge from 25 May 2018 (currently there is a £10 fee) and now are subject to a shorter one month response time.
- *The right to rectification* – we must correct incorrect data
- *The right to erasure* – essentially this is a right to be forgotten – we must delete data that we no longer have consent or a legal basis for holding
- *The right to restrict processing* – individuals can ask us to stop processing their data. Whether we do so is dependent upon our reasons for holding the data because much of what we do is covered by legislation, which effectively gives us implied consent
- *Rights in relation to automated decision making* – essentially this is to provide protection against targeted marketing and automated decision making

4.5 In order to ensure these rights are being respected and are enforceable the GDPR regulations also bring in a number of key changes, which organisations must comply with. These are summarised below:

- *Data Breaches* – where breaches occur and we identify them as being reportable to the Information Commissioner's Office (ICO) we must report them within 72 hours
- *Consent* – in future and where consent is required for processing personal data individuals will have to positively 'opt in'. This means we have to provide clear consent notices which explain what we will use their data for and will need to record the consent provided. Individuals will also be able to remove their consent at any time (i.e. 'opt out') and we have to be able to accommodate this and cease processing their data
- *Subject Access Requests* – this is an existing right, but currently individuals have to pay a £10 fee and we have 40 days to respond. Under GDPR the fee is being removed and the response period is being reduced to a calendar month. This is likely to result in an increase in the number of requests we receive, which can be extremely time consuming for us to deal with
- *Increased fines* – the GDPR regulations significantly increase the fines regime. The regulations state a maximum of £16.8m or 4% of global turnover. This is clearly intended to provided them with the legislative teeth to tackle the multinationals, but potentially has significant implications for all organisations
- *Privacy Impact Assessments* – these are now a mandatory requirement where we are making changes to procedures or policies that involve the use of personal data
- *Data Protection Officer (DPO)* – there is now a legal requirement to employ a

recognised DPO, who needs to be an expert in the legislation and free from conflicts of interest. (NB. We do not have to employ them directly, but can buy this service in from another organisation)

4.6 A more detailed guide to the new regulations can be found on the Information Commissioner's website at the following address: https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf

5 GDPR – Our Compliance Action Plan

5.1 The new regulations introduce a number of significant changes and clearly provide for a much more robust data protection regime. We obviously need to review and change our procedures to ensure we comply with the new regulations. However, it is important that we do this in a positive way and use this as an opportunity (in conjunction with the changes we are implementing through Transformation) to ensure that the changes we make provide us with a robust data and information management approach, which both support GDPR and our future ways of working.

5.2 With this in mind we have devised a GDPR Compliance Action Plan (see Appendix A), which identifies the key actions we need to take and also seeks to align these changes with delivery of the broader transformation changes. As stated above, this is to ensure that we implement a data and information management approach for the future, which both meets the needs of GDPR and our new ways of working.

5.3 The plan is based on the headings and format recommended by the Information Commissioner's Office. It identifies the key outcomes we need to achieve and the key tasks required to deliver them. It is very much a 'living document' and is still being developed and fine-tuned.

5.4 The plan identifies a number of key tasks that we need to complete in advance of the new legislation coming into force on 25 May 2018 e.g. training and awareness, Information Asset Register update, policy and procedure changes, contract procedures etc.

5.5 It also identifies actions that we need to progress and deliver in conjunction with the delivery of the Transformation changes to develop our future approach to data and information management. These will potentially involve some fundamental changes to how we store data and how we work. Logically the delivery of these changes should be aligned with Transformation and the transition to the new operating model.

5.6 Consequently, whilst we will not have delivered the entire plan by 25 May 2018, we will have delivered the basic changes required to enable compliance and can demonstrate that we have a clear roadmap to a robust future approach to data and information management.

6 Links to Corporate Aims / Priorities

6.1 There are no direct links to corporate aims/priorities

7 Finance / Resource Implications

7.1 There are potentially going to be costs associated with implementing software changes to our existing line of business systems, developing our broader information architecture and in providing training in order to ensure GDPR compliance. In particular we need to be able to easily identify, disclose, amend and delete data in future. We are in the process of identifying these costs.

7.2 Additionally, the penalties we can be charged for data breaches are potentially a lot higher (£m's) than under the current legislation, which makes this a higher risk area. Consequently we have identified the detailed Action Plan to deliver compliance and a comprehensive approach to information and data management in future in order to mitigate this risk.

8 Legal Implications

8.1 The GDPR Regulations and new Data Protection Act are significant pieces of new legislation, which we need to fully understand and implement.

9 Environmental Impact Implications

9.1 There are no environmental impact implications associated with this report.

10 Safeguarding and/or Community Safety Implications

10.1 There are no direct safeguarding or community safety implications associated with this report.

11 Equality and Diversity Implications

11.1 There are no direct equality and diversity implications associated with this report.

12 Social Value Implications

12.1 There are no direct social value implications associated with this report.

13 Partnership Implications

13.1 We will need to review our data sharing and processing arrangements with any partner organisations with whom we share personal data.

14 Health and Wellbeing Implications

14.1 There are no health and well-being implications associated with this report.

15 Asset Management Implications

15.1 There are no asset management implications associated with this report.

16 Consultation Implications

16.1 There are no consultation implications associated with this report.

Democratic Path:

- **Corporate Governance – Yes**
- **Executive – No**
- **Full Council – No**

Reporting Frequency: 6 monthly

List of Appendices (delete if not applicable)

Appendix A	GDPR Compliance Action Plan

Contact Officers

Name	Richard Sealy
Direct Dial	01823 217558
Email	r.sealy@tauntondeane.gov.uk

APPENDIX A - GDPR Compliance Action Plan

Outcomes	Key Tasks	Target Date
Communication/Awareness/Training		
Staff and members are aware of the key changes and revised procedures and their responsibilities. A regular training approach & programme identified to ensure ongoing training.	Undertake further communications across the organisation (staff and members) to outline the key changes & timeline.	30/04/2018
	Organise the delivery of training in the legislative changes, new procedures and responsibilities to all staff & members	24/05/2018
	Work with HR to incorporate GDPR training into the new starters induction process	24/05/2018
	Develop and implement a regular refresh training programme.	31/10/2018
Data Protection Officer Role		
Appoint a Data Protection Officer (reports directly to senior management, has no conflict of interests, can be provided by an outside body).	Work with SLT to identify how & where the DPO role fits within the new operating model.	24/05/2018
	Identify our responsibilities / opportunities in relation to parish and town councils	31/03/2018
Information Assets		
A detailed and up to date record of: > WHAT information/data we hold (personal and special categories of data) > WHY we hold it (legal basis) > WHERE we hold it and in what form > HOW LONG (retention period)	Identify the approach to compiling an Information Asset Register (IAR) that allows us to quickly collect the information and in a manner that supports the development of our future Information Management Architecture Create an updated Information Asset Register template & combine with existing IAR	30/03/2018
	Conduct a Data Audit with each service area to populate the new IAR	24/05/2018
	Document and implement procedures to ensure the regular review and update of the IAR.	31/10/2018
Information Management Future Approach		
A new approach to Information Management which supports the delivery of the New Operating Model & GDPR compliance and which delivers a simple, intuitive and easy to manage approach to creating, storing accessing, disclosing, retaining and deleting ALL information and data held by	Identifying and getting agreement to the principles, approach & timeline for developing our future Information Management Architecture	30/03/2018
	Implement our new approach to Information Management including procedural and technology changes including a new Document Management System.	To be identified

Outcomes	Key Tasks	Target Date
both councils.	Identify and implement a plan for all legacy information and data.	To be identified
Consent		
We have a clear and transparent approach to consent which: > Identifies where we are relying on implied consent > Allows customers to give and withdraw consent, where necessary > Enables and aligns with our new ways of working	Review, update and implement our privacy and Fair Processing Notices to comply with GDPR and to align with our future ways of working (NB will need to be undertaken in conjunction with the Transformation Team)	24/05/2018
	Implement procedural and technical changes to ensure we are obtaining positive consent (where consent is required) to allow us to process personal data	24/05/2018
	Implement procedural and technical changes to allow us to automatically cease the processing of personal data where consent is withdrawn (NB this may require the removal of links to certain data or the deletion of data)	To be identified
Data Retention & Deletion		
We are clear on how long we should retain each piece of personal data and have procedures in place for the proactive deletion of data once the retention period has expired	Work with each of our line of business system providers to identify and implement any changes required to ensure compliance with our retention & deletion obligations. (NB. This exercise will include identifying any costs associated with making these changes)	30/09/2018
	Identify data held in other areas i.e. paper records, e-mails, network drives etc. & implement procedural & technology changes to ensure compliance with our retention & deletion obligations. (NB. The solutions for these other areas will be identified as part of our future approach to Information Management as outlined above)	To be identified
Privacy by Design (Privacy Impact Assessments)		
Clear procedures in place which ensure that Privacy Impact Assessments are undertaken in respect of any new projects or procedural changes that involve personal data to ensure that the use of this data is appropriate, complies with GDPR and that proper safeguards are in place	Draft and implement a procedure (including a procedure to ensure ongoing compliance) to ensure that Privacy Impact Assessments are pro-actively carried out for any changes involving the processing of personal data (NB this will need to be built into the Transformation Project BPR process)	30/04/2018

Outcomes	Key Tasks	Target Date
Subject Access Requests		
The SAR process complies with the new legislation (i.e. no fee and 1 month response time). In the longer term, develop this as a self-service function.	Develop, document, implement and provide training in the new procedures.	30/04/2018
	Work with the Transformation Project Team to develop as a self-service function in the longer term.	To be identified
Contracts		
Ensure that future new and renewed contracts comply with the new regulations and provide sufficient protection for the councils.	Work with the procurement team to provide training and to introduce new procedures	31/03/2018
Information Sharing		
Ensure that we have a clear data sharing agreements in place with every organisation with whom we share personal data and that these agreements: > Are clearly written > Comply with GDPR > Set out what data is being shared and what it is used for > Clearly defined roles	Review, update and agree with suppliers/third parties revised data sharing agreements.	24/05/2018
	Consider any additional technology changes required to support the safe transfer of data with partner organisations i.e. e-mail security (Egress) and official protective markings.	24/05/2018
Data Breach Management		
Implement changes to the data breach procedure to ensure compliance with the new legislation (i.e. the 72 hour timeline).	Update our procedures and communicate to staff, members and third party organisations.	24/05/2018
Data Protection Policy		
Our Data Protection Policy and associated procedures are compliant with the new regulations.	Review and update the Data Protection Policy and procedures to ensure compliance with the new regulations (NB need to ensure alignment with our future operating model and Information Management Architecture)	31/03/2018

Project Roles

Project Manager (PM)	Assumes pure project management function
DPA expert	DP expert who will focus on policy & procedure change
Training	Assumes buy in external trainers
Technical/Trans Prog	Technical resource within the Trans Prog Team to deliv
External IM Consultants	To advise on & assist in developing the future Info Man
Admin	Assumes use Corp Business Support Team

working with the Trans Prog team as necessary

er the technical changes required to set up the future Info Man Architecture
Architecture & Info Asset Register