Waveney District Council

5

AUDIT AND GOVERNANCE COMMITTEE

Thursday, 20 September 2018

IMPLEMENTATION OF GENERAL DATA PROTECTION REGULATION (GDPR) AND DATA PROTECTION ACT 2018 (REP1909)

EXECUTIVE SUMMARY

1. The UK's new Data Protection Act 2018 (DPA) came into force on 25 May 2018, alongside the General Data Protection Regulation (GDPR).

2. The DPA is the biggest overhaul of data protection legislation for over 25 years, and introduced new requirements for how organisations process personal data.

3. The Councils Data Protection Officer is the Head of Internal Audit and the Internal Audit Team delivers the Data Protection Service across the Council.

Is the report Open or Exempt?	Open

Wards Affected:	All Wards in the District

Cabinet Member:	Councillor Bruce Provan Cabinet Member for Resources

Supporting Officer:	Name:	Mrs Siobhan Martin
	Job Title:	Head of Internal Audit
	Telephone:	01394 444254
	Email:	siobhan.martin@eastsuffolk.gov.uk

1 INTRODUCTION

1.1 The Data Protection Act 2018 (DPA) covers the use of personal data within the scope of the General Data Protection Regulation (GDPR) and beyond it. Amongst other provisions, it repeals and replaces the Data Protection Act 1998, incorporates the GDPR into UK law, lays the ground for free-flow of data between the United Kingdom and the European Union after Brexit, sets out permitted exemptions under the GDPR and sets out the duties and powers of the UK's Information Commissioner's Office (ICO).

1.2 With administrative fines under the new Act now having an upper limit of 20 million Euros, it is crucial that the Councils are compliant with the DPA/GDPR, as they have been under the Data Protection Act 1998. This report sets out the work undertaken by the Councils' Internal Audit Team to prepare for and implement GDPR across the Councils.

2 PREPARATIONS FOR GDPR

2.1 Preparations for GDPR commenced in early 2017, with extensive research by the Councils' Head of Internal Audit (who is also the Councils' Data Protection Officer) and the preparation of a GDPR Project Plan.

2.2 The Plan commenced in August 2017 with the establishment of a Project Team of representatives (Data Champions) across all teams in the Councils.

2.3 Workshops were held on four dates between September 2017 and January 2018, at which Data Champions were briefed on the main elements of GDPR, and the work streams that they would be part of on behalf of their teams. All members of the Internal Audit Team also came on board with the project at this point, and have taken on the training of other teams across the Councils on GDPR issues.

3 RESOURCES AND POINTS OF CONTACT

3.1 The Councils qualified and experienced Data Protection Officer is the Head of Internal Audit. The Audit Manager is the qualified Deputy Data Protection Officer and five officers in the Internal Audit Team also form the Data Protection Team.

3.2 To assist with the implementation of GDPR, and to provide ongoing Data Protection support to all teams of the Councils, from April 2018 each service area across the Council was allocated a named officer from the Data Protection Team to act as a first point of contact. The aim of this initiative is to add value and to keep in touch and up to date on service changes. This will develop a greater understanding of the risks faced by each service of the Council, and improved targeting of future Data Protection/Internal Audit work.

3.3 We have found that the Audit Team Points of Contact initiative has been well received by teams, and in particular Data Protection queries are being brought direct to the relevant Audit Team member, for example assistance with drafting Data Protection Impact Assessments or Privacy Notices, meaning that the auditor with the greatest understanding of each team is available to help.

3.4 The Data Protection Officer is a member of the regional Data Protection Group, in addition to a number of national groups, and attends events where the Information Commissioner Elizabeth Denham discusses the work of the Information Commissioners Office.

4 DPA/GDPR WORK STREAMS

4.1 A number of work stream (detailed below) are in operation to ensure continued compliance with the law. Future work streams include: Transfers of personal data to third countries and Security Testing.

5 WORK STREAM 1 - TRAINING

5.1 **Corporate Management Team** (CMT) - The Data Protection Officer delivered training to CMT in September 2017 and continues to provide regular updates.

5.2 **E-Learning** - A GDPR e-learning package developed by West Suffolk Councils has been made mandatory for all officers of SCDC and WDC. The Data Protection Officer is monitoring the training records and non completers will be reported to the relevant Heads of Service. To date, 89% of staff with access to a computer have completed the training.

5.3 **Non IT Workers** - Around 100 operatives with no access to IT will be offered workshops in September 2018 to provide GDPR training bespoke to their particular needs.

5.4 **Members** – The Data Protection Officer delivered DPA/GDPR training at WDC Full Council in November 2017. Training was also provided to Members of WDC on 11 June 2018, and 15 Members took up the offer of training. Further dates will be offered in the future, including sessions at SCDC's offices.

5.5 **Intranet** - Regular informative DPA bulletins are posted on the Councils Intranet.

5.6 **Town/Parish Councils** - Training workshops for Clerks and Members of Town and Parish Councils were held on four dates in May 2018, with both afternoon and evening sessions offered. 40 representatives attended, and were provided with templates to complete their Information Asset Registers, Privacy Notices and Data Protection Impact Assessments. The documentation has also been provided free of charge to any other parish or town council representatives in the SCDC/WDC area who have requested it.

5.7 **Partners** – Partner organisations are individually responsible for the application of the DPA and it is the Councils responsibility to gather assurance/evidence that such organisations are implementing the law correctly. This exercise is part of the Contracts work stream and future security work stream.

6 WORK STREAM 2 – ESTABLISH, TRAIN AND COORDINATE DATA CHAMPIONS

6.1 In order to swiftly respond to subject access requests and to comply with the mandatory elements of DPA a pragmatic approach has been taken, whereby Data Champions, have been designated by Heads of Service and trained by the Data Protection Officer. The Data Champions represent the different service areas in the Council and act as a conduit for good DPA practices.

6.2 The following table lists the Councils Data Champions:

Service Area	**Job Title**
Communities	East Suffolk Communities Manager
	Active Communities Officer
Customer Services	Customer Experience Officer
Economic Development and Regeneration	Assistant Economic Development Officer
	Economic Development Officer
Environmental Services and Port Health	Environmental Protection Officer
	Food and Safety Manager
	Operations Manager (Port Health)
	ICT Team Leader (Port Health)
Financial Services, Corporate Performance and Risk Management	Finance Manager (Financial Compliance)
	Finance Manager (Financial Planning)
	Performance Support Officer
Housing Operations and Landlord Services	Housing Strategy Manager
ICT	Business Solutions Manager
Legal and Democratic Services	Legal Services Manager
	Litigation Lead
Operations	Office Administrator (Asset Management)
	Procurement Manager
	Commercial Contracts Manager (Leisure)
	Valuer (Asset Management)
Planning and Coastal Management	Planning Support Services Manager
	Head of Coastal Partnership East
	Planning Policy and Delivery Manager
	Assistant Planning Officer
	Development Management Team Leaders
Revenues and Benefits	Revenues Manager
SMT / CMT / HR	PA
	HR Advisor
	Communications: Vacant

7 WORK STREAM 3 – POLICIES AND GUIDANCE

7.1 A number of documents have been, or are being prepared or reviewed to assist Members, Officers, and members of the public. These include (not exhaustive list):

a. Data Protection Policy
b. Retention Policy
c. Information Asset Policy
d. Data Quality Policy
e. Personal Data Breaches Guidance
f. Privacy Notices
g. Protective Marking Policy
h. Subject Access Request Form
i. Data Protection Impact Assessment (DPIA) Guidance
j. Information Asset Register (IAR) & Policy
k. Town/Parish Councils – Template PP/IAR/DPIA

8 WORK STREAM 4 - INFORMATION ASSET REGISTERS (IAR)

8.1 The creation of Information Asset Registers is an essential ongoing, extensive piece of work to log all data collected across the Councils, both historically and going forward. The IAR templates are being populated (with direction from the Data Protection Officer) by the Data Champions for each team setting out the data collected and, amongst other detail, why the data is collected, retention timescales, legal basis, identification of special data and other information which will inform what further work needs to be undertaken to protect that data.

8.2 Appendix A sets out the dates of the IAR workshop sessions held with officers from across the Councils; as well as these a number of 1:1 sessions were held, and continue to be held, with individual members of the Internal Audit Team.

9 WORK STREAM 5 – PRIVACY NOTICES (PN)

9.1 A generic corporate Privacy Notice was published on the Councils' website covering all services provided by the Councils. Alongside this Privacy Notice, Data Champions were asked to populate Team Privacy Notices for every service provided to the public which required the collection of personal data. Privacy Notices advise our customers what information about them is collected, when it is collected, how it is used, how long it is kept and whether it is shared, and with whom. The Notices also set out peoples' rights under GDPR and DPA 2018. Publication of Privacy Notices is an ongoing task, and the Notices published to date can be found on the Councils' website.

9.2 Appendix A sets out the dates of the PN workshop sessions held with officers from across the Councils; as well as these a number of 1:1 sessions were held, and continue to be held, with individual members of the Internal Audit Team.

10 WORK STREAM 6 – DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

10.1 A Data Protection Impact Assessment (DPIA) must be performed where processing is likely to result in a high risk to the rights and freedoms of natural persons. Where the Information Asset Registers have identified that the Councils are holding special data (for example ethnic origin, religion, health data), a DPIA will need to be completed to risk assess such data and ensure it is held as securely as possible.

10.2 Workshops and 1:1 training to officers and teams on DPIA's have commenced and will continue as and when required. Appendix A sets out the dates of the 17 DPIA workshop sessions held with officers from across the Councils.

11 WORKSTREAM 7 – CONTRACTS

11.1 A review of Navision (General Ledger software) was undertaken to identify potential high risk and/or high value contracts between the Councils and third parties in which data processing could be taking place. Based on financial data for the period 1/4/17 to 15/5/18 a spreadsheet was prepared listing all of the potential contracts. A template Data Processing Agreement was prepared by Legal Services, and the Procurement Team was tasked with issuing the Agreement to a carefully selected group of 45 third parties from the spreadsheet. This task was completed in three tranches commencing on 24 May and culminating on 8 June 2018.

11.2 To date there has been a mixed response to the request for third parties to sign the proposed Data Processing Agreement. There have been 15 responses to the 45 requests that were sent out by the Procurement Team. Six of the third parties have agreed to the terms, 3 are currently negotiating specific details within the terms and the remaining respondents have either referred to their standard terms or sent a holding response. The other third parties (30 in total) have yet to respond, among them some of our more significant contractors such as Sentinel Leisure Trust and Places for People. Follow up will take place in due course; there is scope for the relevant service managers to take this forward.

11.3 Amendments to current contracts and new wording for future contracts and information sharing agreements are underway.

12 OTHER ISSUES

12.1 As we work with officers on implementing GDPR, we are advised of issues which we refer to other teams across the Councils. These include making changes to IT systems to enable easier deletion of data when retention periods are reached, or to amend fields so that the minimum data required is requested from customers. Another issue identified was with hosting of data outside of the EU, and checks were made to ensure that that data was held securely.

13 INCREASE IN DATA PROTECTION REQUESTS AND REQUESTS FOR ADVICE

13.1 As would be expected, with the publicity surrounding GDPR, the number of Data Protection Requests, Subject Access Requests and Alleged Breaches/Incidents has increased. The increase was such that a new Access Database to record these contacts was created. Appendix B provides data showing that from 1 April to 22 August 2018, the Internal Audit Team has dealt with 50 Data Protection Requests, 22 alleged breaches/incidents, and 152 requests for advice from officers across the Councils.

13.2 This equates to 140 days worked by the Auditors on Data Protection, in addition to 37 days by the Audit Manager, but does not include the time spent by the Head of Internal Audit, which will be significant. Despite this, the 2017/18 Audit Plan was completed, and the 2018/19 Plan has been commenced.

13.3 It should also be pointed out that this does not include the work carried out in every team across the Councils to write PNs/IARs/DPIAs, undertake training, carry out housekeeping of historical data and ensure systems are GDPR compliant going forward. Whilst led by Internal Audit, this has been a whole Council exercise, and will continue to be.

14 HOW DOES THIS RELATE TO THE EAST SUFFOLK BUSINESS PLAN?

14.1 One element of the "three pronged strategy" in the East Suffolk Business Plan is Enabling Communities. Our work on GDPR/DPA 2018 will ensure that the personal data of the people we are working for is held securely, and that they are aware of their rights with regard to the retention of their data. The Internal Audit Team has also contributed to the strategy of financial self sufficiency by absorbing the extra workload arising from GDPR.

15 FINANCIAL AND GOVERNANCE IMPLICATIONS

15.1 To date, the significant additional workload arising from GDPR has been undertaken by the Internal Audit Team with no additional resources. Whilst this provides good value for money, inevitably it will have an impact on completion of the 2018/19 Audit Plan. However, in this year leading up to the creation of East Suffolk Council, the focus is necessarily on ensuring the required governance and legal structures are in place, and it will therefore be appropriate to concentrate our Internal Audit work on key risk areas rather than carrying out a full audit plan in this important year. Any revisions to the Internal Audit Plan 2018/19 will be reported to the Audit and Governance Committee.

16 OTHER KEY ISSUES

16.1 This report has not required the preparation of an Equality Impact Assessment, a Sustainability Impact Assessment or a Partnership Impact Assessment, although these issues are taken into account in all our work on Data Protection and the implementation of GDPR.

17 CONSULTATION

17.1 Consultation took place between the Head of Internal Audit and Senior Management Team prior to commencing the work on the implementation of GDPR. Additionally, as the workshops have taken place, this has been an opportunity for all officers and Members of the Councils to feed their ideas into the work on GDPR.

18 OTHER OPTIONS CONSIDERED

18.1 None.

19 REASON FOR RECOMMENDATION

19.1 To update Members on the work undertaken by the Internal Audit Team on the implementation of GDPR and the Data Protection Act 2018.

RECOMMENDATIONS

That Members consider the information in this report and comment upon the implementation of the Data Protection Act 1998/General Data Protection Regulation at the Council.

APPENDICES	
Appendix A	List of GDPR Workshops Held
Appendix B	List of Data Protection Requests and Requests for Advice

BACKGROUND PAPERS		
Date	**Type**	**Available From**
2018	Data Protection Act 2018 (Statutory Instrument) – Data Protection Officer	
2018	General Data Protection Regulation (Statutory Instrument) – Data Protection Officer	

Appendix A – Information Asset Register / Privacy Notice Workshops held

Workshop	Council	Date	Number of Sessions	Number of Attendees
Information Asset Register / Privacy Notices	WDC	15 May 2018	2	5
	SCDC	16 May 2018	3	11
	WDC	22 May 2018	4	11
	SCDC	24 May 2018	2	12
	WDC	30 May 2018	3	5
	SCDC	31 May 2018	1	4
	WDC	1 June 2018	1	2
Information Asset Register / Privacy Notices / Data Protection Impact Assessments	SCDC	6 June 2018	1	2
	SCDC / WDC	7 June 2018	2	4
	SCDC / WDC	8 June 2018	2	4
	SCDC / WDC	11 June 2018	3	7
	WDC	12 June 2018	1	6
Data Protection Impact Assessments	SCDC	20 June 2018	1	12
	WDC	21 June 2018	1	8
	WDC	22 June 2018	3	4
	SCDC	27 June 2018	1	1
	SCDC	28 June 2018	1	2

20 plus 1:1 sessions held with individual officers

Appendix B – Data Protection Requests and Requests for Advice – 1 April 2018 to 22 August 2018

GDPR / DPA Requests	SCDC	WDC	Joint Requests	Total
Address Checks	13	13	1	**27**
Complaint	0	1	0	**1**
Proof of Life Requests	0	0	5	**5**
Subject Access Requests	4	5	1	**10**
Other	4	3	0	**7**
Total	**21**	**22**	**7**	**50**

Breaches and Incidents	SCDC	WDC	Joint incidents	Total
After investigation - Not a Breach	3	4	0	**7**
Disclosed in Error	0	4	0	**4**
Human Error	1	2	0	**3**
Near Miss	0	2	0	**2**
Under Investigation	0	3	0	**3**
Technical / Procedure Failure	2	1	0	**3**
Total	**6**	**16**	**0**	**22**

Advice	SCDC	WDC	Joint advice	Total
Complaints	1	1	0	**2**
Consent	3	0	10	**13**
Contracts and Data Sharing Agreements	9	17	8	**34**
Data Protection Impact Assessments	3	0	9	**12**
FOI / EIR	0	0	1	**1**
GDPR Implementation	1	0	1	**2**
Information Asset Registers	0	0	2	**2**
Information Security	0	0	4	**4**
Other	0	2	8	**10**
Parish and Town Councils	3	3	2	**8**
Privacy Notices	6	8	35	**49**
Publishing and Releasing Information	0	3	4	**7**
Retention and Deletion	0	0	4	**4**
Training and Guidance	2	1	1	**4**
Total	**28**	**35**	**89**	**152**