ADUR & WORTHING
COUNCILS

Joint Governance Committee
25 September 2018
Agenda Item 8

Ward(s) Affected:n/a

GDPR Compliance Progress Report

Report by the Director for Digital & Resources

Executive Summary

1. Purpose

1.1 This report provides an overview of the governance approach of the councils towards GDPR compliance. It provides an update on the actions against audit recommendations in relation to GDPR and an overview on how individual services are progressing.

1.2 The reports sets out the approach to continuously improving the secure management of data.

1.3 The report is being presented in response to a specific request made at the 31 July meeting of this committee.

2. Recommendations

2.1 The Committee is asked to note the progress being made in terms of improving how data is managed and processed by the Councils, specifically in relation to GDPR.

3. GDPR Introduction

3.1 Until the introduction of the General Data Protection Regulations (GDPR) data protection law was based on EU legislation dating from 1995. Since then the volume of personal data flowing electronically and the uses made of it have grown exponentially. This has been the key driver for changes to data protection law, passed by the European Parliament in 2016, which came into force across the European Union on 25 May 2018.

3.2 The fundamental principles of data privacy established under existing laws remain the same but there are significant enhancements to:

- The controls (rights) that individuals (data subjects) can exercise over their own personal data
- The information that organisations must provide to individuals about the data held on them
- The requirement to demonstrate compliance with the new law.

3.3 Non-compliance could result in severe monetary penalties and reputational damage. A summary of the key changes are set out in Appendix 1.

4 Approach to managing GDPR

4.1 Local authorities are complex organisations when it comes to managing data. All services, from front facing services as diverse as Housing, Parking, Environment and Planning through to support services such as Legal and Human Resources all hold their own data in hard and electronic formats. Cross cutting services such as Customer Service and Digital access or manage data on behalf of services. A single customer is likely to have data held on them by a range of services eg Council Tax, Housing and Benefits. Data retention requirements vary significantly within and between services. For example some Planning records need to be retained for decades (specific examples), number plate recognition data from our car parks is only retained for 30 days.

4.2 As a result of this complexity all services are required to assess their individual GDPR compliance requirements. GDPR is an evolution from the previous Data Protection Act, and managing data securely is a practice which is embedded across council services. It is not a new activity but services do need to be aware of changes as a result of GDPR and put additional measures in place.

4.3 The Information Governance Officer plays a key role in supporting services with this work. The council's previous Information Governance Officer led on raising awareness across the Councils on GDPR, advising what the

regulations mean and establishing a toolkit for services to work to. The officer left the councils in April 2018 to pursue a new opportunity and an Interim GDPR lead & Data Protection Officer (Nick Key) was appointed while recruitment for a permanent postholder is pursued. The interim lead has focussed on providing services with hands on support on how to comply with GDPR. Specific activities to support services include:

- Production of a GDPR Toolkit
- Development and roll out of a GDPR e-learning module for all office based staff
- Identification of 30+ GDPR leads across the organisation responsible for progressing compliance in their areas
- Regular themed workshops and drop in sessions on specific challenges for GDPR leads, eg on privacy notices and data retention schedules.
- 1-1 support as and when required for all GDPR leads
- GDPR guidance and training for all councillors.

4.4 Progress is monitored by service by the Interim GDPR Lead and reported to CLT and the Information Governance and Security Board which is chaired by the Director for Digital and Resources in his capacity as Senior Information Risk Officer (SIRO).

4.5 Two internal audits in to data protection have been carried out which have informed the priorities of the work programme. The scope and findings of these audits is summarised in section 5.

5 GDPR Audit Programme

5.1 As part of the Councils Audit programme two GDPR audits were completed in the last 12 months. The first audit, Compliance With Data Protection Legislation was completed in April 2018. The report concluded there was Satisfactory Assurance stating *there is a basically sound system of internal control, there are weaknesses, which put some of the client's objectives at risk.* The progress on the audit recommendations is summarised in the table below.

Priority	Issue	Recommendation (extract)	Progress
High	3.3 Data Protection Training	A method is required to ensure that all new staff undertake data protection training on commencement of employment at the Council	**Complete:** Training mechanism is in place to ensure that all new and existing staff complete data protection training annually. Training for staff who are not office based (and generally do not handle personal data, eg in waste and parks) being developed
Medium	3.7 Fair Processing Statements	All application forms (both paper and online) used by the councils should be examined to confirm whether they include adequate fair processing statements	**Partially Complete:** All webforms link to the Corporate Privacy Notice, which in turns links to service specific privacy notices, which have been completed and published for most service areas. ICT Digital are working through the remaining fair processing statements required for Matsoft applications and online application forms.
Medium	3.8 Subject Access Requests	Where clarification emails/letters are sent/received in respect of Subject Access Requests a means of retaining the requests and responses should be affected within the Matsoft App in order that a full audit trail/history of the request is maintained	**Completed:** Manual SAR process in place with evidence collated on the MATS system by the Insight Team who manage the process.
Medium	3.9 Information Disposal Schedule and Guide	The Councils Information Disposal Schedule and Guide should be reviewed and updated	**Completed:** Disposal Schedule and Guide published online and will be reviewed regularly through GDPR governance schedule.
Medium	3.10 Monitoring Information Disposal	Consideration should be given to effecting a process for the SIO to monitor that the disposal of information is conducted in line with the Councils Information Disposal Schedule	**Completed:** As part of GDPR Governance Framework services will be required to update their records regularly and the Information Governance Officer will carry out QA spot checks.

5.2 Following on from the first high level audit a second audit was requested to carry out a GDPR of a gap analysis of four key services. These services (Housing, Revenues & Benefits, HR and Wellbeing) were specifically selected to be audited due to the volume and nature of data they process, they were considered to be higher risk. The audit was also completed in April 2018. The report concluded there was Limited Assurance stating: *Weaknesses in the system of internal controls are such as to put the client's objectives at risk. The level of non-compliance puts the client's objectives at risk.* Progress against the recommendations is summarised in the table below.

Priority	**Issue**	**Recommendation (extract)**	**Update**
High	1.1 Legal Basis for Processing	The Housing Service relies on consent as legal basis to carry out their processing activities.	**Complete:** Legal basis stated in Housing Privacy Notice which has been completed and is published
High	1.2 Legal Basis for Processing	HR has advised during the fieldwork that HR processing activities were likely to rely mainly upon consent	**Complete:** Legal basis stated in HR Privacy Notice
High	1.3 Legal basis for Processing	When performing a contract for a data subject, consent is not obtained from the data subjects to share their personal data with third parties for the provision of additional services	**Complete:** Well Being have identified programmes delivered by a third party and have amended consent forms to explicitly consent to the sharing of information.
High	2.1 Rights of Data Subjects	The process to respond to a request for access from a data subject is not documented and needs to be reviewed. The requirement to provide the information free of charge has not yet been implemented.	**Complete:** Processes and templates are in place and being tested against the SAR received to date. Process centrally coordinated by the Insight Team.
High	2.2 Rights of Data Subjects	The process for rectification of personal data after a valid request from a data subject is not documented.	**Complete:** Procedure for Rights Request process has been developed. Process centrally coordinated by the Insight Team.

High	2.3 Rights of Data Subjects	The process to restrict the processing of personal data after a valid request from a data subject is not documented.	**Complete:** Procedure for Rights Request process has been developed. Process centrally coordinated by the Insight Team.
High	4.1 Privacy Notices	The timing of the provision of the different privacy notices to data subjects is unclear.	**Partially Complete:** Web-based data collection points are identified. Corporate privacy notices linked to all webforms and majority of service specific privacy notices in place. Privacy notices in customer service teams (telephony and face to face) in place. Members provided with a template Privacy Notice to use for casework.
High	5.1 Security and Data Breach	Security measures, such as pseudonymisation, access management and encryption, are not implemented in a manner proportionate to the sensitivity of the data held and the nature and scope of the processing (special categories of data, criminal records).	**Partially Complete:** Before this recommendation can be completed and closed services needed to produce their ROPA and identify special category data. That has now been collected and they are carrying out Privacy Impact Assessments against that data which will enable this recommendation to be addressed. It should be noted that that services have managed this type of data under the Data Protection Regulations so control measures are in place but they need to be reviewed and upgraded where necessary.

High	7.1 Data Protection Officer and Data Protection Governance	The GDPR project plan and awareness are satisfactory, but a lack of financial resources and staff could compromise the implementation of GDPR in time in the Councils.	**Complete:** Interim DPO appointed, permanent role yet to be appointed. No further resource requirement identified at this stage.
Medium	1.4 Legal basis for Processing	The Housing Service can access Revenues and Benefits databases to update their own records and perform fraud prevention checks, instead of collecting this data directly from the data subjects	**Complete:** Revenues and Benefits have developed a Memorandum of Understanding (MOU) and Data Protection declaration to be signed by the Housing Service
Medium	2.4 Rights of Data Subjects	Direct marketing activities in the Housing Service must be reviewed for compliance.	**Complete:** Housing have confirmed they do not participate in direct marketing activities
Medium	2.5 Rights of Data Subjects	Under Freedom of Information Act, the Councils may disclose personal addresses of their self-employed contractors if they have registered their activity at their place of residence.	**Complete:** This information is not disclosed
Medium	3.1 Obligations of Controllers and Processor	Contracts with third parties have not yet been reviewed for compliance with GDPR and to include updated standard privacy and confidentiality clauses that have been approved by the Councils' legal department or legal counsel.	**Complete:** Addendums to contracts written have been approved by legal and and services are sharing them with suppliers.
Medium	3.2 Obligations of Controllers and Processor	The contract between Adur & Worthing Councils and West Sussex County Council must be reviewed.	**Completed:** WSCC and AWC are designated joint Data Controllers
Medium	5.2 Security and Data Breach	There are no approved notification templates for the ICO and data subjects in case of a confirmed data breach.	**Complete**: The Councils are using the ICO & Article 29 breach guidelines and templates to report any breaches.
Medium	7.2 Data Protection Officer and Data Protection Governance	The previous report raised a recommendation regarding the Data Protection Officer job description, as being not adequate.	**Complete**: Interim DPO appointed, permanent role yet to be appointed. Job description has been reviewed and updated.
Low	1.5 Legal basis for Processing	"Tell Us Once" service should be documented in the records of processing activities.	**Complete**: Tell Us Once Service is being documented in the records of the Customer

			Service Team.
Low	2.6 Rights of Data Subjects	The Electoral Roll is being automatically updated when data subjects update their address with Housing Services.	**Complete**: There is no automatic enrolment
Low	2.7 Rights of Data Subjects	Automated decision making could be used in the future in Revenues & Benefits.	**In Progress:** Service led redesign underway which will address opportunities
Low	4.2 Privacy Notices	A specific query has been raised during the review, whether it is necessary or not to provide a privacy notice in the taxi licensing service.	No activity on this item
Low	6.1 Data Protection Impact Assessments	There are no policies in place that define when a DPIA should be conducted.	**Complete**: DPIA embedded into Service Introduction Plan. Awareness sessions are run on how to complete DPIAs
Low	7.3 Data Protection Officer and Data Protection Governance	The previous report raised a recommendation regarding data protection training for employees, as being not mandatory and regularly taken.	**Complete**: Training for office based staff implemented. Training for field based staff who do not generally handle personal data (eg in waste and parks) being planned.

5.3 The recommendations from the audits will be kept under continuous review. For example updated staff training was rolled out in April 2018, and all staff will be required to complete annual refresher training. New staff will require training as they join the organisation. Services have documentation in place such as data retention schedules and Registers of Processing Activity, and these require cyclical review to maintain compliance.

5.4 All the work being progressed is being fed in to a corporate GDPR Governance Framework which sets out how the Councils comply with GDPR, identifying roles and responsibilities and control measures to ensure compliance with GDPR.

6 Progress By Service Area

6.1 There are approximately 168 service areas across the Councils which all have different GDPR compliance requirements. Each area has a service lead with progress being monitored by the Interim Information Governance Officer. As mentioned previously the volumes and types of data controlled or processed by services varies greatly in sensitivity.

6.2 Key areas are tracked for compliance which include:

- Having a Register of Processing Activity
- Having up to date privacy notices
- Having up to date Information disposal schedules.
- Having up to date consent arrangements
- Updated service documentation
- Updated policies
- Ensuring staff are updated on policies, processes etc.
- Ensuring staff have completed e-learning
- Embedding new practices to show compliance with GDPR accountability principles
- Reviewing contracts for external data processing
- Reviewing where data is held
- Ensuring data breaches are reported
- Embedding data protection by design
- Embedding data protection impact assessment practices

6.3 The tables in Appendix 2 provide an aggregated overview for services, whether they are compliant or making progress on compliance. Overall levels of compliance are good in the following areas:

- GDPR awareness is high and engagement with the GDPR progress is good
- Most services have completed and updated their RoPAs
- Privacy notices are in place and published for most services
- Services have started to update their information retention and disposal schedules
- Corporately processes are in place for people to exercise their rights under GDPR, eg processes for Subject Access Requests.
- A process is in place to monitor staff training, xx staff have completed the e-learning module

6.4 A number of services cut across the councils in terms of GDPR. The customer service teams access systems and data on behalf of services, for

example helping customers with council tax, benefits or housing systems, so they generally do not control data. The Digital team plays a critical role in supporting services to manage and dispose of electronic data in line with their Data Retention and Disposal Schedules. The team has commenced deletion of electronic data in line with these schedules, however there is a significant backlog which will take some time to clear. Similarly with hard copies of data some services have large archives which need to reviewed and managed appropriately in line with GDPR. This is being progressed by services.

6.5 Now that services are up to speed with what they need to do under GDPR, and good progress is being made the priorities for the next six months are as follows:

- Recruit a permanent Information Governance Officer who will also act as the Council's Data Protection Officer
- Complete and publish the Councils GDPR Governance framework, which sets out the Council's overall approach to managing data responsibly including roles and responsibilities, key schedules and review dates.
- Embed GDPR training in the induction process
- Carry out QA checks on services to ensure they operate within the Governance framework.
- On going communication and awareness raising around good practice in relation to data management (eg locking screens, clear desks etc).
- Continue to report progress and performance to the Information Governance and Technology Board.

6.6 Within the Digital Team a project (Google for Teams) is underway to upgrade and relaunch Google. The work will include the adoption of Google Team Drive and limiting use of Microsoft to business critical areas, reducing data duplication and improving security. The project will also result in the cleansing of old data helping meet service disposal schedules. Work is continuously underway to enhance data protection including reviewing options for single sign on which will provide greater control of users signing in to multiple applications.

7 Conclusions

7.1 The GDPR regulations have placed additional requirements on the councils in terms of how we manage customer data. Work towards complying with these additional requirements is progressing well with the majority of the audit recommendations from April 2018 having been completed.

7.2 Given the scale and complexity of our services the Councils will continuously be working towards GDPR compliance rather than compliance being a fixed end point.

8 Financial Implications

8.1 The cost of compliance with the GDPR requirements are being met from existing budgets.

9 Legal Implications

9.1 The General Data Protection Regulations 2018 came into force on 25th May 2018 and are designed to modernise the laws protecting the data of private individuals. The regulations harmonise data protection rights across Europe and give individuals greater rights and control over data relating to themselves.

9.2 The Regulations replace the previous 1995 Data Protections Regulations upon which UK legislation was based. The new regulations are implemented in the Uk by the introduction of the Data Protection Act 2018.

9.3 The new legislation is to be enforced in the UK by the Information Commissioner's Office who have the power to impose financial penalties on those not complying.

Background Papers
None.

Officer Contact Details:
Name: Nicholas Key
Role: Interim GDPR Lead
Telephone:
Email: nicholas.key@adur-worthing.gov.uk

Name: Jan Jonker
Role: Head of Customer & Digital Services
Telephone: 07881255291
Email: jan.jonker@adur-worthing.gov.uk

Appendix 1 Changes to European Union Data Protection Legislation

1. **Being more transparent with individuals**

The new legislation requires data controllers to give individuals more information at the time their data is collected including an explanation of the legal basis for the processing, data retention periods, the individual's rights and the data controller's obligations.

2. **Demonstrating compliance**

An overarching theme of the legislation is the principle of 'accountability'. There are new requirements on data controllers to demonstrate compliance by fully documenting all their data processing activities.

3. **Mandatory personal data breach notification**

Data controllers have 72 hours to report a personal data breach to the ICO and where the breach is likely to result in a high risk to the privacy of individuals, they must also notify the individual without undue delay.

4. **High penalties when things go wrong**

There are much stiffer, proportionate penalties for non-compliance; the ICO will be able to issue fines of up to £17 million.

5. **Enhanced rights for individuals**

The legislation includes increased rights for individuals. In addition to existing subject access rights, they will have the following;

- Right to rectification (if inaccurate data is held)
- Right to erasure (also known as 'right to be forgotten') in certain circumstances
- Right to restriction of processing in certain circumstances
- Right to data portability (personal data transferred from one data controller to another)
- Right to object (to profiling, direct marketing, automated decision-making)

The councils are obliged to each of the above requests within one calendar month.

6. **Compensation for individuals**

Individuals will be entitled to receive compensation from councils if they suffer material / non-material damage as a result of Adur and Worthing Councils not meeting their obligations under the legislation.

7. Security

Members will need to comply with the new legislation and should ensure appropriate security of individuals personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisational measures including but not limited to;

- Using only your official Adur and Worthing Council email address for correspondence
- Only share personal data with authorised individuals
- Don't keep personal data longer than required

The legislation places a duty on all data controllers keeping certain records to prove they are compliant.

8. New Requirements

The following is a summary of the new requirements when collecting personal data under GDPR;

- Record your processing activities using the Register of Processing Activity (ROPA)
- Share your Privacy Notice when you collect personal data
- Inform individuals of their rights
- Delete data that is no longer required
- Report any personal data breaches within 72 hours

9. Data protection principles

There are six principles under the GDPR (seven if you include 'accountability') as opposed to eight under current legislation. These are:

1. Personal information shall be processed lawfully, fairly and in a transparent manner.

2. Personal information shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

3. Personal information shall be adequate, relevant, and limited to what is necessary

4. Personal information shall be accurate and, where necessary, kept up-to-date

5. Personal information shall be retained only for as long as necessary.

6. Personal information shall be processed in an appropriate manner to maintain security.

10. New Definitions

'Personal data' means any information relating to an identifiable living individual ('data subject').

'Identifiable living individual' means a living individual who can be identified, directly or indirectly, in particular by reference to;

a) An identifier such as a name, an identification number, location data or an online identifier, or

b) One or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

'Special category' (sensitive) personal data includes:

- Racial or ethnic origin
- Political opinions
- Religious/philosophical beliefs
- Trade union membership
- Processing of biometric/genetic data to identify someone
- Health
- Sex life or sexual orientation

'Processing', in relation to personal data, means an operation or set of operations which is performed on personal data or on sets of personal data, such as:

a) Collection, recording, organisation, structuring, storage

b) Adaptation or alteration

c) Retrieval, consultation, use

d) Disclosure by transmission, dissemination or otherwise making available

e) Alignment or combination, or

f) Restriction, erasure or destruction

'Data subject' means the identified or identifiable living individual to whom personal data relates.

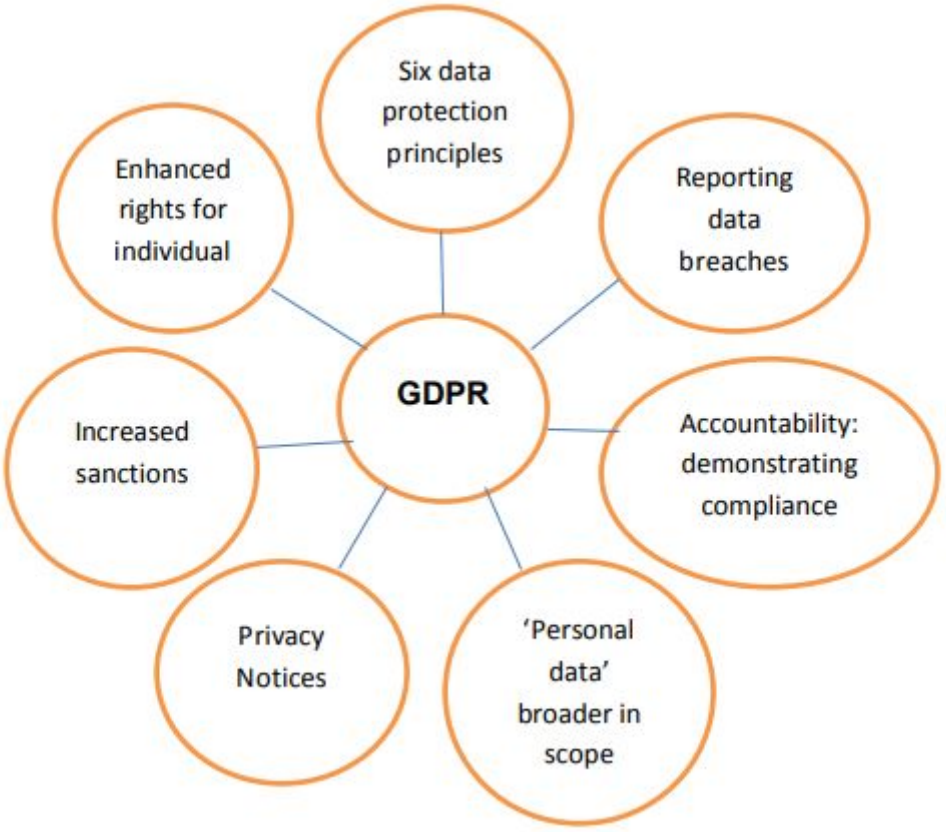
'Controller' means the natural or legal person, public authority, agency or other body which, along or jointly with others, determines the purposes and means of the processing of personal data.

'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controllers.

'Filing system' means any structured set of personal data which is accessible according to specific criteria, whether held by automated means or manually and whether centralised, decentralised or dispersed on a functional or geographical basis.

'Consent' of the data subject, when required, means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

11. GDPR at a Glance



Appendix 2 Summary of GDPR Compliance Progress By Service Area

Sustainability & Risk Assessment

1. Economic

- Matter considered and no issues identified

2. Social

2.1 Social Value

- Matter considered and no issues identified

2.2 Equality Issues

- Matter considered and no issues identified

2.3 Community Safety Issues (Section 17)

- Matter considered and no issues identified

2.4 Human Rights Issues

- Matter considered and no issues identified

3. Environmental

- Matter considered and no issues identified

4. Governance

- Effective GDPR Governance is critical to the council managing data risks and reputational damage. The report sets out how these issues are being managed.