Public Protection Partnership | Bracknell Forest West Berkshire Wokingham

Briefing Note – 23/02/2018
GDPR for the Public Protection Partnership

Purpose:
The EU's General Data Protection Regulation (GDPR) will apply from 25 May 2018, when it supersedes the UK Data Protection Act 1998. Significant and wide-reaching in scope, the new law brings a 21st century approach to data protection. It expands the rights of individuals to control how their personal information is collected and processed, and places a range of new obligations on organisations to be more accountable for data protection.

Proposed Action:
The ability to prove compliance is critical, and a comprehensive and effective privacy compliance framework will develop evidence to support your claims of compliance. UK organisations handling personal data will still need to comply with the GDPR, regardless of Brexit. The GDPR will come into force before the UK leaves the EU, and the government has confirmed that the Regulation will apply, a position that has been stated by the Information Commissioner's Office (ICO).

The 6 Principles of the Act are;

- Lawful, fair and transparent
- Collected for a legitimate, explicit purpose
- Adequate, relevant and limited
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary
- Security of the personal data

July-Dec 2017 - Phase One: Preparation and understanding of the legislation
Jan-Mar 2018 - Phase Two: Data Mapping process [DFM]
April-May 2018 - Phase Three: Review of practices and procedures (Practising what to do after 25 May 2018)

- Policies
- Processes
- Security
- DPIA
- Privacy Notice

Reason for decison to be taken:
The General Data Protection Regulation (GDPR) demands greater accountability and transparency from the public protection Partnership in how they collect, process and store personal information.

Some obligations can be resolved fairly simply and quickly. Others could have significant budgetary, IT, personnel, governance and communications implications and could require a great deal of work or specific expertise. Ensuring buy-in from senior management and key stakeholders is critical to meeting the obligations.

High risk areas for PPP

- G/M/I Drive – Access and security levels
- Flare and Uniform System - Access and security levels, Data in relation to retention and destruction policy
- Idox EDRMs- Access and security levels, Data in relation to retention and destruction policy
- Personnal Drives - Data

Policy:
Retention and destruction policy needs to be written for PPP, currently three policies are all being updated
Information Sharing Agreement need to be published
Data Breech Policy need to be reviewed
Data Privacy impact assessments being reviewed
PIA need to be idenifity and Information Asset Register brought in line with the new legisation

Financial:

Uniform Retention and destrction Module West Berks – Purchased
Uniform Retention and destrction Module Bracknell – 13k waiting for Planning to decide if 3 or 4 way slip
Flare Wokingham Retention and destrction Module – Price to be comfirmed

Personnel:
The main contacts at the three councils are Chucks Golding (Bracknell Forest), James Gore (West Berkshire) and Stuart Brignell (Wokingham). Emma Coles is leading the project for the Public protection partnership. Team Managers are updating Retention and Destruction policies currently in place at the three councils. Process for data management in line with the retention and destruction policy will require management input. Assessing the current forms used by all areas of the PPP need to be reviewing in line with the new legislation, due to the high volume of forms for the service area this will require input from all teams.

Conclusion:

Progress has been made by each of the three councils yet we will not be compliant by the 25th May 2018. There are plans and projects in place across the Public Protection Partnerships to show that we are working towards best practise. Phase 1 has been completed (there have been presentations at West Berks for the staff to raises awareness of GDPR at both a manager and staffing level). The Berkshire GDPR Networking Group and are supporting each other with Phase 2 and Phase 3 to reduce the capacity and financial implications of the project. The risk assessment shown in appendix A shows BFC, James and Stuart are currently updating the risk assessments for West Berks and Wokingham yet the high risk area point 15 is the same across all three councils and is becoming the current main focus point. Training has been provided yet refresher close to the time of implementation will highlight the roles and responsibilities of both the staff and the Management team.

Risk	BFC Action	Wokingham Action	West Berkshire Action
G/M/I Drive – Access and security levels	Implementing Share save. Access to each drive being reviewed	Implementing Information At work. Access to each drive being reviewed	Still Waiting for confirmation

Idox EDRMs / Smart Office- Access and security levels, Data in relation to retention and destruction policy	Retention and destruction policy being reviewed. Module being purchased. Security review of Uniform access being completed.	Retention and destruction policy being reviewed. Looking at cost of module purchase.	Retention and destruction policy being reviewed. Module has been purchased. Security review of Uniform access being completed.
Personal Drives – Data	Are to be removed	Still Waiting for confirmation	Still Waiting for confirmation
Do Managers Know their Roles	More Training Needed - PPP	More Training Needed - PPP	More Training Needed - PPP
Do the team know their roles	More Training Needed - PPP	More Training Needed - PPP	More Training Needed - PPP

Appendix A

GDPR RISK REGISTER 2018

	Potential Risks - Bracknell	Risk Appetite Score			Current Residual Risk Score			Status	Actions to Mitigate Risk	Responsible Officer	Target Date
		Likelihood	Impact	Total	Likelihood	Impact.	Total				
1	Senior officer not made aware of delays and issues with implementation of GDPR due to limited number of IMG meetings before GDPR comes into effect.	2	3	6	2	3	6		Engagement Plan being implemented. IMG meetings scheduled for next few months and additional ad hoc IMG meetings will be arranged if required.	Lawyer (Information. Management & Security)	30/4/18
2	Limited central resources to implement GDPR together with competing for limited officer time in the directorates to undertake tasks to support implementation such as data flow mapping.	2	3	6	3	3	9		IMG will monitor progress. Departmental representatives will feed back to IMG on progress and flag any resourcing issues.	Borough Solicitor/ Lawyer (Information. Management & Security)	30/4/18

3	Policies do not reflect GDPR.	2	3	6		3	3	9		Policies to be updated. Schedule for updating policies being developed. Need to be reviewed across PPP to provide consistent service delivery.	Lawyer (Information. Management & Security) EC	30/4/18
4	Staff in high risk areas are not aware of the introduction of	1	3	3		2	3	6		Engagement Plan to be drawn	Lawyer (Information.	30/4/18

	Potential Risks	Risk Appetite Score			Current Residual Risk Score			Status	Actions to Mitigate Risk	Responsible Officer	Target Date
		Likelihood	Impact	Total	Likelihood	Impact.	Total				
	GPDR and do not understand the consequences for their teams.								up and implemented. Departmental representatives will act as GDPR champions. Presentation to representatives on GDPR at November IMG has flagged to managers in high risk areas. Various other existing communication channels will be used – • Staff newsletter (Forestviews) • Staff intranet • School bursars meetings attendance to provide GDPR update High risk areas for PPP within BFC • G/M/I Drive – Access and security levels • Uniform System - Access and security levels, Data in relation to retention and destruction policy • Idox EDRMs- Access and security levels, Data in relation to retention and destruction policy • F Drives - Data	Management & Security) EC and Team managers	

5	Members are not aware of the introduction of GPDR and do not understand the consequences.	2	3	6		3	3	9		Engagement Plan to be drawn up and implemented which will include briefing sessions for Members. Email on these sessions has been drafted ready for issue to Members. Outcome from briefing sessions to be set out in a bulletin to be	Lawyer (Information. Management & Security)	30/4/18

	Potential Risks	Risk Appetite Score				Current Residual Risk Score			Status	Actions to Mitigate Risk	Responsible Officer	Target Date
		Likelihood	Impact	Total		Likelihood	Impact.	Total				
										issued to all Members		
6	Residents and the general public are not aware the changes affecting them under GDPR.	2	3	6		3	3	9		To be included in the Town and Country newsletter. Lawyer (Information. Management & Security to liaise with Comms Team on getting this into the next publication.	Lawyer (Information. Management & Security)	30/4/18
7	Lack of current awareness of data transfer risks due to limited knowledge on what data transfers are taking place and who with.	2	3	6		3	3	9		Lawyer (Information. Management & Security to liaise with Departments to communicate the need for data flow mapping to be completed by Departments and to provide guidance on what this should entail. .	Lawyer (Information. Management & Security) DMTs	30/4/18
8	Council processes out of standard office hours, at weekends and over bank holiday periods are not sufficiently robust to ensure we will meet the 72 hour deadline for reporting reportable incidents to the ICO. NB no reportable incidents have occurred to date and likelihood score reflects this	2	3	6		3	3	9		Policy will be updated. Support in the event of the Lawyer (Information Management & Security) being on leave to be considered. Lawyer (Information Management & Security) to work with Emergency Duty Officers , ICT and Forestcare to identify appropriate processes and controls.	Lawyer (Information. Management & Security)	30/4/18

	Potential Risks	Risk Appetite Score			Current Residual Risk Score			Status	Actions to Mitigate Risk	Responsible Officer	Target Date
		Likelihood	Impact	Total	Likelihood	Impact.	Total				
9	Failure to put in place arrangements to respond to subject access requests within the reduced 28 days deadline to avoid financial penalty. NB the number of such requests is low and likelihood score reflects this	2	3	6	3	3	9		Subject Access Request procedure to be updated. PPP process needs to be reviewed	Lawyer (Information. Management & Security) ?	30/4/18
10	Failure to put in place arrangements to seek explicit consent	2	3	6	2	3	6		Discussions to be held with departments. Legitimate activity/intent means consent is not required.	Lawyer (Information. Management & Security)	30/4/18
11	Current legislation/ mandatory retention periods the various Councils Teams not being adhered to and lack of clarity about how to process deletion requests may result in breach of the GDPRs “right to be forgotten” requirement.	2	3	6	3	3	9		National guidance to be referred to when it is issued. IAR to be updated All retention and destructions policies need to be reviewed and updated	Lawyer (Information. Management & Security) EC to send out all managers to amend	30/4/18
12	Failure to put in place adequate procedures and processes.to obtain parental or guardian consent for data collected on children under the age of 13.	2	3	6	3	3	9		To monitor national guidance which will clarify the age limit in the UK to assess if this is relevant to local authorities given this is legitimate activity.	Lawyer (Information. Management & Security)	30/4/18
13	Children may not understand the Privacy Notice.	2	3	6	3	3	9		The Privacy Notice will be written in a language for children to understand	Lawyer (Information. Management & Security)	30/4/18
14	Inaccuracies are not addressed as subject access	2	3	6	3	3	9		The SAR process to be reviewed.	Lawyer (Information.	30/4/18

	Potential Risks	Risk Appetite Score			Current Residual Risk Score			Status	Actions to Mitigate Risk	Responsible Officer	Target Date
		Likelihood	Impact	Total	Likelihood	Impact.	Total				
	requests for amendments to data are not processed in all departments. N.B. low number of subject access requests and likelihood score reflects this								Introduction of a central list to inform staff who to contact. IAR may be a useful starting place for this. E-form for online requests to be drafted. The e-form to be received into a single point at the Council to be logged and appropriately disseminated	Management & Security)	
15	Data Privacy impact assessments not completed for historic or smaller systems or where a contract waiver has been obtained and the need for a pia is not addressed through a procurement plan.	2	3	6	4	3	12		To ask departments whether DPIAs are in place. Departments to ensure DPIAs are completed where missing.	Lawyer (Information. Management & Security) DMTs	30/4/18
16	Individuals not made aware of breaches and how this might affect them.	2	3	3	3	3	9		A procedure to be implemented. PPP need a written policy of how this will be dealt with	Lawyer (Information. Management & Security ?	30/4/18
17	Loss of officer time through inefficient manual processes to redact information for subject access requests	3	3	9	3	3	9		Redaction software to be investigated to determine whether it could assist staff. Being actioned	Lawyer (Information. Management & Security AS	30/4/18
18	Failure to identify where biometric data is collected to ensure GDPR requirements are met.	2	3	6	3	3	9		Attendance at school bursar meeting next term to update them on GDPR. Biometric data (fingerprint recognition) is possibly being used currently in	Lawyer (Information. Management & Security)	30/4/18

	Potential Risks	Risk Appetite Score				Current Residual Risk Score			Status	Actions
		Likelihood	Impact	Total		Likelihood	Impact.	Total		
										schoo

Appendix B

The key elements of the GDPR

Personal data

The GDPR applies to personal data. This is any information that can directly or indirectly identify a natural person, and can be in any format.

The Regulation places much stronger controls on the processing of special categories of personal data. The inclusion of genetic and biometric data is new.

Personal data	Special categories of personal data
Name	Race
Address	Religion
Email address	Political opinions
Photo	Trade union membership
IP address	Sexual orientation
Location data	Health information
Online behaviour (cookies)	Biometric data
Profiling and analytics data	Genetic data

Wider scope

The GDPR applies to all EU organisations – whether commercial business, charity or public authority – that collect, store or process the personal data of individuals residing in the EU, even if they're not EU citizens.

Organisations based outside the EU that offer goods or services to EU residents, monitor their behaviour or process their personal data will be subject to the GDPR.

Service providers (data processors) that process data on behalf of an organisation come under the remit of the GDPR and will have specific compliance obligations. An example might be a company that processes your payroll or a Cloud provider that offers data storage.

Data protection principles

Personal data must be processed according to the six data protection principles:

- Processed lawfully, fairly and transparently.
- Collected only for specific legitimate purposes.
- Adequate, relevant and limited to what is necessary.
- Must be accurate and kept up to date.
- Stored only as long as is necessary.
- Ensure appropriate security, integrity and confidentiality.

Accountability and governance

You must be able to demonstrate compliance with the GDPR:

- The establishment of a governance structure with roles and responsibilities.
- Keeping a detailed record of all data processing operations.
- The documentation of data protection policies and procedures.
- Data protection impact assessments (DPIAs) for high-risk processing operations.
- Implementing appropriate measures to secure personal data.
- Staff training and awareness.
- Where necessary, appoint a data protection officer.

Data protection by design and by default

There is a requirement to build effective data protection practices and safeguards from the very beginning of all processing:

- Data protection must be considered at the design stage of any new process, system or technology.
- A DPIA is an integral part of privacy by design.
- The default collection mode must be to gather only the personal data that is necessary for a specific purpose.

Lawful processing

You must identify and document the lawful basis for any processing of personal data. The lawful bases are:

- Direct consent from the individual;
- The necessity to perform a contract;
- Protecting the vital interests of the individual;
- The legal obligations of the organisation;
- Necessity for the public interest; and
- The legitimate interests of the organisation.

Valid consent

There are stricter rules for obtaining consent:

- Consent must be freely given, specific, informed and unambiguous.
- A request for consent must be intelligible and in clear, plain language.
- Silence, pre-ticked boxes and inactivity will no longer suffice as consent.
- Consent can be withdrawn at any time.
- Consent for online services from a child under 13 is only valid with parental authorisation.

- Organisations must be able to evidence consent.

Privacy rights of individuals

Individuals' rights are enhanced and extended in a number of important areas:

- The right of access to personal data through subject access requests.
- The right to correct inaccurate personal data.
- The right in certain cases to have personal data erased.
- The right to object.
- The right to move personal data from one service provider to another (data portability).

Transparency and privacy notices

Organisations must be clear and transparent about how personal data is going to be processed, by whom and why.

- Privacy notices must be provided in a concise, transparent and easily accessible form, using clear and plain language.

Data security and breach reporting

Personal data needs to be secured against unauthorised processing and against accidental loss, destruction or damage.

- Data breaches must be reported to the data protection authority within 72 hours of discovery.
- Individuals impacted should be told where there exists a high risk to their rights and freedoms, e.g. identity theft, personal safety.

Data protection officer (DPO)

The appointment of a DPO is mandatory for the council

A DPO has set tasks:

- Inform and advise the organisation of its obligations.
- Monitor compliance, including awareness raising, staff training and audits.
- Cooperate with data protection authorities and act as a contact point.