University of East Anglia

ISC15D032

Title:	**Data protection briefing - GDPR**
Author:	Raymond Scott (ISD)
Date:	5 May 2016
Circulation:	ISSC 14 June 2016
Agenda:	ISC15A003
Version:	Draft v0.1
Status:	Open

Issue
On 14 April 2016, the EU Parliament approved the General Data Protection Regulation (GDPR) after four years of discussion, debate and drafting. This new legislation is considered to be a considerable advance on the protection of personal data and respect for privacy. It accounts for and has been drafted in the context of multi-national global corporations operating without borders across the internet. In the UK, it will replace the Data Protection Act 1998 (DPA) and will take effect within 2 years, i.e. by May 2018.

The GDPR places new legal requirements on data controllers such as UEA, and we need to start now to plan for the transition to compliance with the new regime.

Most significantly, under GDPR, the regulator (ICO) is given the ability to fine up to 20M EUR or 4% of global turnover for breaches (whichever is higher). This is a 30 fold increase on the current provision, and a significant escalation of risk to the organisation due to non-compliance with the legislation.

In particular, it is crucial that the next stage of the IT Security project which aims to address the protection of personal data is fully supported.

Recommendation
Recipients are invited:

- To consider the report.
- To discuss the points raised, and determine a response for action.

Resource Implications
Work to migrate to the new legislative regime will need to be undertaken within ISD and every other department handling personal data. ISD will lead on this piece of work.

Equality and Diversity
The impact on groups with protected characteristics are assessed when a new service is introduced or an existing service is changed.

Timing of decisions
Some timescales are already set within the legislation, further dates are still to be determined by the UK Government and the ICO.

- 14 April 2016 GDPR approved by EU Parliament
- 5 May 2016 GDPR published in the EU Official Journal
- 20 days after publication the GDPR came into force (25 May 2016)
- Each member state of the EU is required to adopt the GDPR within 2 years of its date of entry into force (i.e. by 25 May 2018)

At some point, the UK Government will decide on what exceptions and derogations to apply to the legislation (the regulation allows for a certain amount of localisation), and also it will repeal the DPA at the same time that the GDPR is adopted.

Further Information

- Raymond Scott (ISD), x3561, r.scott@uea.ac.uk

Background

The Data Protection Act 1998 is due to be replaced by new EU legislation – General Data Protection Regulation. We must now plan our transition to the new legislation to put in place all the changes required for compliance with the new legislation.

Discussion

General data protection regulation – 2016/679

On 5 May 2016 the GDPR was published in the EU Official Journal as "Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC". (In the UK, Directive 95/46/EC was implemented as the Data Protection Act 1998.)

The new legislation runs to 99 separate articles (rules, akin to sections of an Act) supported by 173 recitals (explanatory notes). The **Appendix** to this document highlights a selection of areas for comment.

Many of the core principles of the DPA are retained in the GDPR, but the new legislation represents a shift in focus from data controllers to data subjects with a number of enhanced rights for data subjects. The GDPR is expected to be more onerous on data controllers than the DPA with the need to demonstrate compliance with the GDPR; conduct privacy impact assessments; maintain record of processing activities, manage technical and organisation measures, and maintain strict control over processors.

12 steps as recommended by the ICO

In the UK, the supervisory authority is the Information Commissioner's Office (ICO), and they are leading on providing guidance on the implementation of the legislation. The ICO recommends the following 12 steps as a starting point[1]:

1. **Awareness**. Ensure decision makers are aware of the new legislation and the likely impact this will have on the organisation.
2. **Information audit**. We must understand what personal data we hold – where we got it from and who we share it with.
3. **Privacy notices**. Notices tell individuals what data we are collecting and what we will do with it. These must be reviewed and updated.
4. **Individual rights**. While rights given to individuals under DPA are preserved, the GDPR adds further rights. We must ensure we have processes in place to support their being exercised.
5. **Subject access requests**. The GDPR requires these to be handled slightly differently, and reduces the time available for responses. Processes will need to be reviewed and updated.
6. **Legal justification for processing**. The GDPR requires us to have a clear legal basis for the processing of personal data (as discovered under point 2 above). This will need to be documented.
7. **Consent**. The GDPR is more explicit over how we may gain consent for processing and allow individuals to withdraw it. Where the justification for processing is consent, they will need to meet the new rules.
8. **Children**. New rule apply to the processing of the personal data of children.
9. **Data breaches**. Breaches will now need to be reported to the ICO. We will need to review our breach handling process and bring it into line with the GDPR.
10. **Data protection by design**. All changes and projects around the processing of personal data must complete privacy impact assessments as part of the planning of the work.
11. **Data protection officers**. We must appoint a DPO who will take responsibility for data protection. We will need to decide where the role sits in the organisation and its governance arrangements.

[1] https://ico.org.uk/media/for-organisations/documents/1624219/preparing-for-the-gdpr-12-steps.pdf

12. **International operations**. Where we have international operations, we will need to determine which supervisory authority we come under.

Version of GDPR implemented in the UK

The GDPR allows member states some flexibility in the implementation of around 50 of the articles in the legislation. The UK Government has indicated that it intends to use this flexibility to the maximum to the benefit of data controllers[2]. The degree of flexibility applied may be challenged by the European Data Protection Board who will be monitoring the consistency of the implementation of the GDPR across the EU. While a version of the GDPR has now been approved by the EU parliament, the version we will follow in the UK is still to be determined[3]. (It was noted that the Queen's speech of 18 May 2016 which laid out the Government's legislative programme for the coming year did not refer to any changes to data protection[4].)
Our intention is to follow the lead from the UK regulator – the ICO – with a particular focus on the advice they provide for action.

Implications of UK exit from the EU

Should the UK choose to leave the EU, the general view is that while this may in the short term create some confusion, the GDPR will still apply to UK organisations. Many organisations, including UEA, will still be processing the personal data of EU citizens, and the GDPR has been designed to apply to processors outside the EU.
The ICO has also recently commented[5] on the implications of Brexit for data protection. Amberhawk (information law training organisation) has similarly commented[6].

Recommendations

The following high level approach to implementing the GDPR is recommended:

- Monitor ICO published guidance and follow their lead on implementation of the new legislation[7][8]
- Train SPC staff in GDPR
- Draw together a task force to develop a plan and oversee the implementation of GDPR[9]
- Build a complete network of data protection contacts covering every department in the University. SPC staff will work with this group to effect all other actions
- Working with the network of data protection contacts, undertake a discovery exercise to gain a fuller understanding of data processing activities within the University
- Work with the IT security project to ensure that identified personal data is secured to appropriate standards (possibly defined by the ICO)
- Review and update processes, agreements, notices, guidance, user training, and policies in the light of the new legislation and the ICO guidance

References

- ICO data protection reform blog - https://ico.org.uk/for-organisations/data-protection-reform/

---

[2] http://amberhawk.typepad.com/amberhawk/2016/01/data-protection-regulation-update-precise-implementation-depends-on-exceptions-and-recitals.html

[3] http://amberhawk.typepad.com/amberhawk/2016/05/will-the-uks-approach-to-the-gdpr-be-harmonised.html

[4] https://www.gov.uk/government/speeches/queens-speech-2016

[5] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/04/statement-on-the-implications-of-brexit-for-data-protection/

[6] http://amberhawk.typepad.com/amberhawk/2016/02/leave-or-stay-in-the-referendum-gdpr-has-to-be-implemented-by-the-uk-whatever-the-result.html

[7] Priority areas for new guidance are: data portability, high risk data processing, data protection impact assessments, certifications, and data protection officers.

[8] https://ico.org.uk/for-organisations/data-protection-reform/guidance-what-to-expect-and-when/

[9] Outlaw (Pinsent Masons) recommend the task force draws from across the business "IT and HR teams, legal and compliance officers and a senior manager with links into the board". http://www.out-law.com/en/articles/2016/may/data-protection-reforms-to-apply-from-25-may-2018/

- GDPR Regulation (EU) 2016/679 text (PDF) - http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN
- European Commission data protection reform blog - http://ec.europa.eu/justice/data-protection/reform/index_en.htm
- YouTube video by Jan Albrecht MEP on EU's new privacy law - https://www.youtube.com/watch?v=PVaVIOJniSQ

Appendix - Features of the GDPR compared with DPA

The following table describes some areas of current activity within DPA compliance, compares that with the GDPR and comments on current preparedness for the transition, and what actions would be required. Please note that only a selection of areas are being highlighted at this point, and it is possible when implemented in the UK, further adjustments may be made to the legislation.

Area	DPA (current)	GDPR (future)	Actions
Consent	Sched 2 & 3 s.1 of the DPA defines consent as one the means by which data may be processed fairly. The ICO has provided guidance on best practice for the way consent may be collected	Consent is more clearly defined. Art. 7 describes the conditions for consent. It must be clear and unambiguous for each purpose. We must keep records of consent received (so we can demonstrate we have received it). Data subjects must be able to withdraw consent at any time and as easily as it was to give it	Review all processing arrangements which are dependent on receipt of consent and ensure they are compliant with Art. 7. New mechanisms for withdrawal may need to be developed
Data breach notification	There is no requirement to inform the ICO or data subjects, but considered to be good practice. Failure to do so may have a bearing on the size of any fine levied. SPC keeps records of all data breaches brought to its attention (whether or not the ICO are informed)	There is a requirement to inform both the ICO and affected data subjects for breaches which are 'likely to result in a high risk to the rights and freedoms of natural persons' Art. 33(1). The ICO must be informed within 72 hours. Art. 33(5) requires the data controller to keep records of breaches, so that the ICO can verify compliance with Art. 33	Review and update breach notification process
Data portability	No provision	New right for data subject to be provided with their personal data in a portable format (Art. 20)	Monitor advice from ICO. Develop new process. Potentially impacts every information system processing personal data
Data processing agreements	There is a legal requirement in the DPA for data processing arrangements to be described in a written contract (Sched 1, Part II, s.12)	Art. 28 details more precisely exactly what must be specified in the contract between the data controller and processor. Processors also have	Review data processing agreements. Ensure all processing by third parties is covered by a written contract to the standard of Art. 28. Indemnity should reflect the increased risk to the

Area	DPA (current)	GDPR (future)	Actions
		liability under GDPR and can be fined for breaches of articles (Art. 83)	organisation, and an expectation that processors have taken out insurance
Data protection officer (DPO)	No requirement to have dedicated staff assigned to managing data protection. At UEA, there are two Information Policy and Compliance Managers within the SPC team in ISD	Arts. 37-9 define the new requirements for DPOs. It is expected that UEA will be required to appoint a DPO. The DPO shall have expert knowledge of data protection law and practices, and must report directly to the 'highest management level of the controller'	DPO will require specialist training and an update to professional qualifications
Fines	The ICO can fine up to £500K for breaches of the legislation. Most fines have related to breaches of the 7th data protection principle	Art. 83 defines two tiers of fines for infringements of different articles. The ICO will be able to fine up to: (a) 20M EUR or 4% of global turnover, e.g failure to respond to SAR or act on request under 'right to be forgotten' (b) 10M EUR or 2% of global turnover, e.g. failure to carry out PIAs Fines can be imposed on data controllers and data processors	Conduct risk assessment and raise awareness of the consequences of failure to meet requirements of GDPR
Policy	The University has a DPA policy which details how the DPA is to be implemented	Local policy will still be required	The DPA policy will need to be reviewed and updated to reflect the requirements of GDPR
Privacy impact assessments (PIA)	Not required, but good practice. Code of practice published by ICO. SPC guidance on UEA website	Required under Art. 35	Communication with all those affected. Ensure PIA is embedded into all project and change management processes

Area	DPA (current)	GDPR (future)	Actions
Privacy notices	We must inform data subjects of the processing of their data we will undertake and the purposes for that processing. ICO publishes a code of practice for privacy notices	Art. 13 details much more precisely how data subjects should be informed about the processing of their personal data (at the time their data are obtained)	Review privacy notices. Ensure all processing is covered by notices and notices are written to GDPR standards. Follow updated guidance from the ICO
Records of processing	The description of processing is supplied to the ICO as part of our registration as a data controller	Art. 30 requires the University to keep detailed records of processing activities. This includes details of recipients of data, transfers, time limits for erasure and security measures. The GDPR presents a shift towards accountability and the need for the University to prove its compliance with the regulation	Follow ICO guidance. Develop a fuller record of all processing activities across the University. This points to the need to conduct a data protection audit
Right to rectification	Principle 4 requires the data controller to ensure that the data are accurate and up to date	Art. 16 gives data subjects the right to have inaccuracies corrected and the completion of incomplete data	Monitor advice from ICO. Develop a new process. Potentially impacts every information system processing personal data
Right to be forgotten	No direct provision, but continued processing of personal data must be justified	New right for data subject to have their personal data erased without undue delay and we must take reasonable steps to tell others. There are some provisions under which data can be retained (Art. 17)	Monitor advice from ICO. Develop a new process. Potentially impacts every information system processing personal data
Security of personal data	The 7th data protection principles requires 'appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data'. Most fines issued by the ICO relate to breaches of this particular principle	Art. 32 defines the security of processing. It explicitly addresses all aspects of security: confidentiality, integrity and availability. We are expected to regularly test our measures to ensure security of processing. Compliance with the article can be demonstrated by adherence to an approved code of conduct or certification scheme	Personal data held by the University must be identified and secured to a set standard (at least UEA IT security policies). The IT security project will work closely with the implementation of GDPR. We will monitor guidance from the ICO for indications of favoured certification schemes

Area	DPA (current)	GDPR (future)	Actions
Subject access rights	Data subject have right of access to their personal data held by the University. Response must be provided within 40 days. We may (and do) charge £10 admin fee	Right of access preserved, but a response must be provided within a month (Art. 12). Complex requests can be extended by a further 2 months. Extra information must be provided in addition to the requester's personal data. No fee may be charged (unless the request is manifestly unfounded or excessive)	Review and update SAR process. There is a need for the University to reduce the amount of material held about individuals – particularly that held in mailboxes
Training (end user)	The University DPA policy requires all staff handling personal data to have completed DPA training. We have two online courses, scheduled face to face course, and the option for bespoke face to face courses for specific groups	Art. 39 specifies the tasks of the DPO, one of which is 'awareness-raising and training of staff involved in processing operations'. The ICO routinely require organisations to mandate DPA training in undertakings issued following data breaches or examples of poor practice	All training courses will need to be reviewed and updated to reflect the requirements of GDPR