DATA PROTECTION AND GDPR OPPORTUNITIES AND CHALLENGES

By Dr Elizabeth Lomas

DEVELOPED FROM AN IRMS LONDON PARTICPATORY WORKSHOP HOSTED BY UCL, 7 JULY 2016.

Dr Elizabeth Lomas is a fellow of the IRMS and Senior Lecturer in Information Governance at UCL. Email: e.lomas@ucl.ac.uk

1.0 CONTEXT

On 7 July 2016 UCL hosted an IRMS London participatory event to consider the challenges and opportunities for information and records management professionals in the light of the provisions of the General Data Protection Regulation (GDPR). The event was run by Dr Elizabeth Lomas, Professor Elizabeth Shepherd and Katharine Stevenson. All of the IRMS London participants contributed in a personal capacity. In addition, Susan Healy (an ARA member) attended and contributed in a personal capacity. 23 people participated. Together the participants brainstormed the issues and mapped out the opportunities and threats. This newspiece provides a write up of the discussion, mapping and the resulting recommendations from the mapping which are provided for further consideration.

2.0 DISCUSSION ON THE GDPR AND THE IMPLICATIONS OF THE BREXIT

The group discussed the implications of Brexit. The GDPR as a regulation does not require any further domestic legislation in order for it to come into force within EU Member States. The Regulation will be active from May 2018. Given that the UK's departure from the EU is likely to take two years from the point at which Article 50 is triggered this means that in effect the GDPR will come into force by default ahead of the UK's departure from the EU. However, were the UK to decide that strategically it wanted to depart from the GDPR it could negotiate on this point and it is unlikely that there would be resistance from the EU officials. It was noted that derogations do require legislation.

Clearly in order to manage EU Member States' data moving forwards, which is important for trading purposes, the UK does need to be able to prove that it can sufficiently manage that data in line with the GDPR. We discussed, the fact that the UK could have two forms of the legislation – GDPR full for EU data and 'GDPR lite' to leverage advantages with other markets, e.g. USA. However the group concluded that this solution would be complicated and might potentially weaken the UK's position as DP/GDPR is the de facto standard for managing personal data.

DCMS are the lead Government Department for Data Protection policy. The National Archives reports in to DCMS. Cabinet Office has a vested interest in this decision as it holds Government's records management policy responsibility. BIS will be involved in shaping business agendas. The ICO initially issued a statement confirming that GDPR 'adequacy' will be required. On the release of the Commissioner's Annual Report on 1 July 2016 a stronger recommendation for compliance with the GDPR was reported.

3.0 HIGHLIGHTS OF THE GDPR REQUIREMENTS

Key highlights of the GDRP were noted as:

- ☐ Revised DP principles
- ☐ Design of systems to minimize DP risks
- ☐ DP documentation of processes
- ☐ Greater emphasis on Privacy Impact Assessments
- ☐ Fair processing notices
- ☐ A great emphasis on subject consent to processing
- ☐ An emphasis on providing retention schedule information in fair processing notices
- ☐ Provision of processes to manage the 'Right to be forgotten' (NB This excludes personal data being processed 'for archiving purposes in the public interest', the scope of which is yet to be clarified).
- ☐ No charges for subject access requests
- ☐ Requirements to report DP breaches
- ☐ Much larger fines as penalties
- ☐ Accredited courses for DP Officers
- ☐ A requirement for some organisations (based on sector, scale and personal data volume/sensitivities) to have a Data Protection Officer with 'expert knowledge' who will sit in protected positions with the expectation that they will oversee DP but act as whistle-blowers in the event that an organisation fails to comply or take appropriate DP actions. This person can be an external consultant.

4.0 A MAPPING OF SOME OF THE OPPORTUNITIES AND THREATS

A **STEEPLE** model was utilised to map the opportunities and threats.

S- Socio-cultural

Opportunity: To link to stakeholders and provide clearer information on processing. This provides an opportunity for IRM to present more clearly to the public the role and value of IRM practitioners. We may learn from the LIS community which is more public facing. LIS tools such as information literacy may be beneficial. (Solution to have an IRM Manifesto. See the CILIP work on fair processing for copyright at http://www.cilip.org.uk/advocacy-campaigns-awards/advocacy-campaigns/copyright/london-manifesto).

Opportunity: To have a clearer, stronger mandate to better manage information.

Opportunity and threat: Organisational and wider stakeholder demands present opportunities for engagement but expectations need to be clearly managed to ensure they are realistic and appropriate.

Opportunity and threat: Need to have titles which distinguish whistle-blowers from business as usual professionals or people may be reluctant to go IRM for day-to-day assistance.

Threat: Lack of support for whistle-blowers (Solution: provide Union level support but consider how this would mean RM professionals are perceived).

Threat: Nature of consent and social contract (Solution: provide more advice and support tools)

T- Technological (which encompasses the research domain)
Opportunity: The requirement to develop privacy by design (i.e. from the point of system creation) presents opportunities for collaboration (with IT, law and information security) and improved IRM links to resources. However these systems needs to be flexible and accessible in new and exciting ways.

Opportunity and threat: Risk management resides at the heart of GDPR which is complicated. Whilst some processes can be automated IRM must set policies and processes but it needs to be clear where manual/human intervention is required.

Opportunity and Threat: To develop research in order to gather a better evidence base for this domain. IRM should look to the work undertaken in the copyright sector.

Threat and opportunity: right to be forgotten presents challenges in terms of how technically feasible it is to remove individual records where they reside within audited systems. This is an opportunity for the field of research to work to better resolve the challenge this will present.

Threat: E-discovery failures resulting in failures to locate personal data with sufficient accuracy.

Threat: Will linked data work carry on when it relates to the potential identification of individuals?

E - Economic

Opportunity: Whilst GDPR is about personal data, the implications for trade and economic policy underpin the rationale for its development and use to share information across international boundaries in understood safe ways. IRM needs to continue to be part of the trading agenda.

Opportunity: In the light of the need for DP experts the IRMS and ARA can work on clearer salary structures to recognise the expertise required.

Opportunity: FOI focused IRM on public sector. GDPR straddles public and private sector.

Opportunity and Threat: Large fines are a threat but they may assist IRM to leverage appropriate resources to properly deliver IRM objectives.

Threat – No notification requirements or charges are regulated for and this currently forms a significant funding stream for the ICO. The ICO has already identified this threat and the UK can still make this a requirement.

Threat – There can be no charge for data protection subject access requests in UK. The charge is of no real economic significance in terms of covering access charge costs. However it is significant in ensuring that requestors stop and consider the consequences of their request. Whilst charging should not be a barrier to access there is a concern about the number of requests which will now be received. This could be looked at in the UK context.

E - Environmental

Opportunity: The principle, which was rarely seen to be enforced, was that data should be kept no longer than necessary. The GDPR potentially provides a stronger mandate for the

delivery of retention schedules. The need to dispose of information in a timely manner resonates with the green agenda.

P - Political

Opportunity: The UK did obtain some significant derogations which need to be regulated for in any DP system.

Opportunity: ICT is a key part of the UK offering and therefore politicians should take account of this sector.

Opportunity: opportunity to work with and deliver IRM value to key policy makers in ICO, Cabinet Office, DCMS, BIS, TNA and corporate sector.

Opportunity: For information to deliver a truthful picture on what is kept and used relating to individuals. The relationship between organisations and individuals needs to be strengthened in order to rebuild trust.

Threat: The UK no longer has a strong voice within the EU in terms of the further guidance that will now emerge. In addition EU courts will still influence outside EU.

Threat: Politicians understanding of GDPR nuances and value. IRM being heard in a Brexit environment will be challenging.

Threat: Many organisations will have breaches. The PR needs to be managed so IRM are not seen as a negative influences or sources for scapegoating.

L - Legal

Opportunity: to deliver legislation which is public facing and to the benefit of a wide range of stakeholders.

Opportunity and threat: DP experts will be required for certain organisations. These persons will need to have undertaken accredited training. It is important that the courses accredited by IRMS and ARA are acknowledged as having provided training which meets this requirement. Current experts do not want to have to undertake new training.

Opportunity: It is important for IRM to capture the key ground for GDPR thinking and delivery. (Solution: IRM must lead the way on an IRM code of practice or IG code of practice – see also point below)

Opportunity and threat: Lawyers are moving into compliance work but lawyers don't help the delivery of good IRM in practice. It would be possible to have an Information Governance code of practice which was holistic and developed collaboratively but IRM must take the lead on this or it will lose ground. It might be better to have a branded IRM code of practice. (Solution: IRM must lead the way on an IRM code of practice or IG code of practice)

Threat: Common law system does not fit automatically with GDPR.

Threat: Legislation for derogations may not be enacted in time.

Threat: Not all records contain personal data. It is important that retention scheduling does not only focus on personal data. For disposal schedules to be effective they should be holistic. (Solution: Retention schedules linked to fair processing – see points below)

Threat: The status of Category E data (which currently affects public authorities only) is not clarified.

Threat: The requirement for the retention/disposal date to be set at the point of collection under the terms of some fair processing notices may result in legal binding decisions on destruction being set out without proper consultation and sign off from the correct professionals.

E - Ethical

Opportunity: To build frameworks and understanding on the management of information and engage with stakeholders through fair process and consent.

Threat: Problems around the parameters for whistleblowing (Solution: clear guidance on whistleblowing processes and scenarios)

5.0 WORKSHOP CONCLUSIONS

The core recommendations were:

1. The need for IRMS to work with the ARA and other organisations with the same vested interest (e.g. BCS and CILIP) to push the ICO/DCMS for certainty on the route map for GDPR or the alternative compliance as there is potentially less than two years for organisations to be in a position to comply with the legislation.

2. The need to push for legislation to enact derogations if GDPR is to be followed through in the UK.

3. The potential for IRMS and ARA to have a clear IRM Manifesto. See the CILIP work on fair processing for copyright at http://www.cilip.org.uk/advocacy-campaigns-awards/advocacy-campaigns/copyright/london-manifesto). A need for a documentation and action to protect the role of IRM professionals was seen as essential or IRM practitioners could lose out to lawyers. See also point 4.

4. The need for IRMS to work with ARA and other core organisations such as ICO, Cabinet Office and TNA to develop A Records Management Code of Practice or to consider an Information Governance Code of Practice. An Information Governance Code of Practice could be a better route for gaining collaboration across the records management and information security communities. However it was noted that records managers are best placed to deliver the holistic compliance framework engaging people and technology. In addition it might be beneficial to have an IRM Code so that the value of the profession is evident.

5. A need for the current qualifications approved by IRMS and ARA bodies to be recognised as accredited routes for DP expert positions. As experts delivering DP individuals do not want to pay for further training.

6. The need to consider how to support those in whistle-blower positions. It was suggested that the professional societies could acts as unions but others were concerned about how this might alter the perception of the records management profession.

7. The need for professional societies to develop a union level offering to support those in whistle-blower positions.

8. A clear title to denote those in whistleblowing positions and those in ‘business as usual’ roles.

9. A recommended salary structures to ensure appropriate remuneration and recognition for the increase in responsibilities.

10. To develop an evidence base for better decision making within this domain. This needs to include a recommendation to research how individual records can be detached from audited systems to fulfil the requirements that individuals have the right to be forgotten.

In conclusion GDPR presents an opportunity for IRM practitioners to face outwards to stakeholders and provide a positive and responsive service better resourced by senior management. It further provides a rationale for IRM to lead collaborations with the wider information sector and practitioners including IT, lawyers, information security, data scientists and library and information science professionals. There is a need to have clarity on the legislation. The IRM sector provides a pivotal role which should be harnessed to develop and deliver guidance which will be effective in practice.

6.0 FINAL NOTE

This workshop was a brainstorming exercise which provided initial reactions and ideas about the opportunities and threats for IRM practitioners from GDPR. Whilst not all of the recommendations will be taken forward it is clear that there is a need for the IRMS (in conjunction with other key bodies) to initiate action to ensure the continuation of IRM professionals as leaders in the field.