Scottish Universities Legal Network on Europe

Data protection and Privacy in EU law

Written by
Lorna Gillies, University of Strathclyde

Contact: Lorna.Gillies@strath.ac.uk

In your allocated sector:

1. **Please explain the key rights that are protected and are therefore at risk following the UK's exit from the EU?**

   For the purposes of considering how Scotland may continue to protect these rights following an exit from the EU and for exploration of further future devolution of powers in certain areas to Scotland, please explain whether the rights fall within areas devolved to Scotland or currently reserved areas.

   Please also identify, broadly, the main EU and implementing (UK/Scotland) legal sources (and where relevant make reference to other international legal sources for example, the Council of Europe).

Data Protection: A Fundamental Right

As a first and guiding principle, the protection of data is enshrined in the Charter of Fundamental Rights (hereafter the Charter). This "third generation" (EU Commission) Freedom is contained in Article 8.

In the context of EU law, the Charter applies between the institutions and bodies of the EU and is applied by the national authorities in implementing EU law. Where the Charter does not apply, reference to the equivalent protection is contained in national constitutions or constitutional traditions (EU Commission). Whether or not EU law continues to apply directly in the field of data protection, the constitutional traditions and respect for human rights throughout the UK should ensure data protection is recognised as a fundamental right. The timing of the Article 50 procedure may give some indication as to the UK's compliance with the new Data Protection regime, which is due to apply across the EU Member States by 24 May 2018.

Article 8(1) of the Charter provides that everyone has the right to the protection of personal data concerning the individual. Article 8(2) provides that such data must be processed fairly for the specified purpose and on the basis of consent of the person concerned or some other legitimate basis laid down by law. In addition, Article 8(2) also provides that everyone with the right of access to data also has a right to have that data rectified. Article 8(3) requires compliance to be subject to control by an independent authority.

Data: An Evolving Concept

Data protection is concerned with the control, use, authentication and protection of information relating to the identified or identifiable person. As Casagran recently confirmed, "Data protection is a rather new issue due to the astounding computer science and technology of the latter half of the twentieth primarily prevents data from being misused or lost by private and public entities." (Casagran, 2017, Recital 6 EU 2016/679)

The EU has, through a number of Directives and a Regulation, established common EU rules to ensure that personal data enjoys a high standard of protection everywhere in the EU.[1] Individuals have the right to complain and obtain redress if their data is misused anywhere within the EU. The main piece of current legislation is Directive 95/46/EC (the EU's Data Protection Directive) which was implemented in the UK by the Data Protection Act 1998. The Data Protection Directive sets up a regulatory framework which seeks to strike a balance between a high level of protection for the privacy of individuals and the free movement of personal data within the EU. To do so, the Directive (and the Data Protection Act therefore) sets strict limits on the collection and use of personal data and demands that each Member State set up an independent national body responsible for the supervision of any activity linked to the processing of personal data. The Data Protection Directive also foresees specific rules for the transfer of personal data outside the EU. Amendments to the Data Protection Directive have led to the introduction, in the UK, of the Privacy and Electronic Communications ("EC Directive") Regulations 2003 which contain provisions that govern (among other things) direct marketing by email and/or when using Short Message Services ("SMS" or "text messages"). Finally, yhe Privacy and Electronic Communications (EC Directive) Amendment Regulations 2011 obliges organisations using cookies (which includes equivalent technologies) only to place cookies on the machines of users who have given their consent. There has also been a large amount of case law of the Court of Justice of the European Union (CJEU) in relation to data protection which has had a significant impact on the protection of individual data, including the extent to which data can be sent outside of the EU and whether individuals have a 'right to be forgotten' online.[2]

The EU Commission has acknowledged that due to the combination of "rapid technological developments and globalisation" the existing rules were not fit for purpose and necessitated reform. A new General Data Protection Regulation EU 2016/679 published in the Official Journal OJ L119/1 (4 May 2016) and entered into force on 25 May 2016. Member States have two years in which to

[1] An overview can be found here: http://ec.europa.eu/justice/data-protection/law/index_en.htm.
[2] An overview of the cases can be found here: https://ec.europa.eu/anti-fraud/sites/antifraud/files/caselaw_2001_2015_en.pdf.

ensure compliance with the Regulation. It will come into force on 25 May 2018. The Regulation replaces Directive 95/46/EC and reforms data protection rules in the European Union, introducing several key changes directly applicable to all Member States from 25 May 2018. Key principles of the new Regulation are contained in Article 5, 6 and 7. Key points of the new Regulation include the following. Where appropriate a brief comment on the post-Brexit position is suggested.

(i) The first principle is Article 8 of the Charter of Fundamental Rights.

(ii) Processing should be "lawful, fair, transparent" (Article 5(1)(a)). These principles should underpin legislation which may have to replace Regulation EU 2016/679.

(iii) External reach of Regulation (Article 50). Extension to Data Processors and Data Controllers outside the EU who provide goods, services or monitor behaviour through profiling data of EU subjects. In the event of the UK's withdrawal from the EU, a comparable approach should be taken, for from the opposite perspective the processing of personal data of subjects who are in the Union by a controller or processor not established in the Union (for example possible future UK position) should, according to Recitals 23 and 24, be subject to Regulation EU 2016/679 irrespective of whether the commercial activities require payment or where the monitoring of behaviour takes place in the Union.

(iv) Introduction of more stringent status for Data Processors to maintain records; designate a Data Protection Officer and inform Data Controller of any breach. This requirement ought to be maintained in the event of the UK's withdrawal.

(v) Introduction of a Data Protection Officer where processing is carried out by a public authority; where core activities consist of processing which, by its nature, scope or purpose, require regular and systematic monitoring of data subjects or where processing on a large scale of special categories of data. Again, this ought to be maintained in the event of the UK's withdrawal from EU Membership.

(vi) Data Controllers' role developed. Introduction of more stringent compliance requirements of Data Controllers to (a) maintain documents (b) conduct impact assessments vis. higher risk data (c) introduce data protection by design. Data controllers must provide data subjects with transparent information. Processing of data must continue to be fair, provided in a comprehensive manner and enable data subjects to exercise their rights and inform data subjects how long data will be stored. Given UK and international businesses are seeking to actively plan and comply with this new Regulation by the time it comes into force, this too ought to be maintained in any future UK legislation.

(vii) Consent and Fair Processing, Articles 6 and 7. Consent to processing data must be freely given: must be explicit for sensitive data, withdrawal of consent must be easy; data subject can object to data being used for direct marketing; parental consent for children to receive information society services will be reduced from 16 to 13 years. The reduction in age requirement raises questions of minimum harmonisation occur, in essence a race to the bottom should be avoided where users are attracted to the jurisdiction with the lowest age limit for children to access information society services.

(viii) Data Breach and the Data Controller: breaches must be notified to the Data Protection Authority and data subjects without undue delay / within 72 hours unless the breach does not risk the rights and freedoms of individuals; proceedings may be brought in local jurisdiction facilitated by a 'one stop shop' through introduction of lead and concerned authority (Article 60 on cooperation). Withdrawal from the EU Membership could prevent UK data subjects from accessing the One Stop Shop mechanism.

(ix) Introduction of the concept of data protection by design (Article 25) to overcome the ability of commercial entitles to monitor data subjects by requiring technical and organisational measures to ensure appropriate safeguarding of data.

(x) Rectification principles: Articles 16 and 17 provide for the right of rectification and the right to be forgotten (following on from C-131/12 *Google Spain SL and Google Inc. v AEPD and Gonzalez*, 13 May 2014, Grand Chamber). Both principles should continue if the UK were to withdraw from the EU.

(xi) Fines; criteria for determining extent of fines included in Regulation; scope for imposing Euros 20 million or 4% of annual worldwide turnover or if a specified infringement Euros 10 million or 2% of annual worldwide turnover. Withdrawal from EU Membership would require review of these remedies, again to ensure a race to the bottom does not occur.

(xii) Introduction of a new Independent European Data Protection Board (Article 68); this Board will replace the previous Article 29 Working Party and will report directly to the EU Commission. Withdrawal from EU Membership would exclude the UK from contributing to valuable opinions and guidance on the new Regulation through representation from the national supervisory authority.

Regulation EU 2016/679, Recital 27 confirms that it does not extend to deceased persons. Given new technologies and increasing concerns as to digital identities and the transmission of data of deceased persons in social media platforms (Harbinja in Mangan and Gillies, eds, 2017), the

regulation of data protection vis-à-vis deceased persons and new media platforms could be investigated by the UK for the benefit of bereaved families.

2. Please explain as clearly as possible the impact these rights have; what are the public benefits of these rights? Give specific examples where possible.

The EU's data protection rules have had a major impact on individuals and enterprises in the UK. The Data Protection Act 1998 establishes rules which regulate the processing of personal data and, in particular, nformation that is processed automatically (i.e. computer-based records); information recorded on paper; health records and certain public authority records. Enterprises have an obligation to comply with the rules of the Act and individuals have rights to protection of their data.

4 What are the reasonably anticipated developments in this area of rights? (At the EU and / or Council of Europe).

How might this be found out and explored further (contacts in Brussels/Strasbourg?)

From Data Protection to 'Data By Design': Scope, Rationale and Transition of Regime

The regulatory framework for Data Protection is, for the time being, contained in Directive 95/46 EC, the Data Protection Directive. However this instrument is short lived and will cease to have effect from 25 May 2018 (Article 94 Regulation EU 2016/679) when Regulation 2016/679 will come into effect. Whilst the specific date for triggering Article 50 EU is not yet known, it is likely that the UK will have to ensure compliance with the terms of the new EU Regulation by 25 May 2018. In the event of a subsequent complete withdrawal from the EU and the repeal of the European Communities Act 1972, the Regulation would cease to have direct effect in the UK. In order that the UK is responsive to the continuing technological challenges for data protection, it would be pragmatic, facilitate a coherent, robust and equivalent approach and be cost-effective to maintain the new regime set up by Regulation EU 2016/679. In addition, Brexit and withdrawal of the UK from the EU does not mean that the EU's data protection rules will cease to have effect and the Information Commissioner's Office released a statement saying in the wake of the referendum stating: 'If the UK wants to trade with the single market on equal terms we would have to prove "adequacy" – in other words UK data protection standards would have to be equivalent to the EU's General Data Protection Regulation framework starting in 2018.'

5 What is the sectoral potential for Scotland to progress/lead in this area of social protection/rights? Practically, how might it do so? (For example what kind of engagement could Scotland pursue with supra-national and international treaty bodies or organisations?)

You may wish to consider: a) current devolved position;

b) with further devolution of powers (explaining which powers would need to be devolved to enable Scotland to be a leader);

c) as an independent nation.

In the UK, data protection is a reserved matter which leaves little room for Scotland to progress/lead in this area at present.However, the Law Society of Scotland has recently suggested to the Smith Commission that data protection should be a devolved matter: (http://www.lawscot.org.uk/media/387968/smith-commission-october-2014-final.pdf).

Irrespective of the recent Referendum vote in favour of the UK to withdraw its Membership of the EU, there are key opportunities for policy development and wider challenges to the future direction of data protection regulation. These opportunities must address matters of individual and commercial data security, privacy, technological change, the protection of consumers and employees, whilst maintaining respect for protection of data protection as a fundamental right. These challenges are briefly outlined as follows:

Security and Criminal Law: Murray (2013) identified identity theft and identity fraud the core challenges of data protection. National security is excluded from the scope of Regulation EU 2016/679: Recital 16

Interface with Privacy: social media platforms provide greater scope for connectivity, but may result in breach of privacy, personality, “misapplication, mishandling or misprocessing of data” (Murray 2013, 486), bringing into question the rights and interests of the parties affected and the balance offered in data protection.

Technological convergence: this concept is concerned with the ability of businesses to transfer of data across different media platforms for different commercial or personal reasons. Commercial use may entail price comparison websites for various sectors and utility services and retail store cards, loyalty cards, memberships. Private use of communication/network platforms is excluded from the Regulation Article 2(2)(c).

Interaction with EU Consumer Protection and the Digital Single Market Agenda: There are corresponding challenges to the protection of the personal data of consumers. Consumer protection remains a matter of shared competence between the EU and the Member States, therefore on withdrawal of the UK's Membership of the EU it is anticipated that existing EU consumer protection measures would be adopted into existing UK legislation which would in turn require replacement of the Consumer Rights Act 2014 (in the event the relevant Directive ceased to have effect) or its amendment.

Questions regarding the compatibility of the existing and future EU regime for data protection with fundamental rights will persist. Future responses to the access to, sharing and storing of information must be to uphold the protection of personal data as a fundamental right, whether this is framed in the context of the Charter of Fundamental Rights, the UK Human Rights Act or some other instrument.