SCC.441 Information System Security Management

# GDPR: What will it mean for you?

—as presented to the University of Lancaster—

Ben Goldsworthy, 32098584
MSc Cyber Security

April 28, 2018

# 1 Introduction

The EU's General Data Protection Regulation (GDPR) (a.k.a. Regulation (EU) 2016/679) comes into effect on May 25th of next year. Much has been written about this unprecedentedly pro-consumer data protection legislation, not least of all regarding its applicability (or perhaps not) to a post-Brexit Britain. As an institution that caters to large numbers of EU and non-EU citizens each year, the University of Lancaster is in a potentially particularly difficult position. In this report, I shall briefly outline the history behind the GDPR before detailing the areas most applicable to the University. These technical, organisational and legal implications will, to the best of my ability, be considered with an eye to Britain's leaving of the European Union on March 29th 2019, just under a year after GDPR comes into effect.

# 2 The University of Lancaster

The University of Lancaster (henceforth 'Lancaster University') describes itself as "[...]an internationally highly-ranked leader in the provision of inspiring teaching and research" (Lancaster University 2015*b*). It regularly achieves highly in various league tables, and currently has around 9,000 undergraduates and 3,500 postgraduates (HESA 2017). Roughly 30–40% of first-year postgraduate students are UK domiciled, whilst the same is only true for first-year undergraduate students aged 18 or under; past that, the percentage ranges from 20.2% to as low at 5.9%.

Lancaster University also has a range of partner institutions across the globe, with whom it reciprocally exchanges students for years abroad. The University also has a collection of foreign institutions with which it has International Teaching Partnerships, "[...]where Lancaster University degrees are delivered with local institutions in countries including India and Malaysia" (Lancaster University 2015*a*). This also includes a branch campus based in Ghana.

# 3 The Road to the GDPR

One could certainly make the case that something like the GDPR has been a long time coming. Article 8(1) of the Council of Europe (CoE)'s European Convention on Human Rights (ECHR), signed over half a century ago, plainly states that "[e]veryone has the right to respect for his private and family life, his home and his correspondence" (Council of Europe 1950). This was followed by the Organisation for Economic Co-operation and Development (OECD)—a global, not just European, body—publishing their own guidelines a few decades later (Organisation for Economic Co-operation and Development 1980). The OECD's recommendations outlined seven principles, which were the largely self-explanatory

1. Collection Limitation Principle;

2. the Data Quality Principle;
3. the Purpose Specification Principle;
4. the Use Limitation Principle;
5. the Security Safeguards Principle;
6. the Openness Principle;
7. the Individual Participation Principle; and
8. the Accountability Principle.

Despite the CoE's own convention regarding automatic processing of personal data being signed a year later (Council of Europe 1981), adherence to the OECD's non-binding guidelines was spotty at best. In order to consolidate the disparate individual implementations across its member bodies, the European Union (EU) produced the Data Protection Directive (DPD) (European Union 1995). This spurred on the UK Parliament to incorporate the ECHR into UK law in the Human Rights Act 1998 (H.M. Parliament 1998*b*), and the Article 8 elements specifically in the Data Protection Act 1998 (H.M. Parliament 1998*a*). The data world has clearly changed since 1998. Myspace was five years away from launching then; now, Facebook takes in almost $30bn annualy. SINTEF (2013) report that 90% of all the data every created was done so over the last two years. Thus, in 2016, the General Data Protection Regulation (GDPR) was signed off, to come into effect just over two years later.
To summarise:

- The EU's GDPR replaces the UK government's Data Protection Act, and supercedes the EU's earlier DPD;
- which unified the various attempts to adhere to the OECD's guidlines, including a CoE convention;
- which, in turn, were an attempt to provide guidance for compliance to Article 8 of the CoE's ECHR.

However, two months after the GDPR was signed, Britain voted to leave the European Union. Article 50 was invoked on March 29th 2017, meaning that (barring an agreed-upon extension to negotiations) Britain shall cease to be an EU member on March 30th 2019. This means that, for just under a year, the Data Protection Act 1998 will be replaced with the GDPR. After that time, what happens next is unclear. However, government attitudes appear promising, as will be covered later in this report.

# 4 Implications of the GDPR prior to the UK leaving the EU

Unavoidably, Lancaster University shall be subject to the GDPR for at least 10 months. This is independent of whether it is later included for incorporation into UK law with the passage of the European Union (Withdrawal) Bill, or forms part of some future trade deal between the newly-independent UK and the EU. Prior to March 2019 we shall continue to be in Rome and must, as it were, do as the Romans do. Crucially, the GDPR is a *regulation*, where the DPD was only a *directive*—the latter requires enabling legislation to be passed by each national government (e.g. the Data Protection Act 1998), whilst the former becomes immediately applicable upon effect. What might all this mean to Lancaster University?

Luckily, a lot of groundwork will have already been laid in order to comply with the Data Protection Act 1998. Lancaster University (2016*b*) details the University's Data Protection Statement, much of which shall still be applicable under the GDPR. Minor amendments, such as the removal of the subject access fee (currently £10) and shortening of the response period (currently 40 days, soon to become one month), should be easily implemented. The primary changes relate to how consent to process data is gained, as well as the accountability of the institution in its processing.

In the former case, the foregrounding of the data subject's right to withdraw consent may make its mere granting a less desirable basis for lawful data collection, due to the impact on the sort of long-term processing that a university may be expected to perform. Thankfully, consent of the data subject is only one of a number of possible bases to collect data. Article 6(1)(b) allows for lawful processing in instances where "[...]processing is necessary for the performance of a contract to which the data subject is party[...]", such as a student's contract of study with the University.

In the latter case, expect an increase in paperwork. A Data Protection Officer (DPO) shall have to be designated and their details passed onto the Information Commissioner's Office (ICO). Article 37(5) states that the DPO must posess "[...]expert knowledge of data protection law and practices[...]". Whether an existing member of staff will be able to take on this role, or a new member of staff be required from outside of the University in order to achieve such knowledge, is a question for the University.

Additionally, Article 25 calls for "[...]data protection by design and by default[...]", requiring that "[t]he controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed." It shall be vital to perform an audit of all current Lancaster University forms and web pages in order to ensure that they comply with this—for example, prechecked checkboxes are now forbidden as an indicator of data subject consent, which must now be active rather than passive.

Article 30 covers the new requirement that "[e]ach controller [...] shall maintain

a record of processing activities under its responsibility[...]". This is liable to be the source of the greatest volume of paperwork going forward, as it obligates the University to keep a written record, on all of the data it holds, of such aspects as "[...]the purposes of the processing[...]", "[...]the envisaged time limits for erasure[...]" and so on.

The most arduous requirement of the GDPR, and guaranteed to be the cause of many a headache going forward, is that it applies retroactively. This gives the University a little over half a year to recontact everybody it holds data on in order to confirm their continued GDPR-compliant consent, or otherwise make a case for lawful retention under one of the other Article 6(1) provisions. Brazier (2017) points out that GDPR compliance requires also "[...]looking through physical records, including drawers full of business cards, to make sure you're not holding 'expired' data acquired without consent." As a small respite, however, the Regulation explicitly states that it "[...]does not apply to the personal data of deceased persons."

Finally, the most numerical change between the old and the new Regulations is clearly fines. Whereas the maximum fine possible under the Data Protection Act 1998 was £500,000, the GDPR allows for fines of up to €20 million or 4% of annual turnover (whichever is higher). With a reported 2016 budget of £255.5 million (Lancaster University 2016*a*), that is not-insignificant fee which must be borne in mind when looking over the predicted costs of compliance.

## 4.1 Post-Brexit

How much, then, will the UK's iminent divorce from the EU affect what has been said prior? Luckily, the answer looks to be very little. The UK Government appears committed to implementing most, if not all, of the provisions of the GDPR in UK law (Department for Digital, Culture, Media & Sport 2017). Indeed, Department for Exiting the European Union (2017) suggests a cognisance of the need to continue the free flow of data post-Brexit. It is hoped that by subsuming EU standards into our own legislation, the UK's data protection standards will be considered adequate to allow the continuing of the free flow of data that we currently enjoy as a member state. Frustratingly, only time will tell if this is the case. If not, the UK may be required to negotiate our own equivalent of the EU–US Privacy Shield agreements. This, however, is delving too far into the hypothetical for the scope of this report. Indeed, even if the GDPR were to be completely discarded upon the UK's exit of the EU, it would still be in the University's best interest to continue to comply—the GDPR applies to the handling of EU citizens' data, regardless of the location of the handler or the citizen, which would mean the University was still beholden to the rules for as long as it continued to admit EU citizens for study.

# 5 Conclusion

The GDPR cannot be ignored. Compliance, which appears to be inescapable, will require not-insubstantial amounts of effort and capital. In particular, the re-acquisition of consent from still-living data subjects for the continued storage and processing of all their historic data may prove an especially onerous requirement for an institution such as Lancaster University. However, it has been a 6-decade-long road to reach the GDPR and many processes previously implemented in order to comply with the Data Protection Act 1998 can be retained with minimial, or no, tweaking. Further aiding matters, there seems to be a consensus amongst all concerned parties that it is in everyone's best interest to adopt GDPR (or GDPR-like legistion) in the UK, Brexit or no Brexit. Assuming this remains the case, it should massively simplify the compliance process and minimise wasted effort come March 2019. Further guidance on the GDPR can be found in Information Commissioner's Office (2017) and, as McCall (2016) suggests, "[y]ou might want to sit down with your Data Protection Officer or equivalent sooner rather than later to work through an appropriate action plan.'

# References


Brazier, R. (2017), 'Gdpr and events: What europe's new laws mean for data collection at events'.
**URL:** *https://www.rapiergroup.com/news/gdpr-events/*

Council of Europe (1950), 'Protocol to the convention for the protection of human rights and fundamental freedoms (european convention on human rights) as amended by protocol no. 11'.
**URL:** *https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/005*

Council of Europe (1981), 'Convention for the protection of individuals with regard to automatic processing of personal data'.
**URL:** *https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108*

Department for Digital, Culture, Media & Sport (2017), *Government to strengthen UK data protection law.*
**URL:** *https://www.gov.uk/government/news/government-to-strengthen-uk-data-protection-law*

Department for Exiting the European Union (2017), *The exchange and protection of personal data - a future partnership paper.*

European Union (1995), 'Directive 95/46/ec of the european parliament and of the council of 24 october 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data'.

HESA (2017), 'Students in higher education 2015/16'.
**URL:** *https://www.hesa.ac.uk/data-and-analysis/publications/students-2015-16*

H.M. Parliament (1998*a*), 'Data protection act 1998'.
**URL:** *http://www.legislation.gov.uk/ukpga/1998/29*

H.M. Parliament (1998*b*), 'Human rights act 1998'.
**URL:** *http://www.legislation.gov.uk/ukpga/1998/42*

Information Commissioner's Office (2017), 'Overview of the general data protection regulation (gdpr)'.
**URL:** *https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/*

Lancaster University (2015*a*), 'International teaching partnerships'.
**URL:** *http://www.lancaster.ac.uk/study/international-students/international-teaching-partnerships/*

Lancaster University (2015*b*), 'Our campus'.
**URL:** *http://www.lancaster.ac.uk/about-us/theuniversity/*

Lancaster University (2016*a*), *Lancaster University Financial Statements 2016*, Lancaster University.
**URL:** *http://www.lancaster.ac.uk/media/lancaster-university/content-assets/documents/annual-review/2016-Lancaster-University-Annual-Accounts.pdf*

Lancaster University (2016*b*), 'Lancaster university's data protection statement'.
**URL:** *https://gap.lancs.ac.uk/dataprotection/Pages/default.aspx*

McCall, R. (2016), 'The €20 million question: Will you be ready for the general data protection regulation?'.
**URL:** *https://ahua.ac.uk/general-data-protection-regulation/*

Organisation for Economic Co-operation and Development (1980), *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*.

SINTEF (2013), 'Big data, for better or worse: 90% of world's data generated over last two years'.
**URL:** *www.sciencedaily.com/releases/2013/05/130522085217.htm*