SCOTTISH ARCHIVES 2018 Volume 24

Viewpoint

The General Data Protection Regulation (GDPR)[1]

Fred Saunderson

Europe's data protection law changed in May 2018, a revision to which many would have struggled to remain oblivious. The acronym 'GDPR' became nearly ubiquitous. Particularly in early 2018, one could scarcely avoid urgent requests from businesses, organisations and charities to 'confirm their contact preferences' or 'opt in' to continue communications. On the day the law changed, 25 May 2018, European internet users found some non-European-based websites, including the *Los Angeles Times* and *Chicago Tribune* elected to suspend access to IP addresses within countries covered by the GDPR for fear of non-compliance.[2] The possible business risks of the new legislation were well-touted, especially in relation to monetary penalties. Leaders and consumers alike were widely informed of the possible scale and severity of non-compliance fines under the GDPR, which could be up to the higher of €20 million or 4 per cent of a firm's global annual turnover.[3] It was quickly reported on 'GDPR day' that complaints lodged against Google, Facebook and Facebook-owned WhatsApp and Instagram under the new law could lead to total fines of $9.3 billion.[4]

It is true that the GDPR is a substantial piece of legislation with a global impact. It affects multinational corporations, small businesses, charities, public services and individuals. Given this scale, it shouldn't be surprising that its implementation garnered headlines and widespread attention. However, while this legislation certainly relates to and impacts records and archives, there are pragmatic ways to approach the legislation. It need not be as vast and, perhaps, intimidating as at first it may feel.

This article sets out some of the basic concepts of the legislation, provides context in terms of the GDPR in the UK and highlights some of the steps that my organisation, the National Library of Scotland, has taken in response to

1 The content of this article is provided as general guidance only and is not legal advice. If you require legal advice on data protection you should contact a legal advisor.

2 http://www.theguardian.com/technology/2018/may/25/gdpr-us-based-news-websites-eu-internet-users-la-times.

3 Regulation (EU) 2016/679, Article 83.

4 http://www.cnet.com/news/gdpr-google-and-facebook-face-up-to-9-3-billion-in-fines-on-first-day-of-new-privacy-law/.

the changes to set up a 'gradual approach' to ensuring responsible handling of personal data when users access our collections. This article will illustrate that, far from needing to be an intimidating creator of compliance-based tasks, Europe's revised data protection law can be considered as a proportionate, perhaps even supportive, framework. The clearest approach is to break matters down to the fundamentals.

Regulation (EU) 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, or the 'General Data Protection Regulation' (GDPR), to give it its full name, is a substantial piece of European Union (EU) legislation. The GDPR is a Regulation, a form of EU legislation that applies directly in all Member States.[5] This contrasts with an EU Directive, which is a form of legislation that applies in a Member State once that state has 'transposed' it by laying its own legislation. Directives allow states more scope for interpreting and applying EU legislation, while Regulations lead to greater consistency of law across all Member States, because the original text of the Regulation *is* the law in each Member State.

While this particular Regulation is 'new', legislation on data protection is not. As many practitioners are likely to be aware, immediately preceding the GDPR, EU Member States had significant data protection laws. The legislative basis for these is referenced at the end of the GDPR's full title – Directive 95/46/EC. That 1995 'Data Protection Directive'[6] was the preceding bedrock for EU law on the protection of personal data. The 1995 Directive was transposed into UK law by the Data Protection Act 1998, which was our core data protection legislation until May 2018.

In short, the GDPR has not invented data protection. However, it has had two major effects. First, it has substantially updated and revised European data protection law. Second, it has increased the harmonisation of data protection law within (and, to a degree, outwith) Europe.

The basics of the GDPR are comparatively straightforward. In summary, the law says that one may only 'process' (which, effectively, means collect, use, share, or store) personal data (information about an identifiable living person) if the processing meets certain safeguards and criteria,[7] which are set out in six principles:

[5] http://ec.europa.eu/info/law/law-making-process/types-eu-law_en#types-of-eu-legal-acts.

[6] 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.

[7] The GDPR applies to most, but not all, forms of processing. Crucially, the Regulation only applies to 'processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system' (Article 2(1)). The UK's

1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Data minimisation
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality[8]

A further principle – accountability – mandates that the 'controller' (the person or organisation that determines the purposes and means of the processing in the particular situation) is responsible for, and must be able to demonstrate compliance with, these principles.

From here, the GDPR expands, clarifies and caveats these basics through a total of 99 Articles. When first seeking to understand the GDPR and Europe's current laws on data protection, it is helpful and beneficial to dwell on the fundamentals before considering the subsequent details. The legislation is *about* the principles. It is *about* providing the structures to ensure that the use of personal information is reasonable, logical and safe. The details are important, but a pre-emptive or simplified focus on the specifics is not, in my experience, the most logical path towards understanding the rationale and *raison d'être* of the GDPR, to ensuring effective and sustainable compliance, nor (most of all) to ensuring the spirit of the law is met and personal data is properly managed. The GDPR does not, for example, require consent before anyone may use personal data.[9] Equally, the legislation is not simply about keeping personal data confidential or private.[10]

Although the GDPR is a Regulation, so directly applicable in the UK, it does not sit in isolation. The legislation only goes part way toward the objective of a harmonised European law of data protection. This is because the Regulation permits Member States to 'derogate' from the original text in a number of places. States are permitted to create supplementary legislation that expands on or alters the GDPR. The UK has derogated to some considerable extent, through the Data Protection Act 2018. Unlike the 1998 Act, the 2018 Act is

Data Protection Act 2018 takes a variety of approaches to applying forms of the GDPR to other processing activities. Notably for archives, Chapter 3 and Schedule 6 to the 2018 Act develop the 'applied GDPR', which inter alia applies to 'manual unstructured processing' of personal data by any organisation subject to freedom of information laws. Accordingly, there are some differences in law when processing is of manual unstructured personal data. This article focuses on processing within the scope of the GDPR only.

8 Regulation (EU) 2016/679, Article 5.

9 Anecdotally, this may be a common misconception about the GDPR. As addressed in this article, 'consent' is one of the possible 'lawful bases' for processing personal data in accordance with the first part of the first principle (lawful processing). There are other possible lawful bases available, including operating under a public task or under a contract.

10 These may be elements of the seventh data protection principle, but the legislation is framed around how one may safely and responsibly use personal data, not around how one should keep personal data confidential.

not our primary data protection legislation. The 2018 Act sits alongside the GDPR, it does not replace it.[11] The 2018 Act has a number of functions, not all of which will be directly relevant to archival professionals or users (for example, the Act effectively 'recreates' the GDPR in different forms for certain processing activities beyond the scope of EU law, such as processing by intelligence services or the police). Other elements of the 2018 Act are directly pivotal to archives, so warrant further exploration.

Chapter IX of the GDPR contains various 'provisions relating to specific processing situations'. Two of the Articles in this Chapter – Article 89 on processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, and Article 85 on freedom of expression and information – are particularly relevant for archiving practices. These Articles permit Member States to derogate in order to protect and enable responsible processing of personal data in relation to these activities and subjects. The UK has primarily derogated for Article 89 in Schedule 2, Part 6 of the 2018 Act and for Article 85 in Schedule 2, Part 5 of the Act. These derogations do not exempt or exclude archiving activities from the scope of data protection legislation, but they do take substantive steps towards ensuring that responsible archiving or use of information for purposes including research, statistics, journalism and academia are not unduly inhibited by the legislation.

Section 19 of the 2018 Act makes a more wide-ranging refinement to the GDPR as it applies to archiving and research. This section sets out what constitutes the relevant safeguards in respect of processing of personal data for archiving in the public interest and for research and statistical purposes. These safeguards are applicable both in relation to the derogations noted above, and to the data protection principles as these apply to archiving, research and statistics.

Two of the principles – purpose limitation and storage limitation – contain direct references to processing for archiving in the public interest and for research and statistical purposes. The language permits that further processing and extended retention of personal data will not be contrary to the GDPR if done for the purposes of archiving in the public interest, research or statistics, provided such activities are carried out in line with the safeguards. Under section 19 of the UK's 2018 Act,[12] these safeguards are:

[11] NB This article has been written in the context of the UK as a Member State of the EU. At the time of writing, all indications are that the substance of the GDPR will remain the law of the UK after the UK leaves the EU. Considering the precise ways in which the legislation may be changed as a result of, or at the time of, Brexit is beyond the scope of this article, and at the time of writing remains subject to potential change, depending on the outcome of the UK's exit negotiations with the EU. The UK Government has published advice on data protection and Brexit at http://www.gov.uk/guidance/using-personal-data-after-brexit.

[12] Data Protection Act 2018, c. 12, s. 19.

1. That the processing must not be likely to cause substantial damage or substantial distress to an individual
2. That the processing must not be carried out for the purposes of measures or decisions with respect to a particular individual (except in the case of certain forms of medical research)

From the perspective of an archive professional, contributor, or user, these safeguards should be considered as fundamental as the core data protection principles. Broadly, if you start with consideration of the need to ensure these safeguards are met, your interactions with the data protection legislation in respect of archiving and research activities will be comparatively rational and pragmatic, and your ability to undertake responsible archiving or research will be significantly more likely to succeed in a lawful and compliant, as well as effective, manner.

In purposefully simple and high-level terms, in the principles, derogations, and safeguards, the GDPR and the UK's 2018 Act effectively help to ensure that:

1. Personal data can only be processed in limited, responsible and secure ways
2. Processing of personal data for the purposes of archiving in the public interest, research or statistics is likely to be suitable and acceptable within these restrictions, so long as the safeguards are met

With these fundamentals in mind, it's worth concluding with an exploration of some of the work that the National Library of Scotland (NLS) has undertaken over the last year in relation to its collections and personal data therein. As stated, the GDPR didn't introduce data protection, or even the notion of data protection principles. The current principles are largely the same as those that existed under the 1995 Directive[13] and the UK's 1998 Act.[14] Instead, the 2018 changes have refined and revised the law, and placed (deserved) new focus on how personal data are processed and managed. These factors were instrumental in leading the Library to re-examine aspects of its approaches to personal data and use of the collections in 2018.

The NLS is one of Europe's major research libraries and Scotland's only legal deposit library. The legal deposit right to collect a copy of works published in print and, since 2013, in non-print (for example, electronic and online) formats has naturally led to significant holdings of published works. In addition, since 1683 the NLS and its predecessor, the Advocates' Library, has collected manuscript and archival collections.[15] These continue to form a core element of the Library's holdings, which today cumulatively number in excess of 24 million physical items.[16] The Library has long collected and provided access

[13] Directive 95/46/EC, Article 6.
[14] Data Protection Act 1998, c. 29, s. 1.
[15] http://www.nls.uk/collections/manuscripts.
[16] http://www.nls.uk/about-us/what-we-are.

to books, manuscripts, films, sound recordings and other formats that contain personal data.

In October 2018 the Library published fresh guidance for users in relation to personal data held in the collections.[17] This guidance was issued in tandem with a change in approach to how access to personal data in the collections is managed. These developments were informed by, and rooted in, the changes made earlier in 2018 to data protection law.

The most substantive aspect of the change was to harmonise approaches to managing user access to personal data. Previously, the Library's focus was on unpublished collections, on the logic that personal data contained therein was not, or was unlikely to be, in the public domain. This was a rational approach but, in the context of the more expansive GDPR, one worthy of reconsideration. Using the opportunity of the GDPR to re-examine data protection fundamentals and principles, together with the new legislative specifics around archiving and research, we found it evident that the Library should be broader in its approach. Published materials also contain personal data, of course. Published personal data is also subject to the legislation.

Taking this broader consideration does not mean personal data in the collections cannot be collected, retained and, in most cases, made available (as has been discussed above), but it does mean the Library needed to provide greater and clearer advice and support to users about the personal data implications of accessing and using all of the contemporary collections. As of October 2018, the Library provides consistent data protection advice to users in all reading and access spaces, not just where unpublished or archival works are accessed, and runs a single data protection and collections procedure for staff across all of these spaces.

The other major factor considered and more clearly elucidated under this review was the Library's express understanding of which party functions as the 'controller' in relation to personal data in the collections. As set out in the Library's guidance, the Library considers itself to be the controller in respect of most personal data in its collections. On occasion, other parties may be controllers (alone, or jointly with the Library), for example when materials are held on loan or deposit. The Library's guidance explains this and, crucially, clarifies that the Library is only the controller *up to the point* at which personal data is accessed from the collections. A user who consults material from the collections and elects to take away or use information that relates to an identifiable living person (whether through notes, copies, or even facts and details simply remembered) becomes the controller of that personal data.[18] The Library does not determine the purpose and means of the processing of such data, the user does.

[17] http://www.nls.uk/guides/using-personal-data.

[18] Again, it is important to caveat that in some cases individual processing in this manner may be outside the scope of the GDPR. If it is outside the scope of the GDPR, it may be within scope of the 2018 Act.

On this logic, it was essential for the Library to provide sufficient and accessible guidance to users about their responsibilities as potential controllers of personal data. The guidance informs users of a number of fundamentals:

1. The principles
2. The 'lawful bases for processing', which are six routes (such as 'consent', 'contract', 'legitimate interests' or 'public task') under which a controller can comply with the first element of the first principle (lawful processing)
3. The 'special categories' of personal data (previously known as 'sensitive personal data'), which are specific forms of personal data, such as data about political opinions or religious beliefs, that are subject to additional protections under the legislation

The guidance provides an overview of certain routes to compliant use of personal data that, from experience, we expect to be the most applicable to users. These routes relate to the personal use of personal data, as well as the derogated uses discussed above, including research and academic purposes. Along with a series of definitions, the guidance concludes with a concise overview of how and why one may seek to undertake anonymisation or pseudonymisation (two facilities given considerable prominence by the legislation) of personal data to support compliance with the safeguards or to meet the criteria of certain principles, such as integrity and confidentiality.

When registering as a Library user, individuals agree to the Library's terms and conditions. These were updated in 2018 to more clearly iterate that users have data protection responsibilities in relation to their own use of personal data. These revised terms and conditions form the basis of the Library's 'gradual' approach to ensuring it functions as a responsible controller in respect of enabling access to personal data in the collections.

To round out this 'gradual' approach, the data protection guidance is available in all reading and access spaces, and on the Library's website. Posters are visible in these spaces as well, highlighting user responsibilities and noting the availability of more detailed guidance. Perhaps most importantly, training on the legislation, the Library's approach to managing personal data, and the subject matter of the guidance has been provided to curatorial and access staff. The approach is designed with the purpose of ensuring that any user has due opportunity to understand their potential obligations and to access supportive information.

Supplementary to this passive, consistent provision of information and guidance, the Library takes proactive steps to highlight responsibilities directly to users when we provide access to certain materials. This forms a final 'layer' of the 'gradual' approach. Staff have access to training and procedures to help understand when best to actively highlight data protection rules and responsibilities to collection users, for example when issuing collections that contain large amounts of unpublished personal data. This ensures guidance about acting as a controller is directly communicated, for example in conversation at the point of access or through handing over a copy of

the guidance along with the collection items, in instances where this is most likely to be relevant.

The Library's approach to informing staff and users of the realities of data protection can feel a far cry from the world of $9.3 billion fine scares and website outages, yet the underlying legislation is the same. The GDPR is significant. The Regulation and its UK companion, the 2018 Act, place new (and occasionally tough) requirements on controllers and users of personal data. The legislation is complex. However, the requirements are rooted in what is perhaps a remarkably logical basis and the legislation is structured on overarching principles and fundamentals which are comparatively simple, logical and clear.

Approached rationally, the GDPR and the 2018 Act are perhaps not as intimidating or overwhelming as they may seem at first pass. Indeed, in the experience of the NLS described here, the legislation can even be a helpful and pragmatic opportunity to take stock, reconsider the basics, and adjust practices. These steps should help the Library, the individuals whose data are contained in the collections, and the collection users in equal measure. Ultimately, the legislation is about ensuring personal data is used and managed fairly and safely. Safe and fair management of data is far from alien to archive professionals and users. Once stock is taken of the fundamentals, and then of specifics, some of which, as illustrated here, are directly designed to support responsible archiving and research practice, a logical and pragmatic approach to data protection under the GDPR is certainly achievable.