How I Learned to Stop Worrying and Love the GDPR

By Ariane Adam

This work was developed thanks to a grant from the William and Flora Hewlett Foundation to support the GovLab’s work toward the systematization of responsible private-sector data stewardship in the public interest. For more information, visit DataStewards.net.

The General Data Protection Regulation (GDPR) was approved by the EU Parliament on 14 April 2016 and came into force on 25 May 2018. It is designed to protect and empower all EU citizens’ data privacy and to reshape the way data controllers across the region approach data protection. The GDPR not only applies to organisations located within the EU but also to those located outside if they offer goods or services to, or monitor the behaviour of, EU data subjects. It applies to all companies processing and holding the personal data of data subjects residing in the EU, regardless of the company’s location. In the UK, the GDPR has been incorporated into domestic law by the Data Protection Act 2018, which received royal assent on 23 May 2018. This means it will apply in the UK regardless of the outcome of the Brexit negotiations. Organisations can be fined up to 4% of annual global turnover or €20 million, whichever is higher, for serious infringements, e.g. violations of the basic principles for processing, including conditions for consent; and up to 2% of the annual global turnover or €10 million, whichever higher, for infringements of the organisation’s obligations, e.g. failure to notify the supervising authority and data subject about a breach or not conducting an impact assessment.

The coming into force of this important regulation has created confusion and concern about penalties, particularly in the private sector. In the UK, it has been reported that the Information Commissioner’s Office (ICO) received 6,281 complaints between 25 May and 3 July 2018, a 160% rise on the same period in 2017; this has worried many businesses. Some of the US’ biggest newspapers have taken the view that blocking half a billion people from accessing their products is easier than complying with the GDPR – the Los Angeles Times, the Chicago Tribune and The New York Daily News became unavailable to readers in most EU countries on 25 May 2018 stating: ‘Unfortunately, our website is currently unavailable in most European countries.’ They remained unavailable until at least September 2018.

There is also apprehension about how the GDPR will affect the opening and sharing of valuable databases. At a time when open data is increasingly shaping the choices we make, from finding the fastest route home to choosing the best medical or education provider, misinformation about data protection principles leads to concerns that ‘privacy’ will be used
as a smokescreen to not publish important information. Allaying the concerns of private organisations and businesses in this area is particularly important as often the datasets that most matter, and that could have the most impact if they were open, do not belong to governments.

Looking at the regulation and its effects about a year on, this paper advances a positive case for the GDPR and aims to demonstrate that a proper understanding of its underlying principles can not only assist in promoting consumer confidence and therefore business growth, but also enable organisations to safely open and share important and valuable datasets.

Why is data protection important?
The right to privacy is a precondition to, and guarantor of, other human rights; it enables individuals to independently develop and express thoughts and ideas, to choose which, if any, religion to worship and which political party to support. It has become one of the most important human rights issues in the modern era due to the increasing sophistication of information technology, which has enhanced the capacity of public bodies and private enterprises to collect, analyse and disseminate information on individuals. As recognised by the European Court of Human Rights in the case of *S and Marper v UK*, the protection of personal data is of fundamental importance to a person’s enjoyment of his or her right to privacy.iii It is recognised that the right to protection against the collection and use of personal data forms part of the right to respect for private and family life guaranteed by international and regional human rights instruments.

The right to privacy is closely linked with self-identification and personal identity issues. The UN Human Rights Committee (HRC) has defined privacy as ‘a sphere of a person’s life in which he or she can freely express his or her identity’iv and has made it clear that the right to privacy encompasses the right to protection against arbitrary or unlawful interferences and unlawful attacks whether they emanate from State authorities or from natural or legal persons.v Privacy however is not an absolute right; international and regional human rights instruments guaranteeing the right to privacy state that it can be interfered with where such interference is provided for by law and is reasonable in the particular circumstances. The HRC has interpreted the concept of reasonableness to indicate that ‘any interference with privacy must be proportional to the end sought and be necessary in the circumstances of any given case.’vi

Importantly, privacy is a right of fundamental importance to the public, as the reaction to the recent Cambridge Analytica and Facebook scandal has demonstrated.vii The loss of
public confidence in an organisation’s management of data feeds directly into reputational damage. Public confidence will also determine whether the public is willing to share data with a private or public organisation; if it thinks that data will be misused or irresponsibly published in the open, then the organisation may ultimately be starved of data. A recent survey conducted by the Open Data Institute on British consumer attitudes to sharing personal data shows that trusting organisations increases the likelihood consumers will share personal data about them. A backlash against open data more widely may hurt companies, especially smaller start-ups whose business model depends on exploiting open datasets.

What does the GDPR actually say?
At first glance the length of the text of the regulation, together with the misinformation that has accompanied its coming into force, leads many to take the view that it has been designed with the primary purpose of complicating organisations’ administrative processes. But, breaking it down to its basic principles demonstrates that compliance should not in fact be that difficult. Although any data management and protection policy will need to address the specific needs and operations of an organisation – and so there is no ‘template’ to guarantee compliance – a good starting point in aligning practices to the GDPR requirements is for organisations to ask two key, simple questions: ‘are we collecting person data for a legitimate purpose?’ and ‘are we managing it in a way that is necessary for that purpose and proportionate to the rights of the data subject?’

Although the GDPR has a wide jurisdictional application, understanding it is facilitated by awareness of its EU law context. Prior to the GDPR, the principal instrument governing data protection in the EU was Directive 95/46/EC of the European Parliament and 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 (Data Protection Directive). It was adopted in 1995, at a time when several EU states had already adopted national data protection laws. Free movement of goods, capital, services and people within the internal market required the free flow of data, which could not be realised unless EU states could rely on a uniform high level of data protection. It was designed to give substance to the principles of the right to privacy (article 8 of the European Convention on Human Rights) and to expand them. The GDPR seeks to protect all EU citizens from privacy and data breaches in an increasingly data-driven world that is vastly different from the time in which the 1995 Directive was established. The key underlying principles of data privacy remain its guiding force, but changes have been introduced to the regulatory policies to address technological advances and protect the exploitation of personal data, which is becoming more and more valuable. As noted in Recitals 6-7 of the GDPR (emphasis added):
Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Natural persons increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life... Those developments require a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance of creating the trust that will allow the digital economy to develop across the internal market. Natural persons should have control of their own personal data. Legal and practical certainty for natural persons, economic operators and public authorities should be enhanced.

The GDPR applies to both controllers – i.e. any person, public authority, agency or other body which determines the purposes and means of the processing of personal data – and processors, i.e. any person, public authority, agency or other body which processes personal data on behalf of the controller. ‘Processing’ includes any operation which is performed on personal data or on sets of personal data, whether or not by automated means; ‘clouds’ are therefore not exempt from GDPR enforcement.

The regulation appropriately defines personal data broadly as ‘any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.’ (emphasis added). Having such a wide definition is key to ensuring comprehensive protection of individuals, especially taking into account that it is becoming increasingly possible to identify a person using less and less data, or to re-identify data that supposedly can no longer be linked to a natural person back to that person (re-identification). The aim of this wide definition is to also cover situations in which the controller itself is not able to identify persons, but a third party to whom the data might be disclosed might be. For example, a controller knows the birth date and the last three post codes of areas where a person lived, together with the dates when the person moved. This does not on its own allow the controller to identify the person. However, other controllers, such a mobile phone operator, could be able to cross-reference the data with their own records to find out who this person is.

The regulation then sets out seven key principles to govern the processing of personal data: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality (security); and accountability. Compliance with the spirit of these principles is a fundamental building block for good data protection practice and promotes public confidence in the collection and sharing of data. What do the principles actually require? ‘Lawfulness, fairness and transparency’ prompts the identification of valid
grounds under the GDPR for collecting and using personal data. Further it ensures that you (i.e. the data controller/processor) do not do anything with the data in breach of any other laws; that you use personal data in a way that is fair, i.e. not in a way that is unduly detrimental, unexpected or misleading to the individuals concerned; and that you are clear, open and honest with people from the start about how they will use their personal data. ‘Purpose limitation’ demands that you are clear about your purposes for processing from the start, that you record these purposes and specify them in your privacy information for individuals, and that you only use personal data for a new purpose if this is compatible with your original purpose, you get consent, or you have a clear basis in law. ‘Data minimisation’ ensures that personal data processed is sufficient to properly fulfil the stated purpose, has a rational link to that purpose, and is not held for longer than is necessary to fulfil that purpose. ‘Accuracy’ simply asks that you take all reasonable steps to ensure personal data held is not incorrect or misleading, while ‘storage limitation’ demands that you do not keep personal data for longer than you need it. Finally, ‘integrity and confidentiality’ ensures that you have appropriate security measures in place to protect the personal data you hold and ‘accountability’ requires you to take responsibility for what you do with personal data and how you comply with the other principles.

So, what is a lawful basis for processing? It cannot be repeated enough that consent is not the only basis. One of the most widely promulgated myths about the GDPR is that organisations/businesses/etc. must have consent if they want to process personal data. There are six available lawful bases for processing and no single basis is ‘better’ or more important than the others – which basis is most appropriate to use will depend on the organisation’s purpose and relationship with the individual. Under article 6 of the GDPR, processing shall be lawful if at least one of the following applies:

1) the individual has given clear consent to the processing of his or her personal data for one or more specific purposes;
2) it is necessary for the performance of a contract an organisation has with an individual, or because the individual has asked them to take specific steps before entering into a contract;
3) it is necessary to comply with a legal obligation, i.e. the processing is necessary for the organisation to comply with the law (not including contractual obligations);
4) it is necessary to protect someone’s life;
5) it is necessary for the performance of a task in the public interest or for official functions, and the task or function has a clear basis in law;
6) it is necessary for the purposes of the legitimate interests pursued by the organisation or the legitimate interests of a third party unless there is a good reason to protect the individual’s personal data which overrides those legitimate interests, in particular where the individual concerned is a child (but, NB that public authorities cannot rely on this basis).

Most lawful bases require that processing is ‘necessary’ – this means that if you can reasonably achieve the same purpose without the processing, you shouldn’t process the data. It reflects
the underlying principle that interference with privacy can only be prima facie justified if it is in accordance with the law, and necessary. The accompanying principles of data minimisation and storage limitation also incorporate the principle of proportionality, i.e. that interference can be justified if it is in accordance with the law, necessary and proportionate.

The GDPR also guarantees a number of rights to individuals related to the principles, namely: the right to be informed about the collection and use of their personal data; the right to access it; to rectify inaccurate personal data or have it completed if incomplete; to have personal data erased or restricted, or to object to processing (which however are not absolute and only apply in certain circumstances); rights in relation to automated decision making and profiling; and the right to data portability. The latter is particularly important in promoting best data management and practice and encouraging individuals to share their personal data. The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. Think of a social network: a user may be dissatisfied with their current provider, but by cancelling their account they would lose all the content they submitted. Data portability fixes this problem. Good practice in this area encourages users to sign up to services knowing the personal datasets they develop are portable. By the same token, it also stimulates competition by making market entry easier for new businesses.

Moreover, the GDPR introduces new obligations that require organisations/companies etc. to integrate data protection concerns into their processing activities and business practices, from the design stage right through the lifecycle. These are referred to as ‘data protection by design and by default’ within the regulation however the underlying concept of data protection by design is not new; under the name ‘privacy by design’ it has existed for many years and been adopted by organisations as a matter of good practice. The two principles can serve to enhance user trust in systems. Some fear that these requirements introduce a significant administrative burden for data controllers. Yet, they are an administrative burden only in the sense that installing double-glazed windows in homes is. It should be seen as an investment: privacy-friendly products can create competitive advantages, just as energy efficient homes are more attractive to buyers. Another associated requirement introduced by the GDPR is documentation, i.e. most organisations are required to maintain a record of their processing activities, covering areas such as processing purposes, data sharing and retention. Information audits or data-mapping exercises represent best practice.
We need to talk about consent

The GDPR sets a high standard for consent – an indication of consent must be unambiguous and involve a clear affirmative action. But it is important to first check if consent is needed or whether another basis, such as ‘legitimate interests’, is more appropriate. It is important to get the basis right before commencing processing; for example, if a company decided to process on the basis of consent and obtained it however this was subsequently withdrawn, the company could not ‘switch’ to legitimate interests to keep processing even if it could have relied on legitimate interests from the start. It should have made it clear to the individual from the beginning that it was processing on the basis of legitimate interests. Leading the individual to believe they had a choice is inherently unfair if that choice will be irrelevant. When the individual withdraws consent therefore the company must therefore stop processing. Consent means offering individuals free choice and control. Genuine consent should put individuals in charge, build trust and engagement, and enhance your reputation. Under the GDPR, consent requires a positive opt-in, which means companies should not use pre-ticked boxes or any other method of default consent. Explicit consent is required for processing sensitive personal data, i.e. data revealing race, sexual orientation, political opinions or religious beliefs, health data, etc. For such data, only a very clear and specific statement of consent will suffice.

Was there a need to ‘refresh’ consent when the GDPR came into force? If you are resident in the EU, your inbox in April and May 2018 is likely to have been filled with messages hoping to persuade you to stay subscribed. The process prompted a slew of complaints and memes on social media. The vast majority of emails were criticised by experts as unnecessary and potentially illegal. Dozens of websites shut down their activities completely, while others forced users to agree to new terms of service. The answer however to this question was ‘not necessarily’. If a company has an existing relationship with customers who have purchased goods or services and had already, before the coming into force of the GDPR obtained consent for processing in an ‘opt-in’ way, it is not necessary to obtain fresh consent. Conversely it may not be lawful to seek fresh consent using contact information a company is unsure about how it collected. The biggest concern is that companies will lose customers by raising their consent obtainment to the GDPR standards. Another view is that they will have better engagement with them and build customer trust.
What is freely given consent? Companies must not make use of services conditional on individuals giving consent; this does not amount to a free choice. On the day of the coming into force of the GDPR, complaints were filed by the European consumer rights organisation Noyb against Facebook, Instagram, WhatsApp and Google’s Android operating systems arguing that the companies have forced users into agreeing to new terms of service. Max Schrems, the chair of Noyb, said: ‘Facebook has even blocked accounts of users who have not given consent. In the end users only had the choice to delete the account or hit the agree button – that’s not a free choice...’ The issue at stake is whether the processing of data for targeted advertising can be argued to be necessary for the social networking/instant messaging service. ‘In our view, these companies sought to tie consent to such (unnecessary) processing purposes and operations in their terms and then asked data subjects to “take it or leave it”,’ Noyb’s spokesman said. ‘Considering the powerful position these companies have and the consequent pressure the data subject is put under, to agree to irrelevant processing/advertising purposes, we believe that any such consent obtained should be considered invalid.’ It will be interesting to see how these complaints are determined; for now, an important lesson for companies is to separate data processing that is necessary for using a service, which can and should be covered by the legal basis of ‘contract’, from additional processing for advertisement or to sell the data on, which is likely to require a user’s free opt-in consent. Keeping privacy in mind when designing products and services will assist in thinking about what lawful bases can and should be used for processing, and when consent is actually required from users and for what.

Is the GDPR a friend or foe to open data?

Open data is free, public data that anyone can access, use and republish. Open data serves two primary objectives: firstly, it promotes good governance and accountability; secondly, it increases access to data to citizens and private organisations, thus promoting economic growth, development and scientific research. Countries’ economies are increasingly driven by data as more action and behaviour takes place online. Data’s value resides in its use and to that end, there has been a move in the last decade or so towards the promotion of open data, which can be used and reused without restriction, either legal or technological. There are other arguments for opening data; for example, data collected by the state is citizens’ data, in an analogous sense to which government money is taxpayer’s money. Governments have a specific duty that goes beyond that of the private sector to facilitate access to data. The focus however of this paper is on private organisations. In the private sector, the network effects of opening data collected by private firms can outweigh the competitive advantage created by keeping the data closed. This is analogous to the ways in which opening documents, such as inventories, onto the world wide web is counterintuitively more valuable than keeping them private, a lesson that some firms took a long time to learn as e-commerce developed.

Open data by definition is ‘not personal’; privacy however is an inevitable concern about opening data particularly in the context of re-identification. There is the possibility that information about individuals could be identified by inference from data in an open dataset augmented by other information in the intruder’s hands, or even information readily available elsewhere. The example given above was of a mobile phone operator, who could be able to
cross-reference the birth date, post codes and moving dates of a person shared by another

data controller to find out who this person is. Another scenario is publication of a dataset

containing reference to individuals’ height, which would not typically be personal data – that

someone is 1.70m is hardly identifying. However, some people are abnormally tall or short,

and so if one possesses further information about, say, who is the tallest person in a population

then it is easy to gather other information about that person from the data. The emerging

concern in the open data movement is that as data protection regulations are tightened by

instruments such as the GDPR, government departments, and more importantly private

organisations, will become more reluctant to publish important and reusable data for fear that

it may inadvertently lead them to breach their obligations vis a vis personal data. However, a

proper understanding and application of the GDPR should actually make it easier for

organisations to safely open and share data.

Firstly, the GDPR contains clear provisions governing the pseudonymising and

anonymising of personal data. The GDPR defines pseudonymisation as ‘...the processing of

personal data in such a manner that the personal data can no longer be attributed to a specific

data subject without the use of additional information, provided that such additional

information is kept separately and is subject to technical and organisational measures to

ensure that the personal data are not attributed to an identified or identifiable natural person’

(article 4(5)). Pseudonymisation may involve replacing names or other identifiers which are

easily attributed to individuals with, for example, a reference number. Whilst you can tie that

reference number back to the individual if you have access to the relevant information,

organisations should put measures in place to ensure that this additional information is held

separately. However, pseudonymisation is effectively only a security measure and the GDPR

makes it clear that pseudonymised personal data remains personal data and therefore within

the scope of the regulation: ‘[p]ersonal data which have undergone pseudonymisation, which

could be attributed to a natural person by the use of additional information should be

considered to be information on an identifiable natural person...’ (Recital 26).

Anonymised data on the other hand is not within the scope of the GDPR (Recital 26).

However, organisations must exercise caution when attempting to anonymise personal data.

In particular, in order to be truly anonymised under the GDPR, personal data must be stripped

of sufficient elements that mean the individual can no longer be identified. If at any point

reasonably available means can be used to re-identify the individuals to which the data refers,

that data will not have been effectively anonymised but will have merely been pseudonymised,

and within the scope of the GDPR despite the organisations bona fide attempts to strip the

data of identifiers. A concern with this is that true anonymisation reduces data below any level

of utility. A way to address this is to ensure that anonymisation is not associated with a ‘release

and forget’ mentality. Sharing and publishing anonymous data requires a stewardship mentality on the part of data controllers.

The UK Anonymisation Network guidance identifies ten steps which enable the data controller to understand, measure and control the risk of anonymised data being compromised: (1) describe the data situation; (2) know your data; (3) understand the use case; (4) understand the legal and governance issues; (5) understand consent and ethical obligations; (6) identify the processes you will need to go through to assess disclosure risk; (7) identify the relevant disclosure control processes; (8) identify stakeholders and plan how to communicate with them in the event of a disclosure; (9) plan what happens after the data is shared; and (10) plan how to react if things go wrong.\textsuperscript{vii} It is incumbent upon an organisation to understand why someone might want the data, what other data could be used to reidentify people, what consent governs that data, and what to do in the event of a data breach. Adherence to the GDPR principles of ‘lawfulness, fairness and transparency,’ and ‘accountability,’ as well as observance of the requirements to document and integrate data protection concerns into their processing activities and business practices from the design stage should facilitate organisations to anonymise and share/publish data in a safe way. A responsible attitude to publishing anonymised data will be taken into account if there is a data breach and will affect the seriousness in which regulators will treat such a breach.

More generally, privacy by design and good documentation assists private organisations in mapping the data they hold and process and therefore facilitate the publication or sharing of their datasets, either as ‘open data’ via responsible anonymisation, or ‘personal data’ when properly recorded lawful bases allow such publication. It also makes it easier for governments and private organisations to converse about datasets held in sectors and to collaborate in opening and/or sharing useful information.

Conclusion

Several jurisdictions around the world are adopting ‘the GDPR approach’ and it is anticipated that this will soon become a de facto global standard for data protection. A proper understanding of its provisions should demonstrate to organisations the commercial benefits of adopting best practice and a ‘privacy by design’ approach. Firstly, such an approach enhances public confidence in the organisation, leading to individuals becoming less apprehensive about sharing their data and therefore increasing the organisation’s data assets. Secondly, good documentation and adherence to the GDPR principles should enable organisations to publish and share data in a risk-reduced way; it is an investment that ultimately leads to commercial and reputational growth. Finally, the GDPR should be seen as a friend to the open data movement, promoting good practice in the creation and storage of
data sets and facilitating discussion about the information held across the public and private sectors, as well as how such information can be made publicly available, usable and reusable.

Ariane Adam, September 2018

Ariane is barrister and human rights consultant experienced in assisting public and private actors develop privacy and data protection policies.

To learn more about the Data Stewards Network, contact datastewards@thegovlab.org.
References


5. General Comment No. 16: The right to respect of privacy, family, home and correspondence, and protection of honour and reputation (Art. 17), adopted 4 August 1988, para. 1.


13. See https://noyb.eu


15. Ibid.
