simprints
every person counts

The Case for Better Privacy Standards

Why development organisations should comply with the key aspects of the EU data protection regime

Global development organisations are increasingly turning to digital tools to track individual beneficiaries and monitor the provision of aid and services. Whilst such tools have many advantages, their use also gives rise to potentially significant privacy risks for the beneficiaries of development efforts.

This paper argues that, given such privacy risks, any development organisation that uses digital tools to gather data on beneficiaries should comply with at least the key aspects of the EU data protection regime, including its transparency, fairness, justification, proportionality, and data security requirements.

Ben Hooper
April 2017

Introduction

The EU data protection regime is one of the most rigorous in the world. But it is not, of course, a global regime. Development organisations that are based outside the EU / EEA are in general not legally required to comply with it. Even within Europe, the Brexit vote has raised questions about how long the EU data protection regime (or at least something close to it) will continue to apply to UK-based organisations and, indeed, about its significance and relevance more generally.

But the key point is that the EU data protection regime is not simply a set of compliance hurdles that could be replaced by others without any real consequence. Although the EU rules were designed primarily with individuals in the developed world (and in particular, the EU) in mind, they are ultimately an attempt to secure an underlying *universal* good: a proper respect for privacy.

Anecdotal evidence suggests that, in the context of development work, data protection compliance is often considered to be a mere 'box ticking' exercise, if it is considered at all. This is not the right approach. Instead, development organisations should actively engage with data protection compliance as a way of uncovering what respect for privacy can mean 'on the ground' in all the locations where they operate, and of working out how respecting privacy might enable them at the very least to minimise the risk of inadvertently doing harm as they pursue their development aims.

The risk of inadvertent harm is real. Rapid advances in technology have made it easier to intrude into the privacy of individuals on a massive scale. In this context, any mistake or oversight can cause wide scale harm. Further, a generalised intention to do good on the part of a development organisation is no guarantee against such harm occurring.

"Rapid advances in technology have made it easier to intrude into the privacy of individuals on a massive scale."

The practical impact of respecting privacy

The EU data protection regime (as contained, until May 2018, in Directive 95/46/EC) regulates the use of 'personal data', which in simple terms includes most types of information about individuals. The EU regime is at present implemented in the UK by the Data Protection Act 1998, which sets out eight so-called 'data protection principles' (DPP1-DPP8).

Some of the details of this regime are not an obvious fit for the developing world or development organisations that work there.

DPP8 is a good example. DPP8 restricts the ability of organisations to transfer personal data out of the EEA. If a development organisation in a developing country obtains the personal data of beneficiaries who are resident there, then that data may never enter the EEA in the first place, rendering DPP8 irrelevant.

Even if data is transferred to the EEA for processing or storage, the beneficiaries in the developing country may not have any concerns about their data being returned back to that country, and may indeed be utterly bemused if they are asked to specifically consent to this.

Another example is the right of individuals, under DPP6, to access the personal data that organisations hold on them. This right is unlikely to be of any practical use to an illiterate farmer in a remote rural community who is receiving medical care or other aid or services from a development organisation.

However, when applied with creativity and an awareness of the particular context for, and challenges of, development work, many of the rules of the EU data protection regime can uncover real value for beneficiaries.

"When applied with creativity and an awareness of the particular context for, and challenges of, development work, many of the requirements of the EU data protection regime can uncover real value for beneficiaries."

Five key examples of this process of uncovering value are explored below. (For ease of exposition, this will be done by reference not to the somewhat technical DPPs themselves, but to key requirements identified at the outset: transparency, fairness, justification, proportionality, and data security.)

(1) Avoiding 'mission creep'

A development organisation may - with the best of intentions - gather personal data for a specific and legitimate development purpose, and may at first use that data only for that purpose. Over time, however, it is possible that the aims of the organisation may change. Even without a change in the organisation's aims, it is possible that the data may be shared with other organisations with different aims, or are less conscientious with their approaches to data sharing. Those other organisations may in turn share the data more broadly, including with states, or the for-profit sector. Along the way, the data may come to be combined with other data that allows for novel or expanded uses. Eventually, the data may end up being used in unexpected ways that risk prejudicing the beneficiaries at issue and that neither they nor the original organisation that gathered the data would ever have agreed to, had they been asked. To give a practical example: the creation of a medical records database by a development organisation might, down the line, lead to a beneficiary being denied an essential micro-loan by a loan company because she can be matched to data, now in the hands of that company, that potentially raises concerns about her long-term health.

As the above shows, the good intentions of the original organisation that gathers the data are not in themselves enough to guard against the risk of this type of 'mission creep'. By contrast, the EU regime usefully imposes specific and practical constraints that help to minimise this risk.

First, transparency requires an organisation that gathers personal data to summarise - for the benefit of the individuals in question - all the ways in which that data may in the future be used or shared (for more, see DPP1). A summary of this type is known as a 'privacy notice'.

This obligation in turn imposes a useful discipline on organisational thinking in that, in order to be able to produce the required privacy notice, potential uses and types of sharing will need to be identified and considered with care, and at the outset of any project.

More significantly, an organisation that produces the required privacy notice and that has also committed to acting fairly (again, see DPP1), will thereby be limiting itself in terms of how it may use or share the data in the future. In particular, what will be 'fair' in this regard will depend in significant part on what was said - and/or *not* said - in the privacy notice in question.

For instance, a statement that personal data may be shared with other development organisations, without a corresponding statement about sharing with commercial organisations, may well preclude any subsequent sharing of that data with such commercial organisations. And these types of limits to future uses and future sharing will be relatively transparent, because they will derive from the privacy notice itself, which has to be made available to the beneficiaries at issue.

Secondly, once personal data has been gathered, any subsequent use or sharing of that data has to be justified on one of a number of bases that include (i) the consent of the beneficiaries at issue, and (ii) that the interests behind the proposed use / sharing are both legitimate and of sufficient weight to outweigh any prejudice for those beneficiaries (for more, see DPP1). This justification requirement similarly reduces the risk of 'mission creep' by placing further prudent limits on the future freedom of action of organisations that gather personal data.

(2) The value of privacy notices in the developing world

As already noted, transparency requires the production of a privacy notice that summarises all the ways in which data may in the future be used or shared. Such notices merit further attention.

In the developing world, individuals may lack the experience or education to understand matters that might routinely find their way into a privacy notice in the developed world. They may also be illiterate, meaning that a written notice alone is unlikely to be sufficient. Not least given practical difficulties of this type, it may be tempting to conclude that it is unnecessary to inform beneficiaries in the developing world about how their data will be used, or ask their consent to such use. After all, it might be thought, the development work that is being done is straightforwardly for their benefit.

But in fact, the obligation to provide a privacy notice offers a further illustration of how an active engagement with the EU data protection regime can serve to uncover value for development organisations working in the developing world, as well as for their beneficiaries.

First, because - as has already been noted - the discipline of drafting and disseminating a privacy notice in turn imposes limits on a development organisation that helps to guard against 'mission creep'.

Secondly, there is a risk of dangerous paternalism in the assumption that a development organisation will always know what is in the best interests of their beneficiaries, such that there is no need to be transparent with those beneficiaries or involve them in any way in the decision-making process. Many individuals in the developing world may indeed lack the capacity or interest to grapple with privacy issues. But that cannot justify proceeding on an assumption that none of them has any capacity or wish to do so, or that none of them might reasonably have concerns. Whether in the developed world or the developing world, the underlying ambition is the same: individuals should be educated and informed so as to empower them to make the best choices for themselves. The fact that this process may be more challenging in the developing world is no reason to dispense with it altogether.

The third point flows from the fact that any use of new technology may be met with resistance, including - particularly in the developing world - resistance that is based upon misconceptions about that technology. In this context, the requirement to provide information about the uses of any personal data that is to be obtained can have an important role to play in building and maintaining trust. In particular, in the developing world, privacy notices and related documentation, such as Q&As, can be put to use correcting rumours and misinformation that may have spread through the local population, in addition to performing their core task of providing basic information about how the data will in fact be used.

"Many individuals in the developing world may indeed lack the capacity or interest to grapple with privacy issues. But that cannot justify proceeding on an assumption that none of them has any capacity or wish to do so, or that none of them might reasonably have concerns."

(3) How much data to gather, and how long to keep it

From an operational point of view, it is natural for a development organisation to want to gather as much data as possible and keep it for as long as possible. For example, a microfinance provider might seek to gather multiple data points on each of its beneficiaries and keep the data indefinitely, in case the future brings some innovative use for them that may help those beneficiaries or their communities. Indeed, for an organisation that wants to do as much good as possible, and that can easily gather and store the data in question, any other approach might at first seem foolish or short-sighted.

But such an approach does not necessarily respect privacy. In particular, it fails to recognise that obtaining and retaining personal data is always an interference with privacy rights - in the developing world as much as in the developed world - and that therefore the possible benefits of obtaining and retaining data must always be weighed against the interferences that will result. This weighing process is the requirement of proportionality in action: an organisation should only interfere with privacy rights if that interference is 'proportionate' to what it wants to achieve (see, for instance, DPP3 and DPP5).

What does this mean in practice? A development organisation should not obtain personal data merely because it is possible that at some unspecified point in the future that data may become useful in some unspecified way. Similarly, such an organisation should not keep data past its operational usefulness merely because it is possible that at some unspecified point in the future the data may become useful once more, again in some unspecified way. An uncritical 'rainy day' mind-set of this type does not properly respect - that is, weigh up - the privacy rights of the individuals at issue.

Further, whilst respecting privacy in this way is an important abstract good, it is not only an abstract good. Maintaining a suitably 'lean' (that is, proportionate) approach to what data is obtained, and how long it is stored for, is also an important line of defence against the 'mission creep' risk identified above. To put the point the other way: mission creep is more likely if more data has been gathered than the organisation actually needs to achieve its particular development aims, or if that data is kept beyond the point that the organisation actually needs it to achieve those aims.

In addition, such a lean approach helps reduce the risks to the individuals concerned that might flow from any loss or theft of data (see (4) below) and from any acquisition - including forcible acquisition - of that data by state organisations (see (5) below).

"Mission creep is more likely if more data has been gathered than the organisation actually needs to achieve its particular development aims, or if that data is kept beyond the point that the organisation actually needs it to achieve those aims. "

(4) Avoiding data theft / loss

The EU data protection regime imposes an important data security requirement. In particular, appropriate technical and organisational measures must be taken against theft, loss, or other misuse of personal data (see DPP7). 'Technical' measures include the use of encryption, firewalls, and so forth. 'Organisational' measures cover, for instance, internal measures to prevent access to the data by staff who may not have a legitimate reason for such access, or who may lack the technical knowledge to access data without risking its loss or corruption.

In addition to imposing these security standards, the EU regime also provides a process – known as the 'Privacy Impact Assessment' – which, among other things, facilitates disciplined and structured thinking about the security risks of any significant project or policy that might be under consideration by a development organisation.

(5) Sharing data with states

Whether in the developed world or the developing world, states often use personal data to bring benefits to their residents and citizens. However, not least given the wide array of data at the disposal of states with which any new data may be combined or cross-referenced, and the extensive coercive powers that states enjoy, any decision to share data with a state should only ever be taken after careful consideration. In the developing world in particular, an organisation may need to consider issues such as (i) whether the state in question has appropriately robust laws and internal mechanisms to guard against abusive use of the data in question and, if there is any risk of a deterioration in the political stability or security of the state, (ii) how the data might be used if that risk were to eventuate.

To give an example of the latter issue: a biometric database set up to monitor participation in an adult education programme might, in the event of serious civil strife, become a dangerous tool for security forces to identify members of a rival tribal or ethnic group.

The EU data protection regime once more yields value by providing a structure for thinking about issues of this type.

Before deciding whether to share data with any host state in the developing world, a development organisation must consider the 'fairness' of doing so from the point of view of its beneficiaries. In addition, the requirement of justification means that consideration has to be given to whether the beneficiaries at issue have specifically consented to such sharing, or to whether the interests behind the processing are both legitimate and of sufficient weight to outweigh any prejudice for those individuals.

Further, if at the outset an organisation is planning to share its data with the host state, then that fact should be communicated to its beneficiaries through the privacy notice (and / or any related Q&A documentation). This gives rise, at the very least, to the possibility that the merits of that course of action may be subject to public scrutiny and debate, which in turn functions as a useful safeguard against paternalistic thinking.

The EU data protection regime

Given its intricacy and complexity, the EU data protection regime cannot straightforwardly be summarised. It is nevertheless useful for the purposes of this paper, and this paper's argument, to draw out five key requirements.

Transparency. An organisation that wants to acquire the personal data of individuals should make available to those individuals a summary of what it will (or may) do with the data if it is acquired

Justification. Any acquisition, storage, use or sharing of personal data needs to be justified on at least one of a number of specified bases, the two most relevant being (i) the individual in question has given his or her consent, and (ii) that the interests behind the proposed acquisition / storage / use / sharing are both legitimate and of sufficient weight to outweigh any prejudice for those individuals

Fairness. Personal data should only be acquired, stored, used, or shared if that is fair to the individuals - including given the way in which that data is to be or was acquired, and given what was said and / or not said in any summary produced for the purposes of transparency

Proportionality. When acquiring, retaining, using, or sharing personal data, organisations should limit themselves to doing only what is truly necessary to achieve their particular aims

Data security. An organisation that handles personal data should take appropriate technical and organisational measures to guard against the risk of theft, loss, or other misuse of that data

Author notes

Ben Hooper is an independent consultant specialising in data protection and privacy issues. He previously spent 15 years as a barrister at the London bar specialising in these areas, including for clients such as the UK's data protection regulator, the UK Government, and various regulated entities in the technology and telecoms sectors.

This paper is not intended to be a source of legal advice, and should not be relied on as such.