The Problem with Data Sharing

Eleonor Duhs, Partner and Head of Data and Privacy at Bates Wells, ***discusses why human rights law helps to navigate the issue of over-cautious data sharing policies and practices***

In certain contexts, data sharing crosses the line between being useful from being absolutely vital. For example, data sharing enables doctors to find the right treatments for patients with complex conditions cutting across several specialisms; helps governments to protect the public during pandemics; and enables economic growth by allowing banks to understand their customers' needs and provide services and products which best suit their circumstances and requirements. Similarly crucial are cross-border data flows, which are set to be worth 11 trillion dollars to global GDP in 2025, and to overtake the value of the global trade in goods.

Yet significant misunderstandings about the dangers of data sharing, and the reluctance to share data even in situations where that data sharing is either innocuous or in the public interest, appears widespread. Examples include schools providing class photographs obscuring pupils' faces — with the only face still visible being that of the child who is receiving the photo — to commercial organisations fearing regulatory action if they share data to try to prevent scams.

In December 2018, the UK Information Commissioner's Office ('ICO') published a blog post (now removed) citing frequent misunderstandings, including schools thinking that the GDPR stopped them from telling parents which stall they were managing at a Christmas fair, to shops being told that the GDPR prevented them from telling their delivery drivers where to go to drop off their parcels. To paraphrase the ICO's words: if the supposed restrictions on data sharing seem wrong, then someone's probably misinterpreted the law.

Where has it all gone wrong?

Although the practices above suggest otherwise, the ICO's Data Sharing Code of Practice ('the Code') describes data protection law as "an enabler rather than a blocker". The work of academics in the data protection field gives us some clues as to where the problem lies.

In his eloquent (and still relevant) article 'The Trouble with European Data Protection Law', Bert-Jaap Koops points out that the legislation's emphasis on form filling is in tension with the 'spirit of data protection law'. In other words, reducing data protection compliance to completing a series of templates gets us no further in applying the regime in a way which results in sensible outcomes.

How Human Rights law can shed light on the issue

Human rights law has had a bad press in recent years, but its origins in the UK go back a long way.

In the aftermath of the second World War, then Prime Minister Winston Churchill spearheaded the establishment of the Council of Europe and the drafting of the first European human rights treaty: the European Convention on Human Rights ('ECHR'). Still in force, the ECHR continues to protect the human rights of the citizens of signatory states. In the UK, the ECHR is implemented in domestic law through the Human Rights Act 1998, enabling UK citizens to assert their human rights before UK domestic courts.

Article 8 of the ECHR, which sets out the right to a private and family life, is one of the main foundations of UK data protection law. At the end of 2023, the government brought forward legislation to clarify that the references to rights and freedoms in the UK GDPR should be read as references to human rights as set out in the ECHR. However, it's important to recognise that the right to a private and family life is not an absolute right: it is qualified. It can be interfered with where it is lawful and proportionate to do so.

This is a critical point. Privacy rights (and as a subset of those rights, the right to the protection of personal data) are not absolute rights and in many circumstances can be outweighed by other rights and interests. The act of weighing competing rights is referred to as a 'human rights balancing test'.

Ensuring that the human rights balancing test is at the core of organisations' thinking on data sharing is the key to getting the correct outcomes.

(Continued on page 6)

(Continued from page 5)

Data sharing and the human rights balancing test

A mandatory element of deciding whether to share data is in considering whether there is a legal basis available for doing so. With the exception of consent, the legal bases in Article 6 of the UK GDPR require the controller to consider whether the processing is 'necessary'. The necessity test is not a question of considering whether the processing is strictly necessary. In the case of *Michael Stone v SE Coast Strategic Health Authority* ([2006] EWHC 1668), Mr Justice Davis stated that: "it is common ground that the word 'necessary'...carries with it the connotations of the ECHR. Those include the proposition that a pressing social need is involved and that the measure employed is proportionate to the legitimate aim pursued."

The human rights balancing test becomes an integral part of the consideration of whether personal data can be processed by virtue of the word 'necessary'. ICO guidance also helps us to understand the approach that controllers should take.

The Code states that in order to meet the necessity test and share the data, the processing must be 'a targeted and proportionate way of achieving a specific purpose'. Another way of considering the question is set out in clear terms in the ICO's blog post, which asks if the processing is "too far-fetched" and whether it "makes sense".

How should we test the proportionality of data sharing?

Human rights balancing tests in the context of data protection require the controller to weigh the rights and freedoms of individuals on the one hand against the interests of the controller, and the rights and interests of third parties or society on the other.

Applied to the examples discussed above: in considering the matter of the school photograph, it is strongly arguable that the level of intrusion into the pupils' privacy is negligible. If the photograph is taken in the usual classroom setting, then it is depicting a sight which the children and their parents who pick them up and drop them off see every day. The school as the controller is merely creating a memento of their primary school days for their students to keep. Covering up all the faces to comply with data protection law is absurd.

Similarly, refusing to share personal data of a potential scammer places that individuals' privacy rights above the rights of vulnerable individuals to be protected from highly distressing criminal activity. Calibrating the balancing test in favour of potential scammers is plainly a misreading of the framework.

The same is true for the school Christmas fair example: the privacy intrusion in knowing who is running what stall is minimal, and the school has a well-founded interest in ensuring that the Christmas fair is efficiently run. Similarly, enabling deliveries requires the sharing of addresses and the privacy intrusion in these activities is negligible, and is outweighed by the interests of the sender and the business delivering parcels in ensuring that purchases can get to the right place.

As is seen above, taking an overly restrictive interpretation of the UK GDPR inhibits sensible and proportionate data sharing. Existing case law has confirmed that the controller is the 'primary decision maker' when deciding how to process personal data and has a 'wide margin of discretion' in making that decision. The case law in question relates to the interpretation of the exemption from having to comply with the subject access right where the data relate to both the requestor and a third party (see *Harrison v Cameron & Anor* [2024] EWHC 1377 (KB) and DB v GMC [2018] EWCA Civ 1497). However, there is a credible argument that the balancing test conducted in the context of third party rights is essentially the same as the balancing test for data sharing, and that this case law is also relevant in the context of the sharing of personal data.

It is the controller who should decide on the 'factors to treat as relevant to the balancing exercise' as well as the 'weight to be given to each factor' (see *Harrison*). This means that provided a controller's analysis is well crafted, balanced and credible, then it is unlikely that the regulator or a court would disagree with the analysis. This should give controllers confidence to share personal data where it makes sense to do so.

Organisations should also note that data sharing should comply with the Code. Although not legally binding, the ICO has warned that if organisations do not comply with the Code, they may find it more difficult to demonstrate that their data sharing is fair, lawful and accountable and complies with the UK GDPR or the Data Protection Act 2018. The Code sets out a number of practical steps for ensuring that sharing is compatible with data protection law, such as entering into an agreement as the basis for the data sharing. (See '*The ICO's Data Sharing Code — fit for a digital age?*', Volume 22, Issue 4 of *Privacy & Data Protection,* pages 3-6).

The solution

Data protection practitioners urgently need to be part of the solution when it comes to data sharing. The key to this is appreciating that data protection law is human rights law. A carefully calibrated assessment of human rights in a data sharing context will help to ensure that data sharing isn't simply a mechanical, box-ticking exercise which results in outcomes which undermine perfectly sensible activities. Rather, it should be a credible and pragmatic analysis of the right to privacy in a particular context.

Eleonor Duhs
Bates Wells
e.duhs@bateswells.co.uk