

Submission from Gener8 to the Scrutiny Committee for the Data Protection and Digital Information Bill (2)

About Gener8

Gener8 is a UK business empowering people to control and be rewarded from their data. On one side of our platform, we offer our users the chance to access, control, and earn rewards from their online data. On the business-facing side of the platform, we sell fully consented, anonymised and aggregated data products to the market intelligence sector. The revenue we earn from these sales then funds the rewards that our users can redeem. With this unique business model, we believe we are building the first commercially viable Personal Information Management Service (PIMS) in the world.

With consumers and regulators all around the world wising up to the extent of online surveillance, personal data management has the potential to be a multi-billion-pound, winner-takes-all global market. As it stands, Gener8 is well-positioned to win this race, and to bring more digital success to the UK.

Headquartered in London, we have grown to 25 employees, and our award-winning business is on track to be another UK tech unicorn this decade. Referred to as having given 'the best pitch ever' on Dragons Den, Gener8's founder Sam Jones has since been awarded 'Disruptor of the Year' in 2022 at the Great British Entrepreneur Awards, featured on the BBC, and has attracted investment from a range of high-profile individuals.

The regulatory framework for PIMS

Personal Information Management Services (PIMS) were made theoretically possible through data access rights in the GDPR, but these rights have proven to be too loose and difficult for people to make use of in practice. The ability to request historic data on a discrete basis with up to a 30-day turnaround is nowhere near good enough to empower people and to unlock the innovative power of open data. This has been one of the main reasons why no PIMS has yet managed to turn academic ideas into a commercial reality.

In order for the personal data economy to thrive, individuals must have a legal right to access a continuous stream of their own data from online services, which should be actioned via a single, straightforward request.

We have clear evidence of the impact that these kinds of friction-reducing changes could have on our business. For example, where our users are able to access their data from a third-party service in a real-time and continuous manner, the retention rate for these data connections in our app is more than double the rate when the user has to rely on repeated subject access requests on a weekly or monthly basis. This translates directly into higher growth and revenue.

The European Commission is currently winning the race to open up this opportunity for individuals and businesses in the EU. Through Article 6(9) of the Digital Markets Act, which is in an implementation phase, Digital Gatekeepers have an obligation to give their users (and third parties operating with consent on their behalf) real-time and continuous access to their data on the gatekeeper's platform. Though there are some substantial uncertainties around implementation, this

Act could be the key piece in the puzzle for unlocking the personal data economy, which will make the EU a highly attractive place to set up new businesses in this sector.

The Data Protection and Digital Information (DPDI) Bill is an opportunity for the UK to take a similar leap forward and avoid being left behind by the EU as a hub for data driven innovation, but as it stands the Bill adopts a paradoxical approach and could harm our prospects.

The data portability paradox

The DPDI Bill contains two important legislative changes that will affect an individual's ability to see and access the data that companies are collecting on them. Unfortunately in this respect, the new powers for Smart Data Schemes, and the amendments to Subject Access Request rights, appear to be pulling in different directions.

Smart Data Schemes

The unsung hero within the DPDI Bill is undoubtedly the new powers for the government to introduce Smart Data schemes. This is expected to lead to new schemes in a range of traditional sectors such as finance, communications, and energy that unlock the flow of consumers' personal data from their providers to trusted third parties.

As has now proven to be the case with Open Banking, this could revitalise competition in sectors where the game has for too long been rigged towards a small number of large incumbents, and at the same time unleash a wave of innovation with brand new services and markets not currently possible.

It is essential that these powers are retained within the Bill and not watered down. In the meantime, as the Bill progresses, Gener8 will be engaging with government and the Smart Data Council to promote [our proposals for Open Digital](#). We foresee that the most powerful candidate for a Smart Data Scheme would relate to large online platforms, through which consumers could (if they wish) seamlessly provide continuous real-time access for accredited third parties to their online data generated by web browsing, app downloads, online shopping, music and video streaming, and travel etc. In addition, if the individual was able to provide the third party with 'read' and 'write' access to their online data, they could use that service to push out consents and delete requests from a centralised service. This would deliver transformative change for the online ecosystem and solve numerous policy challenges by creating a level playing field for data access, giving people control over their data and privacy, and removing the problems of consent fatigue.

Subject Access Requests

You simply cannot reduce burdens on business from data protection law without reducing protections for individuals and without increasing the risks to privacy. These costs might in some instances be small, and they might be deemed socially acceptable for the greater good, but there are costs from the Bill that are not being fully acknowledged. We hope that the scrutiny provided by the Committee will help to provide greater transparency.

Despite the government's position that people will still be able to make subject access requests (SAR) and access their data, the government's impact assessment attributes substantial financial savings to a change to the SAR rules, with assumptions of significant reductions in costs responding to requests. Lower costs no doubt, because the government is lowering the threshold for companies to not respond at all, or alternatively to charge a fee for doing so.

Data portability rights as established through access rights in the GDPR are already extremely flimsy from an individual's perspective, and the user experience is extremely clunky and slow. The government admitted as such in justifying the Smart Data proposals, stating that 'UK GDPR created a right to data portability but does not enable data sharing as envisaged for Smart Data, lacking strong standards and secure data sharing requirements.' Rather than directly addressing this shortcoming, the government is proposing to make it worse in the short term, while Smart Data Schemes may take decades to implement across multiple sectors.

There are undoubtedly circumstances where organisations with limited resources may be disproportionately affected by the current regime for SARs, and I can understand why the government might wish to address this situation and allow for a bit more flexibility with response times in targeted circumstances. But on the other hand there are some very large firms with near-limitless resources for which the existing rules are far too lax. This is one area of the rulebook that is crying out for a departure from the so-called 'one-size-fits-all' approach.

In our view this element of the Bill sends a strong message from government that data portability is the enemy of businesses. Rather than make it easier for people to access their data, it is making it even easier for companies to resist. This is not just a missed opportunity, but a harmful and backward step, in contrast with the broader direction of travel in the online ecosystem, and risks undermining the positive progress towards Smart Data schemes.

Proposed amendments to the DPDI Bill

Definition of vexatious under 12A and 204A.

The text of the Bill will respond to some legitimate challenges faced by smaller organisations, but could create a loophole for larger businesses that want to create friction for people that want to access their data. Specifically, we are concerned that individuals that want to make regular updated requests for their data in order to access an ongoing time series will be flagged by big tech companies as excessive.

In order to limit the risk of this loophole, we propose the following amendments to the Bill:

- In part (d) insert 'identical' after previous so that it reads 'the extent to which the request repeats a previous identical request made by the sender to the recipient'.
- In part (e), insert at the end 'and the extent of data collection in the period since any previous request' so that it reads 'how long ago any previous request was made, and the extent of data collection in the period since any previous request'.
- Insert new part (g), to say 'the extent to which the controller offers a more streamlined alternative to making repeated requests in order for the individual to exercise their right to access on an ongoing basis.'

Time periods for responding to access requests under 12B

As with the ability to reject requests that are vexatious or excessive, the amendments to time periods also appear to create loopholes for data-driven big tech companies to add friction to the process and hold onto the data within their walled gardens.

If we were starting from scratch, we would recommend that the time limit be substantially reduced, at least for businesses that have the capacity and resources to handle the requests efficiently. Given this kind of reversal is unlikely, we pragmatically propose the following amendment to limit the harm from this element of the Bill:

- Under paragraph 3, insert something to the effect of ‘In doing so, the controller must give due consideration to the resources it has available for responding to such requests.’
- Paragraph 6 reads ‘An example of a case in which a controller may reasonably require further information is where the controller processes a large amount of information concerning the data subject.’ We propose deleting or amending this example, as these companies are precisely the organisations that should face higher rather than lower expectations on their performance.

Continuous access to data

While some individuals may out of curiosity wish to take a one-off look at the data that a company is holding on them, in practice this data will have little economic value unless it can be accessed as a continuous ongoing flow. The above proposed amendments will limit the harm that the Bill will do to individuals’ ability get this via clunky repeated requests at regular intervals, but there is more that could be achieved through a more ambitious amendment that makes continuous access possible.

While we do not know how best to draft such an amendment or where to place it within the Bill, we propose introducing something to the effect of:

- A data controller with sufficient resources and technical capabilities,* that processes large volumes of personal data as a core element of its business, must provide data subjects (and third parties acting on their behalf) with an option of accessing their data on a continuous and real-time basis.
- *Sufficient resources and technical capability could be demonstrated by the fact that the data controller already provides such access in another context or legal jurisdiction.

Introducing such a provision could quickly ensure that the 15-20 tech companies that will be designated by the European Commission as digital gatekeepers will roll out the provisions from the DMA in the UK also.

This would immediately unleash the power of the personal data economy in the UK, bring the UK to the front of the race alongside the EU, and transfer power from powerful global corporations to UK consumers. Waiting a decade or more for a Smart Data Scheme to deliver this change will already be too late for UK innovators and disruptors.

Further evidence

If you need further information from us or would like to discuss these proposed amendments in more detail, we would be delighted to send a further submission or to provide oral evidence to the Committee at a time of your convenience.

You may also be interested to read the two blogs we have written related to these topics:

[Data Wars: Return of the DPDI \(Episode II\)](#)

[Open Digital: An entirely unoriginal idea](#)

Please do not hesitate to get in touch:

Tom Fish, Head of Public Policy: tom@gener8ads.com

Sam Jones, Founder and CEO: sam@gener8ads.com