Data Protection and Digital Information (DPDI) Bill briefing

Introduction

Unlock is a national independent advocacy charity that supports, speaks up and campaigns for people facing stigma, prejudice and discrimination because of their criminal record. A core mission for Unlock is to provide advice for people in respect of their criminal record, including help overcoming the barriers they're facing. Our website provides vital information and guidance for people with criminal records, but we also have a helpline provided by dedicated staff and volunteers, which deals with specific queries. People can contact the helpline in various ways, including via email, WhatsApp or our free phone line.

This document sets out Unlock's position on a number of elements of the DPDI Bill where we have concerns about the impact it may have on individuals with criminal records.

Background

A criminal record often acts as a barrier to individuals' future opportunities far beyond its initial intention, whether through examples of idiosyncrasies in the system or misunderstanding of the law. This is often entrenched by the stigma people with criminal records face. It is crucial, therefore, that organisations are supported by legislation to treat criminal records data appropriately and that the right of individuals with criminal records to move on and rehabilitate are not hampered by processing of their personal data. As a charity focussed on the needs of individuals with criminal records, the lens through which we are viewing the Data Protection and Digital Information Bill ("the Bill") is that of the status of criminal record data. Currently, criminal records data is defined as a specific category of sensitive data by UK GDPR. We believe this must remain the case.

Issues

Abolition of the Information Commissioner's Office

The issue: the Bill seeks to replace the Information Commissioner's Office (ICO) with an Information Commission. This body is at risk of being less independent of the politicians who oversee it which could have wider ramifications.

What the bill says: clauses 107–110 (and Schedule 13) of the Bill lay out the replacement of the ICO with an Information Commission. The Bill's explanatory notes argue that "the nature of the regulator's role and responsibilities remains fundamentally unchanged" as a result of this process.

Under the provisions of the Bill, it is unclear whether the new Information Commission would retain the ability to set its own strategy, with this being one area in which the Secretary of State is proposed to be given greater power of oversight. The independence of the ICO (or its replacement body) is crucial to safeguarding individuals' rights and to setting the right priorities to protect those rights. This is particularly true for vulnerable cohorts (both those with criminal records and where this intersects with other examples of disadvantage) whose data rights may otherwise be compromised.

Legitimate interests

The issue: the Bill allows the definition of recognised legitimate interests to be broadened at the discretion of the Secretary of State. A recognised legitimate interest allows an organisation to process sensitive data.

What the bill says: "regarding recognised legitimate interests", clause 5 gives the Secretary of State power regarding the "(a) adding or varying provisions, or (b) omitting provisions added by regulations made under this paragraph". Although the following paragraph outlines the things the Secretary of State needs to "have regard to" in doing so, this remains a broad power. The definitions of "recognised legitimate interest" are outlined in Schedule 1 of the Bill.

Unlock has some concerns about the potential issues these provisions create. Firstly, we are concerned that identifying legitimate interests which automatically apply will mean that organisations relying on these examples will be exempt from having to carry out a balancing exercise between their interest in the data and the individual's right to data privacy. Secondly, we are concerned that the Bill introduces a risk that, without having to carry out the normal process of deciding that there was a legitimate interest in any given situation, this may allow for too broad a justification without considering context. We would argue that a legitimate interest should always be contextual, rather than deemed to be automatic. For example, it may be that one organisation would be able to justify data processing because of a stated legitimate interest (safeguarding, as an example that may leave criminal record data vulnerable to excessive processing) but another organisation should not be able to rely on the same legitimate interest. Finally, we are concerned that the powers noted above allow the Secretary of State to add to these "recognised legitimate interests" in very broad terms lacking effective limitation, either through parliamentary scrutiny or effective public consultation. We are sympathetic to concerns raised in the Bill committee regarding limitations that could be placed on this, where there was also ministerial confirmation that the Bill in its current form would not compel the Secretary of State to publish an impact assessment or ICO comment on any proposed changes.

Requirement, or otherwise, for organisations to have a data controller

The issue: the Bill proposes that organisations will only be required to designate a "senior responsible individual" where there is a high risk to individuals resulting from data processing. The Bill would be strengthened by clarity on when risk is sufficiently high as to trigger such an appointment.

What the bill says: clause 15 states that a "senior responsible individual" need only be appointed if the organisation is a public body or their activity in processing data is "likely to result in a high risk to the rights and freedoms of individuals".

Although the Bill's explanatory notes suggest that the processing of criminal records data would constitute a sufficient risk for an organisation to appoint a senior responsible individual, we still have two concerns. Firstly, the fact that this is not included in the Bill itself means clarity is lacking. Secondly, we fear that this is opening the issue up to organisations' discretion to a far greater degree than is suitable. In order to safeguard the data rights of individuals with criminal records the fact that this is sensitive data constituting a high risk is something that should not be left open to interpretation, as this would put existing safeguards at risk. Taken together, these issues may also undermine public trust in organisations' data management practices.

Logging of law enforcement processing

The issue: we would be concerned if the need to provide a justification for law enforcement agencies to keep a log of data processing activities is lost, as a process of justification embeds good practice.

What the bill says: clause 17 removes the need for "justification" of law enforcement processing activities.

The Bill's explanatory notes argue that there are two facts upon which the removal of a justification is based. Firstly, that a justification, if later scrutinised, may not constitute reliable information. Although this may be true in certain circumstances, the need for authorities to 'step back' and consider the justification for their action embeds good practice nonetheless. That adding a justification is "technologically challenging" and would require "manual input". This focus on logistics rather motivation risks creating an imbalance between the rights of data subjects and the burden on organisations. We are concerned that these provisions could leave people with criminal records vulnerable to excessive data processing if the safeguard of justification is removed.

Data Protection Impact Assessments (DPIAs)

The issue: the Bill proposes to replace DPIAs with a requirement for organisations to carry out an "assessment of high risk processing". In its present form, this puts at risk safeguards designed to ensure organisations' data processing takes due regard of individuals' rights.

What the bill says: clause 18 omits a number of features of UK GDPR (including around criminal records data and the extent to which processing is necessary or proportionate). It also places a burden on a future Information Commission to define the circumstances in which "high risk processing" would occur, rather than providing this here.

This aspect of the Bill currently removes elements of the UK GDPR (Article 35) that ensure that organisations wishing to process criminal records data must account for the impact of doing so. The renaming of the process does not effectively account for the actual changes being made here, seemingly to reduce administrative burden on organisations. We would argue that a DPIA (or similar) should maintain the need to demonstrate whether the data processing being undertaken is proportionate and necessary, to ensure best practice and to ensure practice is continually reviewed. The current process for DPIAs to identify potential poor practice, which is then flagged to ICO prior to implementation, is also an important preventative tool that should not be lost. We are also concerned that the Bill leaves it to a future Information Commission to define the circumstances in which "high risk processing" would occur, which fails to offer any clarity.

Data subjects' ability to submit complaints

The issue: the Bill alters the circumstances in which a complaint from a data subject can be taken forward. Those vulnerable to poor practice concerning data processing are at risk of having their access to redress hampered.

What the bill says: clause 32 replaces "manifestly unfounded" with "vexatious" (maintaining "excessive" alongside this) to describe the types of requests that can be rebuffed by the Information Commission. Clauses 41 and 42 places the same bar to be met on complaints to the Information Commission, and sets out that a complaint must first be made via the data controller before it can be escalated to the Information Commission.

Anything which limits access to redress is of concern, specifically in relation to vulnerable individuals with criminal records. The Bill requires complaints from data subjects to be lodged with data controllers in the first instance, posing particular challenges for individuals with criminal records. A likely scenario in which an individual with a criminal record may feel compelled to make a complaint would be if they are being asked to disclose information that an organisation is not legally entitled to. In such circumstances, by making a complaint to the data controller they would be at risk of highlighting criminal record data that they do not need to. The lack of opportunity to lodge a complaint with the independent Information Commission is concerning in this context.

Reduction of burden on data processors to identify purpose of processing

The issue: the Bill reduces the burden upon data processors to identify a new purpose in order to process data more than once.

What the bill says: clause 10 allows for organisations to re-process data without provision of additional information to the data subject if that activity is for research, archival or statistical (RAS) purpose and if provision of information is deemed to be a "disproportionate effort".

We are concerned that that the purposes may be interpreted very broadly. While we recognise there is potential for benefits in relation to something like equality monitoring, we would be concerned that without appropriate safeguards, this could widen the scope for collecting and processing data without full impact assessments or understanding of what risks this entails for individuals.

Conclusion

One of the key themes of the concerns with specific provisions of the Bill that we have outlined in this document is a lack of clarity, and this is something that we have concerns about more generally. Through both our helpline and the work we do with organisations to ensure their criminal record data policies and practices are appropriate, we know that understanding of, and compliance with, the existing data protection requirements is patchy. We note the government assertion that this Bill does not represent significant change to the status quo but fear that organisations may, nonetheless, see new measures as a deterrent to compliance with existing ones. We would welcome any government statement to encourage organisations to comply with existing legislation. This would both allow organisations to comply with current legislation and to be well placed to comply with future legislation. The data rights of individuals need to be met irrespective of potential future legislative changes.

Overall, we believe there are provisions in this Bill that make more significant changes to the status quo than might initially appear to be the case. We have highlighted here instances where we believe that this will have an adverse effect on individuals with criminal records.