Written evidence submitted by TransUnion International UK Limited

Data Protection and Digital Information (No. 2) Bill

Public Bill Committee

About TransUnion

TransUnion is a global information and insights company and one of the UK's leading credit reference agencies. We make trust possible in the modern economy by providing an actionable picture of each person so they can be reliably represented in the marketplace. As a result, businesses and consumers can transact with confidence and achieve great things. We call this Information for Good®.

A leading presence in more than 30 countries across five continents, TransUnion provides solutions that help create economic opportunity, great experiences and personal empowerment for hundreds of millions of people. Having operated in the UK since 2000, we offer specialist services in fraud, identity and risk management, automated decisioning and demographics. We support organisations across a wide variety of sectors including finance, retail, telecommunications, utilities, gaming, government and insurance.

TransUnion has a proven track record in the development of innovative solutions, including the pioneering over-indebtedness initiative (designed to improve lenders' understanding of customer indebtedness and ability to repay), the development of solutions to minimise fraud risk across different industries, and free credit scores for life for consumers.

Consumers are at the heart of what we do, and as data custodians we encourage consumers to understand their data identity and how it can help them make better decisions.

The current Bill

We support the Government's objective to create an improved business environment under the new Bill, relieving compliance burdens while maintaining critically important high standards of data protection.

We were encouraged by several of the new changes proposed, including:

- **Clarity on the distinction between profiling and automated decision-making**

  We welcome the much-needed clarity in the new Bill over the distinction between profiling and automated decision-making: profiling is a form of automated processing on which a decision may be based, but it is not an automated decision in and of itself. That position is already reasonably clear in key parts of the original EU and UK GDPR, but in other places the wording is ambiguous and appears to conflate automated decision-making with profiling.

  The new Article 22A(2) is useful in clarifying the relationship between profiling and decision-making. This helps to address legal uncertainty and bring the law in line with the policy intention:

to put guardrails around automated decisions, while allowing the use of processing and analysis to inform decisions alongside human involvement where appropriate.

The distinction between profiling and automated decision-making is particularly important in cases where one organisation is making decisions based on the data analysis of another organisation. For example, credit reference agencies analyse personal data to produce a credit score – an estimate of the data subject's creditworthiness – which may then be used by a lender as part of a wider decision-making process. The lender will generally consider many other factors, in addition to the credit score, as part of its lending decision, ultimately making its decision by reference to its own lending criteria and other data it may have access to.

Credit scores are crucial for helping lenders to make fair and accurate lending decisions, enabling them to minimise the cost of credit and avoid inappropriate or irresponsible lending to vulnerable consumers who would otherwise risk falling into unmanageable debt. Credit scores also help consumers to easily comprehend their overall financial status and understand how they might be evaluated by potential lenders. This important activity should have a clear and unambiguous legal status under the UK GDPR.

- **A risk-based approach to record keeping**

  The Government's proposals on record keeping are welcome, and we fully support a pragmatic and risk-based approach. We also support the requirement that the ICO produce and publish examples of processing that are likely to result in high risk to rights and freedoms; it is important that data processors and controllers are clear which activities should be considered high risk so that individuals' rights are properly protected and there is a common understanding (and therefore a level playing field) between different organisations.

Likewise, we were pleased that the Bill did not diverge too far from the EU GDPR, as maintaining data adequacy is important to our, and many other businesses', operational processes. We would caution against any changes to the current legislation that would risk the UK's adequacy arrangement with the EU.

Areas for improvement

Notwithstanding these positive developments, there remain a few areas where we think the Bill could go further to help businesses and consumers, by making a few simple changes:

- **Introduce new conditions for processing special category data to help protect vulnerable consumers**

  Within the financial services sector there is currently a great deal of focus on the need to treat vulnerable consumers fairly, taking into account their specific circumstances. To do this, businesses need to be able to identify vulnerable consumers and keep a record of that vulnerability in order to implement appropriate measures to address their needs. However, many types of vulnerability – such as physical or mental health issues – are treated as special category data and so require a legal basis under Article 9 of the UK GDPR to process the data. In some

cases, it might be possible to get explicit consent from the individual, but in other cases a controller must meet specific conditions in Schedule 1 of the Data Protection Act 2018 to allow the processing of the special category data.

The conditions in Schedule 1 are limited in scope. For example, the condition to allow processing for "Safeguarding of economic well-being of certain individuals" only applies for the purposes of protecting economic well-being; where consent is inappropriate; to data concerning health; and where an individual is less able to protect their own economic well-being because of physical or mental injury, illness or disability. By contrast, the FCA has adopted a broad definition of vulnerability, and broad requirements on financial services firms; this therefore requires a broader set of circumstances in which data relating to vulnerability can be processed.

As an example, consumers often wish to include a notice on their credit file explaining the reasons why they have encountered financial difficulties in the past, allowing lenders to consider this as part of their lending decisions. This is very important, as it helps to avoid financially vulnerable consumers taking out unmanageable loans. The information in the consumer's notice sometimes includes special category data such as information about mental health conditions. Yet it is not always possible to make a clear judgment as to whether the individual is "less able to protect their own economic wellbeing" (which would potentially allow us to process the data under Schedule 1) or whether they have full capacity and sufficient freedom of choice to provide valid consent. This leaves a gap where it is difficult to judge on what basis we can legally process the data that the consumer has shared, even though it would be of great benefit to them.

Clearer conditions for processing special category data in contexts such as this would help businesses ensure that their most vulnerable customers are properly protected. We suggest that Schedule 1 of the Data Protection Act 2018 should include a condition for processing special category data relating to a (broadly defined) vulnerability of the data subject when the processing is taking place to mitigate the effects and help the individual with their vulnerability.

- **Clarify the rules on electronic marketing to ensure they are up to date and easy to apply**

  The Bill represents an opportunity to clarify and simplify certain aspects of the rules on electronic marketing in the Privacy and Electronic Communications (EC Directive) Regulations 2003 ("PECR").

  First, we recommend that the definition of "electronic mail" in regulation 2(1) of PECR is amended to ensure that it remains up to date and future-proofed – for example, by clarifying whether it applies to direct messaging over social media, and smartphone notifications.

  Additionally, we think it would make more sense for the rules on email marketing in regulation 22 of PECR to distinguish between business recipients and consumer recipients, rather than between corporate-owned and non-corporate owned email addresses. Under the current system, consent is required when sending email marketing to a business formed as a partnership, but not when sending it to a business formed as a company. It is not clear why that should be, and it is

often not easy to automatically determine whether any given email address belongs to an incorporated or unincorporated entity.

- **Support transparency by facilitating the use of personal data to provide privacy notices to data subjects**

  It would be helpful to ensure that controllers can use any contact details available to them in order to provide data subjects with privacy notices. This could be supported by adding the provision of privacy notices into the new Annex 1 (recognised legitimate interests) and Annex 2 (compatible purposes) that the Bill proposes to insert into the UK GDPR.

  These measures would help to promote transparency for data subjects and remove potential concerns among controllers, such as whether the use of email addresses collected for one purpose (such as service delivery or marketing) can also be used to provide privacy information to data subjects.

- **Improve consumers' awareness of the use of information on public registers**

  Many individuals are not clear how organisations receive and use information from public registers, such as the electoral register and the register of court judgments. For example, when an individual registers to vote, they may not be provided with sufficient detail about how their data may be used and shared by credit reference agencies and their clients. Similarly, when an individual is made subject to a county court judgment (CCJ), they may not be informed about the way in which credit reference agencies use that information, and the potential resulting impact on their ability to obtain credit in the future. Even if some information is provided, it will not satisfy all the expectations of Articles 13 and 14 of the UK GDPR. This means that consumers whose data appears on public registers may not be sufficiently well-informed about how the data is used and are therefore less able to exercise their data protection rights.

  Resolving these issues may be relatively complex and would require input from the relevant public bodies as to the practicalities of providing the relevant information to data subjects. Nonetheless, we consider that the Bill could be amended to include a power for the Secretary of State to specify information which must be included in the privacy notices given to data subjects by the relevant public bodies. Following an appropriate degree of consultation, the Secretary of State could then require that the relevant public bodies provide individuals with specific privacy information, which could include a link to the credit reference agencies' privacy notice and other useful information.

- **Completing the amendments to the rules on automated decision-making**

  As mentioned above, the new version of Article 22A(2) helps to clarify the relationship between profiling and automated decision-making. However, we believe that further consequential changes are needed in the amendments to Article 47(2)(e). It would also be helpful to update Article 13(2)(f) and 14(2)(g) (for example, by deleting the words "including profiling") to avoid confusion and ensure consistency with the new version of Article 22A.

