Equality Commission
FOR NORTHERN IRELAND

Submission on the Data Protection and Digital Information Bill

March 2024

1 Introduction

1.1 The Equality Commission for Northern Ireland ("ECNI") is an independent public body established under the Northern Ireland Act 1998. Its powers and duties derive from a number of equality statutes providing protection against discrimination on the grounds of age, disability, race, religion and political opinion, sex and sexual orientation. Its remit also includes overseeing the statutory duties on public authorities on the promotion of equality of opportunity and good relations under Section 75 of the Northern Ireland Act 1998.

1.2 ECNI, along with the Northern Ireland Human Rights Commission ("NIHRC"), as the dedicated mechanism, also has a mandate to monitor, advise, report on, promote, and enforce the UK Government's commitment under Article 2(1) of the Ireland/Northern Ireland Protocol, now known as the Windsor Framework ("WF Article 2") to the UK-EU Withdrawal Agreement to ensure there is no diminution of rights protected in the 'Rights, Safeguards and Equality of Opportunity' chapter of the Belfast (Good Friday) Agreement 1998 ("GFA") as a result of the UK's withdrawal from the EU.

1.3 ECNI provides this submission to the House of Lords on the Data Protection and Digital Information Bill, in advance of the Committee stage of the Bill. This briefing focuses only on those matters which fall within the scope of the role and remit of ECNI, including as the dedicated mechanism.

1.4 We note that significant concerns have already been raised by a range of stakeholders, including by the NIHRC[1] and the Equality and Human Rights Commission [2] ("EHRC") that the Bill breaches the European Convention of Human Rights ("ECHR"), and that NIHRC has also raised concerns in the context of compliance with WF Article 2.

2 Compliance with 'non-diminution of rights commitment' in Article 2 of the Windsor Framework

Introduction

2.1 The Commission has set out below its views on the Bill's compliance with WF Article 2. These views are on the basis of the provisions of the Bill to date, and if enacted.

2.2 It should be noted that we support a number of the concerns raised by the NIHRC in its submission on the Bill in terms of its views on the Bill's compliance with WF Article 2.

2.3 The UK Government's ("UKG") commitment in WF Article 2 means that the UKG must ensure there is no diminution of rights, safeguards and equality of opportunity, as set out in the relevant chapter of the GFA, resulting from the UK's withdrawal from the EU.[3] In addition to the no diminution commitment, the law in Northern Ireland must 'keep pace' with EU law developments relating to six EU Equality Directives listed in Annex 1 to the Windsor Framework. As part of the UK EU Withdrawal Agreement, WF Article 2 is incorporated into domestic law via Section 7A of the European Union (Withdrawal) Act 2018 ("EUWA 2018").

2.4 As the UK Government is aware, prior to Brexit, the EU General Data Protection Regulations (2016/679) (the "EU GDPR"), applied directly in the UK and was supplemented by the Data Protection

[1] NIHRC Briefing on the Data protection and Digital Information Bill January 2024
[2] EHRC Briefing on Data Protection and Digital Information Bill for HoL second Reading 15th December 2023
[3] Windsor Framework Article 2 states:
"The United Kingdom shall ensure that no diminution of rights, safeguards or equality of opportunity, as set out in that part of the 1998 Agreement entitled Rights, Safeguards and Equality of Opportunity results from its withdrawal from the Union, including in the area of protection against discrimination, as enshrined in the provisions of Union law listed in Annex 1 to this Protocol, and shall implement this paragraph through dedicated mechanisms."

Act 2018 ("DPA 2018"). At the end of the Brexit transition period, the EU GDPR was incorporated into UK law under Section 3 of the EUWA 2018 and modified by the Data Protection, Privacy and Electronic Communication (Amendments etc) (EU Exit) Regulations 2019 under the power in Section 8 EUWA 2018 to create the UK GDPR. The UK GDPR is therefore the retained version of the EU GDPR[4] and at present the two align, subject to ECNI's view of the amendment made by the Data Protection (Fundamental Rights and Freedoms) (Amendment) Regulations 2023, discussed below.

2.5 We note that the Government's intention in introducing the Data Protection and Digital Information Bill (No 2) ("the Bill") is to update and simplify the UK's data protection framework.[5] ECNI has concerns that some of the changes proposed by the Bill could potentially breach the UKG's obligations under WF Article 2.

2.6 In particular, ECNI has concerns that should the Bill be passed into law in its current format, the changes it will introduce with regard to subject access requests (Clause 9), automated decision making (Clause 14), the requirement to produce data impact assessments (Clauses 20 and 21) and the power of the Department of Work and Pensions ("DWP") to access the bank accounts of benefit claimants (Clause 128 and Schedule 11), may result in a diminution of rights contrary to WF Article 2.

WF Article 2: Test for breach and Scope

2.7 The Court of Appeal in ***Re SPUC Pro-Life Ltd [2023] NICA 35*** [para 54[6]] held, broadly in line with ECNI's submissions as an intervenor in the case, that a breach of Article 2 is established by satisfying the following six element test[7]:

(i) A right (or equality of opportunity protection) included in the relevant part of the Belfast/Good Friday 1998 Agreement is engaged.

[4] This has been confirmed by the High Court in The3million & Open Rights Group v Secretary of State for the Home Department [2023] EWHC 713 (Admin), at para 9.
[5] Data Protection and Digital Information Bill Explanatory Notes
[6] SPUC Pro-Life Ltd (2023) NICA 35
[7] For further information on the views of the Commission, and the NIHRC, on the questions that are relevant to establishing a potential breach of Article 2 see ECNI, NIHRC Working Paper: The Scope of Article 2(1) of the Ireland/ Northern Ireland Protocol, (ECNI and NIHRC, December 2022) page 32

(ii) That right was given effect (in whole or in part) in Northern Ireland, on or before 31 December 2020.

(iii) That Northern Ireland law was underpinned by EU law.

(iv) That underpinning has been removed, in whole or in part, following withdrawal from the EU.

(v) This has resulted in a diminution in enjoyment of this right; and

(vi) This diminution would not have occurred had the UK remained in the EU.

2.8 ECNI considers that the EU right to data protection falls within scope of the commitment in the relevant chapter of the GFA to protect the "civil rights and religious liberties of everyone in the community". In this regard, we would point to the judgment of the Northern Ireland High Court in the case of *Re Angesom* [2023] NIKB 102[8] and more recently *Re Dillon* [2024] NIKB 11[9], both of which make clear that the rights covered within the relevant chapter of the GFA include a wide range of civil rights.

2.9 Relevant EU law that we consider falls within the scope of WF Article 2, as regards the right to data protection, includes Articles 7 and 8 of the Charter of Fundamental Rights ("CFR"), the recitals to the EU GDPR, in particular 1,2,3 and 4 and Article 1(2) of the EU GDPR. For example, the recitals to the EU GDPR and Article 1(2) of the EU GDPR make clear that that data protection is a fundamental right. We would point out that at the time of the drafting of the GFA, data protection was already established as a fundamental right under the general principles of EU law.

[8] In *Re Angesom [2023] NIKB 102*, (paragraphs 107-8) the High Court concluded that GFA rights were applicable to asylum seekers and were not confined to those rights related, or connected with, the conflict.

[9] In *Re Dillon* [2024] NIKB 11 (paragraph 561)the court was clear that the right to life, the right to be free from torture, cruel, inhuman or degrading treatment, the right to access a court, the right to be free from discrimination and the right to dignity of the applicants, in their capacity as victims (or relatives of victims) of the 'Troubles' were included within the notion of 'civil rights', though the court also relied, in its reasoning about these victims' rights, on the fact that paras 11 and 12 of the relevant Section of the GFA also contain certain commitments about victims.

2.10 In addition to the above, as made clear in the joint working paper[10] on the scope of WF Article 2, by ECNI together with the NIHRC, we are adopting a working assumption that the non-diminution commitment in WF Article 2 encompasses the full range of rights set out in the ECHR, to the extent that they are underpinned by EU legal obligations in force in NI on or before 31 December 2020.

2.11 In particular, data protection is recognised as a right in Article 8 of the ECHR which protects the right to respect for private and family life. We are also of the view that Article 14 of the ECHR, which provides protection from discrimination, may also be engaged in conjunction with Article 8 ECHR, as stated by the Joint Committee on Human Rights in its letter to the Secretary of State for the Science, Innovation and Technology Department on 20th July 2023: namely it stated that : "*inadequate data protection can result in bias that violates Article 14 of the ECHR (which prohibits discrimination in the enjoyment of other Convention rights).*" [11]

2.12 We consider that the rights engaged by the relevant chapter of the GFA, in the context of data protection, were clearly given effect in Northern Ireland prior to the end of the Brexit transition period. We would refer, *in particular*, to the protections provided by the EU GDPR, which, as noted above, had direct effect in Northern Ireland prior to Brexit as domestic law and were underpinned by EU law, including the rights to privacy and personal data in the CFR whose content, by judicial assessment [See *Angesom*, [2023] NIKB 102 para 94], remains enforceable in Northern Ireland.

2.13 We are concerned that the Bill, if introduced, could potentially remove this EU law underpinning; underpinning which could not have been removed had the UK remained in the EU. Whilst the UK GDPR and the DPA 2018 currently align with the EU GDPR, we are concerned that the Bill, if introduced in its current format, may result in a diminution of rights that would not have occurred had the UK remained part of the EU. Consequently, we are concerned that the Bill may potentially breach WF Article 2. We have noted above specific Clauses in the Bill which are of particular concern to ECNI in the context of WF Article 2. We have set out our concerns in further detail below.

---

[10] ECNI, NIHRC Working Paper: The Scope of Article 2(1) of the Ireland/ Northern Ireland Protocol, (ECNI and NIHRC, December 2022) page 60.

[11] Joint Committee on Human Rights Letter 20th July 2023

2.14 Whilst we have focused on the EU GDPR in our submission, we wish to make clear that we also consider that the EU E-Privacy Directive[12] and the EU Data Protection and Law Enforcement Directive[13] fall within scope of WF Article 2.

Clause 9 – Changes to Subject Access requests

2.15 Clause 9 of the Bill amends Article 12 of the UK GDPR. SubSection 3 inserts into the UK GDPR new Article 12A. New Article 12A permits a controller to charge a reasonable fee for/or refuse to act on a request which is ***'vexatious or excessive'***. If passed into law, this will replace the current provision in Article 12 which permits a controller to refuse or charge a reasonable fee for ***'manifestly unfounded or excessive'*** requests. Of particular note is that, under Clause 9, ***'the resources available to the controller'*** is listed as a reason in which a request may be considered vexatious.

2.16 We note that the House of Lords Select Committee on the Constitution has commented on Clause 9 stating that, "The Government should provide assurances that Clause 9 will not significantly limit an individual's ability to access information about their personal data or information about how it is being collected and used"[14].

2.17 ECNI considers that should Clause 9 become law, the alteration of the standard by which a controller may refuse to accept a data request, and the addition of the factor that the controller may take its resources into account when considering whether a request is vexatious, may result in a diminution of the protections afforded to individuals under Article 12 of the EU GDPR prior to the end of the Brexit transition period.

2.18 In particular, we consider a diminution may arise due to the fact that the facility for a data controller to refuse a request is widened, thereby restricting the data subject's right to access the information and to understand how their personal data is processed and for what purposes.

---

[12] E-Privacy Directive 2002

[13] EU Data Protection and Law Enforcement Directive 2016

[14] House of Lords Select Committee on the Constitution 2nd Report 23-24, 25th January 2024 page 4

2.19 Article 12 (5) of the EU GDPR requires that the data search shall be free of charge: 'any actions taken under Articles 15 to 22 and 34 shall be provided free of charge.' It is only where the data requests are '*manifestly unfounded or excessive, in particular because of their repetitive character*' that the controller may either refuse the request or charge a fee.

2.20 The new test of *'vexatious'* is defined as situations in which there is an abuse of process, where the request is not made in good faith or is intended to cause distress. We consider these new features to be wider than the notion of a request being *'manifestly ill-founded*' because they relate to the reasons why the application is being made, rather than whether it is properly grounded or is a misconceived request for some reason. We would point to the ICO's Code of Access[15] which makes clear how central the word *'manifestly'* is to the assessment of whether the request is unfounded.

> "*This is not a simple tick list exercise that automatically means a request is manifestly unfounded. You must consider a request in the context in which it is made, and you are responsible for demonstrating that it is manifestly unfounded.*
>
> *Also, you should not presume that a request is manifestly unfounded because the individual has previously submitted requests which have been manifestly unfounded or excessive or if it includes aggressive or abusive language.*
>
> *The inclusion of the word "manifestly" means there must be an obvious or clear quality to it being unfounded. You should consider the specific situation and whether the individual genuinely wants to exercise their rights. If this is the case it is unlikely that the request will be manifestly unfounded."*

2.21 For the reasons outlined above, ECNI is concerned that Clause 9 may, if passed into law, lead to a diminution of the EU law underpinning in permitting a data controller to rely on its resources in deciding whether to process a data request and also in the replacement of the notion of 'manifestly unfounded' with 'vexatious'. We also consider that this Clause may interfere with

[15] ICO Guidance page 19

Article 8 (right to privacy) and Article 14 (right to non-discrimination) of the ECHR.

Clause 14 – Automated Decision Making

2.22 Automated decision-making is the process of making a decision solely by automated means, without any human involvement.

2.23 Article 22 of the UK GDPR does not divide the automatic processing of data into categories of decisions using 'sensitive data' and those using 'non-sensitive' data and limits the circumstances in which **solely automated decisions**, that have a **legal or similarly significant effect on individuals can be carried out to the following three situations:**

- **The decision is necessary for a contract.**
- **The decision is authorised by law.**
- **The decision is based on an individual's explicit consent.**[16]

This includes automated decisions based on 'profiling' which is defined in Article 4 of the UK GDPR as:

> *…….any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;*

2.24 The essential deviation from the EU GDPR standard is that Clause 14 if passed into law will replace Article 22 of the UK GDPR with new Articles 22A-D, which will mean that automatic processing of non-sensitive or non-personal data can be performed without being restricted by the three conditions set out in Article 22 UK GDPR.

[16] As set out in the ICO website: When can we carry out this type of processing? | ICO

2.25 We also note that Article 22D (1) would permit the Secretary of State to promulgate Regulations that would decide what automated decision-making processes involved human involvement and those that did not. It will permit the Secretary of State in those Regulations to state when "there is, or is not, to be taken to be meaningful human involvement in the taking of a decision in cases described in the regulations" [new Article 22D (1)].

2.26 Those situations that were designated as including meaningful human involvement would not be subject to the new automatic processing regime. We consider that this power has the potential to broaden the scope of data processing that would not be subject to the conditions and safeguards in the proposed amendments if a low standard is applied to what is 'meaningful human involvement'.

2.27 Of particular concern to ECNI is the implications of Clause 14 in relation to the area of 'profiling'. Clause 14 removes references to profiling from Article 22 of the UK GDPR. Although subject to some safeguards, Clause 14 of the Bill, if passed into law, will reframe Article 22 to generally allow automated decision-making, including profiling.

2.28 We note and share the concerns raised by the EHRC in its submission[17]that the proposed changes "*do not offer sufficient safeguards to protect individuals from unfair or discriminatory outcomes of automated decision-making".* In particular, we note the concern that "*Data used to help AI-based tools to make decisions may contain biases, or that the design of algorithms may reflect biases. This could lead to potentially discriminatory automated decision-making*." For example, an AI system used to monitor an employee's attendance record may not take account of factors such as disability or pregnancy. The NIHRC raises similar concerns.[18]

2.29 ECNI is also concerned that the proposed changes in relation to profiling could lead to discriminatory decision-making, if limited data sets that contain existing stereotypes and biases are relied upon. For example, it could give rise to a situation where individuals are assumed to have preferences and are, as a result,

[17] EHRC Briefing on Data Protection and Digital Information Bill for HoL Second Reading 15th December 2023(p.4)
[18] NIHRC Briefing on the Data Protection and Digital Information Bill January 2024 page 16 -21

disadvantaged in terms of the services and opportunities available to them.

2.30 For the reasons set out above, ECNI considers that Clause 14, in limiting the prohibition of automatic data processing to situations in which sensitive personal data is involved, and therefore permitting automatic processing in categories beyond that, albeit with safeguards, may result in a diminution of the protection provided by the EU GDPR prior to the end of the Brexit transition period.

Clauses 20 - Assessment of high-risk processing and 21 - Consulting the Commissioner prior to processing

2.31 Currently under Article 35 of the UK GDPR, a Data Protection Impact Assessment ("DPIA") must be performed whenever the processing of personal data is likely to pose a high risk to the rights and freedoms of natural persons. Section 35(7) provides that the DPIA assessment must include 'at least' the following:

(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

(c) an assessment of the risks to the rights and freedoms of data subjects; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

2.32 Furthermore, Article 36 of the UK GDPR provides that where a DPIA carried out under Article 35 indicates that processing would result *'in a high risk in the absence of measures taken by the controller to mitigate the risk,'* the controller shall consult the

Information Commissioner's Office ("ICO") prior to processing the data.

2.33 Clause 20 of the Bill, amends Article 35 of the UK GDPR and replaces the requirement to produce DPIAs with new **Assessments of High-Risk Processing.** Clause 20 also replaces the requirements currently set out in Article 35(7) with regard to DPIAs with new requirements. Assessment of High-Risk Processing will require the controller to produce a document which includes at least-

(a) a summary of the purposes of the processing,
(b) an assessment of whether the processing is necessary for those purposes,
(c) an assessment of the risks to individuals and
(d) a description of how the controller proposes to mitigate those risks.

The controller must also confirm in the document that s/he has complied with Article 35(7).

2.34 ECNI notes that **Assessments of High-Risk Processing** will have fewer requirements in terms of recording information on processing operations, purposes and proportionality checks[19] and that there will no longer be any references to *'legitimate interests'* and *'the rights and freedoms of data subjects'.* We also note that Clause 20 removes the current requirement under Article 35(2) for the controller to seek the advice of the data protection officer when carrying out the DPIA. In light of this, ECNI is concerned that the safeguards relating to the processing of high-risk data may be weakened if Clause 20 is passed into law in its current format.

2.35 Clause 21 of the Bill is also of concern to ECNI. As noted above, currently Article 36 of the UK GDPR requires the controller to consult the Information Commissioner's Office prior to processing high risk data in circumstances where mitigation measures are not

[19] We note that the HOL Select Committee has also raised a concern in respect of Clause 20 and states in its Report that *'The House may wish to seek further information from the Government as to whether an assessment of proportionality is no longer required when undertaking high risk processing, and if so, why."* (See House of Lords Select Committee on the Constitution 2nd Report 23-24, 25th January 2024 p.5)

possible. Clause 21, however, removes this requirement to consult the ICO with the result that this safeguard is lost.

Clause 128 and Schedule 11- Proposed new powers for the Department for Work and Pensions to access the bank accounts of benefit claimants.

2.36 Currently, Article 6 of the UK GDPR provides that data should be collected for specified, explicit and legitimate purposes. Clause 128 of the Bill introduces new Schedule 11, *"Power to require information for social security purposes".* The Clause will make amendments to the Social Security Administration (Northern Ireland) Act 1992 ("the 1992 Act") as well as its GB equivalent. It will allow the Department for Communities to obtain information about bank accounts into which social security benefit payments are made.

2.37 We note that there appear to be three changes or developments of significance arising from Clause 128: 1) the new Clause will allow more numerous checks than the present regime which were only on an individual basis; 2) these checks will take place where there is no suspicion of fraud, or no requirement for such a suspicion; 3) the checks could be regular and ongoing in order to identify patterns of use.

2.38 We note too that Clause 128 seeks to add a Section 115CB to the 1992 Act, to a list of other provisions, all of which authorise the collection of information from bodies like the Inland Revenue, from authorities administering housing benefit and other benefits, and from landlords and agents.

2.39 The Clause, in conferring a power to demand account information, specifically excludes the impact of Section 103B of the 1992 Act on the new Schedule 3B, i.e. where the detail of the account information notice regime is found. The Clause states as follows:

> "(6A) Nothing in this Section limits the powers conferred on the Department by Schedule 3B"

2.40 As Section 103B requires that no information may be sought unless there are reasonable grounds for suspecting that a person has committed a criminal offence [s.103B(2C)], and that no one is required to disclose information that may incriminate them

[s.103B(a)], the exclusion of these limits on the manner in which the proposed powers under new Schedule 3B are to be exercised, reduce the level of privacy protection provided by the proposed regime.

2.41 In essence, the Clause 128 power may be used regardless of whether there are reasonable grounds for suspecting that a person has committed a criminal offence, and in circumstances where someone might be required to self-incriminate.

2.42 We note that Lord Vaux of Harrowden,[20] in the second reading of the Bill in the House of Lords, expressed his concern that Clause 128, if passed into law, would introduce "*draconian rules that would enable the DWP to access welfare recipients' personal data by requiring banks and building societies to conduct mass monitoring without any reasonable grounds for suspecting fraudulent activity… this includes anyone receiving any kind of benefit, including low-risk benefits such as state pensions*" .

2.43 Similarly, the House of Lords Select Committee report[21] refers to Clause 128 and Schedule 11. They state that they are "*concerned by the breadth of these provisions, which empower the Government to demand access to individual bank accounts without grounds for suspicion. We recommend this power should be limited to circumstances in which the Secretary of State has reasonable grounds for inquiry".*

2.44 ECNI shares these concerns and considers that the proposed changes in Clause 128 and Schedule 11, if passed into law, may lead to unnecessary and disproportionate checks and interference with the right to privacy under Article 8 and Article 14 of the ECHR, given the risk that this could disproportionately impact people with certain protected characteristics and consider that this may therefore weaken the protections that were afforded to individuals under Article 6 of the EU GDPR prior to the end of the Brexit transition period.

[20] HOL Debate 19th December 2023

[21] House of Lords Select Committee on the Constitution 2nd Report 23-24, 25th January 2024

2.45 We note that the NIHRC have also raised concerns in respect of the following Clauses:

- Clause 25 and Schedule 5 (Transfer of data to third countries)
- Clauses 2, 5 and 6 (Processing of personal data for the purposes of research)
- Clause 17 (Senior responsible individual)
- Clause 18 (Duty to keep records)
- Clause 19 (Logging of law enforcement processing)

We support these concerns in respect of a possible diminution of rights in contravention of WF Article 2.

Consideration of compliance with Windsor Framework Article 2

2.46 The Commission is concerned that the Explanatory Notes to the Bill make no reference to any consideration being given to ensuring compliance with WF Article 2. The Commission has previously recommended that this should be the case regarding all relevant legislation. It is also of the view that compliance with WF Article 2 should be considered from the earliest stages in the development of policy and legislation.

2.47 The Explanatory Notes to the Bill and the Human Rights Impact Assessment do not contain a detailed consideration of the Bill's compliance with WF Article 2.

Data Protection (Fundamental Rights and Freedoms) (Amendment) Regulations 2023

2.48 ECNI also takes this opportunity to highlight its concerns in relation to recent Regulations passed by the Department for Science, Innovation and Technology in the data protection field and which extend to Northern Ireland.

2.49 As the UK Government is aware, the Data Protection (Fundamental Rights and Freedoms) (Amendment) Regulations 2023, which came into force on 31 December 2023, amended the

definition of fundamental rights and freedoms in the UK GDPR and the DPA 2018 to refer to those set out under the ECHR as opposed to the CFR.

2.50 The CFR applied in Northern Ireland up to 31 January 2020 and contains a specific right that governs the use of personal data. The EU GDPR was promulgated under, inter alia, Article 8 CFR, [see Recital 1]. We therefore consider that removing the CFR from the range of applicable fundamental rights in the DPA 2018 may diminish the rights protection provided on or before the end of the Brexit transition period. Further we consider there may also be a diminution of rights protections in the fact that an individual could not now rely on case law of the CJEU in relation to those rights. We therefore consider that these Regulations amount to a potential breach of WF Article 2.

3 Conclusion and Recommendations

3.1 In conclusion, the Commission is of the view that, were the above-mentioned changes proposed by the Bill to pass into law in its current form, the provisions may amount to a breach of the UK's obligations under WF Article 2.

4 Recommendations

Clause 9 - Subject Access Requests

4.1 We recommend that there should be no alteration to the standard by which a controller may refuse to accept a data request and that it should continue to be permitted only when the requests are '*manifestly unfounded or excessive."* Further, we recommend that *'the resources available to the controller'* should not be taken into account.

Clause 14 – Automated Decision Making

4.2 We consider that the changes to automated decision-making proposed in the Bill, if introduced, may reduce the safeguards that currently exist in Article 22 of the UK GDPR to protect individuals from the unfair and discriminatory outcomes of decisions which

may occur as a result of there being no meaningful human oversight. We therefore recommend retaining the protections in Article 22 of the UK GDPR.

Clauses 20 - Assessment of high-risk processing and 21 - Consulting the Commissioner prior to processing

4.3 We consider that Clause 20, if passed into law, may reduce the effectiveness of assessments in terms of evaluating the impact of data processing and that this could as a result increase the risk of violation of individuals' data rights. We consider that this risk may be further increased if Clause 21 is passed into law and the current requirement to consult the ICO is removed. We therefore recommend retaining the current protections in Article 35 and 36 of the UK GDPR.

Clause 128 - Proposed new powers for the Department for Work and Pensions to access the bank accounts of benefit claimants.

4.4 As noted above, ECNI has concerns that these powers may lead to unnecessary and disproportionate checks and interference with rights to privacy under Article 8 and Article 14 of the ECHR, given the risk that this could disproportionately impact people with certain protected characteristics.

We accordingly recommend removing Clause 128 from the Bill.

Consideration of compliance with Windsor Framework Article 2

4.5 The Commission recommends that the UK Government sets out, in detail, in the Explanatory Notes to the Bill, what consideration was given to compliance with Windsor Framework Article 2 in the development of the Bill. Any assessment of the proposals' compliance with WF Article 2 should not be limited to the impact of the proposals on the substantive rights but should also include the remedial dimensions of those rights.

Equality Commission

19 March 2024