



NORTHERN
IRELAND
HUMAN
RIGHTS
COMMISSION

**NIHRC Briefing on the Data Protection and
Digital Information Bill**

January 2024

Table of Contents

Summary of advice and recommendations	3
1.0 Introduction	5
2.0 Human Rights Framework	7
International and regional human rights standards	7
Article 2 of the Windsor Framework.....	8
EU Legal Framework for Data Protection	10
3.0 Data Protection and Digital Information Bill: Overview	13
Background to the Data Protection and Digital Information Bill	13
Changes to rights protections for data subjects	14
4.0 Automated Decision-Making: Clause 14	16
Powers of the Secretary of State.....	21
5.0 Transfer of data to third countries: Clause 25 and Schedule 5.....	22
Current standards	23
Proposed changes	24
6.0 Processing of personal data for the purposes of research: Clauses 2, 5 and 6	28
Current provisions	28
Proposed changes	29
7.0 Additional concerns	31

Summary of Advice and Recommendations

The NI Human Rights Commission advises and recommends:

- 2.8 that, as a fundamental right, the right to personal data protection would fall within the scope of “civil rights” under the Belfast (Good Friday) Agreement. Further, as an essential element of the right to respect for private and family life in Article 8 ECHR, any right to personal data protection afforded by EU law, by which the UK was bound on 31 December 2020, falls within the scope of the non-diminution commitment in Windsor Framework Article 2.**
- 2.9 that all EU law in force in NI on or before 31 December 2020 which underpins an ECHR right, falls within scope of the non-diminution commitment in Windsor Framework Article 2.**
- 2.22 that that the EU GDPR, the EU E-Privacy Directive and the EU Data Protection and Law Enforcement Directive all fall within scope of Windsor Framework Article 2.**
- 2.23 that the Secretary of State review and table any amendments required to ensure that none of the data protection rights contained in EU GDPR, the EU Data Protection Law Enforcement Directive and the EU E-Privacy Directive are weakened or removed via the Data Protection and Digital Information Bill.**
- 3.13 that the Secretary of State amends the Human Rights Memorandum to the Bill to set out in detail an assessment of the compliance of the Bill with Windsor Framework Article 2, including all relevant EU data protection laws, which, by virtue of Windsor Framework Article 2, continue to set standards in NI.**
- 4.16 that the Secretary of State reviews Clause 14, proposed Articles 22A-22C, of the Data Protection and Digital Information Bill and brings forward amendments as required**

to ensure no diminution of rights relating to automated decision-making under the UK GDPR.

4.20 that the Secretary of State reviews Clause 14, new Article 22D, and brings forward amendments as required to ensure no diminution of rights relating to automated decision-making as compared with UK GDPR.

4.21 that the Secretary of State provides a written assurance on how access to cross-border services requiring the free-flow of data between the UK and the EU will be protected in light of Clause 14 of the Bill on automated decision-making.

5.23 that the Secretary of State reviews Schedule 5 of the Bill and brings forward amendments as required to ensure no diminution of rights in NI relating to data transfer to third countries, measured against relevant EU GDPR standards.

6.10 that the Secretary of State reviews Clause 2 and brings forward amendments as required to ensure no diminution of rights in NI in relation to the processing of personal data for scientific purposes.

6.11 recommends that the Secretary of State reviews the provisions of Clause 5 of the Bill and brings forward amendments as required to avoid a divergence of data protection standards between the UK and the EU that might result in the free flow of data between the UK and the EU being compromised.

1.0 Introduction

1.2 The Northern Ireland Human Rights Commission (NIHRC), pursuant to section 69(1) of the Northern Ireland (NI) Act 1998, reviews the adequacy and effectiveness of law and practice relating to the protection of human rights in NI.¹ Pursuant to section 78A(1) of the NI Act 1998, the NIHRC is also mandated to monitor the implementation of Article 2(1) of the Windsor Framework, the UK Government commitment 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 as a result of the UK's withdrawal from the European Union (EU).²

1.3 The NIHRC bases its advice on the full range of internationally accepted human rights standards, including the European Convention on Human Rights (ECHR), as incorporated by the Human Rights Act 1998, and the treaty obligations of the Council of Europe (CoE) and the United Nations (UN). The right to one's personal data being protected is a recognised human right enshrined in international, regional, and domestic legislation. Relevant regional and international treaties in this context include:

- Universal Declaration of Human Rights 1948 (UDHR);³
- European Convention for the Protection of Human Rights and Fundamental Freedoms 1950 (ECHR);⁴
- UN International Covenant on Civil and Political Rights 1966 (UN ICCPR);⁵
- CoE Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981 (CoE Convention 108+);⁶
- UN Convention on the Rights of the Child 1989 (UN CRC).⁷

¹ Northern Ireland (NI) Act 1998.

² The Windsor Framework was formerly known as the Protocol on Ireland/Northern Ireland to the UK-EU Withdrawal Agreement and all references to the Protocol in this document have been updated to reflect this change. (See Decision No 1/2023 of the Joint Committee established by the Agreement on the Withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community of 24 March 2023 laying down arrangements relating to the Windsor Framework).

³ Ratified by the UK 1951.

⁴ Ratified by the UK 1951.

⁵ Ratified by the UK 1976.

⁶ Ratified by the UK 1987.

⁷ Ratified by the UK 1979.

1.4 In addition to these treaty standards, the following guidelines provide further guidance in respect of specific areas:

- CoE Committee of Ministers Recommendation No.R(99)5 for the protection of privacy on the Internet 1999;
- UN General Assembly Resolution 69/166, 'The right to privacy in the digital age', 18 December 2014.

1.5 The NIHRC further advises on the UK Government's commitment in Article 2 of the Windsor Framework to ensure there is no diminution of rights, safeguards and equality of opportunity in the relevant section of the Belfast (Good Friday) Agreement as a result of the UK's withdrawal from the EU. This is given effect in UK law by section 7A of the EU (Withdrawal) Act 2018.⁸ Section 6 of the NI Act 1998 prohibits the NI Assembly from making any law which is incompatible with Windsor Framework Article 2. Section 24 of the 1998 Act also requires all acts of NI Ministers and NI Departments to be compatible with Windsor Framework Article 2. As explained in section 2 of this submission, relevant EU measures in this context include:

- EU E-privacy Directive;⁹
- EU General Data Protection Regulation;¹⁰
- EU Data Protection Law Enforcement Directive;¹¹
- EU Processing of Data by Union Institutions Regulation.¹²

1.6 In accordance with its functions, the NIHRC provides the following advice on the Data Protection and Digital Information Bill. This submission will focus on particular areas of concern regarding the possibility of future divergence between the UK and the EU data protection standards that might result in a diminution of the

⁸ European Union (Withdrawal) Act 2018.

⁹ Directive 2009/136/EC, 'Amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws', 25 November 2009.

¹⁰ Regulation 2016/679/EU, 'Protection of natural persons with regard to the processing of personal data and on the free movement of such data (EU GDPR)', 27 April 2016.

¹¹ Directive 2016/680/EU, 'Protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data', 27 April 2016.

¹² Regulation 2018/1725/EU, 'Protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data', 23 October 2018.

relevant rights pursuant to Windsor Framework Article 2. The NIHRC will continue to monitor the implications of the cross-over between this Bill and other legislative developments. Currently we are aware of The Data Protection (Fundamental Rights and Freedoms) (Amendment) Regulations 2023 and will continue to explore any possible concerns arising. The NIHRC is willing to follow up with Peers to further discuss this advice or to provide advice on more specific elements.

2.0 Human Rights Framework

International and regional human rights standards

- 2.1 The protection of personal data is a fundamental human right and a key component of the right to privacy. The right to privacy is enshrined in Article 12 of the UDHR (protection from arbitrary interference with privacy).¹³ Article 12 stipulates that everyone has the right to be protected from arbitrary interference with their privacy, family, home or correspondence and from attacks to their honour and reputation. The right to privacy, which includes the right to data protection, is also enshrined in Article 17 of the ICCPR (protection from unlawful interference with privacy).¹⁴
- 2.2 The UN CRC further guarantees the same right to privacy, including protection of personal data, to children.¹⁵ Article 16 contains a commitment to no child being subjected to arbitrary or unlawful interference with their privacy, family, home or correspondence, and guarantees all children the right to be protected from such interferences or attacks.
- 2.3 The right to data protection is also contained in Article 8 of the ECHR on the right to respect for private life.¹⁶ Article 8 guarantees all individuals the right to respect for their private and family life, their home and correspondence, as well as freedom from interference by a public authority when exercising this right, except

¹³ Article 12, UN Declaration on Human Rights 1948.

¹⁴ Article 17, UN International Covenant on Civil and Political Rights 1976.

¹⁵ Article 16, UN Convention on the Rights of the Child 1989.

¹⁶ Article 8, European Convention of Human Rights 1950.

for a number of exceptions concerning public safety or the protection of the rights and freedoms of others.

- 2.4 The European Court of Human Rights (ECtHR) has also acknowledged that the protection of personal data is of fundamental importance to the realisation of the right to respect for private and family life, home and correspondence, as guaranteed by Article 8 of the Convention.¹⁷ Further, the ECtHR has clarified that “the mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8” of the ECHR.¹⁸
- 2.5 The UK is also a signatory to the CoE Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.¹⁹ Article 9 of the Convention provides for the rights of the data subject and in particular grants all individuals protection from being subjected to decisions made solely on the basis of automated data processing.²⁰

Article 2 of the Windsor Framework

- 2.6 Windsor Framework Article 2 requires the UK Government to ensure that no diminution of rights, safeguards and equality of opportunities contained in the relevant part of the Belfast (Good Friday) Agreement 1998 occurs as a result of the UK’s withdrawal from the EU. This includes an obligation to “keep pace” with any changes made by the EU to the six Annex 1 Equality Directives which improve on the minimum levels of protection available, on or after 1 January 2021.²¹

¹⁷ *Satakunnan Markkinapörssi Oy and Satamedia Oy v Finland* (2015) ECHR 713, at para 137.

¹⁸ *S and Mapers v UK* (2008) App No 30562/04 and 30566/04, at para 67.

¹⁹ CoE Convention for the Protection of Individuals with Regard to the Processing of Personal Data 1981.

²⁰ Article 9, CoE Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981.

²¹ Directive 2000/43/EC, ‘EU Council Directive on Implementing the Principle of Equal Treatment between Persons Irrespective of Racial or Ethnic Origin’, 29 June 2000; Directive 2000/78/EC, ‘EU Council Directive on Establishing a General Framework for Equal Treatment in Employment and Occupation’, 27 November 2000; Directive 2004/113/EC, ‘EU Council Directive on Implementing the Principle of Equal Treatment between Men and Women in the access to and supply of goods and Services’, 13 December 2004; Directive 2006/54/EC, ‘EU Council Directive on the Implementation of the Principle of Equal Opportunities and Equal Treatment of Men and Women in Matters of Employment and Occupation’, 5 July 2006; Directive 2010/41/EU, ‘EU Parliament and EU Council Directive on the Application of the Principle of Equal Treatment between Men and Women Engaged in an Activity in a Self-employed Capacity’, 7 July 2010; Directive 79/7/EEC, ‘EU Council Directive on the Progressive Implementation of the Principle of Equal Treatment for Men and Women in Matters of Social Security’, 19 December 1978.

- 2.7 The Belfast (Good Friday) Agreement chapter entitled 'Rights, Safeguards and Equality of Opportunity' begins with a section on "Human Rights" containing a general commitment to the "civil rights and religious liberties of everyone in the community" and a non-exhaustive list of rights "affirmed in particular", as well as a commitment to the incorporation of the ECHR with direct access to the courts and remedies for breach. It is the NIHRC's view that, read in the context of the additional pledges on rights within this chapter, the general commitment of the Belfast (Good Friday) Agreement signatories to the range of rights referenced within the chapter must be understood as embracing, as a minimum, those rights set out in the ECHR.²²
- 2.8 **The NIHRC considers that, as a fundamental right, the right to personal data protection would fall within the scope of "civil rights" under the Belfast (Good Friday) Agreement. Further, as an essential element of the right to respect for private and family life in Article 8 ECHR, any right to personal data protection afforded by EU law, by which the UK was bound on 31 December 2020, falls within the scope of the non-diminution commitment in Windsor Framework Article 2.**
- 2.9 **The NIHRC considers that all EU law in force in NI on or before 31 December 2020 which underpins an ECHR right, falls within scope of the non-diminution commitment in Windsor Framework Article 2.**
- 2.10 The definition of EU law within the UK-EU Withdrawal Agreement includes the EU Treaties, which encompasses the EU Charter of Fundamental Rights.²³ UK Courts have recently confirmed the continuing relevance of the EU Charter of Fundamental Rights for the interpretation of obligations arising under the UK-EU Withdrawal Agreement.²⁴

²² NI Human Rights Commission and Equality Commission for NI, 'Working Paper: The Scope of Article 2(1) of the Ireland/Northern Ireland Protocol' (NIHRC and ECNI, 2022).

²³ Article 2(a)(i), UK-EU Withdrawal Agreement.

²⁴ See *Angesom's (Aman) Application and in the matter of a decision by the Secretary of State for the Home Department and the Human Rights Commission and the Equality Commission Intervening* [2023] NIKB 102; and *Secretary of State for Work and Pensions and AT and Advice on Individual Rights in Europe (AIRE) Centre and Independent Monitoring Authority for the Citizens' Rights Agreements intervening* [2022] UKUT 330 (ACC).

EU Legal Framework for Data Protection

- 2.11 The right to data protection is enshrined in Article 7 and Article 8 of the EU Charter of Fundamental Rights. Article 7 of the EU Charter of Fundamental Rights corresponds to Article 8 of the ECHR and guarantees the right to respect to private life, including correspondence, as well as protection from interference with these rights by a public authority except in limited circumstances. Article 8 of the EU Charter of Fundamental Rights guarantees everyone the right to protection of their personal data and requires that personal data must be processed fairly, for specified purposes and on the basis of consent or some other legitimate basis laid down by law.²⁵ All relevant EU data protection rules must be interpreted in light of these obligations.
- 2.12 The right to data protection is given effect in a number of EU measures. The main EU law laying down rules for the protection of personal data is the EU General Data Protection Regulation (EU GDPR).²⁶ The EU GDPR is clear that “the protection of natural persons in relation to the processing of personal data is a fundamental right”.²⁷
- 2.13 The EU GDPR sets out in detail the rights of data subjects (Chapter III); the obligations to protect fundamental rights placed on those processing personal data (Chapter IV); and the principles that govern the handling of personal data (Chapter II), which include lawfulness, fairness and transparency.²⁸
- 2.14 The EU GDPR also outlines the duty of each Member State to provide for an independent supervisory authority responsible for monitoring the application of the Regulation (Chapter VI). It sets out the means for ensuring the cooperation, consistency and mutual assistance between supervisory authorities in the EU tasked with

²⁵ Article 8(2), EU Charter of Fundamental Rights 2009.

²⁶ Regulation 2016/679/EU, 'Regulation of the of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data', 27 April 2016.

²⁷ Recital 1, Regulation 2016/679/EU, 'Regulation of the European Parliament and Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data', 27 April 2016.

²⁸ Recital 39, Regulation 2016/679/EU, 'Regulation of the of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data', 27 April 2016.

protecting individuals' personal data (Chapter VII). EU GDPR also outlines the provisions for remedies, liability and penalties for breaches of the rules on data protection (Chapter VIII), among other provisions.

- 2.15 As a Regulation, the EU GDPR is a binding legislative act that must be applied in its entirety across the EU in all Member States. Regulations are directly applicable without the need for them to be incorporated in domestic law.
- 2.16 The UK further implemented the EU GDPR in domestic law with the Data Protection Act 2018. Section 1(2) of the Data Protection Act 2018 states that most processing of data is governed by the EU GDPR.²⁹ The UK High Court has confirmed that the UK GDPR is the retained version of the EU GDPR with amendments made to secure its political effectiveness,³⁰ read together with the Data Protection Act 2018.³¹ Currently, the UK GDPR aligns with the EU GDPR.
- 2.17 The NIHRC considers that the EU GDPR falls within the scope of Windsor Framework Article 2 and any legislative proposal that seeks to amend the data protection regime in Northern Ireland must comply with the principle of non-diminution under Windsor Framework Article 2.³²
- 2.18 Further to the EU GDPR, the EU has adopted additional laws that set out rules regarding the protection of personal data in specific contexts. These include the EU Data Protection Law Enforcement

²⁹ Section 3(10), Data Protection Act 2018.

³⁰ Data Protection, Privacy and Electronic Communications (Amendments, etc) (EU Exit) Regulations 2019 (SI 2019/419).

³¹ *The3million & Open Rights Group v Secretary of State for the Home Department* [2023] EWHC 713 (Admin), at para 9.

³² NI Human Rights Commission and Equality Commission for NI, 'Working Paper: The Scope of Article 2(1) of the Ireland/Northern Ireland Protocol' (NIHRC and ECNI, 2022), at 55 and at 61.

Directive,³³ the EU E-Privacy Directive³⁴ and rules regarding the processing of personal data by EU bodies and institutions.³⁵

2.19 The EU E-Privacy Directive provides harmonisation across the EU Member States in terms of the requirement to ensure an equivalent level of protection of fundamental rights and freedoms, in particular the right to privacy and the right to confidentiality, with respect to the processing of personal data in the electronic communications sector.³⁶ Alongside the EU GDPR, the E-Privacy Directive protects the right to data protection by providing rights holders with specific privacy rights in the context of marketing calls, emails, cookies and similar technologies. The UK transposed the obligations via provisions including the Privacy and Electronic Communications (EC Directive) Regulations 2003. As the EU E-Privacy Directive lays down rules for the protection of the fundamental right to privacy in specific contexts, the NIHRC considers it to fall within the relevant chapter of the Belfast (Good Friday) Agreement and therefore within scope of Windsor Framework Article 2.

2.20 The EU Data Protection and Law Enforcement Directive lays down safeguards for the protection of personal data in the context of law enforcement that are without prejudice to any of the EU GDPR rules, but instead extends them to the field of law enforcement. The UK took additional steps to incorporate the EU Data Protection and Law Enforcement Directive into UK law via Part 3 of the Data Protection Act 2018, which sets out rules on the processing of personal data for criminal law enforcement purposes.

³³ Directive 2016/680/EU, 'Regulation of the of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data', 27 April 2016.

³⁴ Directive 2009/136/EC, 'Directive of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws', 25 November 2009.

³⁵ Regulation 2018/1725/EU, 'Regulation of the of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data', 23 October 2018.

³⁶ Recital 51, Directive 2009/136/EC, 'Directive of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws', 25 November 2009.

- 2.21 For capacity reasons, this submission focuses on the EU GDPR in particular and does not include analysis on the extent to which the Data Protection and Digital Information Bill complies with data protection rules and safeguards for rights holders contained in the other EU measures outlined above.
- 2.22 **The NIHRC advises that that the EU GDPR, the EU E-Privacy Directive and the EU Data Protection and Law Enforcement Directive all fall within scope of Windsor Framework Article 2.**
- 2.23 **The NIHRC recommends that the Secretary of State review and table any amendments required to ensure that none of the data protection rights contained in EU GDPR, the EU Data Protection Law Enforcement Directive and the EU E-Privacy Directive are weakened or removed via the Data Protection and Digital Information Bill.**

3.0 Data Protection and Digital Information Bill: Overview

Background to the Data Protection and Digital Information Bill

- 3.1 The two main pieces of legislation governing data protection in the UK are the UK GDPR and the Data Protection Act 2018. The full name for “UK GDPR” is ‘Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (United Kingdom General Data Protection Regulation)’. While the abbreviated title was changed, the substance of the legislation and the protections it offers are largely unchanged to date.
- 3.2 The Data Protection and Digital Information Bill aims to simplify and update current UK data protection framework whilst maintaining data protection standards.³⁷ The Bill has been presented as the UK Government’s proposals to address those aspects of data protection

³⁷ Department of Science, Innovation and Technology, ‘Data Protection and Digital Information (No 2) Bill - Explanatory Notes’ (DSIT, 2023), at para 1.

in the UK that are seen as unnecessary burdens to businesses, private companies, researchers and the consumers themselves. The Bill aims to move data protection in the UK away from a “box ticking” compliance regime and achieve clarity, flexibility and a streamlined approach.³⁸

- 3.3 To achieve these aims, the Bill establishes a legal framework for the provision of digital verification services in the UK (Part 2 of the Bill). It proposes changes to the oversight of police use of surveillance cameras and biometrics (Part 5 of the Bill). It further proposes changes to the legal framework on the registration of births and deaths (Part 4 of the Bill). The Bill also extends the powers under Section 35 of the Digital Economy Act 2017 (disclosure of information to improve public service delivery) to private businesses. In addition, the Bill makes amendments to the data sharing framework in the context of the health and social care system (Part 4 of the Bill), among other provisions.
- 3.4 In light of the breadth of the Bill, the focus of this submission is on the proposed changes to the data protection legal framework in the UK contained in Part 1 of the Bill, in particular the rules and safeguards on automated decision-making; onward transfers of data to third countries and international organisations; and the processing of personal data for the purposes of research.

Changes to rights protections for data subjects

- 3.5 In Part 1 (Data Protection), the Bill proposes changes to the UK GDPR, which currently aligns with the EU GDPR, and to the Data Protection Act 2018 that aim to offer organisations greater flexibility on how to comply with certain aspects of the data protection legislation and improve the clarity of the legal framework on data protection.³⁹
- 3.6 The amendments to the UK GDPR that the Bill proposes concern the rules around how researchers can use online personal data for their

³⁸ Department of Science, Innovation and Technology, ‘Data Protection and Digital Information (No 2) Bill – Explanatory Notes’ (DSIT, 2023), at para 12.

³⁹ Department of Science, Innovation and Technology, ‘Data Protection and Digital Information (No 2) Bill – Explanatory Notes’ (DSIT, 2023), at para 2.

work;⁴⁰ the rules on how organisations must demonstrate they are complying with data protection principles under the UK GDPR;⁴¹ and the rules on how organisations can respond to vexatious or excessive requests for information, among other provisions.⁴²

- 3.7 The Bill is also proposing amendments to Part 3 and 4 of the Data Protection Act 2018, which further enforced the EU GDPR in UK domestic law. These amendments concern the rules on law enforcement processing and intelligence service processing.⁴³
- 3.8 Under the UK GDPR, rights holders have the right to access information about their personal data (Section 2, UK GDPR). Rights holders also have the right to rectification and erasure of any inaccurate personal data or any personal data they would like to be “forgotten”, in other words no longer available online (Section 3, UK GDPR). Rights holders can also avail of the right to be protected from the impact of decisions made solely by the automated processing of their data (Section 4, UK GDPR). All the rules put in place to protect individuals’ rights can only be deviated from under permitted restrictions (Section 5, UK GDPR).
- 3.9 This submission will provide examples of where the NIHRC has concerns that rights relating to data protection might be weakened if the Bill should pass in its current form. As outlined in section 2 of this briefing, the NIHRC considers that a diminution of fundamental rights in this area may breach the UK Government’s international treaty commitment in Windsor Framework Article 2.
- 3.10 In addition, consideration must be given to how the Data Protection and Digital Information Bill might impact the data adequacy agreements between the UK and the EU. After the UK’s exit from the EU, the free flow of data between the EU and the UK is currently made possible by the power of two data adequacy decisions by the EU which recognise the “essentially equivalent level of protection” in

⁴⁰ Clause 2 (Meaning of research and statistical purposes), Data Protection and Digital Information Bill.

⁴¹ Clause 5 (Lawfulness of processing) and Clause 6 (The purpose limitation), Data Protection and Digital Information Bill.

⁴² Clause 8 (Vexatious or excessive requests by data subjects), Data Protection and Digital Information Bill.

⁴³ Clause 21 (Law enforcement processing and codes of conduct) and Clause 27 (Joint processing by intelligence services and competent authorities), Data Protection and Digital Information Bill.

the UK and the EU.⁴⁴ The data adequacy decisions are respectively under the EU GDPR⁴⁵ and under the EU Data Protection Law Enforcement Directive.⁴⁶

- 3.11 The data adequacy decisions are vital for ensuring that data can continue to flow freely between the UK and the EU. This is particularly important for data flows between NI and Ireland, for the purposes of facilitating the cross-border aspects of health, education, justice, policing, tourism and environmental protection on the island of Ireland.⁴⁷ This submission will provide examples of where the NIHRC has concerns that the Bill might result in such divergences which could impact on the data adequacy decisions.
- 3.12 Although the UK Government has prepared a Human Rights Memorandum on the Bill's compliance with the ECHR, the NIHRC is concerned that consideration of compliance with Windsor Framework Article 2 is missing.⁴⁸
- 3.13 **The NIHRC recommends that the Secretary of State amends the Human Rights Memorandum to the Bill to set out in detail an assessment of the compliance of the Bill with Windsor Framework Article 2, including all relevant EU data protection laws, which, by virtue of Windsor Framework Article 2, continue to set standards in NI.**

4.0 Automated Decision-Making: Clause 14

⁴⁴ EU Commission 'Press Release: Data protection: Commission adopts adequacy decisions for the UK', 28 June 2021.

⁴⁵ Commission Implementing Decision (EU) 2021/1772, pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom, 28 June 2021.

⁴⁶ Commission Implementing Decision (EU) 2021/1773, pursuant to Directive (EU) 2016/680 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom, 28 June 2021.

⁴⁷ The NIHRC has commissioned several research projects that describe the challenges and complexities of shared services, facilities and resources on the island of Ireland for health, justice and workers' rights, among other issues. The free flow of data is a key condition underpinning the all-island aspects of life in NI. See NIHRC, 'Brexit and the Implications for Justice Co-operation' (NIHRC, 2019); Tamara Hervey, 'Brexit, Health and its potential impact on Article 2 of the Ireland/Northern Ireland Protocol' (NIHRC, 2022); Sylvia de Mars and Charolotte O'Brien, 'Frontier workers and their Families: Rights after Brexit' (NIHRC, 2023).

⁴⁸ Department of Science, Innovation and Technology, 'Policy Paper: Data Protection and Digital Information (No 2) Bill: European Convention on Human Rights Memorandum' (DSIT, 2023).

- 4.1 Automated decision-making is the process of making a decision solely by automated means, without any human involvement.⁴⁹ Such decisions can be based on factual data about a data subject, as well as on data from digitally created profiles of data subjects. The process of creating a digital profile of a data subject is called “profiling”.⁵⁰ Profiling is the automated processing of personal data (personal data like internet searches histories, buying habits, lifestyle and behavioural data, etc). This is then used to evaluate certain aspects of an individual’s personality or to make predictions and decisions about them (for example, to analyse or predict an individual’s performance at work, economic situation or health).⁵¹
- 4.2 Automated decision-making can have a real and detrimental effect on the rights and experiences of rights holders. A recent report on the cross-border transfer of personal data on the island of Ireland highlighted an example of such impact: the A-level grading algorithm scandal.⁵² In 2020, A-level grades were determined in a problematic way by an algorithm, resulting in 40% of students receiving lower grades than what they anticipated. The data processed by the algorithm when deciding what grade to award was not sensitive personal data. It was based on historic academic performances of the schools and the school rankings of the students. Yet, the decision had a profound negative effect on the students whose grades were lower than the predictions.⁵³
- 4.3 The provisions protecting rights holders from automated decision-making in the UK GDPR currently mirror the EU GDPR. The European Data Protection Board, which is the independent EU body overseeing the consistent application of EU GDPR throughout the EU, has noted in their Opinion on the EU Commission data adequacy

⁴⁹ EU GDPR provides a definition of automated decision-making in Article 22 (Automated individual decision-making, including profiling). See Article 22(1), Regulation 2016/679/EU, ‘Protection of natural persons with regard to the processing of personal data and on the free movement of such data (EU GDPR)’, 27 April 2016.

⁵⁰ EU GDPR provides a definition of profiling in Article 4 (Definitions). See Article 4(4), Regulation 2016/679/EU, ‘Protection of natural persons with regard to the processing of personal data and on the free movement of such data (EU GDPR)’, 27 April 2016.

⁵¹ Information Commissioner’s Office, available at <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/automated-decision-making-and-profiling/what-is-automated-individual-decision-making-and-profiling/>

⁵² Orla Lynskey, Maria Helen Murphy and Katherine Nolan, ‘Understanding the risks to cross border transfer of personal data: EU-UK Data Adequacy’ (LSA and MU, 2023), at 75.

⁵³ Daan Kolkman, ‘What the world can learn from the UK’s A-level grading fiasco’, *London School of Economics blog*, 26 August 2020.

decision between the UK and EU that this is one of the areas where there is currently a “strong alignment” between the two regimes.⁵⁴

- 4.4 Article 22(1), UK GDPR, which currently aligns with the EU GDPR, recognises the right of a data subject not to be subject to a decision based solely on automated processing, including profiling, which produces a legal effect concerning the data subject or has a similarly significant effect on the data subject.⁵⁵
- 4.5 Three exemptions are set out in Article 22(2), firstly in relation to a decision necessary for a contract between the data subject and the data controller. Second, a decision based solely on automated processing of data can also be permitted if the decision is allowed by law, as long as it still in accordance with the safeguards laid down in law to protect data subjects’ rights, freedoms and legitimate interests. The third exemption is for decisions based on the explicit consent of the data subject.⁵⁶ Where one of these exemptions is utilised, the data controller is still under a duty to adopt measures to safeguard the rights and freedoms of the data subject.⁵⁷
- 4.6 The UK GDPR currently protects individuals from automated decision-making based on all types of data, not just personal or sensitive data.
- 4.7 Clause 14 of the Bill (Automated decision-making) is intended to replace Article 22, UK GDPR with new proposed articles 22A-22D which will amend the rules on automated decision-making.

⁵⁴ European Data Protection Board, ‘Opinion 14/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the UK’ (EDPS, 2021), at para 8.

⁵⁵ Article 22 (1), Regulation 2016/679/EU, ‘Regulation of the European Parliament and Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data’, 27 April 2016.

⁵⁶ All the exemptions are under Article 22(2), Regulation 2016/679/EU, ‘Regulation of the European Parliament and Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data’, 27 April 2016.

⁵⁷ Article 22(3), Regulation 2016/679/EU, ‘Regulation of the European Parliament and Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data’, 27 April 2016.

- 4.8 Article 4 (definitions), UK GDPR currently aligns with the EU GDPR and defines personal data as any information relating to an identified or identifiable natural person.⁵⁸
- 4.9 The UK GDPR and the EU GDPR further align in their definition of special categories of personal data. These special categories of personal data are data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data and biometric data for the purpose of uniquely identifying a natural person, health data and data concerning a person's sex life or sexual orientation. Where such categories of personal data are engaged, prohibitions on processing apply.⁵⁹
- 4.10 Currently, the UK GDPR, aligned with the EU GDPR, prohibits the processing of special categories of personal data, unless one of the exceptions applies.⁶⁰ Article 9, UK GDPR also contains a number of exceptions to the general rule of prohibiting the processing of special categories of personal data, including if the data subject has given explicit consent for the processing of personal data;⁶¹ or if the processing is needed for reasons of substantial public interest.⁶² In addition, processing of special categories of data has to be legitimate, proportionate and mindful of data subjects' fundamental rights and interests.⁶³
- 4.11 The Data Protection and Digital Information Bill proposes a significant change to the current protection from automated decision-making. Clause 14 of the Bill (Automated decision-making) is intended to replace Article 22, UK GDPR with new proposed articles 22A-22D and will allow fully automated decision-making

⁵⁸ Article 4 (1), Regulation 2016/679/EU, 'Regulation of the European Parliament and Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (EU GDPR)', 27 April 2016.

⁵⁹ Article 9(1), Regulation 2016/679/EU, 'Regulation of the European Parliament and Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (EU GDPR)', 27 April 2016.

⁶⁰ Article 9(1), Regulation 2016/679/EU, 'Regulation of the European Parliament and Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (EU GDPR)', 27 April 2016.

⁶¹ Article 9(2)(a), Regulation 2016/679/EU, 'Regulation of the European Parliament and Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (EU GDPR)', 27 April 2016.

⁶² Article 9(2)(g), Regulation 2016/679/EU, 'Regulation of the European Parliament and Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (EU GDPR)', 27 April 2016.

⁶³ Recital 39, Regulation 2016/679/EU, 'Regulation of the European Parliament and Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (EU GDPR)', 27 April 2016.

based on the processing of the broader category of personal data. Automated decision-making based on the narrower special categories of personal data is still restricted. By contrast, the EU GDPR prohibits automated decision-making, unless one of the permissible exceptions is engaged, without making a distinction between the broader personal data and the narrower special category of personal data.

- 4.12 Proposed Article 22B retains some safeguards which align with the EU GDPR safeguards regarding automated decision-making. For example, the protection from significant decisions based entirely or partially on processing special categories of personal data can still only be made if one of two conditions is met, the first condition being that the individual has given explicit consent and second condition being that it is necessary for a contract between the data subject and controller or that it is required or authorised by law.⁶⁴ These exceptions are in alignment with the current safeguards offered by the EU GDPR.
- 4.13 However, by limiting the general prohibition of automated decision-making only to the more narrowly defined special categories of personal data, the Data Protection and Digital Information Bill essentially limits some of the important protections data subjects currently enjoy, albeit retaining some of the safeguards.
- 4.14 Special category data is a narrow category of personal data about the data subject. Decisions based exclusively by automated processing of other types of personal data, which are not considered special categories of personal data the same way a person's race or sexual orientation would be, could still have significant effects on the data holder, hence why automated decision-making is generally prohibited by the GDPR.
- 4.15 Limiting the protection from automated decision-making only to the processing of sensitive personal data is a weakening of the current standard of data subject rights protection and therefore engages the no diminution of rights commitment under Windsor Framework Article 2.

⁶⁴ New Article 22B(2) and (3), in Clause 14, Data Protection and Digital Information Bill.

4.16 The NIHRC recommends that the Secretary of State reviews Clause 14, proposed Articles 22A-22C, of the Data Protection and Digital Information Bill and brings forward amendments as required to ensure no diminution of rights relating to automated decision-making under the UK GDPR.

Powers of the Secretary of State

4.17 Article 22D would grant the Secretary of State a wide margin of appreciation relating to automated decision-making, including the power to deem by regulations whether or not a decision with an effect on the data subject been made solely by automated means or if it has had human involvement.⁶⁵ The Secretary of State can also determine if a decision has had an effect on the data subject which is similarly significant to a legal effect.⁶⁶ The Secretary of State would further be empowered to amend the provisions of Article 22, UK GDPR, which is currently aligned with the EU GDPR, by deciding what does or does not satisfy the safety requirements around automated decision-making and can add, vary or omit safeguards granted to the data subject.

4.18 Further to the issue outlined above, the NIHRC is concerned that the effect of proposed Article 22D may be to further weaken the safeguards for data subjects contained in Article 22, UK GDPR, currently aligned with the EU GDPR.

4.19 In addition, the NIHRC is concerned that the resulting divergence in levels of protection from automated decision-making, between the UK and the EU, may put enormous pressure on the current data adequacy agreement between the UK and the EU. This in turn could have a detrimental effect on NI in particular, as the enjoyment of some rights, such as access to all-island healthcare, is facilitated by the ability to share data freely on a North-South basis.

4.20 The NIHRC recommends that the Secretary of State reviews Clause 14, new Article 22D, and brings forward amendments

⁶⁵ New Article 22D(1), UK GDPR in Clause 11, Data Protection and Digital Information Bill.

⁶⁶ New Article 22D(2), UK GDPR in Clause 11, Data Protection and Digital Information Bill.

as required to ensure no diminution of rights relating to automated decision-making as compared with UK GDPR.

- 4.21 **The NIHRC recommends that the Secretary of State provides a written assurance on how access to cross-border services requiring the free-flow of data between the UK and the EU will be protected in light of Clause 14 of the Bill on automated decision-making.**

5.0 Transfer of data to third countries: Clause 25 and Schedule 5

- 5.1 The rules on the transfer of personal data to third countries is at the core of the data protection regimes in both the EU and the UK. Currently the two regimes are in substance identical.⁶⁷ A key condition of the continuation of the data adequacy agreement between the UK and the EU is the UK continuing to uphold the current UK GDPR standards on international transfer of personal data.⁶⁸
- 5.2 The European Data Protection Board has noted in their opinion on the adequacy agreement between the UK and the EU that in order for the adequacy agreement to continue the UK and the EU must offer the same level of protection to data users. Therefore, both the UK's legislation on processing data that has been transferred to the UK and the UK legislation on onward transfers of data to third countries must be "essentially equivalent" to that of the EU.⁶⁹
- 5.3 The Data Protection and Digital Information Bill proposes changes to the current regulation of onward transfers of data to third countries that could have implications for both data subjects' rights and for the adequacy agreements currently in place between the UK and the EU.

⁶⁷ Commission Implementing Decision (EU) 2021/1772, pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom, 28 June 2021, at para 75.

⁶⁸ Commission Implementing Decision (EU) 2021/1772, pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom, 28 June 2021, at para 74.

⁶⁹ European Data Protection Board, 'Opinion 14/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the United Kingdom' (EDPB, 2021), at para 15.

Current standards

- 5.4 The transfer of data to third countries and international organisations is governed by Chapter V of the UK GDPR, which is currently aligned with the EU GDPR.⁷⁰ Article 44, UK GDPR is the main provision which provides for transfers of personal data to take place only if the conditions laid down in the UK GDPR for the protection of the rights of data subjects are complied with.⁷¹ Article 6, UK GDPR sets out rules for the lawful processing of data, and Article 9, UK GDPR prohibits special categories of sensitive personal data from being processed.
- 5.5 Currently Article 45, UK GDPR allows for transfers of personal data to third countries and international organisations to take place without specific authorisation if the transfer is based on adequacy regulations (in other words, an adequacy decision by the Government to share data with a third country or international organisation which is deemed to have the same style of data protection as the UK). When assessing the adequacy of the level of data protection in the third country or international organisation for the purposes of making an adequacy decision, the Secretary of State must take into consideration “the rule of law, respect for human rights and fundamental freedoms”, among other elements, in the third country.⁷²
- 5.6 When the transfer of data to a third country or an international organisation happens without an adequacy decision in place, data can only be shared if appropriate safeguards of data subjects’ rights are put in place and if effective legal remedies for data subjects are made available.⁷³

⁷⁰ Articles 44-49, Regulation 2016/679/EU, ‘Regulation of the European Parliament and Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data’, 27 April 2016.

⁷¹ Article 44, Regulation 2016/679/EU, ‘Regulation of the European Parliament and Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data’, 27 April 2016.

⁷² Article 45(2), Regulation 2016/679/EU, ‘Regulation of the European Parliament and Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (UK GDPR)’, 27 April 2016.

⁷³ Article 46, Regulation 2016/679/EU, ‘Regulation of the European Parliament and Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (UK GDPR)’, 27 April 2016.

- 5.7 Article 49 currently contains derogations from these rules for specific situations, which would allow the transfer of data to third countries or international organisations to take place without an adequacy decision under Article 45, UK GDPR, and without the safeguards pursuant to Article 46, UK GDPR. Article 49 further allows for onward transfers of data even if none of the derogations for specific situations are applicable, subject to a range of conditions.⁷⁴
- 5.8 Article 18(1) and (2) of the Data Protection Act 2018 empowers the Secretary of State to specify by regulation, the circumstances in which data can be transferred to third countries or international organisations under Articles 45 and 49, UK GDPR, subject to the safeguards referenced above.

Proposed changes

- 5.9 The Bill seeks to make changes to the legal framework on onward transfers of data. Clause 25 and Schedule 5 of the Bill (Transfer of data to third countries) replace and amend provisions in Chapter V, UK GDPR, concerning the general principles for transfers, the approval of transfers by regulation and a data protection test to safeguard the rights of the data subject.
- 5.10 Whilst the current UK GDPR provisions on onward transfers of data under Articles 46 (appropriate safeguards) and 49 (derogations) of UK GDPR will remain largely the same, Schedule 5 replaces the provisions under Article 45 (adequacy agreements) with new Articles 45A and 45B that appear to grant the Secretary of State wider discretion, in deciding whether transfers of personal data can take place.⁷⁵
- 5.11 Proposed Article 45A(1) allows the Secretary of State to approve by regulations transfers of data to third countries and international organisations. Article 45A(2), however, also requires the Secretary of State to abide by the test in new Article 45B to determine whether the third country or international organisation that data is

⁷⁴ Article 49(1), Regulation 2016/679/EU, 'Regulation of the European Parliament and Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (UK GDPR)', 27 April 2016.

⁷⁵ New Articles 45A and 45B, UK GDPR in Schedule 5, Data Protection and Digital Information Bill.

to be transferred to provides an adequate level of protection of data subjects' rights.⁷⁶

5.12 New Article 45B states that the data protection test would be met for transfers if the standard of the protection provided "is not materially lower" in the third country (or the international organisation) than the standard of the protection provided under relevant UK law and sets out a non-exhaustive list of factors to be considered. Under current provisions, the powers are subject to the conditions in Article 45 being met, as well as a periodic review of the protections.⁷⁷

5.13 In exercising these powers, both the test contained in current Article 45, UK GDPR, and the new test in proposed Article 45B of the Bill require the Secretary of State to take into consideration the rule of law and respect for human rights in the third country or organisation; the existence of data protection rules, including rules on onward transfers; the existence of an authority responsible for protecting the rights of data subjects with adequate enforcement powers; the relevant international obligations of the country or organisation; and other relevant legislative frameworks put in place.

5.14 What is missing from Article 45B is the consideration of "relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law" in the third country or organisation; how public authorities can access personal data; and how this legislation has been implemented including case-law.⁷⁸ New Article 45B also provides for additional consideration of "the constitution, traditions and culture of the country or organisation".

5.15 Furthermore, the requirement to take into account of:

⁷⁶ Article 45, Regulation 2016/679/EU, 'Regulation of the European Parliament and Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data', 27 April 2016.

⁷⁷ See sections 17A and 17B, Data Protection Act 2018 for Secretary of State's powers and duties in this regard.

⁷⁸ Article 45(2)(b), Regulation 2016/679/EU, 'Regulation of the European Parliament and Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (EU GDPR)', 27 April 2016.

“the existence and *effective functioning*⁷⁹ of one or more *independent* supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including *adequate enforcement rules*”,

is replaced with a duty to consider:

“the existence, and powers, of *an authority* responsible for enforcing the protection of data subjects with regard to the processing of personal data” and “arrangements for judicial and non-judicial redress”.⁸⁰

- 5.16 The NIHRC is concerned that the proposed Article 45B test could potentially lower data protection standards by requiring less rigorous considerations than the ones currently provided by the UK GDPR and could pull it out of alignment with the EU GDPR. In particular, the lack of consideration of how public authorities in a third country would access personal and potentially sensitive data. This may allow for data subjects rights to privacy to be compromised, without adequate safeguards in place and opportunities for independent enforcement and redress.
- 5.17 This gives rise to further concerns about the proposed UK rules on sharing personal data with third countries. For example, the NIHRC is concerned about the possibility of the Secretary of State deciding that a third country offers an adequate standard of data protection in the context of sending asylum seekers and refugees to this country as part of the new immigration rules contained in the Illegal Migration Act 2023.
- 5.18 Sections 2 and 5 of the Illegal Migration Act 2023 results in asylum claims from individuals arriving in the UK through unofficial routes being deemed inadmissible and requires the Home Secretary to remove such people without prior examination of the merits of their claim.⁸¹ The NIHRC has separately outlined how these provisions are in stark contrast to ECHR obligations and have expressed grave

⁷⁹ Article 45(2)(b), Regulation 2016/679/EU, 'Regulation of the European Parliament and Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (EU GDPR)', 27 April 2016. Our emphasis throughout.

⁸⁰ New Article 45B, Data Protection and Digital Information Bill.

⁸¹ Section 2, Illegal Migration Act 2023.

concerns regarding the compliance of these powers with requirements under EU standards relevant for the determination of minimum human rights standards in NI under Windsor Framework Article 2.⁸²

- 5.19 Under the proposed UK-Republic of Rwanda partnership agreement, the removal of an asylum seeker to Rwanda would inevitably involve the transfer of personal data, which could be sensitive.⁸³ The Republic of Rwanda is not one of the countries listed on the EU Commission's website with which the EU has a data adequacy decision in place.⁸⁴
- 5.20 For the transfer of data to the Republic of Rwanda during the removal process to be legal under the provisions of the UK GDPR, the UK Government must be certain that the level of data protection is equivalent to the level required by the EU GDPR, as currently the UK GDPR and the EU GDPR align. On the same note, the UK Government must be sure an independent monitoring authority in the Republic of Rwanda can properly enforce data protection rules and that data subjects have effective and enforceable rights and access to effective administrative and judicial redress for any data rights violations.
- 5.21 This is in addition to current safeguards referenced above, to protect rights holders from having their important, potentially identifying and sensitive data stored or used inappropriately.
- 5.22 The High Court in NI has recently confirmed that refugees and asylum seekers fall within the protection of Windsor Framework Article 2.⁸⁵ For the reasons set out in section 2, above, any transfer of personal data to a third country which reduces safeguards could

⁸² NIHRC, 'Submission to House of Lords on the Illegal Migration Bill' (NIHRC, 2023), at para 3.2.

⁸³ The partnership agreement between the UK and the Republic of Rwanda reflects this reality. See Home Office, 'Memorandum of Understanding between the government of the United Kingdom of Great Britain and Northern Ireland and the government of the Republic of Rwanda for the provision of an asylum partnership arrangement' (Home Office, 2023), Part 3 (Data management and protection).

⁸⁴ EU Commission, 'Adequacy decisions: How the EU determines if a non-EU country has an adequate level of data protection'. Available at: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en?prefLang=de#:~:text=How%20the%20EU%20determines%20if,adequate%20level%20of%20data%20protection.&text=The%20European%20Commission%20has%20the,adequate%20level%20of%20data%20protection.

⁸⁵ NI Human Rights Commission and Equality Commission for NI, 'Working Paper: The Scope of Article 2(1) of the Ireland/Northern Ireland Protocol' (NIHRC and ECNI, 2022). See also *In the Matter of an Application by AA for Judicial Review* [2023] NIKB 102, at para 107.

potentially diminish data protection rights contrary to the commitment to no diminution of rights under Windsor Framework Article 2.

- 5.23 **The NIHRC recommends that the Secretary of State reviews Schedule 5 of the Bill and brings forward amendments as required to ensure no diminution of rights in NI relating to data transfer to third countries, measured against relevant EU GDPR standards.**

6.0 Processing of personal data for the purposes of research: Clauses 2, 5 and 6

- 6.1 The Bill proposes changes to the circumstances when personal data can lawfully be collected and processed for the purpose of research under the UK GDPR, which currently aligns with EU GDPR. The NIHRC has concerns that this change to a key definition and a corresponding safeguard of the personal data of data subjects may diminish rights contrary to Windsor Framework Article 2.

Current provisions

- 6.2 Currently Article 4, UK GDPR provides key definitions regarding data protection, including a definition of personal data and a definition of processing of personal data for research purposes.⁸⁶ Article 5, UK GDPR contains the principles for the lawful processing of personal data, including for the purposes of scientific research.⁸⁷ Article 9, UK GDPR further provides the rules for processing special categories of personal data. UK GDPR, which aligns with the EU GDPR, generally prohibits the processing of special categories of personal data, subject to specified exemptions including where the processing is necessary for achieving purposes in the public interest, scientific or historic research purposes or statistical purposes.⁸⁸

⁸⁶ Article 4(1), Regulation 2016/679/EU, 'Regulation of the European Parliament and Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data', 27 April 2016.

⁸⁷ Article 5(1)(b), Regulation 2016/679/EU, 'Regulation of the European Parliament and Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data', 27 April 2016.

⁸⁸ Article 9(2)(j), Regulation 2016/679/EU, 'Regulation of the European Parliament and Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data', 27 April 2016.

Proposed changes

- 6.3 Clause 2 of the Data Protection and Digital Information Bill (Meaning of research and statistical purposes) adds a definition of scientific research to the definitions provided by Article 4, UK GDPR (Definitions). The Bill defines “scientific research” as “any research that can reasonably be described as scientific, whether publicly or privately funded and whether carried out as a commercial or non-commercial activity” and includes a public interest test as regards research in the area of public health.⁸⁹
- 6.4 The UK GDPR, which is currently aligned with the EU GDPR, allows for the lawful processing of both personal data⁹⁰ and special categories of personal data⁹¹ for specified, explicit and legitimate purposes, including scientific research, provided that safeguards are put in place. These safeguards include proportionality, respect for the right to data protection and the provision of suitable and specific measures to safeguard rights.⁹²
- 6.5 The NIHRC is concerned about this wide definition allowing for personal data and special categories of personal data to be processed for research purposes which the UK GDPR, aligned with the EU GDPR, would not have permitted before. This gives grounds for concern that this is a weakening of the current safeguards on the processing of personal data that the UK GDPR, aligned with the EU GDPR, awards.
- 6.6 The Data Protection and Digital Information Bill proposes further amendments to the lawful processing of data rules that grant the Secretary of State wide powers. Under Article 6(1)(f), UK GDPR, which is aligned with EU GDPR, the processing of personal data is lawful if it is necessary for the purposes of legitimate interests. Clause 5 of the Data Protection and Digital Information Bill adds a

⁸⁹ Clause 2, Data Protection and Digital Information Bill.

⁹⁰ Article 5(1)(b), Regulation 2016/679/EU, ‘Regulation of the European Parliament and Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data’, 27 April 2016.

⁹¹ Article 9(2)(j), Regulation 2016/679/EU, ‘Regulation of the European Parliament and Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data’, 27 April 2016.

⁹² Article 9(2)(j), Regulation 2016/679/EU, ‘Regulation of the European Parliament and Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data’, 27 April 2016.

new provision to Article 6, UK GDPR which allows the Secretary of State to amend by regulation the list of the legitimate interests that justify the collection and processing of personal data.⁹³

- 6.7 The NIHRC welcomes the maintaining of some safeguards, such as the requirement for the Secretary of State to have regard to the interests and fundamental rights and freedoms of the data subject and to provide special protections for children’s personal data. The NIHRC is nevertheless concerned that these safeguards are not as robust as the ones currently provided by the UK GDPR. The proposed provisions grant the Secretary of State a wide power to determine whether data processing has been lawful.
- 6.8 NI continues to be bound by the standards set in the EU GDPR, therefore we have a concern that the wide powers granted to the Secretary of State in relation to the processing of personal data for the purposes of scientific research, or when necessary for the purposes of a legitimate interest, might be used in a way that causes a diminution of data protection rights contrary to the commitment under Windsor Framework Article 2.
- 6.9 In addition, Article 5, UK GDPR currently stipulates that further processing of personal data would be considered lawful if it is done for “archiving purposes in the public interest, scientific or historical research purposes”.⁹⁴ Clause 6 of the Data Protection and Digital Information Bill proposes a new Article 8A which allows for the lawful further processing of personal data, as long as it meets a condition under Annex 2 of the Bill, which may be amended by regulation to add or omit provisions that allow for the lawful further processing of personal data.
- 6.10 The NIHRC recommends that the Secretary of State reviews Clause 2 and brings forward amendments as required to ensure no diminution of rights in NI in relation to the processing of personal data for scientific purposes.**

⁹³ Schedule 1, Data Protection and Digital Information Bill.

⁹⁴ Article 5 (1) (b), Regulation 2016/679/EU, ‘Regulation of the European Parliament and Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data’, 27 April 2016.

- 6.11 **The NIHRC recommends that the Secretary of State reviews the provisions of Clause 5 of the Bill and brings forward amendments as required to avoid a divergence of data protection standards between the UK and the EU that might result in the free flow of data between the UK and the EU being compromised.**

7.0 Additional concerns

- 7.1 In addition to the concerns outlined above, the NIHRC is considering other potential diminutions of data protection rights contrary to minimum standards required by the EU GDPR. For example, the additional power to deem repeated requests for information as excessive and vexatious (Clause 8(3)), as well as the possibility for the data controller to extend the allowed period for responses to data requests by asking for further information (Clause 9), might result in a weakening of data subjects' rights which may be incompatible with Windsor Framework Article 2.
- 7.2 NIHRC is also concerned about the cumulative effect of Clause 17 (Senior responsible individual), Clause 18 (Duty to keep records), Clause 19 (Logging of law enforcement processing) and Clause 20 (Assessment of high-risk processing). Together these clauses may result in less strict rules for the assessment of the risks that data collection and processing pose for individuals and may result in a weakening of individuals' rights below the standard required by EU GDPR and therefore in breach of the commitment to no diminution of rights under Windsor Framework Article 2.

Contact us

Any queries: Eilis.Haughey@nihrc.org

www.nihrc.org | info@nihrc.org | +44 (0)28 9024 3987
4th Floor, Alfred House, 19-21 Alfred Street, Belfast, BT2 8ED

