

Data (Use and Access) Bill [HL]

SECOND MARSHALLED LIST OF AMENDMENTS TO BE MOVED IN GRAND COMMITTEE

The amendments have been marshalled in accordance with the Instruction of 19th November 2024, as follows –

Clauses 1 to 56	Schedule 10
Schedule 1	Clauses 103 to 107
Clauses 57 and 58	Schedule 11
Schedule 2	Clauses 108 to 111
Clauses 59 to 65	Schedule 12
Schedule 3	Clauses 112 and 113
Clauses 66 to 70	Schedule 13
Schedule 4	Clauses 114 and 115
Clause 71	Schedule 14
Schedule 5	Clauses 116 to 119
Clauses 72 to 80	Schedule 15
Schedule 6	Clause 120
Clauses 81 to 84	Schedule 16
Schedules 7 to 9	Clauses 121 to 138
Clauses 85 to 102	Title

[Amendments marked ★ are new or have been altered]

**Amendment
No.**

Clause 67

VISCOUNT COLVILLE OF CULROSS
LORD CLEMENT-JONES
BARONESS KIDRON

59 Clause 67, page 75, line 9, after “processing” insert “solely”

Member's explanatory statement

This amendment prevents misuse of the scientific research exceptions for data reuse by ensuring that the only purpose for which the reuse is permissible is for the scientific research - with no additional purposes.

LORD FREYBERG
LORD CLEMENT-JONES

60 Clause 67, page 75, line 10, leave out from “scientific” to end of line 12

Member's explanatory statement

This amendment seeks to ensure that the Bill does not extend the meaning of “research purposes” to include privately funded or commercial activity, to avert the possibility that such ventures might benefit from exemptions in copyright law relating to data mining.

VISCOUNT CAMROSE
LORD MARKHAM

61 Clause 67, page 75, leave out lines 11 and 12 and insert “and when carried out only as a non-commercial activity.”

Member's explanatory statement

This amendment ensures data companies cannot justify data scraping for AI training as scientific research.

VISCOUNT COLVILLE OF CULROSS
LORD CLEMENT-JONES
BARONESS KIDRON
VISCOUNT CAMROSE

62 Clause 67, page 75, line 14, after “processing” insert “solely”

Member's explanatory statement

This amendment prevents misuse of the scientific research exceptions for data reuse by ensuring that the only purpose for which the reuse is permissible is for the scientific research - with no additional purposes.

VISCOUNT COLVILLE OF CULROSS
LORD CLEMENT-JONES
BARONESS KIDRON
VISCOUNT CAMROSE

63 Clause 67, page 75, line 18, leave out “in the area of public health”

Member's explanatory statement

This amendment ensures that to qualify for the scientific research exception for data reuse, that research must be in the public interest. This requirement already exists in the Bill for medical research, but should apply to all scientific research wishing to take advantage of the exception.

LORD CLEMENT-JONES
BARONESS KIDRON

64 Clause 67, page 75, line 21, at end insert –

- “(c) only include processing for the purposes of a study in the area of education that can reasonably be described as scientific where the study is conducted in the public interest, and is conducted on an opt-in basis where the data subject is a child, their parent, carer or legal guardian.”

Member's explanatory statement

An amendment to probe the meaning of research and statistical purposes

VISCOUNT COLVILLE OF CULROSS
LORD CLEMENT-JONES
BARONESS KIDRON

65 Clause 67, page 75, line 21, at end insert –

- “(c) do not include processing unless the research –
- (i) is consistent with generally recognised ethical standards relevant to the area of research, and
 - (ii) is considered appropriate by a research ethics committee that meets UKRI guidance and criteria for research ethics committee review.”

Member's explanatory statement

This amendment ensures research seeking to make use of the scientific research exception for reuse meets minimum levels of academic rigour and ethical standards.

LORD HOLMES OF RICHMOND

65A Clause 67, page 75, line 21, at end insert –

- “(c) do not include processing for the development or improvement of AI training, and
- (d) do not include re-using personal data scraped from the internet.”

VISCOUNT CAMROSE
LORD MARKHAM

66 Clause 67, page 75, line 21, at end insert –

- “3A. Research considered scientific research that is carried out as a commercial activity must be subject to the approval of an independent ethics committee.”

Member's explanatory statement

This amendment ensures personal data is not used for commercial purposes, which is subject to fewer ethical safeguards; preventing data being used in a matter data subjects may not consider an appropriate, such as training Large Language Models.

Clause 68

VISCOUNT CAMROSE
LORD MARKHAM

67 Clause 68, page 76, leave out lines 9 and 10

Member's explanatory statement

The amendment ensures that data controllers cannot gain consent for research purposes that cannot be defined at the time of data collection.

LORD CLEMENT-JONES

68 Clause 68, page 76, line 16, at end insert –

“(e) the data subject has been given the opportunity to express dissent or an objection, and has not so expressed.”

Member's explanatory statement

This amendment is to make clear that when the purpose limitations are changed, that does not reduce or weaken the obligations around dissent.

LORD CLEMENT-JONES

69 Clause 68, page 76, line 16, at end insert –

“(e) the data subject has been given the opportunity to express dissent or object.”

Member's explanatory statement

This amendment makes clear that when the purpose limitations are changed, a choice must be offered to data subjects.

LORD STEVENSON OF BALMACARA
LORD CLEMENT-JONES

70 Clause 68, page 76, leave out lines 17 and 18 and insert –

“7. For the avoidance of doubt, consent as defined here is not sufficient for the purposes of Article 6(1)(a) (lawful processing) and Article 9(2)(a) (processing of special categories of personal data).”

Member's explanatory statement

This amendment would mitigate the lowering of the threshold for a data subject to be deemed to have given consent.

LORD STEVENSON OF BALMACARA
LORD CLEMENT-JONES

71 Clause 68, page 76, line 18, at end insert –

- “8. Notwithstanding other provisions in this Regulation, no NHS patient data may be shared with any commercial body for any non-NHS purpose without the explicit consent of the data subject.”

Member's explanatory statement

This will ensure that no NHS Patient Data can be made available for scientific research without the explicit consent of the data subject.

After Clause 68

LORD STEVENSON OF BALMACARA
LORD CLEMENT-JONES

72 After Clause 68, insert the following new Clause –

“Personal data for scientific research: public interest

In the UK GDPR, after Article 11 insert –

“Article 11A

Personal data for scientific research: public interest

1. References in this Regulation to the processing of personal data for the purposes of scientific research will not be effective unless the research has been reviewed by an appropriate body and certified by them as being in the public interest.
2. The Secretary of State must within six months of the day on which the Data (Use and Access) Act 2024 is passed specify by regulations made by statutory instrument which public bodies are appropriate for the purposes of certifying whether research is in the public interest.
3. A statutory instrument containing regulations under 11(2) may not be made unless a draft of the instrument has been laid before and approved by a resolution of each House of Parliament.
4. For the avoidance of doubt, explicit patient consent is required to allow access to personal data for scientific research in the public interest.””

Member's explanatory statement

This amendment will make it clear that any person or body wishing to use NHS patient data must gain the approval from an authorised body that the research in contemplation is in the public interest.

Clause 70

LORD CLEMENT-JONES
BARONESS KIDRON

73 Clause 70, page 77, leave out lines 34 to 38

Member's explanatory statement

This amendment and another amendment in Lord Clement-Jones's name to clause 70 omits paragraphs 70(2)(b)-(c), (4), (5) and (6) which make amendments to UK GDPR to define certain data processing activities as "recognised legitimate interests".

LORD SCRIVEN
LORD CLEMENT-JONES

74 Clause 70, page 77, line 36, after "interest" insert ", excluding personal health data"

Member's explanatory statement

This amendment excludes personal health data from being a recognised legitimate interest.

LORD CLEMENT-JONES
BARONESS KIDRON

75 Clause 70, page 78, line 5, leave out subsections (4), (5) and (6)

Member's explanatory statement

This amendment and another amendment in Lord Clement-Jones's name to clause 70 omit paragraphs 70(2)(b)-(c), (4), (5) and (6) which make amendments to UK GDPR to define certain data processing activities as "recognised legitimate interests".

LORD CLEMENT-JONES

76 Clause 70, page 78, leave out lines 9 to 30.

Member's explanatory statement

This amendment deletes powers for Secretary of State to override primary legislation and modify key aspects of UK data protection law via Statutory Instrument.

LORD CLEMENT-JONES

- 77 Clause 70, page 79, line 4, leave out “affiliated to a central body” and insert “or separate undertakings affiliated by contract”

Member's explanatory statement

This amendment would allow businesses that are affiliated by contract to be treated in the same way as large businesses that have data from multiple companies in a group structure.

After Clause 70

LORD CLEMENT-JONES

- 78 After Clause 70, insert the following new Clause –

“Statement on changes to recognise legitimate interest

- (1) The Secretary of State must publish a statement outlining the purpose of any additions or variations to what constitutes a recognised legitimate interest if they exercise powers contained under section 70.
- (2) This statement must reference –
 - (a) the purpose of the addition or variation,
 - (b) whether it is appropriate to specific data controllers, and
 - (c) the timeline for its relevancy.”

Member's explanatory statement

This amendment requires the Secretary of State to publish a statement if they add or vary what constitutes a recognised legitimate interest which outlines the purpose of the new addition, the timeline for its relevancy and whether it is appropriate to specific data controllers.

Schedule 4

LORD CLEMENT-JONES

- 78A★ Schedule 4, page 182, leave out lines 14 to 21

LORD CLEMENT-JONES

Lord Clement-Jones gives notice of his intention to oppose the Question that Schedule 4 be the Fourth Schedule to the Bill.

Member's explanatory statement

This amendment seeks to restore accountability over how data is shared and accessed for law enforcement and other public security purposes.

Clause 71

LORD STEVENSON OF BALMACARA
BARONESS KIDRON

79 Clause 71, page 80, line 34, after “consents” insert “in accordance with Article 4(11)”

Member's explanatory statement

This amendment would clarify that the definition of consent to be used in this article is the definition in Article 4(11) of the UK GDPR.

VISCOUNT CAMROSE
LORD MARKHAM

80 Clause 71, page 80, line 38, leave out “scientific interest or”

Member's explanatory statement

This amendment prevents the data reuse test being automatically passed if the reuse is for the purposes of scientific research as under the current definition may capture research for commercial purposes.

LORD STEVENSON OF BALMACARA
BARONESS KIDRON

81 Clause 71, page 81, line 1, at end insert –

“and the data subject consents to the processing in accordance with Article 4(11),”

Member's explanatory statement

The amendment would clarify that consent in accordance with the existing provisions of the UK GDPR is required for processing for research, archiving, or statistical purposes.

LORD CLEMENT-JONES
BARONESS KIDRON
LORD RUSSELL OF LIVERPOOL
BARONESS HARDING OF WINSCOMBE

82 Clause 71, page 81, line 14, at end at end insert –

“4A. Where the controller collected the personal data based on Article 6(1)(a) (data subject’s consent), processing for a new purpose is not compatible with the original purpose if –

- (a) the data subject is a child,
- (b) the processing is based on consent given or authorised by the holder of parental responsibility over the child,
- (c) the data subject is an adult to whom either (a) or (b) applied at the time of the consent collection, or
- (d) the data subject is a deceased child.”

Member's explanatory statement

This amendment seeks to exclude children from the new provisions on purpose limitation for further processing under Article 8A.

LORD CLEMENT-JONES

83 Clause 71, page 81, leave out lines 15 to 28

Member's explanatory statement

This amendment removes powers for Secretary of State to override primary legislation and modify key aspects of UK data protection law via statutory instrument.

Schedule 5

LORD CLEMENT-JONES

84 Schedule 5, page 184, line 15, at end insert—

“(iii) is not carried out for commercial purposes, and”

Member's explanatory statement

This amendment seeks to clarify whether the government intends to allow personal data processing for purposes that are commercial under the conditions described in this provision.

LORD CLEMENT-JONES

85 Schedule 5, page 186, line 7, at end insert—

“10A. This condition is met only where the controller has made an assessment of vulnerability and makes it publicly available to the data subjects prior to processing, repeated on an annual basis for any subsequent processing.”

Member's explanatory statement

This amendment seeks to ensure transparency and accountability obligations are not removed from data controllers when processing personal data for the purposes of safeguarding vulnerable individuals based on an undefined characteristic that may change, and that may apply or not apply to any given individual at any point in time.

LORD CLEMENT-JONES

86 Schedule 5, page 186, line 7, at end insert—

“10A. The condition ceases to apply when the nature of the vulnerability for the individual, or the type of individual, is no longer present or has otherwise expired.”

Member's explanatory statement

A probing amendment to seek clarity on the safeguards and processes for ensuring that processing activities tied to an undefined and changeable characteristic of 'vulnerability' do not persist unnecessarily or disproportionately.

LORD CLEMENT-JONES

Lord Clement-Jones gives notice of his intention to oppose the Question that Schedule 5 be the Fifth Schedule to the Bill.

Member's explanatory statement

This amendment seeks to restore accountability over how data is shared and accessed for law enforcement and other public security purposes.

After Clause 72

LORD THOMAS OF CWMGIEDD

LORD CLEMENT-JONES

87 After Clause 72, insert the following new Clause—

“Application of the European Convention on Human Rights to the processing of personal data by private bodies

- (1) Where personal data is processed by any private body not subject to the obligations under the European Convention on Human Rights as enacted by the Human Rights Act 1998, that private body is to be treated as subject to the obligations under the Convention as if it were a public authority and must ensure that such processing is not incompatible with a Convention right.
- (2) If a private body fails to ensure that the processing of personal data is in accordance with subsection (1), the private body is liable to any person whose rights under the Convention are infringed as if it were a public authority.”

Member's explanatory statement

This is a probing amendment to ensure for the purpose of equivalence that the processing of personal data by private bodies is subject to the ECHR on the same basis as public bodies.

BARONESS KIDRON

LORD RUSSELL OF LIVERPOOL

LORD STEVENSON OF BALMACARA

BARONESS HARDING OF WINSCOMBE

88 After Clause 72, insert the following new Clause—

“Protection of children: overarching duty on controllers and processors

- (1) In complying with their UK data protection obligations, data controllers and processors must give due consideration to—

- (a) the fact that children are entitled to a higher standard of protection than adults with regard to their personal data;
 - (b) the need to prioritise children's best interests and to uphold their rights under UN Convention on the Rights of the Child and General Comment 25;
 - (c) the fact that children may require different protections at different ages and stages of development.
- (2) Nothing in this Act is to be construed as reducing, minimising or undermining existing standards and protections of children's data under the 2018 Act or UK GDPR.
- (3) In this section, a “child” is a person under the age of 18.”

Member's explanatory statement

This amendment creates an obligation on data processors and controllers to consider the central principles of the Age-Appropriate Design Code when processing children's data. This ensures greater consistency in the level of protection children receive.

LORD CLEMENT-JONES

89 After Clause 72, insert the following new Clause –

“Determination of what is considered to be personal data

Notwithstanding any other provisions elsewhere in this Act –

- (a) personal data that is then pseudonymised in part, but in which other indirect identifiers remain unaltered, remains personal data under the 2018 Act;
- (b) if data is claimed not to be personal data for the purpose of some processing, and is later determined by the Commissioner to be personal data, then it was personal data at all points in that processing and all penalties for unlawful processing of personal data shall be available.”

Member's explanatory statement

This amendment means that personal data remains personal data, even in instances where that is challenged, and the Commissioner has determined it is personal data.

Clause 74

LORD CLEMENT-JONES

90 Clause 74, page 84, leave out lines 7 to 22

Member's explanatory statement

This amendment removes powers for Secretary of State to override primary legislation and modify key aspects of UK data protection law via statutory instrument.

LORD CLEMENT-JONES

Lord Clement-Jones gives notice of his intention to oppose the Question that Clause 74 stand part of the Bill.

Member's explanatory statement

This amendment removes powers for Secretary of State to override primary legislation and modify key aspects of UK data protection law via statutory instrument.

Clause 75

VISCOUNT CAMROSE
LORD MARKHAM

91 Clause 75, page 87, line 18, at end insert –

“(za) in subsection (1), for “manifestly unfounded” substitute “vexatious,”

Member's explanatory statement

This amendment changes the definition of request by data subjects to data controllers for which a fee can be charged from “manifestly unfounded or excessive” to “vexatious or excessive.”

Clause 77

VISCOUNT COLVILLE OF CULROSS
LORD CLEMENT-JONES

92 Clause 77, page 91, line 5, leave out “the number of data subjects,”

Member's explanatory statement

This amendment reduces the likelihood of misuse of Clause 77 by AI model developers, who may otherwise seek to claim they do not need to notify data subjects of reuse for scientific purposes under Clause 77 because of the way that personal data is typically collected and processed for AI development, for example by scraping large amounts of personal data from the internet.

VISCOUNT COLVILLE OF CULROSS
LORD CLEMENT-JONES

93 Clause 77, page 91, line 7, at end insert –

“6A. For the purposes of paragraph 5(b), the effort involved will not be considered disproportionate because of, among other things, the number of data subjects, the fact the personal data was not collected from the data subject, or any processing undertaken by the controller that makes the effort involved greater.”

Member's explanatory statement

This amendment reduces the likelihood of misuse of Clause 77 by AI model developers, who may otherwise seek to claim they do not need to notify data subjects of reuse for scientific purposes

under Clause 77 because of the way that personal data is typically collected and processed for AI development, for example by scraping large amounts of personal data from the internet.

LORD CLEMENT-JONES
BARONESS KIDRON

94 Clause 77, page 91, line 11, at end insert –

“8. Exemptions from Article 13, Information and access to personal data; and Article 14, Information to be provided where personal data have not been obtained from the data subject; do not apply where the data subject is a child at the time of data collection or at the time of any data processing.”

Member's explanatory statement

The exemption regarding the obligation to provide information about further processing should not apply to children.

BARONESS HARDING OF WINSCOMBE
LORD CLEMENT-JONES
LORD STEVENSON OF BALMACARA
LORD BLACK OF BRENTWOOD

95 Clause 77, page 91, line 16, leave out “to the extent that” and insert “when any one or more of the following is true”

Member's explanatory statement

This amendment would clarify that only one condition under paragraph 5 must be present for paragraphs 1 to 4 to not apply.

BARONESS HARDING OF WINSCOMBE
LORD CLEMENT-JONES
LORD STEVENSON OF BALMACARA
LORD BLACK OF BRENTWOOD

96 Clause 77, page 91, line 16, at end insert –

“(ia) after point (a), insert –

“(aa) the data is from the Open Electoral Register;”

Member's explanatory statement

This amendment would change GDPR Article 14.

VISCOUNT CAMROSE
LORD MARKHAM

97 Clause 77, page 91, line 21, leave out “or would involve a disproportionate effort”

Member's explanatory statement

This amendment ensures AI companies who process data not directly obtained from data subjects are required to provide information to data subjects where possible. Without this amendment, data subjects may not know their data is being held, leaving them unable to enforce their data rights.

BARONESS HARDING OF WINSCOMBE
LORD CLEMENT-JONES
LORD STEVENSON OF BALMACARA
LORD BLACK OF BRENTWOOD

- 98 Clause 77, page 91, line 22, after “effort” insert “in particular where providing the information is not warranted by the impact on the individuals,”

VISCOUNT CAMROSE
LORD MARKHAM

- 99 Clause 77, page 91, leave out lines 28 to 32

Member's explanatory statement

This amendment ensures AI companies which use large data sets cannot avoid providing information to data subjects on the basis their data sets are too large.

BARONESS HARDING OF WINSCOMBE
LORD CLEMENT-JONES
LORD STEVENSON OF BALMACARA
LORD BLACK OF BRENTWOOD

- 100 Clause 77, page 91, line 30, after “things,” insert “the effort and cost of compliance,”

Member's explanatory statement

This amendment adds to the list of what might constitute a disproportionate effort.

VISCOUNT COLVILLE OF CULROSS
LORD CLEMENT-JONES

- 101 Clause 77, page 91, line 30, leave out “the number of data subjects,”

Member's explanatory statement

This amendment reduces the likelihood of misuse of Clause 77 by AI model developers, who may otherwise seek to claim they do not need to notify data subjects of reuse for scientific purposes under Clause 77 because of the way that personal data is typically collected and processed for AI development, for example by scraping large amounts of personal data from the internet.

BARONESS HARDING OF WINSCOMBE
LORD CLEMENT-JONES
LORD STEVENSON OF BALMACARA
LORD BLACK OF BRENTWOOD

- 102 Clause 77, page 91, line 30, after “subjects,” insert “the damage and distress to the data subjects,”

Member's explanatory statement

This amendment adds to the list of what might constitute a disproportionate effort.

BARONESS HARDING OF WINSCOMBE
LORD CLEMENT-JONES
LORD STEVENSON OF BALMACARA

- 103 Clause 77 page 91, line 30, after “subjects,” insert “the reasonable expectation of the data subjects,”

Member's explanatory statement

This amendment adds to the list of what might constitute a disproportionate effort.

BARONESS HARDING OF WINSCOMBE
LORD CLEMENT-JONES
LORD STEVENSON OF BALMACARA
LORD BLACK OF BRENTWOOD

- 104 Clause 77, page 91, line 32, at end insert “and whether the information has been collected and made publicly available by a public body.”

Member's explanatory statement

This amendment adds to the list of what might constitute a disproportionate effort.

VISCOUNT COLVILLE OF CULROSS
LORD CLEMENT-JONES

- 105 Clause 77, page 91, line 32, at end insert –

“6A. For the purposes of paragraph 5(e), the effort involved will not be considered disproportionate because of, among other things, the number of data subjects, the fact the personal data was not collected from the data subject, or any processing undertaken by the controller that makes the effort involved greater.”

Member's explanatory statement

This amendment reduces the likelihood of misuse of Clause 77 by AI model developers, who may otherwise seek to claim they do not need to notify data subjects of reuse for scientific purposes under Clause 77 because of the way that personal data is typically collected and processed for AI development, for example by scraping large amounts of personal data from the internet.

BARONESS HARDING OF WINSCOMBE
LORD CLEMENT-JONES
LORD STEVENSON OF BALMACARA

106 Clause 77, page 91, line 36, at end insert –

“8. An appropriate safeguard might be a risk assessment, including limiting the extent and purpose of the processing for which the data might be used.”

LORD CLEMENT-JONES
LORD SCRIVEN

The above-named Lords give notice of their intention to oppose the Question that Clause 77 stand part of the Bill.

Clause 78

LORD CLEMENT-JONES

Lord Clement-Jones gives notice of his intention to oppose the Question that Clause 78 stand part of the Bill.

Member's explanatory statement

This amendment would restore transparency rights.

After Clause 78

LORD CLEMENT-JONES

107 After Clause 78, insert the following new Clause –

“Guidance on reasonable and proportionate searches

The Secretary of State must publish guidance within six months of the day on which this Act is passed to clarify what constitutes a reasonable and proportionate search for personal data.”

Member's explanatory statement

This amendment requires the Secretary of State to publish guidance within six months of the Act's passing to clarify what constitutes 'reasonable and proportionate' in protection of personal data.

Clause 79

LORD CLEMENT-JONES

108 Clause 79, page 93, line 18, leave out “court” and insert “tribunal”

Member's explanatory statement

This amendment is consequential on the new Clause (Transfer of jurisdiction of courts to tribunals).

After Clause 79

LORD CLEMENT-JONES

109 After Clause 79, insert the following new Clause –

“Data protection impact assessments

- (1) The UK GDPR is amended in accordance with subsections (2) to (7).
- (2) In Article 35(1), after “natural persons” insert “or the public interest”.
- (3) In Article 35(7)(c), after “paragraph 1” insert “and to the public interest, including to equality and the environment”.
- (4) In Article 35(7)(d), after “other persons concerned” insert “and the public interest”.
- (5) In Article 35(9) –
 - (a) delete “Where appropriate,”, and
 - (b) replace “data subjects” with “people affected by the intended processing”.
- (6) In Article 13(2), after point (e) insert –

“(ea) the results of the data protection impact assessment referred to in Article 35 and the nature of the consultation carried out under Article 35(9) to inform that assessment;”
- (7) In Article 14(2), after point (f) insert –

“(fa) the results of the data protection impact assessment referred to in Article 35 and the nature of the consultation carried out under Article 35(9) to inform that assessment””

Clause 80LORD CLEMENT-JONES
LORD KNIGHT OF WEYMOUTH

110 Clause 80, page 94, line 24, at end insert –

- “3. To qualify as meaningful human involvement, the review must be performed by a person with the necessary competence, training, authority to alter the decision and analytical understanding of the data.”

Member's explanatory statement

This amendment would make clear that in the context of new Article 22A of the UK GDPR, for human involvement to be considered as meaningful, the review must be carried out by a competent person.

VISCOUNT CAMROSE
LORD MARKHAM

111 Clause 80, page 94, line 24, at end insert –

- “3. When an automated decision-making process involves artificial intelligence (AI), the AI programme must have due regard for the five principles set out in Annex A of “A Pro-Innovation Approach to AI Regulation White Paper” –
- (a) safety, security, and robustness;
 - (b) appropriate transparency and explainability;
 - (c) fairness;
 - (d) accountability and governance;
 - (e) contestability and redress.”

Member's explanatory statement

This amendment inserts the five principles from the “A pro-innovation approach to AI regulation” White Paper, ensuring AI programmes used in automated decision making have due regards for safety, security, robustness, appropriate transparency and explainability, fairness, accountability and governance, and contestability and redress.

LORD CLEMENT-JONES
LORD KNIGHT OF WEYMOUTH

112 Clause 80, page 94, line 26 at end insert –

- “A1. The data subject may not be subject to any decision based on data processing which contravenes a requirement of the Equality Act 2010.”

Member's explanatory statement

This amendment to new Article 22B of the UK GDPR, aims to make clear that data processing which contravenes any part of the Equality Act 2010 is prohibited.

LORD THOMAS OF CWMGIEDD
LORD CLEMENT-JONES

113 Clause 80, page 94, line 27, leave out from “on” to “may” in line 28 and insert “personal data”

Member's explanatory statement

The amendment seeks to remove the restriction of the operation of the clause so that provision applies generally to all automated processing.

LORD CLEMENT-JONES
BARONESS KIDRON
LORD KNIGHT OF WEYMOUTH

114 Clause 80, page 95, line 12, leave out “solely” and insert “predominantly”

Member's explanatory statement

This amendment would mean safeguards for data subjects' rights, freedoms and legitimate interests would have to be in place in cases where a significant decision in relation to a data subject was taken based predominantly, rather than solely, on automated processing.

VISCOUNT CAMROSE

- 114A★** Clause 80, page 95, line 15, leave out “and any regulations under Article 22D(3)”

LORD LUCAS
LORD CLEMENT-JONES
LORD KNIGHT OF WEYMOUTH

- 115** Clause 80, page 95, line 23, at end insert –

“(e) communicate to the data subject the fact that automated decision-making has been involved, the automated decision-making system’s reasoning in reaching the conclusion that it has, and the extent of any human involvement.”

Member's explanatory statement

This amendment seeks to ensure that, for example, a job applicant who has been rejected by an automated system is given clear reasons for the rejection.

VISCOUNT CAMROSE

- 115A★** Clause 80, page 95, leave out from the beginning of line 24 to the end of line 28 on page 98

Member's explanatory statement

The amendment removes the Secretary of State’s power to make regulations under Article 22D; and it removes other provisions inserted into the 2018 Act about automated decision-making.

VISCOUNT CAMROSE
LORD MARKHAM

- 116** Clause 80, page 96, line 33, at end insert –

“(4) The Secretary of State must publish guidance on how data controllers may obtain explicit consent, which must be published and reviewed at least annually, and any changes to which must be published as soon as practicable.”

Member's explanatory statement

This amendment will ensure the Secretary of State provides guidance on how consent should be obtained for automated decision-making involving special category data. It also ensures that this guidance is readily available and is reviewed frequently.

VISCOUNT CAMROSE
LORD MARKHAM
LORD KNIGHT OF WEYMOUTH

117 Clause 80, page 96, line 33, at end insert –

“(4) Consent in accordance with subsection (2) cannot be given by persons under the age of 18.”

Member's explanatory statement

This amendment prevents children giving consent for their special category data to be used in automated decision-making.

VISCOUNT CAMROSE
LORD MARKHAM
LORD KNIGHT OF WEYMOUTH

118 Clause 80, page 97, line 9, after “intervention” insert “, by a human with sufficient competency and authority,”

Member's explanatory statement

This will ensure that recourse to human intervention is carried out by a person with sufficient competency and authority and is, therefore, effective.

LORD CLEMENT-JONES

Lord Clement-Jones gives notice of his intention to oppose the Question that Clause 80 stand part of the Bill.

After Clause 80

VISCOUNT COLVILLE OF CULROSS
LORD CLEMENT-JONES
LORD KNIGHT OF WEYMOUTH

119 After Clause 80, insert the following new Clause –

“Use of the Algorithmic Transparency Recording Standard

- (1) The Secretary of State must by regulations make provision requiring Government departments, public authorities and all persons exercising a public function using algorithmic tools to process personal data to use the Algorithmic Transparency Recording Standard (“the Standard”).
- (2) The Standard is that published by the Central Digital and Data Office and Centre for Data Ethics and Innovation as part of the Government’s National Data Strategy.
- (3) Regulations under subsection (1) must require the submission and publication of algorithmic transparency reports as required by the Standard.

- (4) Regulations under subsection (1) may provide for exemptions to the requirement for publication where necessary –
 - (a) to avoid obstructing an official or legal inquiry, investigation or procedure,
 - (b) to avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties, and
 - (c) to protect public security, or to safeguard national security.
- (5) Regulations under subsection (1) are subject to the affirmative resolution procedure.”

Member's explanatory statement

This new clause puts a legislative obligation on public bodies using algorithmic tools that have a significant influence on a decision-making process with direct or indirect public effect, or directly interact with the general public, to publish reports under the Algorithmic Transparency Recording Standard ('ATRS').

LORD CLEMENT-JONES
LORD KNIGHT OF WEYMOUTH

120 After Clause 80, insert the following new Clause –

“Algorithmic Impact Assessments

- (1) Prior to deployment of an algorithmic or automated decision-making system, public authorities are responsible for completing an Algorithmic Impact Assessment prescribed in regulations made under this Act.
- (2) Subsection (1) does not apply when the algorithmic or automated decision-making system is –
 - (a) used solely for the formulation of policy in relation to that public authority, and
 - (b) is not expected to, in practice, fully or predominantly determine the content of the policy.
- (3) The Algorithmic Impact Assessment must be updated when the functionality, or the scope, of the algorithmic or automated decision-making system changes.
- (4) The final Algorithmic Impact Assessment must be published in accessible format within 30 days of the results being known.
- (5) The Secretary of State must by regulations prescribe the form of an Algorithmic Impact Assessment framework with the aims of ensuring public authorities –
 - (a) procure, develop, and implement algorithmic and automated decision-making systems such that the decisions made in and by a public authority are responsible and comply with procedural fairness and due process requirements, and its duties under the Equality Act and the Human Rights Act 1998,
 - (b) assess the impacts of algorithms on administrative decisions, minimise negative outcomes, and evaluate the potential to maximise positive outcomes,

- (c) make data and information on the use of algorithmic and automated decision-making systems in public authorities available to the public,
 - (d) better understand and reduce the risks associated with algorithmic and automated decision-making systems,
 - (e) introduce the appropriate governance, oversight, and reporting and auditing requirements that best match the risks associated with the application envisaged, and
 - (f) undergo responsible innovation of algorithmic and automated decision-making systems.
- (6) The framework as prescribed by regulations made under subsection (5) must include the requirement for –
- (a) a detailed description of the algorithmic or automated decision-making system,
 - (b) an assessment of the relative benefits and risks of the system including the risks to the privacy and security of personal information, risks to the safety of a service user or group of service users, and risks and likely impacts on employees of public authorities,
 - (c) an explanation of the steps taken to minimise those risks,
 - (d) independent external scrutiny of the efficacy and accuracy of the system, and
 - (e) mandatory bias assessment of any algorithmic or automated decision-making system to ensure it abides by the Equality Act and the Human Rights Act 1998.
- (7) The Secretary of State must publish regulations made under subsection (5) in draft and consult such persons they consider appropriate on the draft regulations before laying the regulations before both Houses of Parliament.
- (8) Regulations under this section are subject to the affirmative resolution procedure.
- (9) “Algorithmic Impact Assessment” means a framework in the form laid down in Regulations made by the Secretary of State under this Act.”

LORD CLEMENT-JONES

121 After Clause 80, insert the following new Clause –

“Algorithmic Transparency Records

- (1) Prior to use or procurement of an algorithmic or automated decision-making system, public authorities must complete an Algorithmic Transparency Record prescribed in regulations made under this Act.
- (2) Subsection (1) does not apply when the algorithmic or automated decision-making system is –
 - (a) used solely for the formulation of policy in relation to that public authority, and
 - (b) is not expected to, in practice, fully or predominantly determine the content of the policy.

- (3) The Algorithmic Transparency Record must be published in accessible format within 30 days of the completion of the record.
- (4) The Algorithmic Transparency Record must be updated when the functionality, or the scope, of the algorithmic or automated decision-making system changes.
- (5) The Secretary of State must by regulations prescribe the form of transparency records with the aim of ensuring public authorities increase the transparency of algorithm-assisted decisions.
- (6) The Algorithmic Transparency Record as prescribed by regulations made under subsection (1) must include the requirement for –
 - (a) a detailed description of the algorithmic or automated decision-making system,
 - (b) an explanation of the rationale for using the system,
 - (c) information on the technical specifications of the system,
 - (d) an explanation of how the system is used to inform administrative (se) decisions concerning a service user or group of service users, and information on human oversight of the system.
- (7) Regulations under this section are subject to the affirmative resolution procedure.”

LORD CLEMENT-JONES

122 After Clause 80, insert the following new Clause –

“Requirements of public sector organisations on use of algorithmic or automated decision-making systems

- (1) No later than the commencement of use of a relevant algorithmic or automated decision-making system, a public authority must –
 - (a) give notice on a public register that the decision rendered will be undertaken in whole, or in part, by an algorithmic or automated decision-making system,
 - (b) make arrangements for the provision of a meaningful and personalised explanation to affected individuals of how and why a decision affecting them was made, including meaningful information about the decision-making processes, and an assessment of the potential consequences of such processing for the data subject, as prescribed in regulations to be made by the Secretary of State,
 - (c) develop processes to –
 - (i) monitor the outcomes of the algorithmic or automated decision-making system to safeguard against unintentional outcomes and to verify compliance with this Act and other relevant legislation, and
 - (ii) validate that the data collected for, and used by, the system is relevant, accurate, up-to-date, and in accordance with the Data Protection Act 2018, and

- (d) make arrangements to conduct regular audits and evaluations of algorithmic and automated decision-making systems, including the potential risks of those systems and steps to mitigate such risks, as prescribed in regulations to be made by the Secretary of State.
- (2) Algorithmic decision system” or “automated decision system” mean any technology that either assists or replaces the judgement of human decision-makers.
- (3) Regulations under this section are subject to the affirmative resolution procedure.”

LORD CLEMENT-JONES
LORD KNIGHT OF WEYMOUTH

123 After Clause 80, insert the following new Clause –

“Definition of meaningful human involvement in automated decision-making

The Secretary of State must, in conjunction with the Information Commissioner’s Office and within six months of the day on which this Act is passed, produce a definition of what constitutes meaningful human involvement in automated decision-making or clearly set out their reasoning as to why a definition is not required.”

Member's explanatory statement

This amendment requires the Secretary of State to produce a definition of meaningful human involvement in automated decision-making, in collaboration with the Information Commissioner’s Office, or clearly set out its reasoning as to why this is not required, within six months of the Act’s passing.

LORD HOLMES OF RICHMOND

123A After Clause 80, insert the following new Clause –

“Safeguards: personalised explanation for automated decision-making

- (1) Wherever automated decision-making has been deployed, any individual subject to that automated decision is entitled to a personalised explanation of that decision.
- (2) The personalised explanation must –
 - (a) be clear, concise and in plain language of their choice,
 - (b) be understandable, and assume limited technical knowledge of algorithmic systems,
 - (c) address how the decision affects the individual personally, explaining which aspects of the individual’s data have likely influenced the automated decisions (or alternatively a counterfactual of what change in their data would have resulted in a more favourable outcome),
 - (d) be available free of charge and without being time-consuming for the individual to access,
 - (e) be in a readily accessible format that complies with equality duties,

- (f) be provided through an accessible user interface, easily findable and free of deceptive design patterns, and
- (g) enable meaningful challenge if needed.”

LORD HOLMES OF RICHMOND

123B After Clause 80, insert the following new Clause –

“Automated decision-making: obligations

- (1) Data controllers must ensure human reviewers of algorithmic decisions have adequate capabilities, training, and authority to challenge and rectify automated decisions.
- (2) Organisations deploying automated decision-making must ensure that they have sufficient technical capabilities and resources to identify and rectify aspects of algorithms that bear significant responsibility for biased decisions, at the point these systems are implemented.”

Clause 81

LORD CLEMENT-JONES

Lord Clement-Jones gives notice of his intention to oppose the Question that Clause 81 stand part of the Bill.

Member's explanatory statement

This seeks to retain the requirement for police forces to record the reason they are accessing data from a police database.

After Clause 81

BARONESS MORGAN OF COTES
LORD THOMAS OF CWMGIEDD

124 After Clause 81, insert the following new Clause –

“Processing of data in relation to a case file prepared by a police force for submission to the Crown Prosecution Service for a charging decision

In the 2018 Act, after section 40 insert –

“40A Processing of data in relation to a case file prepared by a police force for submission to the Crown Prosecution Service for a charging decision

- (1) Subsections (2) to (6) apply to a set of processing operations consisting of the preparation of a case file by a police force for submission to the Crown Prosecution Service for a charging decision, the making of a charging decision by the Crown Prosecution Service, and the return of the case file by the Crown Prosecution Service to the police force after a charging decision has been made.

- (2) A police force shall not be obliged to comply with the first data protection principle except insofar as that principle requires processing to be fair, or the third data protection principle, in preparing a case file for submission to the Crown Prosecution Service for a charging decision.
- (3) The Crown Prosecution Service shall not be obliged to comply with the first data protection principle except insofar as that principle requires processing to be fair, or the third data protection principle, in making a charging decision on a case file submitted for that purpose by a police force.
- (4) If the Crown Prosecution Service decides that a charge will not be pursued when it makes a charging decision on a case file submitted for that purpose by a police force it shall take all steps reasonably required to destroy and delete all copies of the case file in its possession.
- (5) If the Crown Prosecution Service decides that a charge will be pursued when it makes a charging decision on a case file submitted for that purpose by a police force it shall return the case file to the police force and take all steps reasonably required to destroy and delete all copies of the case file in its possession.
- (6) Where the Crown Prosecution Service decides that a charge will be pursued when it makes a charging decision on a case file submitted for that purpose by a police force and returns the case file to the police force under subsection (5), the police force shall be obliged to comply with the first data protection principle and the third data protection principle in relation to any subsequent processing of the data contained in the case file.
- (7) For the purposes of this section—
 - (a) the preparation or preparing of a case file by a police force for submission to the Crown Prosecution Service for a charging decision shall include the submission of the file, and
 - (b) a case file shall include all information obtained by a police force for the purpose of preparing a case file for submission to the Crown Prosecution Service for a charging decision.””

Member's explanatory statement

This new clause adjusts the Data Protection Act 2018 to exempt the police service and the Crown Prosecution Service from the first and third data protection principles contained within that Act so that they can share unredacted data with one another when making a charging decision.

After Clause 84

LORD CLEMENT-JONES

125 After Clause 84, insert the following new Clause –

“Impact of this Act and other developments at national and international level on EU data adequacy decision

Before the European Union’s next reassessment of data adequacy in June 2025, the Secretary of State must carry out an assessment of the likely impact on the European Union data adequacy decisions relating to the United Kingdom of the following –

- (a) this Act;
- (b) other changes to the United Kingdom’s domestic frameworks which are relevant to the matters listed in Article 45(2) of the UK GDPR (transfers on the basis of an adequacy decision);
- (c) relevant changes to the United Kingdom’s international commitments or other obligations arising from legally binding conventions or instruments, as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.”

Member's explanatory statement

This amendment requires the Secretary of State to carry out an assessment of the impact of this Act and other changes to the UK’s domestic and international frameworks relating to data adequacy.

Schedule 7

LORD CLEMENT-JONES

Lord Clement-Jones gives notice of his intention to oppose the Question that Schedule 7 be the Seventh Schedule to the Bill.

Member's explanatory statement

This amendment removes powers for Secretary of State to override primary legislation and modify key aspects of UK data protection law via Statutory Instrument.

Schedule 8

LORD CLEMENT-JONES

126 Schedule 8, page 197, line 20, leave out sub-paragraph (5)

Member's explanatory statement

These lines are removed to prevent material divergence from the EU Law Enforcement Directive.

LORD CLEMENT-JONES

127 Schedule 8, page 197, line 32, leave out sub-paragraph (b) and insert –

“(b) omit paragraph (b).”

Member's explanatory statement

The current effect of section 73(4)(b) of the Act is to restrict transfers for Competent Authorities who may have a legitimate operating need, and should possess the internal capability to assess that need, from making transfers to recipients who are not relevant authorities or international organisations. Removal of this restriction will enable them to do so where such a transfer is justified and necessary.

LORD CLEMENT-JONES

128 Schedule 8, page 203, line 9, leave out sub-paragraph (2)

Member's explanatory statement

The aim in removing sub-paragraph (2) is to prevent material divergence from the EU Law Enforcement Directive.

LORD CLEMENT-JONES

129 Schedule 8, page 204, line 13, leave out sub-paragraph (10)

Member's explanatory statement

The intention in removing this sub-paragraph would be to prevent material divergence from the EU Law Enforcement Directive.

Clause 85

LORD CLEMENT-JONES

130 Clause 85, page 101, line 18, at end insert –

“(aa) processing of personal data is carried out in a manner which does not permit the identification of a living individual,”

Member's explanatory statement

This amendment prevents processing of personal data for RAS purposes if it permits the identification of a living individual.

LORD STEVENSON OF BALMACARA
BARONESS KIDRON

131 Clause 85, page 102, line 7, at end insert –

“4A. The requirement is only satisfied if the data subject consents to the processing in accordance with Article 4(11).”

Member's explanatory statement

The amendment adds consent within the meaning of the existing UK GDPR as an appropriate safeguard for processing for research, archiving or statistical purposes.

LORD CLEMENT-JONES

132 Clause 85, page 102, line 38, at end insert –

“6. The requirement is not satisfied unless applicable dissents by the data subject are respected.”

Member's explanatory statement

This amendment ensures that existing patient dissents are respected and cannot be ignored.

LORD CLEMENT-JONES

Lord Clement-Jones gives notice of his intention to oppose the Question that Clause 85 stand part of the Bill.

Clause 87

LORD CLEMENT-JONES

Lord Clement-Jones gives notice of his intention to oppose the Question that Clause 87 stand part of the Bill.

Clause 88

LORD CLEMENT-JONES

Lord Clement-Jones gives notice of his intention to oppose the Question that Clause 88 stand part of the Bill.

Clause 89

BARONESS JONES OF WHITCHURCH

133 Clause 89, page 112, line 24, at end insert –

“(10) In section 199(2)(a) of the Investigatory Powers Act 2016 (bulk personal datasets: meaning of “personal data”), after “section 82(1) of that Act” insert “by an intelligence service”.”

Member's explanatory statement

Clause 88 of the Bill amends section 82 in Part 4 of the Data Protection Act 2018 (intelligence services processing). This amendment makes a consequential change to a definition in the Investigatory Powers Act 2016 which cross-refers to section 82.

LORD CLEMENT-JONES

Lord Clement-Jones gives notice of his intention to oppose the Question that Clause 89 stand part of the Bill.

Clause 90

LORD CLEMENT-JONES

134 Clause 90, page 113, leave out lines 1 to 5 and insert—

- “(a) to monitor the application of GDPR, the applied GDPR and this Act, and ensure are fully enforced with all due diligence;
- (b) to act upon receiving a complaint, to investigate, to the extent appropriate, the subject matter of the complaint, and to take steps to clarify unsubstantiated issues before dismissing the complaint.”

Member's explanatory statement

This amendment removes the secondary objectives introduced by the Data Use and Access Bill, which frame innovation, competition, crime prevention and national security as competing objectives against the enforcement of data protection law.

BARONESS KIDRON
LORD RUSSELL OF LIVERPOOL
LORD STEVENSON OF BALMACARA
BARONESS HARDING OF WINSCOMBE

135 Clause 90, page 113, leave out lines 15 to 17 and insert—

- “(e) the fact that children are entitled to a higher standard of protection than adults with regard to their personal data;
- (f) the need to prioritise children's best interests and to uphold their rights under UN Convention on the Rights of the Child and General Comment 25;
- (g) the fact that children may require different protections at different ages and stages of development;

(2) In this section, a “child” is a person under the age of 18.”

Member's explanatory statement

This amendment provides a list of the protections, rights and needs to children at different ages and stages of development that the Information Commissioner's must take into account when exercising their regulatory functions.

Clause 91

LORD CLEMENT-JONES

Lord Clement-Jones gives notice of his intention to oppose the Question that Clause 91 stand part of the Bill.

Clause 92

BARONESS JONES OF WHITCHURCH

136 Clause 92, page 117, line 24, leave out from “of” to the end of line 27 and insert “ –

- (a) a code prepared under section 124A, or
- (b) an amendment of such a code,

that is specified or described in the regulations.”

Member's explanatory statement

New section 124B(11) of the Data Protection Act 2018 provides that the Information Commissioner's duty to establish a panel to consider draft codes of practice may be disapplied or modified by regulations. This amendment ensures that regulations can make provision in relation to a particular code or amendment or a type of code or amendment.

LORD CLEMENT-JONES

Lord Clement-Jones gives notice of his intention to oppose the Question that Clause 92 stand part of the Bill.

After Clause 92

BARONESS KIDRON
LORD RUSSELL OF LIVERPOOL
LORD STEVENSON OF BALMACARA
BARONESS HARDING OF WINSCOMBE

137 After Clause 92, insert the following new Clause –

“Code of practice on children and AI

- (1) The Commissioner must prepare a code of practice in accordance with sections 91 and 92 which contains such guidance as the Commissioner considers appropriate on standards of fairness and ethical practice in the use of children's data and personal information in the development of AI including general purpose AI and use of foundational models that impact children.
- (2) In preparing a code or amendments under this section, the Commissioner must –
 - (a) have regard to –
 - (i) children's interests and fundamental rights and freedoms as set out in the United Nations Convention on the Rights of the Child

- and General Comment 25 on Children’s Rights in relation to the Digital Environment,
- (ii) the fact that children are entitled to a higher standard of protection than adults with regard to their personal data as established in the 2018 Act, and
 - (iii) the potential harm to future life chances, income, health and wellbeing,
 - (iv) the need for products and services likely to impact on children to be safe and equitable by design and default.
- (b) must consult with—
- (i) academics with expertise in the field, and
 - (ii) persons who appear to the Commissioner to represent the interests of children.
- (3) In this section—
- “fairness and ethical practice in the use of children’s data and personal information in the development of AI” means having regard to—
- (a) risk assessment;
 - (b) accountability;
 - (c) transparency;
 - (d) lawfulness;
 - (e) accuracy;
 - (f) fairness;
 - (g) ethical use;
- “impacts children” means AI technology that is—
- (a) based on data sets that include (or may include) children’s data;
 - (b) used to automate services likely to be accessed by children and access their data;
 - (c) used to make decisions that impact children;
 - (d) used to surface or deprioritise content, information, people, accounts, services or products to children;
 - (e) used to predict or inform children’s behaviour, opinions, opportunities and decision-making using personal data;
 - (f) used to imitate children’s physical likeness, movements, voice, behaviour and thoughts using personal data;
- “risk assessment” includes guidance on how controllers articulate and evaluate the following four stages—
- (a) the intention and goals in creating an AI model and how these have evolved over time;
 - (b) the inputs used to build, train and evolve an AI model;
 - (c) the assumptions and instructions that inform the AI model's decision-making;
 - (d) intended and actual outputs and outcomes of the AI model;

- (e) sufficient and consistent routes for complaint, redress and identification of emerging risk.”

Member's explanatory statement

Given the rapid acceleration in the development of AI technology, this Code of Practice ensures that data processors prioritise the interests and fundamental rights and freedoms of children and sets out what this means in practice.

LORD CLEMENT-JONES
BARONESS KIDRON

138

After Clause 92, insert the following new Clause –

“Code on processing personal data in education where it concerns a child or pupil

- (1) The Information Commissioner must consult on, prepare and publish a Code of Practice on standards to be followed in relation to the collection, processing, publication and other dissemination of personal data concerning children and pupils in connection with the provision of education services in the United Kingdom, within the meaning of the Education Act 1996, the Education (Scotland) Act 1996, and the Education and Libraries (Northern Ireland) Order 1986; and on standards on the rights of those children as data subjects which are appropriate to children’s capacity and stage of education.
- (2) For the purposes of subsection (1), the rights of data subjects must include –
 - (a) measures related to responsibilities of the controller, data protection by design and by default, and security of processing,
 - (b) safeguards and suitable measures with regard to automated decision-making, including profiling and restrictions,
 - (c) the rights of data subjects including to object to or restrict the processing of their personal data collected during their education, including any exemptions for research purposes, and
 - (d) matters related to the understanding and exercising of rights relating to personal data and the provision of education services.”

Member's explanatory statement

This amendment requires the Commission to consult on, prepare and publish a Code of Practice on standards to be followed in relation to the collection, processing, publication and other dissemination of personal data concerning children and pupils in connection with the provision of education services in the UK.

BARONESS KIDRON
LORD STEVENSON OF BALMACARA
LORD CLEMENT-JONES
LORD KNIGHT OF WEYMOUTH

139 After Clause 92, insert the following new Clause –

“Code of practice on data communities

- (1) The Commissioner must prepare a code of practice which contains –
 - (a) practical guidance on establishing, operating and joining a data community,
 - (b) practical guidance for data controllers and data processors on responding to requests made by data communities, and
 - (c) such other guidance as the Commissioner considers appropriate to promote good practice in all aspects of data communities schemes.
- (2) The data subject has the right to specify which data and which rights over that data they assign to the data community for what purpose and for how long, with respect to which data controllers.
- (3) In this section –

“good practice in data community” means such practice in as appears to the Commissioner to be desirable having regard to the interests of data subjects whose data forms part of a data community, including compliance with the requirements mentioned in subsection (1).”

Member's explanatory statement

This amendment requires the Commissioner to draw up a code of practice setting out the way in which data communities must operate and the requirements on data controllers and processors when engaging with data rights activation requests from data communities. In addition to the code of conduct, there would also be the full range of protections already in place with respect to any controller. It is one of a series of amendments that would establish the ability to assign data rights to a third party.

BARONESS KIDRON
LORD STEVENSON OF BALMACARA
LORD CLEMENT-JONES

140 After Clause 92, insert the following new Clause –

“Register and oversight of data communities

- (1) The Information Commissioner must maintain a register of data communities and make the register publicly available.
- (2) The criteria for suitability for inclusion in the register will be set out in the Code of Practice on Data Communities.
- (3) The Information Commissioner must create a complaints mechanism to receive, review and adjudicate complaints raised by data subjects about a data community controller.

- (4) Complaints under subsection (3) can only be based on a failure to meet the standards set out in the Code of Practice on Data Communities.
- (5) The Information Commissioner must create a complaints mechanism to receive, review and adjudicate complaints raised by a data community controller on behalf of its members about a data controller or processor.
- (6) Complaints under subsection (5) must be based on a failure to meet the standards set out in the Code of Practice on Data Communities.”

Member's explanatory statement

This amendment ensures that data communities operate transparently and are subject to regulatory oversight. It is one of a series of amendments that would establish the ability to assign data rights to a third party. A data community controller will have the responsibilities assigned to a controller as well as additional protections as set out the proposed code of conduct.

BARONESS KIDRON
LORD KNIGHT OF WEYMOUTH
LORD RUSSELL OF LIVERPOOL
BARONESS HARDING OF WINSCOMBE

141 After Clause 92, insert the following new Clause—

“Code of practice on Children's Data and Education

- (1) The Commissioner must prepare a code of practice which contains such guidance as the Commissioner considers appropriate on the processing of data in connection with the provision of education.
- (2) Guidance under subsection (1) must include consideration of—
 - (a) all aspects of the provision of education including learning, school management and safeguarding;
 - (b) all types of schools and learning settings;
 - (c) the need for transparency and evidence of efficacy on the use of AI systems in the provision of education;
 - (d) the impact of profiling and automated decision-making on children's access to education opportunities;
 - (e) that children have a right to know what data about them is being generated, collected, processed, stored and shared;
 - (f) that those with parental responsibility have a right to know how their children's data is being generated, collected, processed, stored and shared;
 - (g) the safety and security of children’s data;
 - (h) the need to ensure children's access to and use of counselling services and the exchange of information for safeguarding purposes are not restricted.
- (3) In preparing a code or amendments under this section, the Commissioner must have regard to—
 - (a) the fact that children are entitled to a higher standard of protection than adults with regard to their personal data as set out in the UK GDPR, and the ICO’s Age Appropriate Design code;

- (b) the need to prioritise children's best interests and to uphold their rights under UN Convention on the Rights of the Child and General Comment 25;
 - (c) the fact that children may require different protections at different ages and stages of development;
 - (d) the need to support innovation to enhance UK children's education and learning opportunities, including facilitating testing of novel products and supporting the certification and the development of standards;
 - (e) ensuring the benefits from product and service developed using UK children's data accrue to the UK.
- (4) In preparing a code or amendments under this section, the Commissioner must consult with—
- (a) children,
 - (b) educators,
 - (c) parents,
 - (d) persons who appear to the Commissioner to represent the interests of children,
 - (e) the AI Safety Institute, and
 - (f) the relevant Education department for each nation of the United Kingdom.
- (5) The Code applies to data processors and controllers that—
- (a) are providing education in school or other learning settings;
 - (b) provide services or products in connection with the provision of education;
 - (c) collect children's data whilst they are learning;
 - (d) use education data, education data sets or pupil data to develop services and products;
 - (e) build, train or operate AI systems and models that impact children's learning experience or outcomes;
 - (f) are public authorities that process education data, education data sets or pupil data.
- (6) The Commissioner must prepare a report, in consultation with the EdTech industry and other stakeholders set out in paragraph 3, on the steps required to develop a certification scheme under Article 42 of the UK GDPR, to enable the industry to demonstrate the compliance of EdTech services and products with the UK GDPR, and conformity with this Code.
- (7) Where requested by an education service, evidence of compliance with this Code must be provided by relevant providers of commercial products and services in a manner that satisfies the education service's obligations under the Code.
- (8) In this section—
- “EdTech” means a service or product that digitise education functions including administration and management information systems, learning and assessment and safeguarding, including services or products used within school settings and at home on the recommendation, advice or instruction of a school;

“education data” means personal data that forms part of an educational record.

“education data sets” means anonymised or pseudonymised data sets that include Education Data or Pupil Data.

“efficacy” means that the promised learning outcomes can be evidenced.

“learning setting ” means a place where children learn including schools, their home and extra-curricular learning services for example online and in-person tutors.

“pupil data” means personal data about a child collected whilst they are learning which does not form part of an educational record.

“safety and security” means that it has been adequately tested.

“school” means an entity that provides education to children in the UK including early years providers, nursery schools, primary schools, secondary schools, sixth form colleges, city technology colleges, academies, free schools, faith schools, special schools, state boarding schools, and private schools.”

Member's explanatory statement

This amendment proposes a statutory Code of Practice on Children and Education to ensure that children benefit from heightened protections when their data is processed for purposes relating to education. Common standards across the sector will assist schools in procurement.

Clause 95

VISCOUNT CAMROSE
LORD MARKHAM

142 Clause 95, page 119, leave out line 16

Member's explanatory statement

This amendment prevents official notices from the Commissioner being sent via email.

VISCOUNT CAMROSE
LORD MARKHAM

143 Clause 95, page 120, leave out lines 11 and 12

Member's explanatory statement

The amendment removes the assumption that an email has been received within 48 hours of being sent.

After Clause 95

LORD CLEMENT-JONES

144 After Clause 95 insert the following new Clause –**“Provision about the use of reprimands under Article 58 of the UK GDPR**

- (1) The United Kingdom General Data Protection Regulation is amended as follows.
- (2) In Article 58, paragraph 2, leave out point (b) and insert –
 - “(b) to issue not more than one reprimand over the course of three years to a controller or a processor where processing operations have infringed provisions of this Regulation.””

Member's explanatory statement

This amendment ensures that the Commissioner cannot over-rely on reprimands by limiting its powers to issuing only one to a given controller over a fixed period.

LORD CLEMENT-JONES

144A★ After Clause 95, insert the following new Clause –**“Duty to report: regulatory activity in United Kingdom nations**

The Information Commissioner must publish an annual report on the regulatory activity they have undertaken in each constituent part of the United Kingdom.”

Clause 101

BARONESS KIDRON
LORD RUSSELL OF LIVERPOOL
LORD STEVENSON OF BALMACARA
BARONESS HARDING OF WINSCOMBE

145 Clause 101, page 129, line 32, at end insert –

- “(5A) The report must –
- (a) set out separately the information required under subsections (2) to (5) where regulatory action or policy relates to children;
 - (b) provide details of all activities carried out by the Information Commissioner to support, strengthen and uphold the Age-Appropriate Design Code;
 - (c) provide information about how it has met its child-related duties under section 120B (e)-(h).”

Member's explanatory statement

This amendment would ensure that the ICO's annual report records activities and action taken by the ICO in relation to children. This would enhance understanding, transparency and accountability.

Clause 103

LORD CLEMENT-JONES

146 Clause 103, page 131, line 23, leave out “court” and insert “tribunal”

Member's explanatory statement

This amendment is consequential on the new Clause (Transfer of jurisdiction of courts to tribunals).

LORD CLEMENT-JONES

147 Clause 103, page 131, line 26, leave out “court” and insert “tribunal”

Member's explanatory statement

This amendment is consequential on the new Clause (Transfer of jurisdiction of courts to tribunals).

LORD CLEMENT-JONES

148 Clause 103, page 131, line 34, leave out “court” and insert “tribunal”

Member's explanatory statement

This amendment is consequential on the new Clause (Transfer of jurisdiction of courts to tribunals).

LORD CLEMENT-JONES

149 Clause 103, page 131, line 35, leave out “court” and insert “tribunal”

Member's explanatory statement

This amendment is consequential on the new Clause (Transfer of jurisdiction of courts to tribunals).

LORD CLEMENT-JONES

150 Clause 103, page 132, line 2, leave out “court” and insert “tribunal”

Member's explanatory statement

This amendment is consequential on the new Clause (Transfer of jurisdiction of courts to tribunals).

After Clause 103

LORD CLEMENT-JONES

151 After Clause 103, insert the following new Clause –

“Right of appeal against Commissioner’s decision on complaint

(1) The 2018 Act is amended as follows.

- (2) After section 166 insert –

“166A Appeals against decisions on complaints

- (1) This section applies where a data subject makes a complaint under section 165 or Article 77 of the UK GDPR and the Commissioner makes a decision on the complaint.
 - (2) The data subject may appeal to the Tribunal against all or any part of the decision.
 - (3) The Tribunal must determine any appeal under this section on the merits by reference to the grounds of appeal set out in the notice of appeal.
 - (4) The Tribunal may review any determination of fact on which the decision against which the appeal is brought was based.
 - (5) If the Tribunal considers –
 - (a) that the decision against which the appeal is brought is not in accordance with the law, or
 - (b) to the extent that the decision involved an exercise of discretion by the Commissioner, that the Commissioner ought to have exercised the discretion differently,the Tribunal must allow the appeal.
 - (6) Where the Tribunal allows the appeal, the Tribunal must set aside the decision and –
 - (a) remit the complaint to the Commissioner, or
 - (b) vary the decision.
 - (7) The power to vary the decision of the Commissioner includes the power to substitute another decision which the Commissioner could have given or made.
 - (8) Otherwise, the Tribunal must dismiss the appeal.”
- (3) In section 202 (proceedings in the First-tier Tribunal: contempt), in subsection (1)(a)(ii) after “166” insert “or 166A”.
- (4) In section 203 (Tribunal Procedure Rules), in subsection (1)(b) after “166” insert “or 166A”.

Member's explanatory statement

This new Clause seeks to address the jurisdictional confusion in the 2018 Act, in addition to the new Clause (Transfer of jurisdiction of courts to tribunals).

LORD CLEMENT-JONES

152 After Clause 103, insert the following new Clause –

“Procedure for Tribunal Procedure Rules

- (1) The first time after the passing of this Act that Tribunal Procedure Rules are made for the purposes of section 203 of the 2018 Act (Tribunal Procedure Rules) in connection with any amendment made by this Act to that Act, the Rules may be made by the Lord Chancellor rather than by the Tribunal Procedure Committee.
- (2) Before making Tribunal Procedure Rules by virtue of subsection (1), the Lord Chancellor must consult –
 - (a) the Senior President of Tribunals;
 - (b) the Lord Chief Justice of England and Wales;
 - (c) the Lord President of the Court of Session;
 - (d) the Lord Chief Justice of Northern Ireland.
- (3) The Lord Chancellor is not required to undertake any other consultation before making Tribunal Procedure Rules by virtue of subsection (1).
- (4) A requirement to consult under subsection (2) may be satisfied by consultation that took place wholly or partly before the passing of this Act.
- (5) Tribunal Procedure Rules made by virtue of subsection (1) are to be made by statutory instrument.
- (6) A statutory instrument containing Tribunal Procedure Rules made by virtue of subsection (1) must be laid before Parliament after being made.
- (7) Tribunal Procedure Rules contained in a statutory instrument laid before Parliament under subsection (6) cease to have effect at the end of the period of 40 days beginning with the day on which the instrument is made unless, during that period, the instrument is approved by a resolution of each House of Parliament.
- (8) In calculating the period of 40 days, no account is to be taken of any whole days that fall within a period during which –
 - (a) Parliament is dissolved or prorogued; or
 - (b) either House of Parliament is adjourned for more than four days.
- (9) If Tribunal Procedure Rules cease to have effect as a result of subsection (7) –
 - (a) that does not affect the validity of anything previously done under the Rules; and
 - (b) subsection (1) applies again as if the Rules had not been made.
- (10) In this section “Tribunal Procedure Committee” means the committee of that name constituted under Part 2 of Schedule 5 to the Tribunals, Courts and Enforcement Act 2007.”

Member's explanatory statement

This new Clause allows the Lord Chancellor to make Tribunal Procedure Rules instead of the Tribunal Procedure Committee for the purposes of the new Clause (Transfer of jurisdiction of courts to tribunals) for the first time, to allow expedition and flexibility.

After Clause 104

LORD CLEMENT-JONES

153 After Clause 104, insert the following new Clause –

“Transfer of jurisdiction of courts to tribunals

In Schedule (*Amendments to the 2018 Act: Transfer of jurisdiction of courts to tribunals*) –

- (a) Part 1 makes provision for and in connection with the transfer of the jurisdiction of courts to tribunals in the 2018 Act; and
- (b) Part 2 makes transitional provision in connection with the amendments made by Part 1 of that Schedule.”

Member's explanatory statement

*This new Clause, and the related new Schedule, seek to address voluminous judgments of certain courts and tribunals (in particular, *Killock and others v Information Commissioner* [2021] UKUT AAC (299) and *R (Delo) v Information Commissioner* [2023] EWCA Civ 1141; [2022] EWHC 3046 (Admin)), of the jurisdictional confusion in the Data Protection Act 2018, by transferring the jurisdiction of courts to tribunals to create a simplified appeals system in the tribunals.*

After Clause 107

LORD CLEMENT-JONES

154 After Clause 107, insert the following new Clause –

“Safeguards: exemptions etc from the UK GDPR

In Schedule 2 to the Data Protection Act 2018 (exemptions etc from the UK GDPR), after paragraph 1 insert –

“Safeguards

- 1A (1) Except where paragraphs 4, 26 or 27 are engaged, an exemption in this Schedule will not be applicable unless the decision to apply that exemption has been made in accordance with this paragraph.
- (2) In this paragraph, “relevant listed GDPR provision” means the relevant listed GDPR provision in Parts I to 4 of this Schedule (other than paragraph 4).
- (3) In this paragraph, “exemption” means a restriction within the meaning of Article 23(1) of the UK GDPR (restrictions).

- (4) Where a controller wishes to rely on an exemption from a relevant listed GDPR provision, that decision must be made –
 - (a) on a case by case basis,
 - (b) separately in respect of each of the relevant listed GDPR provisions which are being restricted in accordance with the relevant provisions of this Schedule, and
 - (c) afresh on each occasion on which the controller considers an exemption to any of the relevant listed GDPR provisions.
- (5) When making a decision to rely on an exemption, the controller must take into account all the circumstances of the case, including at least the following –
 - (a) any potential vulnerability of the data subject that is relevant to the decision,
 - (b) all the rights and freedoms of the data subject, and
 - (c) the need to ensure compliance with the UK GDPR.
- (6) Where compliance with a particular provision listed in Article 23(1) of the UK GDPR (restrictions) and the relevant provisions of this Schedule enable the application of an exemption to the extent that compliance with the UK GDPR would be likely to prejudice a particular matter or activity specified in this Schedule, a decision to apply the exemption may be made only if –
 - (a) the application of that provision or those provisions would give rise to a substantial risk of prejudice to any of the matters mentioned in the relevant provision of Schedule 2,
 - (b) that risk outweighs the risk of prejudice to the interests of the data subject concerned that would arise if the exemption were to apply in relation to that provision or those provisions, and
 - (c) the application of the exemption in relation to that provision or those provisions is necessary and proportionate to the risks in the particular case.

Safeguards: record of decision that exemption applies

- 1B (1) Where a controller makes a decision mentioned in paragraph 1A(4) or (5), the controller must keep a record of it and the reasons for it.
- (2) Where an exemption from a relevant listed GDPR provision has been applied, the controller must also inform the data subject of the decision unless, in the particular circumstances of the case, the controller considers that doing so may be prejudicial to any of the matters mentioned in the relevant provision of Schedule 2.””

Member's explanatory statement

This amendment ensures that the protections which have been applied to the immigration exemption in paragraph 4 of Schedule 2 to the Data Protection Act 2018 through the Data Protection Act 2018 (Amendment of Schedule 2 Exemptions) Regulations 2024 can apply across the board.

LORD CLEMENT-JONES

155 After Clause 107, insert the following new Clause –

“Safeguards: exemptions etc from the UK GDPR: health, social work, education and child abuse data

In Schedule 3 to the Data Protection Act 2018 (exemptions etc from the UK GDPR: health, social work, education and child abuse data), after paragraph 1 insert –

“Safeguards

- 1A (1) An exemption from the relevant listed GDPR provisions in this Schedule will not be applicable unless the decision to apply that exemption has been made in accordance with this paragraph 1A.
- (2) In this paragraph, “relevant listed GDPR provision” means the relevant listed GDPR provision in this Schedule.
- (3) In this paragraph, “exemption” means a restriction within the meaning of Article 23(1) of the UK GDPR (restrictions).
- (4) Where a controller wishes to rely on an exemption from a relevant listed GDPR provision, that decision must be made –
 - (a) on a case by case basis,
 - (b) separately in respect of each of the relevant listed GDPR provisions which are being restricted in accordance with the relevant provisions of this Schedule, and
 - (c) afresh on each occasion on which the controller considers an exemption to any of the relevant listed GDPR provisions.
- (5) When making a decision to rely on an exemption, the controller must take into account all the circumstances of the case, including at least the following –
 - (a) any potential vulnerability of the data subject that is relevant to the decision,
 - (b) all the rights and freedoms of the data subject, and
 - (c) the need to ensure compliance with the UK GDPR.
- (6) Where compliance with a particular provision listed in Article 23(1) of the UK GDPR (restrictions) and the relevant provisions of this Schedule enable the application of an exemption to the extent that compliance with the UK GDPR would be likely to prejudice a particular matter or activity specified in this Schedule, a decision to apply the exemption may be made only if –

- (a) the application of that provision or those provisions would give rise to a substantial risk of prejudice to any of the matters mentioned in the relevant provision of Schedule 3,
- (b) that risk outweighs the risk of prejudice to the interests of the data subject concerned that would arise if the exemption were to apply in relation to that provision or those provisions, and
- (c) the application of the exemption in relation to that provision or those provisions is necessary and proportionate to the risks in the particular case.

Safeguards: record of decision that exemption applies

- 1B (1) Where a controller makes a decision mentioned in paragraph 1A(4) or (5), the controller must keep a record of it and the reasons for it.
- (2) Where an exemption from a relevant listed GDPR provision has been applied, the controller must also inform the data subject of the decision unless, in the particular circumstances of the case, the controller considers that doing so may be prejudicial to any of the matters mentioned in the relevant provision of Schedule 3.””

Member's explanatory statement

Schedule 3 contains exemptions from listed GDPR provisions in the context of health, social work education and child abuse data. This amendment extends the protections which now apply in the context of immigration to these areas.

LORD CLEMENT-JONES

156 After Clause 107, insert the following new Clause –

“Safeguards: exemptions etc from the UK GDPR: disclosure prohibited or restricted by an enactment

In Schedule 4 to the Data Protection Act 2018 (exemptions etc from the UK GDPR: disclosure prohibited or restricted by an enactment), after paragraph 1 insert –

“Safeguards

- 1A (1) An exemption from the relevant listed GDPR provisions in this Schedule will not be applicable unless the decision to apply that exemption has been made in accordance with this paragraph.
- (2) In this paragraph, “relevant listed GDPR provision” means the relevant listed GDPR provision in Parts I to 4 of this Schedule (other than paragraph 4).
- (3) In this paragraph, “exemption” means a restriction within the meaning of Article 23(1) of the UK GDPR (restrictions).

- (4) Where a controller wishes to rely on an exemption from a relevant listed GDPR provision, that decision must be made—
 - (a) on a case by case basis,
 - (b) separately in respect of each of the relevant listed GDPR provisions which are being restricted in accordance with the relevant provisions of this Schedule, and
 - (c) afresh on each occasion on which the controller considers an exemption to any of the relevant listed GDPR provisions.
- (5) When making a decision to rely on an exemption, the controller must take into account all the circumstances of the case, including at least the following—
 - (a) any potential vulnerability of the data subject that is relevant to the decision,
 - (b) all the rights and freedoms of the data subject, and
 - (c) the need to ensure compliance with the UK GDPR.

Safeguards: record of decision that exemption applies

- 1B (1) Where a controller makes a decision mentioned in paragraph 1A(4), the controller must keep a record of it and the reasons for it.
- (2) Where an exemption from a relevant listed GDPR provision has been applied, the controller must also inform the data subject of the decision unless, in the particular circumstances of the case, the controller considers that doing so may be prejudicial to any of the matters mentioned in the relevant provision of Schedule 4.””

Member's explanatory statement

Schedule 4 contains exemptions from listed GDPR provisions where disclosure is prohibited or restricted by an enactment. This amendment extends the protections which now apply in the context of immigration to these areas.

LORD HOLMES OF RICHMOND
LORD CLEMENT-JONES

156A After Clause 107, insert the following new Clause—

“Data use: definition of unauthorised access to computer programs or data

In section 17 of the Computer Misuse Act 1990, at the end of subsection (5) insert—

- “(c) they do not reasonably believe that the person entitled to control access of the kind in question to the program or data would have consented to that access if they had known about the access and the circumstances of it, including the reasons for seeking it, and

- (d) they are not empowered by an enactment, by a rule of law, or by order of a court or tribunal to access of the kind in question to the program or data.””

LORD HOLMES OF RICHMOND
LORD CLEMENT-JONES

156B After Clause 107, insert the following new Clause –

“Data use: defences to charges under the Computer Misuse Act 1990

- (1) The Computer Misuse Act 1990 is amended as follows.
- (2) In section 1, after subsection (3) insert –
- “(4) It is a defence to a charge under subsection (1) to prove that –
- (a) the person’s actions were necessary for the detection or prevention of crime, or
- (b) the person’s actions were justified as being in the public interest.”
- (3) In section 3, after subsection (6) insert –
- “(7) It is a defence to a charge under subsection (1) in relation to an act carried out for the intention in subsection (2)(b) or (c) to prove that –
- (a) the person’s actions were necessary for the detection or prevention of crime, or
- (b) the person’s actions were justified as being in the public interest.””

Member’s explanatory statement

This amendment updates the definition of “unauthorised access” in the Computer Misuse Act 1990 to provide clearer legal protections for legitimate cybersecurity activities.

Before Schedule 11

LORD CLEMENT-JONES

157 Before Schedule 11, insert the following new Schedule –

“SCHEDULE

AMENDMENTS TO THE 2018 ACT: TRANSFER OF JURISDICTION OF COURTS TO TRIBUNALS

PART 1

TRANSFER OF JURISDICTION

- 1 The 2018 Act is amended as follows.
- 2 In section 44(5)(e) (information: controller’s general duties), for “court” substitute “tribunal”.

- 3 In section 45(5)(e) (right of access by the data subject), for “court” substitute “tribunal”.
- 4 (1) Section 48 (rights under sections 46 or 47: supplementary) is amended as follows.
 - (2) In subsection (1)(b)(iv) for “court” substitute “tribunal”.
 - (3) In subsection (4)(d) for “court” substitute “tribunal”.
- 5 In section 51(5) (exercise of rights through the Commissioner), for “court” substitute “tribunal”.
- 6 (1) Section 94 (right of access) is amended as follows.
 - (2) In subsection (11), in both instances, for “court” substitute “tribunal”.
 - (3) In subsection (12), for “court” substitute “tribunal”.
 - (4) In subsection (13), for first “court” substitute “tribunal”.
 - (5) In subsection (13), for “the High Court or, in Scotland, by the Court of Session” substitute “the Upper Tribunal”.
- 7 (1) Section 99 (right to object to processing) is amended as follows.
 - (2) In subsection (5), in every instance, for “court” substitute “tribunal”.
 - (3) In subsection (6), for “court” substitute “tribunal”.
 - (4) In subsection (7), for first “court” substitute “tribunal”.
 - (5) In subsection (7), for “the High Court or, in Scotland, by the Court of Session” substitute “the Upper Tribunal”.
- 8 (1) Section 100 (rights to rectification and erasure) is amended as follows.
 - (2) In subsection (1), in both instances, for “court” substitute “tribunal”.
 - (3) In subsection (2), in both instances, for “court” substitute “tribunal”.
 - (4) In subsection (3), for “court” substitute “tribunal”.
 - (5) In subsection (4), in both instances, for “court” substitute “tribunal”.
 - (6) In subsection (5), in both instances, for “court” substitute “tribunal”.
 - (7) In subsection (6), for first “court” substitute “tribunal”.
 - (8) In subsection (6), for “the High Court or, in Scotland, by the Court of Session” substitute “the Upper Tribunal”.
- 9 (1) Section 145 (information orders) is amended as follows.
 - (2) In subsection (1), for “court” substitute “tribunal”.
 - (3) In subsection (2), in both instances, for “court” substitute “tribunal”.
- 10 (1) Section 152 (enforcement notices: restrictions) is amended as follows.
 - (2) In subsection (1)(b), for “court” substitute “tribunal”.
 - (3) In subsection (2), in both instances, for “court” substitute “tribunal”.
- 11 (1) Section 156 (penalty notices: restrictions) is amended as follows.
 - (2) In subsection (1)(b), for “court” substitute “tribunal”.

- (3) In subsection (2), in both instances, for “court” substitute “tribunal”.
- 12 (1) Section 164 (applications in respect of urgent notices) is amended as follows.
- (2) In subsection (2), for “court” substitute “tribunal”.
- (3) In subsection (3), for “court” substitute “tribunal”.
- (4) In subsection (4), for “court” substitute “tribunal”.
- 13 In the italic heading before section 165 (complaints by data subjects), after “Complaints” insert “and remedies in the tribunal”.
- 14 Omit the italic heading before section 167 (compliance orders).
- 15 (1) Section 167 (compliance orders) is amended as follows.
- (2) In subsection (1), for “court” substitute “tribunal”.
- (3) In subsection (2), for “court” substitute “tribunal”.
- (4) In subsection (5), for “court” substitute “tribunal”.
- 16 (1) Section 168 (compensation for contravention of the UK GDPR) is amended as follows.
- (2) In subsection (2)(a), for “rules of court” substitute “Tribunal Procedure Rules”.
- (3) In subsection (2)(b), for “court” substitute “tribunal”.
- (4) In subsection (3) in both instances, for “court” substitute “tribunal”.
- 17 (1) Section 175 (provision of assistance in special purposes proceedings) is amended as follows.
- (2) In subsection (7), for “rules of court” substitute “Tribunal Procedure Rules”.
- (3) In subsection (7)(a), for “court” substitute “tribunal”.
- (4) In subsection (8), for “rules of court” substitute “Tribunal Procedure Rules”.
- (5) In subsection (8)(a), for “court” substitute “tribunal”.
- 18 (1) Section 176 (staying special purposes proceedings) is amended as follows.
- (2) In subsection (1), in every instance, for “court” substitute “tribunal”.
- (3) In subsection (3), for “court” substitute “tribunal”.
- 19 In section 177(5)(b) (guidance about how to seek redress against media organisations) for “court” substitute “tribunal”.
- 20 In the italic cross heading before section 180 (jurisdiction) for “courts” substitute “tribunals”.
- 21 (1) Section 180 (jurisdiction) is amended as follows.
- (2) For subsection (1) substitute—
- “(1) The jurisdiction conferred on a tribunal by the provisions listed in subsection (2) are exercisable by the First-tier tribunal, subject to subsections (3), (4) and (5).”.

- (3) In subsection (3), for “the High Court or, in Scotland, the Court of Session” substitute “the Upper Tribunal”.
- (4) In subsection (4) for first "court" substitute "tribunal".
- (5) In subsection (4), for “the High Court or, in Scotland, the Court of Session” substitute “the Upper Tribunal”.
- (6) In subsection (5), for “the High Court or, in Scotland, the Court of Session” substitute “the Upper Tribunal”.
- 22 In section 202 (proceedings in the First-tier Tribunal: contempt), for subsection (1)(a) substitute –
- “(a) person does something, or fails to do something, in relation to proceedings before the First-tier Tribunal under sections 27, 45, 46, 51, 79, 94, 99, 100, 111, 162, 166, 167, 168, 175, 176, 177, and”
- 23 In section 203 (Tribunal Procedure Rules), for subsection (1) substitute –
- “(1) Tribunal Procedure Rules may make provision for regulating –
- (a) the exercise of the rights of appeal conferred by, or
- (b) the rights of data subjects (including their exercise by a representative body) under,
- sections 27, 45, 46, 51, 79, 94, 99, 100, 111, 162, 166, 167, 168, 175, 176, 177.”

PART 2

TRANSITIONAL PROVISION

- 24 Any proceedings before a relevant court listed in paragraph 26 which are pending immediately before this Schedule comes into force must continue on after this Schedule comes into force as proceedings before the Upper Tribunal.
- 25 Any proceedings before a relevant court listed in paragraph 27 which are pending immediately before this Schedule comes into force must continue on after this Schedule comes into force as proceedings before the First-tier Tribunal.
- 26 The relevant courts listed in this paragraph are –
- (a) in England and Wales, the High Court;
- (b) in Scotland, the Court of Session;
- (c) in Northern Ireland, the High Court.
- 27 The relevant courts listed in this paragraph are –
- (a) in England and Wales, the County Court;
- (b) in Scotland, the sheriff;
- (c) in Northern Ireland, a county court.
- 28 It is immaterial the stage of the proceedings in the court before the proceedings are transferred.
- 29 The Upper Tribunal may by order transfer any proceedings automatically transferred to it from a court in pursuance of this Schedule to the First-tier Tribunal, if the Upper Tribunal considers it appropriate.

- 30 The Upper Tribunal may by order transfer any proceedings from the First-tier Tribunal to the Upper Tribunal which have been automatically transferred to the First-tier Tribunal from a court in pursuance of this Schedule, if the Upper Tribunal considers it appropriate.
- 31 The First-tier Tribunal may by order transfer any proceedings automatically transferred to it from a court in pursuance of this Schedule to the Upper Tribunal, if the First-tier Tribunal considers it appropriate.
- 32 The decision to transfer proceedings under this Schedule is final and is not liable to be questioned in any court or tribunal.”

Member's explanatory statement

This new Schedule, and the related new Clause, seek to address voluminous judgments of certain courts and tribunals (in particular, Killock and others v Information Commissioner [2021] UKUT AAC (299) and R (Delo) v Information Commissioner [2023] EWCA Civ 1141; [2022] EWHC 3046 (Admin)), of the jurisdictional confusion in the Data Protection Act 2018, by transferring the jurisdiction of courts to tribunals to create a simplified appeals system in the tribunals.

Clause 109

LORD LUCAS

- 158 Clause 109, page 139, line 14, after “individuals” insert “and does not include communications that are necessary to avoid harm or improve consumer outcomes when complying with a legal basis or legislative measure provided by a regulatory authority”

Member's explanatory statement

This amendment would ensure that financial services firms are able to comply with current and future regulatory requirements, such as the FCA’s new Consumer Duty, which expect firms to communicate with customers to ensure good customer outcomes. This amendment aligns to the wording of the UK GDPR (Recital 41) and includes Consumer Duty language of avoiding harm/improving outcomes.

Schedule 12

LORD CLEMENT-JONES

- 159 Schedule 12, page 219, line 12, at the end insert –
- “(4) The means by which the subscriber or user may signify consent may not require the subscriber or user to make a payment in order to signify their consent to the storage or access.”

Member's explanatory statement

This amendment would ban cookie paywalls.

VISCOUNT CAMROSE

159A★ Schedule 12, page 219, line 12, at end insert –

“(4) The means by which the subscriber may decline the storage or access may require the subscriber or user to make a payment.”

Member's explanatory statement

This amendment would permit the use of cookie paywalls in statute.

LORD CLEMENT-JONES

LORD LUCAS

160 Schedule 12, page 220, line 15, at end insert –

“(iii) to measure or verify the performance of advertising services delivered as part of the service requested to enable website owners to accurately charge for their advertising services.”

Member's explanatory statement

This amendment seeks to ensure that the technical storage of, or access to, information is considered strictly necessary if it would support the measurement or verification of the performance of advertising services to allow website owners to charge for their advertising services more accurately.

After Clause 114

LORD LUCAS

161 After Clause 114, insert the following new Clause –

“Extending the soft opt-in to workplace pensions

- (1) Regulation 22 of the PEC Regulations (use of electronic mail for direct marketing purposes) is amended as follows.
- (2) In paragraph (2), after “paragraph (3)” insert “or (3A)”.
- (3) After paragraph (3) insert –

“(3A) A person may send or instigate the sending of electronic mail for the purposes of direct marketing where –

- (a) that person has obtained the contact details of the recipient of that electronic mail in the course of establishing a product or service for the benefit of that recipient as instructed by or on behalf of the employer of that recipient fulfilling a legislative requirement;
- (b) the direct marketing is in respect of that person’s product or service established for the recipient or that person’s similar products and services only;
- (c) the recipient is given, at the time of each communication, a simple means of refusing (free of charge except for the costs of the transmission of the

refusal) the use of their contact details for the purposes of such direct marketing.””

Member's explanatory statement

This is to rectify an unintended consequence of the UK's Automatic Enrolment policy, where it is employers who set up pension arrangements. Individuals, therefore, often have not been given the opportunity to consent to receive communications for that product, meaning that they may be losing out on engaging and helpful content from their pension provider. This amendment gives that individual the opportunity to opt-out of direct marketing where previously they did not have the opportunity to opt-in.

LORD CLEMENT-JONES
LORD BLACK OF BRENTWOOD
BARONESS HARDING OF WINSCOMBE

162 After Clause 114, insert the following new Clause –

“Soft opt-in for email marketing for charities

- (1) Regulation 22 of the PEC Regulations (use of electronic mail for direct marketing purposes) is amended as follows.
- (2) In paragraph (2), after “paragraph (3)” insert “or (3A)”.
- (3) After paragraph (3) insert –
 - “(3A) A person may send or instigate the sending of electronic mail for the purposes of direct marketing where –
 - (a) the direct marketing is solely for the purpose of furthering a charitable objective of that person,
 - (b) that person obtained the contact details of the recipient of the electronic mail in the course of the recipient expressing an interest in or offering or providing support for the furtherance of that objective or a similar objective, and
 - (c) the recipient has been given a simple means of refusing (free of charge except for the costs of the transmission of the refusal) the use of their contact details for the purposes of such direct marketing, at the time that the details were initially collected, and, where the recipient did not initially refuse the use of the details, at the time of each subsequent communication.””

Member's explanatory statement

This amendment will enable charities to communicate to donors in the same way that businesses have been able to communicate to customers since 2003. The clause will help facilitate greater fundraising and support the important work charities do for society.

Schedule 14

LORD CLEMENT-JONES

- 163 Schedule 14, page 231, line 21, leave out “the Secretary of State” and insert “person who chairs the relevant Parliamentary Committee”

Member's explanatory statement

This amendment and others in the name of Lord Clement-Jones to Schedule 14 remove the involvement of the Secretary of State with the functions of the Commissioner and transfers the responsibility to appoint the Commissioner from government to parliament.

LORD CLEMENT-JONES

- 164 Schedule 14, page 231, leave out lines 25 to 29

LORD CLEMENT-JONES

- 165 Schedule 14, page 232, leave out lines 4 to 6 and insert “appointed by His Majesty by Letters Patent on the recommendation of the person who chairs the relevant Parliamentary committee, and must include at least two members appointed for the specific task of overseeing regulatory complaints and the rights and freedoms of data subjects.”

LORD CLEMENT-JONES

- 166 Schedule 14, page 232, line 12, leave out “Secretary of State” and insert “person who chairs the relevant Parliamentary Committee”

LORD CLEMENT-JONES

- 167 Schedule 14, page 232, line 16, leave out sub-paragraph (6) and insert –

“(6) The non-executive members must exercise the powers conferred on the non-executive members by sub-paragraph (3) so as to secure that the number of non-executive members of the Commission is, so far as practicable, at all times greater than the number of executive members.”

LORD CLEMENT-JONES

- 167A Schedule 14, page 232, line 22, at end insert –

“Membership: non-executive members expertise

3A In making recommendations of persons for appointment as non-executive members, the Secretary of State must ensure that the membership of the Commission includes non-executive members with expertise in –

(a) civil liberties and freedom of expression,

- (b) public administration,
- (c) international trade,
- (d) business and economics,
- (e) consumer rights, and
- (f) children's rights."

Member's explanatory statement

To ensure that non-executive members of the Commission have a sufficient balance of expertise to inform the Commission outside of purely data protection issues.

LORD CLEMENT-JONES

- 168 Schedule 14, page 232, line 30, leave out "Secretary of State" and insert "person who chairs the relevant Parliamentary committee"

LORD CLEMENT-JONES

- 169 Schedule 14, page 233, line 5, leave out "Secretary of State" and insert "person who chairs the relevant Parliamentary committee"

LORD CLEMENT-JONES

- 170 Schedule 14, page 233, line 7, leave out "Secretary of State" and insert "person who chairs the relevant Parliamentary committee"

LORD CLEMENT-JONES

- 171 Schedule 14, page 233, line 9, leave out "Secretary of State" and insert "person who chairs the relevant Parliamentary committee"

LORD CLEMENT-JONES

- 172 Schedule 14, page 233, line 10, leave out "Secretary of State considers" and insert "they consider"

LORD CLEMENT-JONES

- 173 Schedule 14, page 233, line 15, leave out "Secretary of State" and insert "person who chairs the relevant Parliamentary committee"

LORD CLEMENT-JONES

- 174 Schedule 14, page 233, line 25, leave out "Secretary of State" and insert "person who chairs the relevant Parliamentary committee"

LORD CLEMENT-JONES

- 175 Schedule 14, page 233, line 34, leave out “Secretary of State” and insert “person who chairs the relevant Parliamentary committee”

LORD CLEMENT-JONES

- 176 Schedule 14, page 233, line 35, leave out “Secretary of State” and insert “person who chairs the relevant Parliamentary committee”

LORD CLEMENT-JONES

- 177 Schedule 14, page 234, line 10, leave out “Secretary of State” and insert “person who chairs the relevant Parliamentary committee”

LORD CLEMENT-JONES

- 178 Schedule 14, page 234, line 16, leave out “Secretary of State” and insert “person who chairs the relevant Parliamentary committee”

LORD CLEMENT-JONES

- 179 Schedule 14, page 234, line 19, leave out “Secretary of State” and insert “person who chairs the relevant Parliamentary committee”

LORD CLEMENT-JONES

- 180 Schedule 14, page 234, line 23, leave out “Secretary of State” and insert “person who chairs the relevant Parliamentary committee”

LORD CLEMENT-JONES

- 181 Schedule 14, page 234, line 24, leave out “Secretary of State” and insert “person who chairs the relevant Parliamentary committee”

LORD CLEMENT-JONES

- 182 Schedule 14, page 234, line 31, leave out “Secretary of State” and insert “person who chairs the relevant Parliamentary committee”

LORD CLEMENT-JONES

- 183 Schedule 14, page 234, line 33, leave out “Secretary of State” and insert “person who chairs the relevant Parliamentary committee”

LORD CLEMENT-JONES

- 184 Schedule 14, page 235, line 3, leave out “Secretary of State” and insert “person who chairs the relevant Parliamentary committee”

LORD CLEMENT-JONES

- 185 Schedule 14, page 235, line 9, leave out “Secretary of State” and insert “person who chairs the relevant Parliamentary committee”

LORD CLEMENT-JONES

- 186 Schedule 14, page 235, line 11, leave out “Secretary of State” and insert “person who chairs the relevant Parliamentary committee”

LORD CLEMENT-JONES

- 187 Schedule 14, page 235, line 15, leave out “Secretary of State” and insert “person who chairs the relevant Parliamentary committee”

LORD CLEMENT-JONES

- 188 Schedule 14, page 240, line 9, leave out “Secretary of State” and insert “person who chairs the relevant Parliamentary committee”

LORD CLEMENT-JONES

- 189 Schedule 14, page 240, line 12, leave out “Secretary of State” and insert “person who chairs the relevant Parliamentary committee”

LORD CLEMENT-JONES

- 190 Schedule 14, page 240, line 19, leave out “Secretary of State” and insert “person who chairs the relevant Parliamentary committee”

LORD CLEMENT-JONES

- 191 Schedule 14, page 240, line 20, leave out “Secretary of State” and insert “person who chairs the relevant Parliamentary committee”

LORD CLEMENT-JONES

- 192 Schedule 14, page 241, line 8, leave out “Secretary of State” and insert “person who chairs the relevant Parliamentary committee”

Schedule 15

LORD CLEMENT-JONES

- 193 Schedule 15, page 242, line 33, after “or” insert “existing and future”

Member's explanatory statement

This is part of a package of amendments that to clarify that these Information Standards should explicitly apply to IT providers involved in the processing of data within primary care, as well as secondary care, and that the standards must extend to existing contracts with IT providers, not just new agreements formed after the passage of this Act.

LORD CLEMENT-JONES

- 194 Schedule 15, page 243, line 35, after “technology,” insert “including NHS patient records,”

Member's explanatory statement

This is part of a package of amendments that to clarify that these Information Standards should explicitly apply to IT providers involved in the processing of data within primary care, as well as secondary care, and that the standards must extend to existing contracts with IT providers, not just new agreements formed after the passage of this Act.

LORD CLEMENT-JONES

- 195 Schedule 15, page 243, line 39, at end insert “or of primary care, including General Practice.”

Member's explanatory statement

This is part of a package of amendments that to clarify that these Information Standards should explicitly apply to IT providers involved in the processing of data within primary care, as well as secondary care, and that the standards must extend to existing contracts with IT providers, not just new agreements formed after the passage of this Act.

After Clause 122

LORD CLEMENT-JONES

- 196 After Clause 122, insert the following new Clause –

“Interaction between section 122 and Part 3, Chapter 2 of the Online Safety Act 2023

The Secretary of State must report to Parliament how the provisions of section 122 interact with the provisions on Category 1 services on the Online Safety Act 2023.”

Member's explanatory statement

This is a probing amendment to debate how Category 1 services provisions of the OSB interact with these new DAUB provisions.

Clause 123

BARONESS KIDRON
 LORD RUSSELL OF LIVERPOOL
 LORD STEVENSON OF BALMACARA
 BARONESS HARDING OF WINSCOMBE

- 197** Clause 123, page 153, line 6, leave out “may by regulations” and insert “must, as soon as reasonably practicable and no later than 12 months after the day on which this Act is passed, make and lay regulations to”

Member's explanatory statement

This amendment removes the Secretary of State's discretion on whether to lay regulations under Clause 123 and sets a time limit for laying them before Parliament.

BARONESS KIDRON
 LORD RUSSELL OF LIVERPOOL
 LORD STEVENSON OF BALMACARA
 BARONESS HARDING OF WINSCOMBE

- 198** Clause 123, page 153, line 16, at end insert –
- “(da) requirements to facilitate independent research into online safety matters as they relate to people at different ages and stages of development, and people with different characteristics including gender, race, ethnicity, disability, sexuality, gender;”

Member's explanatory statement

This amendment seeks to ensure the regulations will enable independent researchers to research how online risks and harms impact different groups especially vulnerable users including children.

LORD BETHELL
 BARONESS KIDRON

- 198A** Clause 123, page 153, leave out line 26

LORD CLEMENT-JONES

- 198B** Clause 123, page 153, line 27, at end insert –

“(l) the definition of “independent researcher,””

Member's explanatory statement

This amendment would enable regulations to make provision about the definition of researchers.

LORD BETHELL
BARONESS KIDRON

198C Clause 123, page 153, line 27, at end insert –

“(2A) Regulations under this section may not prevent a person from seeking or accessing information solely because the person is located, or intends to carry out research, outside of the United Kingdom.”

Member's explanatory statement

This amendment clarifies that, provided a researcher wants to carry out UK-relevant research into online safety matters, they will in principle be able to access information under the regime regardless of where they are located.

LORD BETHELL
BARONESS KIDRON

198D Clause 123, page 153, leave out lines 28 to 35 and insert –

“(3) Any requirements or duties placed on providers of regulated services by regulations made under subsection (1) may be enforceable requirement within the meaning of section 131.”

Member's explanatory statement

This amendment provides for any requirements under the researcher access regulations to be enforceable in the same way as other requirements in the OSA, obviating the need to design a bespoke enforcement system.

LORD BETHELL

198E Clause 123, page 154, line 22, at end insert –

“(6A) Regulations under this section may not prevent a person from seeking or accessing information solely because the person is located, or intends to carry out research, outside of the United Kingdom.”

LORD BETHELL
BARONESS KIDRON

198F Clause 123, page 154, line 42, at end insert –

“154B Non-enforceability of contractual restraints on research about online safety matters

(1) No contractual term is enforceable by a provider of a regulated service to the extent that its enforcement would prevent any person from carrying out research of the kind provided for by regulations made under section 154A.

- (2) Subsection (1) applies regardless of whether the person against whom the contractual term is sought to be enforced has obtained any information under regulations made under section 154A.
- (3) A contractual term is not unenforceable pursuant to subsection (1) by reason only of it requiring personal data to be processed in accordance with the data protection legislation.”

Member's explanatory statement

This amendment amends the Online Safety Act, making any contractual provision – such as a provision in a platform’s terms of service – unenforceable if enforcing it would prevent ‘research into online safety matters’ as defined in and provided for by the regulations which the Secretary of State will make.

After Clause 126

VISCOUNT CAMROSE
LORD MARKHAM

199 After Clause 126, insert the following new Clause –

“Data risks from systemic competitors and hostile actors

Data risks from systemic competitors and hostile actors

- (1) The Secretary of State, in consultation with the Information Commissioner, must conduct a risk assessment on the data privacy risks associated with genomics and DNA companies that are headquartered in countries the government determines to be systemic competitors and hostile actors.
- (2) Within 12 months of the day on which this Act is passed, the Secretary of State must present a report on the risk assessment in subsection (1) to Parliament and consult the intelligence and security agencies on the findings, taking into account the need to not make public information critical to national defence or ongoing operations.
- (3) This risk assessment must evaluate –
 - (a) the degree of access granted to foreign entities, particularly those linked to systemic competitors and hostile actors, to genomic and DNA data collected within the United Kingdom,
 - (b) the potential for genomic and DNA data to be exfiltrated outside of the United Kingdom,
 - (c) the potential misuse of United Kingdom genomic and DNA data for dual-use or nefarious purposes,
 - (d) the potential for such data to be used in a manner that could compromise the privacy or security of United Kingdom citizens or undermine national security and strategic advantage.
- (4) The risk assessment must consider and include, but is not limited to –

- (a) an analysis of the data handling and storage practices of genomics companies that are based in countries designated as systemic competitors and hostile actors,
 - (b) an independent audit, including digital and physical forensic examination, at any company site that could have access to United Kingdom genomics data, and
 - (c) evidence of clear disclosure statements to consumers of products and services from genomics companies subject to data sharing requirements in the countries where they are headquartered.
- (5) This risk assessment must be conducted as frequently as deemed necessary by the Secretary of State or the Information Commissioner to address evolving threats and ensure continued protection of the genomics sector from entities controlled, directly or indirectly, by countries designated as systemic competitors and hostile actors.
- (6) The Secretary of State may issue directives or guidelines based on the findings of the risk assessment to ensure compliance by companies or personnel operating within the genomics sector in the United Kingdom, safeguarding against identified risks and vulnerabilities to data privacy.”

Member's explanatory statement

This amendment seeks to ensure sufficient scrutiny of emerging national security and data privacy risks related to advanced technology and areas of strategic interest for systemic competitors and hostile actors. It aims to inform the development of regulations or guidelines necessary to mitigate risks and protect the data privacy of UK citizens' genomics data and the national interest. It seeks to ensure security experts can scrutinise malign entities and guide researchers, consumers, businesses, and public bodies.

After Clause 132

LORD LUCAS

200 After Clause 132, insert the following new Clause –

“Data dictionary

- (1) The Secretary of State may make regulations establishing the definitions of terms used to describe data, and may require that these definitions are used in relation to –
- (a) Parts 2 (digital verification services) and 4 (registers of births and deaths) of this Act, and
 - (b) public data in general.
- (2) Regulations under this section are subject to the negative resolution procedure.”

Member's explanatory statement

This amendment is to ensure consistency of definition of key terms (as requested by CoPilot) across government and over time, e.g. definitions of “sex” and “gender”.

LORD LUCAS

201 After Clause 132, insert the following new Clause –

“Fraud reporting

- (1) The Secretary of State may by regulations make provision requiring all reports of attempted fraud to be logged on a central database.
- (2) If regulations are made under subsection (1), the Secretary of State must, annually, lay a report before Parliament on the levels and types of fraud attempted, success rates, and action taken to combat it.
- (3) Regulations under this section are subject to the negative resolution procedure.”

Member's explanatory statement

This amendment is to raise the standard of recording of online fraud and to focus attention on combating it.

LORD LUCAS

202 After Clause 132, insert the following new Clause –

“Schools admissions data

- (1) The Secretary of State must by regulations make provision requiring all schools admissions authorities in England to contribute to a public register, online and in a specified format, by 1 September each year, their schools admissions rules for the forthcoming year and the outcomes of their schools admissions process for the year just beginning.
- (2) Regulations under this section are subject to the negative resolution procedure.”

Member's explanatory statement

This amendment is to create a national register of schools admissions rules and outcomes, so that parent may obtain a complete and consistent picture of which schools are likely to be available to their children.

BARONESS KIDRON
LORD CLEMENT-JONES
LORD BETHELL
LORD STEVENSON OF BALMACARA

203 After Clause 132, insert the following new Clause –

“Offence to use personal data or digital information to create digital models or files that facilitate the creation of AI- or computer-generated child sexual abuse material

- (1) A person commits an offence if they –
 - (a) collect, scrape, possess, distribute or otherwise process personal data or digital information with the intention of using it, or attempting to use it,

- to create or train a digital model which enables the creation of AI- or computer-generated child sexual abuse material or priority illegal content;
- (b) use personal data or digital information to create, train or distribute or attempt to create, train or distribute a digital file or model that has been trained on child sexual abuse material or priority illegal content, or which enables the creation of AI- or computer-generated child sexual abuse material or priority illegal content;
 - (c) collate, or attempt to collate, digital files or models based on personal data or digital information that, when combined, enable the creation of AI- or computer-generated child sexual abuse material or priority illegal content;
 - (d) possess, or attempt to possess, a digital file or model based on personal data or digital information with the intention of using it to produce or gain access to AI- or computer-generated child sexual abuse material or priority illegal content.
- (2) For the purposes of this section, “AI- or computer-generated child sexual abuse material or priority illegal content” includes images, videos, audio including voice, chatbots, material generated by large language models, written text, computer files and avatars.
 - (3) A person who commits an offence under subsection (1) is liable to the sentences set out in section 160 of the Criminal Justice Act 1988 (possession of indecent photograph of child) and section 6 of the Protection of Children Act 1978 (punishments) for the equivalent offences.
 - (4) For the purposes of this section, “priority illegal content” is content that meets the definition of “priority illegal content” set out in section 59 of the Online Safety Act 2023.”

Member's explanatory statement

It is illegal in the UK to possess or distribute child sexual abuse material including AI- or computer-generated child sexual abuse material. However, while the content is clearly covered by existing law, the mechanism that enables their creation – i.e. the files trained on or trained to create such material – is not. This amendment seeks to address that gap.

BARONESS KIDRON
LORD FREYBERG
LORD STEVENSON OF BALMACARA
LORD CLEMENT-JONES

204

After Clause 132, insert the following new Clause –

“Compliance with UK copyright law by operators of web crawlers and general-purpose AI models

- (1) The Secretary of State must by regulations make provisions clarifying the steps the operators of web crawlers and general-purpose artificial intelligence (AI) models must take to comply with United Kingdom copyright law, including the Copyright, Designs and Patents Act 1988.

- (2) The provisions made under subsection (1) must apply if the products and services of such operators are marketed in the United Kingdom.
- (3) The provisions made under subsection (1) must apply to the entire lifecycle of a general-purpose AI model, including but not limited to –
 - (a) pre-training,
 - (b) fine tuning, and
 - (c) grounding and retrieval-augmented generation.
- (4) The Secretary of State must lay before Parliament a draft of the statutory instrument containing regulations under subsection (1) within six months of the day on which this Act is passed and the regulations are subject to the affirmative procedure.”

Member's explanatory statement

This amendment would require operators of internet scrapers and general-purpose AI models to comply with UK copyright law, and to abide by a set of procedures.

BARONESS KIDRON
LORD FREYBERG
LORD STEVENSON OF BALMACARA
LORD CLEMENT-JONES

205

After Clause 132, insert the following new Clause –

“Transparency of crawler identity, purpose, and segmentation

- (1) The Secretary of State must by regulations make provision requiring operators of web crawlers and general-purpose artificial intelligence (AI) models to disclose information regarding the identity of their crawlers, including but not limited to –
 - (a) the name of the crawler,
 - (b) the legal entity responsible for the crawler,
 - (c) the specific purposes for which each crawler is used,
 - (d) the legal entities to which they provide data scraped by the crawlers they operate, and
 - (e) a single point of contact to enable copyright holders to communicate with them and to lodge complaints about the use of their copyrighted works.
- (2) The information disclosed under subsection (1) must be available on an easily accessible platform and updated at the same time as any change.
- (3) The Secretary of State must by regulations make provision requiring operators of web crawlers and general-purpose AI models to deploy distinct crawlers for different purposes, including but not limited to –
 - (a) web indexing for search engine results pages,
 - (b) general-purpose AI model pre-training, and
 - (c) retrieval-augmented generation.
- (4) The Secretary of State must by regulations make provision requiring operators of web crawlers and general-purpose AI models to ensure that the exclusion of a

crawler by a copyright holder does not negatively impact the findability of the copyright holder's content in a search engine.

- (5) The Secretary of State must lay before Parliament a draft of the statutory instrument containing regulations under this section within six months of the day on which this Act is passed and the regulations are subject to the affirmative procedure."

Member's explanatory statement

This amendment would require operators of internet crawlers and general-purpose AI models to be transparent about the identity and purpose of their crawlers; operate distinct crawlers for different purposes; and not penalise copyright holders who choose to deny scraping for AI by downranking their content in, or removing their content from, a search engine.

BARONESS KIDRON
LORD FREYBERG
LORD STEVENSON OF BALMACARA
LORD CLEMENT-JONES

206

After Clause 132, insert the following new Clause –

“Transparency of copyrighted works scraped

- (1) The Secretary of State must by regulations make provision requiring operators of web crawlers and general-purpose artificial intelligence (AI) models to disclose information regarding copyrighted works their crawlers have scraped, including but not limited to –
- (a) the URLs accessed,
 - (b) information that can be used to identify individual works,
 - (c) the timeframe of data collection, and
 - (d) the type of data collected.
- (2) The disclosure of information under subsection (1) must be updated on a monthly basis and be accessible to the copyright holder upon request.
- (3) The Secretary of State must lay before Parliament a draft of the statutory instrument containing regulations under subsection (1) within six months of the day on which this Act is passed and the regulations are subject to the affirmative procedure.”

Member's explanatory statement

This amendment would require operators of web crawlers and general-purpose AI models to be transparent about the copyrighted works they have scraped, allowing copyright holders to understand when their work has been scraped.

BARONESS KIDRON
LORD CLEMENT-JONES
LORD ARBUTHNOT OF EDROM
THE LORD BISHOP OF ST ALBANS

207 After Clause 132, insert the following new Clause –

“Reliability of computer-based evidence

- (1) Electronic evidence produced by or derived from a computer, device or computer system (separately or together “system”) is admissible as evidence in any proceedings –
 - (a) where that electronic evidence and the reliability of the system that produced it or from which it is derived are not challenged;
 - (b) where the court is satisfied that the reliability of the system cannot reasonably be challenged;
 - (c) where the court is satisfied that the electronic evidence is derived from a reliable system.
- (2) Rules of Court must provide that electronic evidence sought to be relied upon by a party in any proceedings may be challenged by another party as to its admissibility.
- (3) For the purposes of subsection (1)(b), Rules of Court must provide for the circumstances in which the Court may be satisfied that the admissibility of electronic evidence cannot reasonably be challenged.
- (4) When determining whether a system is reliable for the purposes of subsection (1)(c) the matters that may be taken into account include –
 - (a) any instructions or rules of the system that apply to its operation;
 - (b) any measures taken to secure the integrity of data held on the system;
 - (c) any measures taken to prevent unauthorised access to and use of the system;
 - (d) the security of the hardware and software used by the system;
 - (e) any measures taken to monitor and assess the reliability of the system by the system controller or operator including steps taken to fix errors or address unexpected outcomes including the regularity of and extent of any audit of the system by an independent body;
 - (f) any assessment of the reliability of the system made by a body with supervisory or regulatory functions;
 - (g) the provisions of any scheme or industry standard that apply in relation to the system.
- (5) For the purposes of this section –
 - “computer” means any device capable of performing mathematical or logical instructions;
 - “device” means any apparatus or tool operating alone or connected to other apparatus or tools, that processes information or data in electronic form;

“electronic evidence” means evidence derived from data contained in or produced by any device the functioning of which depends on a software program or from data stored on a computer, device or computer system or communicated over a networked computer system.”

Member's explanatory statement

This amendment overturns the current legal assumption that evidence from computers is always reliable which has contributed to miscarriages of justice including the Horizon Scandal. It enables courts to ask questions of those submitting computer evidence about its reliability.

LORD BASSAM OF BRIGHTON
LORD FREYBERG
THE EARL OF CLANCARTY

208 After Clause 132, insert the following new Clause—

“Private copy levy on digital access

- (1) The Secretary of State may by regulations, make provision for the establishment of an annual private copy levy, to be levied when online digital content is accessed or stored.
- (2) Before making regulations under this section, the Secretary of State must consult such persons as the Secretary of State considers appropriate.
- (3) The provisions made under subsection (1) must include but are not limited to—
 - (a) establishing governance arrangements to calculate the rate and application of the levy,
 - (b) permitting relevant copyright collecting societies to collect and distribute monies raised by the levy to rightsholder funds, and
 - (c) distributing any surplus funds raised by the levy for the purposes of funding arts and cultural initiatives in the United Kingdom.
- (4) The Secretary of State must lay before Parliament a draft of the statutory instrument containing regulations under subsection (1) within six months of the day on which this Act is passed and the regulations are subject to the affirmative procedure.
- (5) The Secretary of State must commission an annual transparency report on the operation of the levy.
- (6) The Secretary of State must lay the report made under subsection (5) before Parliament.”

Member's explanatory statement

This amendment seeks to allow the Secretary of State to establish a private copy levy for digital content, with revenue distributed to rightsholder funds and cultural initiatives.

LORD CLEMENT-JONES

209 After Clause 132, insert the following new Clause –

“Digital identity theft

- (1) A person commits an offence of digital identity theft if the person –
 - (a) without permission obtains personal or sensitive information such as passwords, ID numbers, credit card numbers or national insurance numbers relating to an individual, or
 - (b) uses personal or sensitive information under paragraph (a) to impersonate that individual and act in their name to carry out any digital transaction.
- (2) A person guilty of an offence under this section is liable on summary conviction to a fine not exceeding level 5 on the standard scale.”

Member's explanatory statement

This amendment establishes digital identity theft as an offence.

BARONESS OWEN OF ALDERLEY EDGE

210 After Clause 132, insert the following new Clause –

“Deletion of data in relation to sexual offences

In the Sexual Offences Act 2003, after section 66D insert –

“66E Sharing or threatening to share intimate photograph or film: deletion of data

If a person is convicted of an offence under section 66A (sending etc photograph or film of genitals) or 66B (sharing or threatening to share intimate photograph or film), the court may require the person to delete any copies of a photograph or film they have taken, including physical copies and those held on any device, cloud-based programme, or digital or messaging platform they control.”

BARONESS KIDRON
LORD STEVENSON OF BALMACARA
LORD CLEMENT-JONES
LORD TARASSENKO

211 After Clause 132, insert the following new Clause –

“Sovereign data assets

- (1) The Secretary of State may by regulations define data sets held by public bodies and arm's length institutions and other data sets that are held in the public interest as sovereign data assets (defined in subsection (6)).
- (2) In selecting data sets which may be designated as sovereign data assets, the Secretary of State must –

- (a) have regard to—
 - (i) the security and privacy of United Kingdom data subjects;
 - (ii) the ongoing value of the data assets;
 - (iii) the rights of United Kingdom intellectual property holders;
 - (iv) ongoing adherence to the values, laws and international obligations of the United Kingdom;
 - (v) the requirement for public sector employees, researchers, companies and organisations headquartered in the United Kingdom to have preferential terms of access;
 - (vi) the need for data to be stored in the United Kingdom, preferably in data centres in the United Kingdom;
 - (vii) the need to design Application Programming Interfaces (APIs) as bridges between each sovereign data asset and the client software of the authorized licence holders;
 - (b) consult with—
 - (i) academics with expertise in the field;
 - (ii) the AI Safety Institute;
 - (iii) those with responsibility for large public data sets;
 - (iv) data subjects;
 - (v) the Information Commissioner.
- (3) The Secretary of State must establish a transparent licensing system, fully reflecting the security and privacy of data held on United Kingdom subjects, for use in providing access to sovereign data assets.
- (4) The Secretary of State must report annually to Parliament on the ongoing value of the sovereign data assets, in terms of—
- (a) their value to future users of the data;
 - (b) the financial return expected when payment is made for the use of such data in such products and services as may be expected to be developed.
- (5) The National Audit Office must review the licensing system established by the Secretary of State under subsection (3) and report annually to Parliament as to its effectiveness in securing the ongoing security of the sovereign data assets.
- (6) In this section—
- “sovereign data asset” means—
- (a) data held by public bodies and arm’s length institutions of government;
 - (b) data sets held by third parties that volunteer data to form, or contribute to, a public asset.
- (7) Regulations under this section are to be made by statutory instrument.
- (8) A statutory instrument containing regulations under this section may not be made unless a draft of the instrument has been laid before and approved by a resolution of each House of Parliament.”

Member's explanatory statement

The UK has a number of unique publicly-held data assets, from NHS data to geospatial data and the BBC's multimedia data. This amendment would create a special status for data held in the public interest, and a licensing scheme for providing access to them, which upholds UK laws and values, and ensure a fair return of financial benefits to the UK.

LORD HOLMES OF RICHMOND

211A After Clause 132, insert the following new Clause –

“Data use: image, likeness and personality

- (1) The Secretary of State must, within six months of the day on which this Act is passed, make provision by regulations to prohibit the development, deployment, marketing and sale of data related to an individual's image, likeness or personality for AI training or product development without that individual's express consent.
- (2) The characteristics in subsection (1) include but are not limited to an individual's name, face, voice or any physical characteristic.
- (3) Regulations under this section are subject to the affirmative resolution procedure.”

LORD HOLMES OF RICHMOND

211B After Clause 132, insert the following new Clause –

“Consultation: data centre power usage

On the day on which this Act is passed, the Secretary of State must launch a consultation on the implications of the provisions in this Act for the power usage and energy efficiency of data centres.”

LORD HOLMES OF RICHMOND

211C After Clause 132, insert the following new Clause –

“Data use: supply chains

- (1) On the day on which this Act is passed, the Secretary of State must launch a review of all data regulations and standards as they pertain to supply chains for financial, trade and legal documents and products.
- (2) The review must assess how the data regulations and standards align with the principles of traceability, transparency and trust.”

LORD HOLMES OF RICHMOND

211D After Clause 132, insert the following new Clause –

“Data use: review of large language models

- (1) On the day on which this Act is passed, the Secretary of State must launch a review to consider the introduction of standards for the input and output of data of large language models which operate and generate revenue in the United Kingdom.
- (2) The review must consider –
 - (a) the applicability of similar standards, such as those that already exist in industries such as pharmaceuticals, food and drinks;
 - (b) whether there is a need for legislative clarity under section 27 of the Copyright, Designs and Patents Act 1988 about whether the input and output of large language models constitute an “article”, and
 - (c) whether a minimum standard should be a condition for market access.”

LORD HOLMES OF RICHMOND

211E After Clause 132, insert the following new Clause –

“Consultation on public trust

- (1) On the day on which this Act is passed, the Secretary of State must launch a national consultation on the use of individuals’ data.
- (2) The consultation should adopt a human-lead technology-empowered approach to reach a wide range of citizens in the United Kingdom.
- (3) The consultation methodology should be dynamic and should deploy technologies such as AI to analyse the research findings.
- (4) The consultation’s construction and approach should be informed by international examples such as the “alignment assemblies” in Taiwan.”

LORD LUCAS

211F After Clause 132, insert the following new Clause –

“Local Environmental Records Centres (“LERCs”)

- (1) Any planning application involving biodiversity net gain must include a data search report from the relevant Local Environmental Records Centre (LERC), and all data from biodiversity surveys conducted in connection with the application must be contributed free of charge to the LERC in record-centre-ready format.
- (2) All government departments and governmental organisations, local and national, that collect biodiversity data for whatever reason, must contribute it free of charge to the relevant LERCs in record-centre-ready format, and must include relevant LERC data in formulating policy and operational plans.”

Member's explanatory statement

This amendment ensures that all the biodiversity data collected by or in connection with government is collected in Local Environmental Records Centres, so records are as good as possible, and that that data is then used by or in connection with government so that data is put to the best possible use.

Clause 133

VISCOUNT CAMROSE
LORD MARKHAM

212 Clause 133, page 167, line 7, leave out subsection (4)

Member's explanatory statement

This is a probing amendment to assess why this power is necessary.

Clause 135

BARONESS JONES OF WHITCHURCH

213 Clause 135, page 168, line 26, at end insert –

- “(5A) The power conferred by section 63(3) of the Immigration, Asylum and Nationality Act 2006 may be exercised so as to extend to the Bailiwick of Guernsey or the Isle of Man any amendment made by section 55 of this Act of any part of that Act (with or without modification or adaptation).
- (5B) The power conferred by section 76(6) of the Immigration Act 2014 may be exercised so as to extend to the Bailiwick of Guernsey or the Isle of Man any amendment made by section 55 of this Act of any part of that Act (with or without modifications).
- (5C) The power conferred by section 95(5) of the Immigration Act 2016 may be exercised so as to extend to the Bailiwick of Guernsey or the Isle of Man any amendment made by section 55 of this Act of any part of that Act (with or without modifications).”

Member's explanatory statement

The immigration legislation amended by Clause 55 may be extended to the Channel Islands or the Isle of Man. This amendment provides that the amendments made by Clause 55 may be extended to the Bailiwick of Guernsey or the Isle of Man.

BARONESS JONES OF WHITCHURCH

214 Clause 135, page 168, line 26, at end insert –

- “(5A) The power conferred by section 239(7) of the Online Safety Act 2023 may be exercised so as to extend to the Bailiwick of Guernsey or the Isle of Man any

amendment or repeal made by this Act of any part of that Act (with or without modifications).”

Member's explanatory statement

This amendment provides that amendments of the Online Safety Act 2023 made by the Bill (see Clauses 122 and 123) may, like the other provisions of that Act, be extended to the Bailiwick of Guernsey or the Isle of Man.

Data (Use and Access) Bill [HL]

SECOND MARSHALLED
LIST OF AMENDMENTS
TO BE MOVED
IN GRAND COMMITTEE

6 December 2024

PUBLISHED BY AUTHORITY OF THE HOUSE OF LORDS