Information Commissioner's Office

Upholding information rights

3rd Floor, 14 Cromac Place, Belfast, BT7 2JB
Tel. 0303 123 1114
www.ico.org.uk

By email only

21 December 2022

Dear Department of Justice (DoJ)

Re: Public Consultation on Increasing the Minimum Age of Criminal Responsibility in Northern Ireland from 10 Years to 14 Years

Thank you for inviting the Information Commissioner's Office (ICO) to respond to the above consultation. We are pleased to provide comment on the Minimum Age of Criminal Responsibility in Northern Ireland (MACR).

As you will be aware, the Information Commissioner's role includes the regulation of the Data Protection Act 2018 (DPA 2018), the UK General Data Protection Regulation (UK GDPR) and the Freedom of Information Act 2000 (FOIA), among other pieces of legislation. While the four questions raised within the consultation document fall outwith our remit, we have provided comments below which focus on the information rights elements of the consultation.

The ICO recognises that the proposed changes to legislation have been designed to bring Northern Ireland into line with international standards and to comply with the UN Committee's recommendations on the Rights of the Child. This will ensure the best interests of the child are at the forefront of any decision-making. However, the resulting policy will involve the processing of personal data and as such, the implementation of any proposals should be read in conjunction with data protection legislation.

UK GDPR – Article 36(4) statutory requirement to consult the ICO

As the consultation seeks to introduce changes to the current legislation, we would like to draw attention to your obligations under Article 36(4) of the UK GDPR regarding the need to consult with the ICO under specific circumstances.

3rd Floor, 14 Cromac Place, Belfast, BT7 2JB
Tel. 0303 123 1114
www.ico.org.uk

Article 36(4) imposes a requirement on Government Departments and relevant public sector bodies to consult with the ICO when developing policy proposals relating to the processing of personal data. Article 36(4) states that: "*Member States shall consult the supervisory authority during the preparation of a proposal for a legislative measure to be adopted by a national parliament, or of a regulatory measure based on such a legislative measure, which relates to processing*".

If DoJ decides that consultation under Article 36(4) is necessary, we would require the completion and submission of an Article 36(4) Enquiry Form, which can be found here.

Engagement of relevant data protection regime(s)

Prior to implementing any processing activities, DoJ must decide which data protection regime will be engaged and whether the proposed processing falls under the UK GDPR and Part 2 of the DPA 2018 (general processing) and/or Part 3 of the DPA 2018.

Processing by a competent authority for law enforcement purposes, including instances when an offence has been committed by an individual who falls below the MACR, will engage processing under Part 3 of the DPA 2018. However, processing completed by competent authorities whereby the processing is **not** primarily for law enforcement purposes, as well as processing by non-competent authorities will fall under Part 2 of the DPA 2018/UK GDPR. It is therefore important that DoJ maps out which regime will be applied by the relevant controllers.

Data protection by design and default

Data protection by design and default is an approach which features in both data protection regimes; it will ensure the appropriate technical and organisational measures are put in place to implement the data protection principles effectively, safeguarding privacy and individual rights. Due to the collection of children's data and the sensitive nature of the information which will be processed, this requirement will be a particularly

3rd Floor, 14 Cromac Place, Belfast, BT7 2JB
Tel. 0303 123 1114
www.ico.org.uk

important consideration for DoJ when making any amendments to the legislation.

Data protection impact assessments (DPIA's)

The ICO recommends that DoJ complete a DPIA in relation to the proposals. DPIA's are mandated by the UK GDPR and DPA 2018 when the proposed processing is likely to result in a high risk to the rights and freedoms of individuals. It is also good practice to undertake a DPIA when the processing is unlikely to result in a high risk. The DPIA should evolve as the proposals and implementation develops.

The proposed changes to the legislation will likely involve the processing of special category and criminal offence data, as well as information belonging to children. A DPIA will help DoJ justify the proposed amendments, assess the personal data processing activities and minimise any resulting data protection risks. It will also help DoJ establish any risks and the associated harms which may be encountered by controllers who will be obligated to process data under the new legislation.

Please note that there is also an obligation to consult the ICO if any of the DPIA's identify a residual high risk that cannot be reduced.

Data Protection Officers (DPO's)

It is important that DoJ involve their DPO throughout the development and implementation of the proposed legislation. An important part of the DPO's role is to advise the organisation on how to take forward their data protection responsibilities.

Children's data and Recital 38 of the UK GDPR

Children need particular protection and additional safeguarding when their personal data is being collected and processed, as they may not be fully aware of the risks which may arise from any processing. Therefore, we would like to draw your attention to the obligations set out within Recital 38 of the UK GDPR.

3rd Floor, 14 Cromac Place, Belfast, BT7 2JB
Tel. 0303 123 1114
www.ico.org.uk

Amendments to the MACR must consider the best interests of the child and how to safeguard personal data from the outset. For example, DoJ should be mindful of how criminal convictions may affect those of a younger age, in relation to criminal records checks made by employers and education providers. This will require the implementation of processes to help minimise the risks and harms which could arise from the improper processing of children's information.

Fairness and compliance with the data protection principles should be central to the processing of children's personal data. In respect of this matter, it may be useful to refer to the detailed guidance on our website.

Controllers, processors and retention

DoJ must give consideration to who the controllers and processors will be during each stage of the processing, and how data will be retained during and post investigation. The controllers and processors must have suitable processes and appropriate systems in place to handle and safeguard the data in line with the data protection principles, specifically storage limitation and security.

DoJ must determine whether it would be necessary and proportionate for organisations processing for law enforcement purposes (including the Police Service of Northern Ireland and the Public Prosecution Service) to retain the personal data relating to an individual under the MACR. DoJ must also consider retention by non-competent authorities. We recognise that determinations on this matter may have already been implemented under the current legislation however, we suggest that these processes are reviewed to ensure they remain compliant under data protection legislation.

Data sharing

Further to the points raised above, paragraph 31 of the consultation document states that following the investigation of a criminal offence, personal information belonging to a child who is under the MACR may be shared with third parties for purposes such as assessment, intervention and review. Data controllers responsible for sharing this data must identify a suitable lawful basis, and ensure that data is shared in a

3rd Floor, 14 Cromac Place, Belfast, BT7 2JB
Tel. 0303 123 1114
www.ico.org.uk

manner which is compliant with the data protection principles, specifically the data minimisation principle.

In some cases, useful tools such as a data sharing agreement or a memorandum of understanding (MOU) may help controllers to justify the data sharing, while demonstrating that they have been mindful of and have documented the relevant compliance issues. DoJ should consider providing guidance and advice to the relevant controllers in relation to data sharing practices and refer them to our data sharing information hub.

Concluding remarks

To conclude, while the ICO cannot respond with a view on the different questions proposed and issues raised, we take this opportunity to stress the importance of incorporating the appropriate systems and accompanying policies to ensure compliance with data protection legislation.

We look forward to engaging further as the proposals progress and we hope you find the above comments helpful. In the meantime, you may find it useful to consult our website and in particular the information that is contained within the Guide to the UK GDPR and the Guide to Law Enforcement Processing.

Should you require clarification of any of the points made within this response, please feel free to contact us at ni@ico.org.uk or on 0303 123 1114.