

**NOTICE OF INTENT FROM THE UNITED KINGDOM
FOR PARTICIPATION AS AN ASSOCIATE IN THE
GLOBAL CROSS-BORDER PRIVACY RULES FORUM (2023)**

TO: *CHAIR*, Global Forum Assembly, Global CBPR Forum

CC: *DEPUTY CHAIR*, Global Forum Assembly, Global CBPR Forum; *CHAIR*, Membership Committee, Global Forum Assembly, Global CBPR Forum

**LETTER OF INTENT TO PARTICIPATE
AS AN ASSOCIATE IN THE
GLOBAL CROSS-BORDER PRIVACY RULES (CBPR) FORUM**

I am writing this Letter of Intent to seek participation as an Associate in the Global CBPR Forum ("**Forum**") on behalf of the government of the United Kingdom, pursuant to Annex A of the Global CBPR Forum Terms of Reference.

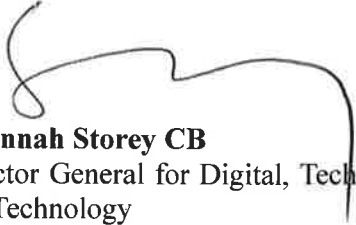
I confirm that:

- (a) The government of the United Kingdom supports the principles and objectives of the Forum set forth in the 2022 Global CBPR Declaration and the Global CBPR Framework;
- (b) The enforcement of the UK's data protection laws, including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018), has the effect of protecting personal information; and
- (c) The Information Commissioner's Office (ICO) is responsible for enforcing the UK GDPR and the DPA 2018, and has the powers to conduct investigations or pursue enforcement proceedings.

Please find a narrative description of the UK's data protection framework and the ICO attached to this letter ([Annex](#)).

Any enquiries regarding this letter should be directed to: Gemma Phillips, Head of Policy and Engagement, International Data Flows Unit, Department for Science, Innovation and Technology <Gemma.Phillips@dcms.gov.uk>.

SIGNED BY



Susannah Storey CB

Director General for Digital, Tech and Telecoms Group, Department for Science, Innovation and Technology

THE UK'S DATA PROTECTION FRAMEWORK AND ITS ENFORCEMENT BY THE INFORMATION COMMISSIONER'S OFFICE

The UK's data protection framework

The UK's main data protection legislation consists of:

- UK GDPR: The EU General Data Protection Regulation (GDPR) was incorporated into UK law by virtue of the European Union (Withdrawal) Act 2018 (EUWA)¹, and modified by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (the "DPPEC Regulations"), and is now known as the UK GDPR². The DPPEC Regulations ensure that the retained EU law continues to be operable in the domestic UK context.
- Data Protection Act (DPA) 2018: The UK GDPR is supplemented by the DPA 2018³ as enacted in May 2018 and amended by the DPPEC Regulations. The DPA 2018 also serves to implement the EU Law Enforcement Directive and contains specific regimes which are applicable to the processing of personal data by competent authorities for law enforcement purposes (Part 3 DPA 2018) and by or on behalf of the intelligence services (Part 4 DPA 2018).

The following legal instruments are also relevant:

- European Convention on Human Rights (ECHR) and the Human Rights Act (HRA) 1998: The UK is a party to the ECHR⁴ and is subject to European Court of Human Rights rulings. The HRA 1998⁵ gives further effect in UK law to the rights and freedoms contained in the ECHR. The HRA 1998 places a duty on public authorities to act compatibly with human rights and enables individuals to enforce those rights directly in courts in the UK.
- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (C108): The UK was a founding member of the Council of Europe and has been a Party to C108⁶ for over 30 years.
- Investigatory Powers Act (IPA) 2016: The IPA 2016 applies further protections and restrictions on the acquisition, retention, handling, and use of personal data (including communications and communications data) by public authorities. The IPA 2016 makes clear the circumstances in which various investigatory powers may be used and the strict safeguards that apply⁷.

The role of the ICO

The Information Commissioner's Office (ICO) is the UK's national data protection authority. The ICO is tasked with monitoring, ensuring, and enforcing compliance with data protection laws, including handling complaints from data subjects. It is one of the largest data protection authorities in Europe, with around 1,050 staff and a budget of £76 million for the financial year 2022-2023, almost all of which supports data protection compliance. Since its establishment in 1984, the ICO has had a strong track record of enforcing data protection regulations.

¹ https://www.legislation.gov.uk/ukpga/2018/16/pdfs/ukpga_20180016_en.pdf

² <https://www.legislation.gov.uk/uksi/2019/419/contents/made>

³ <https://www.legislation.gov.uk/ukpga/2018/12/contents>

⁴ https://www.echr.coe.int/documents/convention_eng.pdf

⁵ <https://www.legislation.gov.uk/ukpga/1998/42/contents>

⁶ <https://rm.coe.int/1680078b37>

⁷ <https://www.legislation.gov.uk/ukpga/2016/25/contents>

The ICO has a wide range of powers to enable it to be an effective data protection authority. Its responsibilities have increased significantly in recent years as the DPA 2018 and UK GDPR extended various existing powers and created new ones to help the ICO effectively fulfil these new responsibilities. The ICO is empowered to:

- Require certain information from data controllers or processors within a specified timeframe. The ICO can also ask a court to order compliance with an information notice.
- Serve assessment notices on data controllers or processors to provide evidence of their compliance, which may include providing access to their premises. The ICO is also able to carry out “no notice” inspections in certain circumstances.
- Serve enforcement notices where there has been an infringement, requiring organisations to take, or refrain from taking, specified steps to comply with the law.
- Levy monetary fines for breaches of data protection legislation or failures to comply with enforcement mechanisms. Under the UK GDPR, fines can be as high as 4% global turnover or £17.5 million, whichever is highest.
- Prosecute those who commit criminal offences under the DPA 2018, or refer cases to the appropriate prosecutor. The Act includes a new offence for deliberately destroying or concealing evidence identified as being relevant to an investigation.

A full list of the ICO’s powers is available on its website.⁸

The ICO is independent of the government. The ICO sets its strategies and plans, and this year published its ICO25 strategic plan. The ICO is directly accountable to Parliament; the Government has no independent right of review over its enforcement decisions. The ICO is financed through the retention of data protection fees collected from data controllers.

⁸ <https://ico.org.uk/about-the-ico/who-we-are/decision-making-structure/scheme-of-delegations/>