

Principles for legislators on the implementation of new technologies:

The Irish Government and Irish legislators must not abandon their legal responsibilities to ensure any tech solution deployed as part of public policies is developed with human rights at the front and centre, and has robust privacy protections.

In a democracy, any technology developed by a government or in partnership with third parties, will need to have the trust and consent of the population to work effectively. Adhering to the following principles is a necessary foundation for building that trust:

1. Have a clear and limited purpose:

To ward off potential abuse, the Government must ensure there is a clear and limited purpose to technologies and the processing of any data collected.¹ The technology and data collection and processing must be used solely for the stated purpose and not for any other purpose such as the sharing of data with third parties or employers, for advertising or for any punitive purpose or legal proceedings. This should also ensure there is no mission creep.

2. Be necessary and proportionate to the problem:

All technologies implemented or supported by the government should be necessary to address the stated problem the technology is addressing. Evidence must demonstrate the technology is necessary and proportionate.²

3. Be effective:

Evidence must be established to show how effective use of the technology will be and its efficacy must be kept under review.³ The necessity and proportionality of the technology is contingent on its effectiveness. The deployment of ineffective technologies will erode public trust and undermine future efforts to implement solutions.

4. Embrace transparency and promote trust:

The Government and any other developers of the technology must be wholly transparent about what data it seeks to acquire, how it will use the data, and with whom it will be shared, and other architectural design choices.⁴ Anything less, or anything beyond its core functionality, will erode public trust in the technology, nullifying its effectiveness. Publication of the Data Protection Impact Assessment, Application Programme Interface, source code and design specifications ahead of the technology's launch and trial run, is vital.

¹ Ada Lovelace Institute [“Exit through the App Store? A rapid evidence review on the technical considerations and societal implications of using technology to transition from the COVID-19 crisis”](#)

² [The European Data Protection Supervisor guidelines for assessing the proportionality of measures that limit fundamental rights to privacy and protection of personal data](#)

³ Ada Lovelace Institute [“Exit through the App Store?”](#)

⁴ ICCL [“HSE app: experts and public need to see details”](#)

Active engagement with the public and a wide range of stakeholders is essential to a successful implementation.

5. Subject to statutory oversight:

A clear and independent oversight mechanism must be able to, and empowered to, receive and address complaints from the public regarding the technology.⁵ Assurances for the technology surrounding data protection, privacy and human rights standards must be grounded in legislation.

6. Subject to timely deletion of personal data:

Any and all personal data collected or processed via the technology and subsequently shared with others must be immediately deleted when there is no longer a need to retain it.⁶ This must be regularly reviewed.

7. Privacy and data protection by design:

Protection of citizens' public data must be considered in the basic design of the technology. The data collected and processed must be the minimum necessary to achieve the technology's purpose. It must be developed in line with the principles of data protection by design and default, as per Article 25 of GDPR.⁷ These protections must be kept under review.

8. Subject to a sunset clause:

Any technology introduced to address an issue which is time dependent should be subject to a "sunset clause".⁸ The effectiveness and necessity of the technology is often contingent on a technologically and societally dynamic environment.

9. Broaden the range of actors involved and foster engagement:

The range of actors positively engaged with the technology's design and implementation decisions should be broad.⁹ This will ensure the evidence base justifying the technology is diverse and robust.

⁵ [UK Joint Committee on Human Rights' warning that data protection and privacy standards in relation to a Covid-19 app must be grounded in legislation](#)

⁶ EDPB "[Guidelines 4/2019 on Article 25 Data Protection by Design and by Default](#)"

⁷ EDPB "[Guidelines 4/2019 on Article 25 Data Protection by Design and by Default](#)"

⁸ Article 29 Data Protection Working Party "[Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data](#)

⁹ Ada Lovelace Institute "[Exit through the App Store?](#)". For example, diverse, independent and expert advisors from a range of disciplines could be established to oversee, examine and make recommendations regarding technical pandemic interventions.

Governments have the responsibility to ensure their processes and outputs are designed with human rights at the front and centre and they are expected and trusted to do so by the public. The effective implementation of any technology by Government is dependent on this public trust; and so Governments should not perceive a dichotomy between recognising and promoting human rights and effective technological solutions.

Signed:

Irish Council for Civil Liberties, Elizabeth Farries, Director of Information Rights

Olga Cronin, Policy Officer, Information Rights, Irish Council for Civil Liberties

Digital Rights Ireland, Antoin O Lachtain, Director

Dr Marguerite Barry, School of Information and Communications Studies, University College Dublin

Dr Stephen Farrell, School of Computer Science and Statistics, Trinity College Dublin

Dr Heike Felzmann, School of Humanities, National University of Ireland, Galway

Dr Aphra Kerr, Department of Sociology, Maynooth University

Prof Rob Kitchin, Maynooth University Social Sciences Institute, Maynooth University

Dr TJ McIntyre, School of Law, University College Dublin

Simon McGarr, Director, Data Compliance Europe

Dr Maria Helen Murphy, Law Department, Maynooth University

Laura Nolan, Tech Won't Build It Ireland

Daragh O'Brien, Founder, Castlebridge

Dr Katherine O'Keefe, Director of Training and Research, Castlebridge

Dr Eoin O'Dell, School of Law, Trinity College Dublin

Prof Barry O'Sullivan, University College Cork and Vice Chair of the European Commission High-Level Expert Group on AI

Prof Kalpana Shankar, School of Information and Communications Studies, University College Dublin

Prof Eugenia Siapera, Head of School, Information and Communications Studies, University College Dublin

Dr Johnny Ryan, Chief Policy and Industry Relations Officer, Brave