# Annex: A summary of the Biometrics guidance impact assessment

## 1. Impact assessment context

Following best practice and the guidance in our 'Impact Assessment Framework[1]', we deem it appropriate to conduct a proportionate impact assessment of our proposed guidance intervention to increase regulatory certainty around what constitutes lawful use of biometric recognition technologies.

We have produced a draft initial assessment, as summarised in Table 1 below. We are seeking feedback on our identified impacts, as well as any other insights stakeholders can provide on impacts, via the consultation on the draft guidance.

It is important to note that we do not intend for this summary to provide an exhaustive assessment of impacts. It is just an initial overview of our considerations. Post consultation we will consider the proportionality of further assessment of the impacts as we move towards final publication of the guidance.

## 2. A summary of the draft impact assessment

Table 1 provides a summary of our draft impact assessment.

**Table 1: Impact assessment summary**

| | |
|---|---|
| **1: Problem definition** | The use of biometric recognition systems is expected to grow significantly over the coming decade. Sectors such as banking & finance; education; entertainment; and retail and commercial are expanding use of these technologies. This has been driven by a several factors including:<br>• the accessibility of facial recognition as a cost-effective means of authentication,<br>• the ease of rapidly analysing biometric data through developments in machine learning and AI, and<br>• the cost of both online and offline-crime, which has increased demand for biometrics within multi-factor authentication.<br>Despite the potential benefits of enhanced security and efficiency, the use of biometric technologies for unique identification can pose a risk to the rights and freedoms of |

[1] The ICO's draft Impact Assessment Framework closed to consultation on the 30 April and the finalised Framework will be published in 2023.

| | |
|---|---|
| | individuals and have the potential to result in harms, such as discrimination and the loss of control of personal data. A previous ICO Call to Evidence highlighted a lack of clarity over the appropriate and lawful use of biometrics for recognition within existing guidance. |
| **2: Rationale for intervention** | Feedback from our previous Call to Evidence highlights a lack of clarity over terminology and context specific data protection guidance. This includes a lack of use cases over what constitutes an appropriate and lawful use of biometric technology for recognition. This creates regulatory uncertainty and impacts on organisations' understanding of what is compliant in the adoption of biometric technology for recognition.<br><br>The potential accuracy of biometric recognition technologies, and the sensitivity of biometric data can also exacerbate the risk of harms (such as discrimination, lack of autonomy, and the loss of control of personal data) driving the need for intervention. |
| **3: Options appraisal** | A previous call to evidence highlighted a lack of clarity over what constitutes the legal adoption of biometric recognition technologies. There are a range of intervention options to increase regulatory certainty. In this case, it was considered that updating the guidance through setting out use cases was the most appropriate policy tool.<br><br>Options considered include:<br><br>1. Do nothing.<br>2. Guidance explaining how data protection law applies when using biometric data in biometric recognition systems.<br>3. Other regulatory tools (eg, engagement, outreach, codes, etc).<br><br>Option 2 was identified as the preferred option. |
| **4: Detail of proposed intervention** | The ICO will provide guidance explaining how data protection law applies when using biometric data in biometric recognition systems. The guidance is for organisations that use or are considering using biometric recognition systems. The guidance describes:<br><br>• the definition of biometric data under GDPR,<br>• what is considered biometric data,<br>• how this data is used in biometric recognition systems, and<br>• the data protection requirements that must be complied with. |

**5: Cost-benefit analysis**

The costs and benefits of the intervention have been identified, quantitatively and qualitatively, as far as is possible and proportionate.

The use of biometric data is governed by the UK GDPR. This guidance seeks to support organisations to better understand their obligations under this legislation. Only costs and benefits of the guidance are considered here.

| | **Benefits** | **Costs** |
|---|---|---|
| **Developers of Biometric Technology** | • Developers of biometric recognition technologies have a better understanding of their legal obligations and the regulatory environment. | • Familiarisation cost with the guidance (initial estimate of approximately £40 per organisation) |
| **Suppliers of Biometric Technology** | • Provision of greater clarity over the respective obligations of suppliers of biometric technologies, and data controllers. | • Potential loss of revenue where users choose to adopt alternatives to biometric recognition technologies. |
| **Users of Biometric Technology** | • Greater regulatory certainty and confidence in the adoption of biometric recognition technology leading to safe and efficient outcomes<br>• Increased trust and confidence amongst customers and wider society. | • Familiarisation with the guidance (initial estimate of approximately £40 per organisation)<br>• Cost of finding and administrating alternatives, where biometric processing is not proportionate. |
| **Data Subjects** | • Reduction in potential DP harms from better understanding of the appropriate safeguards in biometric recognition technology.<br>• Improved clarity on rights in relation to explicit consent, and how this can be withdrawn without detriment to data subjects. | • Potential time costs from using less efficient alternatives for biometric technology |

| | | | |
|---|---|---|---|
| | **The ICO** | • Efficiency savings on advice and support from users of biometric recognition technology.<br>• Potential reduction in supervision costs from improved understanding of compliance. | • Resource cost of developing policy and clarifying guidance |
| | **Wider Society** | • Reduced cost of compensating victims of DP harms.<br>• Reduced risk of social exclusion of individuals unable to engage with biometric technologies (finger printing in over 70s). | |
| | Overall our assessment suggests that the benefits of producing this guidance outweigh the costs. | | |
| **6: Monitoring and evaluation** | In line with best practice and organisational standards, when the proposed guidance is finalised we will put in place an appropriate and proportionate review mechanism. | | |