Information Commissioner's Office

Biometric Recognition Guidance: Impact Assessment

February 2024

ico.
Information Commissioner's Office

Contents

Executive Summary

This impact assessment accompanies the biometrics recognition guidance. The overarching objectives of the guidance are:

- To provide regulatory certainty to organisations processing biometric data on whether or not they are processing personal data.
- To provide regulatory certainty to organisations processing biometric data on whether or not they are processing special category personal data.
- To provide regulatory certainty to organisation regarding our expectations when they are processing special category biometric data.

Problem definition and rationale for intervention

Biometric recognition covers technologies that process biological characteristics for the purposes of identification or verification. Biometric recognition has become embedded across a range of sectors in the economy including finance, education and health.

A previous ICO call for views[1] highlighted a lack of clarity over the appropriate and lawful use of biometric recognition. As the UK's data protection (DP) regulator, the ICO is well placed to provide regulatory certainty and reduce the risk of DP harms to individuals and wider society from the use of biometric recognition. It is expected that without intervention the potential for DP harms arising from the use of these technologies will grow.

Options appraisal

In the context of the identified problem, the following options for intervention were considered:

- **Do nothing:** do not provide any additional regulatory certainty for biometric recognition.
- **Do less:** provide updates to the current guidance on special category data.
- **Preferred option:** provide standalone guidance covering the use of biometric data in biometric recognition systems.
- **Do more:** provide sector-specific guidance outlining specific DP considerations with all known current and emerging use cases for biometric recognition.

[1] ICO (2022) *Biometrics Foresight.* Available at: https://ico.org.uk/media/about-the-ico/documents/4021971/biometrics-foresight-report.pdf (Accessed 1 February 2024).

These options were assessed against a number of critical success factors and the production of standalone guidance covering the use of biometric data in biometric recognition systems was identified as the preferred option.

Details of proposed intervention

The guidance explains how DP 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:

- the definition of biometric data under GDPR;
- what is considered biometric data;
- how this data is used in biometric recognition systems; and
- the DP requirements that must be complied with.

The route to impact for the guidance is set out in the theory of change in Figure 3.

There are various groups that could be affected by the biometric recognition guidance including: developers, vendors and users of biometric recognition; UK citizens; and wider society.

Cost-benefit analysis

The costs and benefits of the intervention have been identified, quantitatively and qualitatively, as far as is possible and proportionate. Our ability to monetise impacts has been limited given the significant evidence gaps around the scale of affected groups.

On balance we expect the guidance to have a net positive impact. The guidance is expected to increase regulatory certainty for developers, vendors and users of biometric recognition and result in these technologies being used on a proportionate basis. Although there will be costs to organisations from reading, understanding and implementing the guidance, this is expected to be outweighed by the wider societal benefits of reduced DP harms.

Monitoring and evaluation

An appropriate and proportionate review structure will be put in place. This will follow best practice and align with our organisational reporting and measurement against ICO25 objectives.

1. Introduction

This document sets out the findings from our ex-ante assessment of the impact of the biometric recognition guidance. The purpose of impact assessments is to:

- inform decision-makers about potential economic, social, and (where relevant) environmental ramifications;
- provide a mechanism to consider the impact of interventions on a range of stakeholders and potential mitigation measures;
- improve the transparency of regulation by explicitly setting out the intervention theory of change and the quality of underlying evidence;
- increase public awareness to improve the legitimacy of the policy; and
- contribute to continuous learning in policy development by identifying causalities that inform ex-post review and improve future policy-making

1.1.1. Our approach to the impact assessment

We have assessed the potential impacts of the guidance using cost-benefit analysis, which aims to identify the full range of impacts by assessing both the costs and benefits. Our approach follows the principles set out in the ICO's Impact Assessment Framework,[2] which in turn is aligned with HM Treasury's Green Book, Regulatory Policy Committee guidance,[3] and Business Impact Target guidance on best practice for impact assessments.[4]

In identifying the potential impacts of the guidance it is important to distinguish between:

- Additional impacts that can be attributed to the guidance – these are affected by how the ICO chooses to develop the guidance.
- Impacts that are not attributable to the guidance. These are impacts that simply arise from the existing legislative requirements that controllers are already expected to comply with.

For the purposes of the impact assessment, we are interested in impacts that are attributable to the guidance, rather than those that would have happened in

---

[2] ICO (2023) *The ICO's Impact Assessment Framework*. Available at: https://ico.org.uk/media/about-the-ico/documents/4027020/ico-impact-assessment-framework.pdf (accessed 16 February 2024).

[3] BEIS (2020) *Better Regulation Framework – Interim Guidance*. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/916918/better-regulation-guidance.pdf (accessed 16 February 2024).

[4] BEIS (2019), Business Impact Target: Appraisal of guidance: assessments for regulator-issued guidance. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/609201/b usiness-impact-target-guidance-appraisal.pdf (accessed 19 January 2024).

the absence of regulatory intervention - a concept known as 'additionality'. Additionality can take a number of forms and may include the realisation of impacts at an earlier stage or to a higher scale or standard than would have been the case without intervention.

Impacts can also be direct or indirect:

- Direct impacts: these are 'first round' impacts that are generally immediate and unavoidable, with relatively few steps in the theory of change between the introduction of the measure and the impact taking place.
- Indirect impacts: these are 'second round' impacts that are often the result of changes in behaviour or reallocations of resources following the immediate impact of the introduction of the measure. These impacts tend to be at the latter stages of a theory of change.

While it is not always feasible to categorise impacts distinctly, we have identified those that are attributable to guidance as far as possible. Our impact assessment draws on a mixture of quantitative and qualitative evidence.

1.1.2. Current data protection (DP) landscape for biometric technologies

Biometric technologies detect physical or behavioural characteristics to deliver a variety of applications. There are a wide range of biometric technologies, which include commonly used fingerprint, facial or voice authentication. The use of biometric technologies is common and is still growing, with applications in diverse contexts. Increasing numbers of organisations are developing and procuring biometric technologies and increasing amounts of biometric data from individuals in the UK are being processed.

To date, the ICO has provided little regulatory guidance on biometric recognition. Despite some ICO involvement in enforcement, stakeholder consultation and research via the grants programme, there is no comprehensive guidance on the use of biometric technologies and the processing of biometric data.

To the extent that there is existing ICO guidance on biometrics data is in two forms:

1. Our special category data guidance makes reference to what biometric data is and when this constitutes special category data.[5]

[5] ICO *A guide to lawful basis*. Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/lawful-basis-for-processing/special-category-data/ (accessed 20 February 2024).

2. Specific guidance (in the form of Opinions) on discrete use-cases (live facial recognition for law enforcement or non-law enforcement purposes).[6]

The combination of strong industry adoption and lack of regulatory input to date has had two impacts on the use of biometric technologies in the UK (these are explored in more detail in Section 2):

1. a lack of clarity on how the UK GDPR and DPA 2018 apply to biometric technologies; and
2. a reduction of the ICO's influence in this field. The abundance of guidance and commentary by other organisations on this topic points to this.

1.1.3. Report structure

The structure of this report is as follows:

- **Section 2: Problem definition and rationale for intervention** sets out the economic, social and political context for the guidance as well as the rationale for producing it.
- **Section 3: Options appraisal** provides a review of alternative policy options against critical success factors.
- **Section 4: Details of proposed intervention** provides an overview of the proposed guidance and the affected groups.
- **Section 5: Cost-benefit analysis** presents the findings of the cost benefit analysis for the guidance.
- **Section 6: Monitoring and evaluation** outlines future monitoring considerations.
- **Annex A** provides more detail on how familiarisation costs are estimated to support the assessment of costs and benefits.

[6] ICO (2021) *The use of live facial recognition technology in public places*. Available at: https://ico.org.uk/media/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf (accessed 20 February 2024).

2. Problem definition and rational for intervention

2.1. Problem definition

Biometric recognition covers technologies that process biological characteristics for the purposes of identification or verification.

Biometric technology has become embedded across a range of sectors in the economy including finance, education and health. Demand for biometric technology has been driven by factors such as: the accessibility of facial recognition technology within modern smart-phones; developments in machine-learning; and the costs of crime to organisations and wider society. While it offers potential benefits of enhanced security and efficiency, the use of biometric technologies also has the potential to result in harms, such as discrimination and the loss of control of personal data. These harms are discussed in more detail in Section 2.3.

The UK GDPR provides a specific legal definition of what constitutes biometric data. This does not directly translate into how it is defined in industry, and the ICO has yet to provide detailed guidance on the status of biometric data within UK DP law, as discussed in Section 1.1.2. A previous ICO call for views highlighted a lack of clarity over the appropriate and lawful use of biometric recognition,[7] giving rise to a need for greater regulatory certainty. As a regulator, the ICO is well placed to provide this regulatory certainty and reduce the risk of DP harms materialising to individuals and wider society from the use of biometric recognition. With the growing adoption of biometric recognition across the economy it is expected that without intervention the potential for these harms will rise.

2.2. Prevalence of biometric recognition

The use of biometric recognition systems such as fingerprint, facial and iris recognition technologies have become embedded across a wide range of sectors in the economy. Areas such as banking & finance; education; entertainment; and the health sector are expanding their use of these technologies. This has been driven by a several factors including:

- The accessibility of facial recognition as a cost-effective means of identity verification has grown in line with rising smart-phone ownership. Deloitte

[7] ICO (2022) *Biometrics: foresight* Available at: https://ico.org.uk/media/about-the-ico/documents/4021971/biometrics-foresight-report.pdf (Accessed 1 February 2024).

found that 85% of UK adults own or have access to a smart-phone and around 80% of those that do have used biometric recognition;[8]
- The ease of accurately analysing biometric data through developments in machine learning and AI; and
- The cost of both online and offline-crime[9] has increased demand for biometrics within multi-factor authentication. The National Audit Office estimates that online crime cost UK consumers nearly £15bn in 2016/17.[10]

Demand for biometric recognition is expected to grow rapidly in coming years, with global market revenues estimated to nearly double from $43 billion in 2022 to $83 billion by 2027.[11]

The use of biometric technology by UK companies is already well established with many using facial recognition, fingerprint and other biometric technologies. A 2023 global survey by Womble Bond Dixon asked companies about DP and their use of technology, finding that:[12]

- Nearly 60% of UK respondents[13] highlighted that they are currently using biometric data, and a further 21% plan to in the future.
- In the UK, companies are processing biometric data for a range of purposes. As shown in Figure 1 below, the majority of respondents are using or plan to use biometric data for identification and verification purposes.
- Nearly half of UK respondents also plan to collect and store biometric data for future purposes, and a smaller proportion of respondents are intending to use it for employee monitoring.

---

[8] Deloitte (2017) *State of the smart*. Available at: https://www.deloitte.co.uk/mobileuk2017/assets/img/download/global-mobile-consumer-survey-2017_uk-cut.pdf (accessed 2 February 2024).

[9] In 2015/16 the Home Office estimated that overall crime cost the UK economy around £50bn. Home Office (2018) *The economic and social costs of crime*. available at: https://assets.publishing.service.gov.uk/media/5b684f22e5274a14f45342c9/the-economic-and-social-costs-of-crime-horr99.pdf (accessed 2 February 2024).

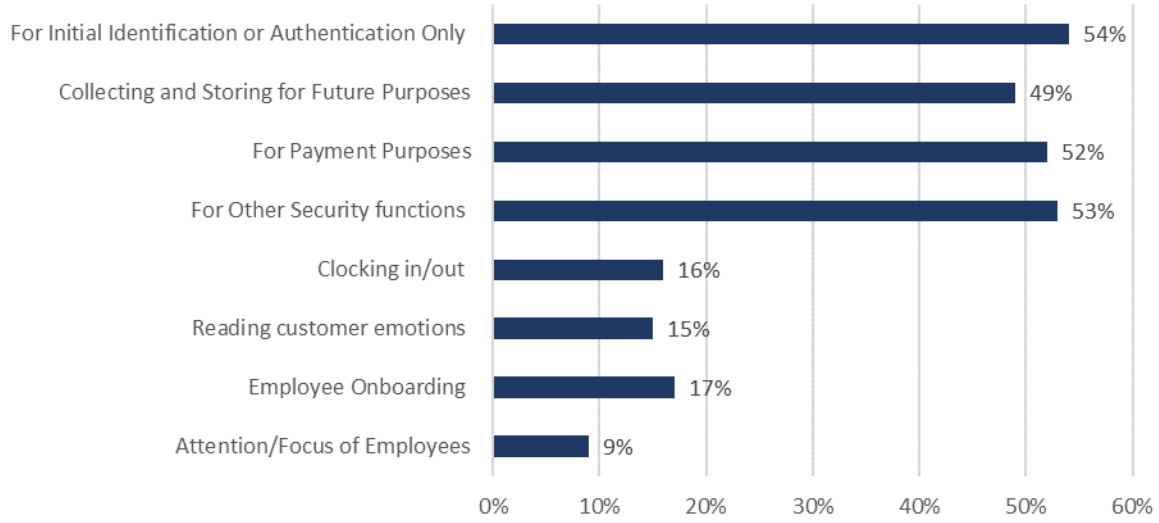
[10] Guardian (2016) *UK failing to keep up with online consumer fraud*. Available at: https://www.theguardian.com/money/2016/dec/15/uk-failing-to-keep-up-with-online-consumer-nao-warns (accessed 2 February 2024).

[11] Statista (2022) *Worldwide biometrics market revenue*. Available at: https://www.statista.com/statistics/1048705/worldwide-biometrics-market-revenue/ (accessed 24 January 2024).

[12] Womble Bond Dixon (2023) *2023 Global data privacy law survey report*. Available at: https://info.womblebonddickinson.com/global-data-privacy-law-2023 (Accessed 2 February 2024).

[13] From a global survey of 205 business leaders, 47% (96 responses) were UK based.

Figure 1: Plans for biometric processing by UK companies



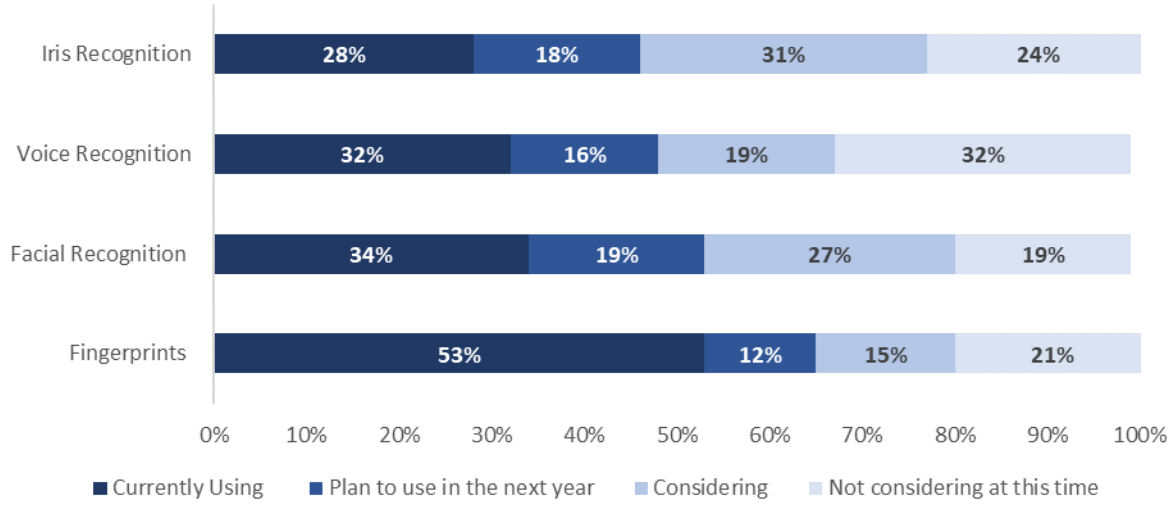
Source: Womble Bond Dixon (2023).

On a global basis, fingerprinting is the most prevalent form of biometric recognition. As shown in Figure 2 below, 53% of respondents are already using the technology and a further 12% planning to adopt it. Facial recognition is the second most common technology currently in use, with 34% of respondent using it. This was followed by voice recognition (32% of respondents) and iris recognition (28% of respondents).

Although iris recognition is less established than other forms of technology, its use looks set to grow. Although only 28% of respondents are currently using it, an additional 18% plan to adopt the technology in the next year, and a further 31% of respondents are considering it for the future. Despite lower adoption than other forms of recognition, iris can be deployed at scale (such as for the Aadhaar programme in India[14]).

[14] Aadhaar is India's national identity database. This contains digital identity information, linked to biometric data such as fingerprint and iris-scans.

Figure 2: Plans for adoption of biometric recognition globally



Source: Womble Bond Dixon (2023)

2.3. Data protection harms

This section describes how DP harms could result from the use of biometric recognition.[15]

2.3.1. Financial harm, loss of control of personal data, psychological harm

The use of biometric recognition increases the risk of DP harm resulting from data being hacked or breached.[16] To administer a biometric recognition scheme biometric data must be collected and stored. In the event of a breach or hacking, this data could be accessed by third parties to mimic individuals and gain access to a system or to use biometric samples to create new accounts.[17]

Individuals whose biometric data is made public are at heightened risk of being impersonated or having biometric samples used without their knowledge. This could lead to:

- financial harm through unauthorised access to a banking app;

[15] ICO (2022) *Overview of DP Harms and the ICO's Taxonomy*. Available at: https://ico.org.uk/media/about-the-ico/documents/4020144/overview-of-data-protection-harms-and-the-ico-taxonomy-v1-202204.pdf (accessed 15 February 2024).

[16] National Cyber Security Centre *Biometric recognition and authentication systems*. Available at: https://www.ncsc.gov.uk/collection/biometrics/how-biometrics-are-attacked#section_2 (accessed 19 January 2024).

[17] National Cyber Security Centre (2019) *Biometric recognition and authentication systems*. Available at: https://www.ncsc.gov.uk/collection/biometrics/how-biometrics-are-attacked#section_2 (accessed 19 January 2024).

- psychological harm through online impersonation or the accessing of photos or medical records; and
- loss of control of personal data leading to anxiety around its potential uses.

Unlike alternative recognition systems such as passwords or pin codes, biometric data describes aspects of an individual's appearance that is very difficult or impossible to change. Without further privacy-preserving measures being embedded in biometric recognition systems, biometric data is not readily replaceable so the risk of harm can be persistent.

Example: Major breach found in biometric system used by banks, UK police and defence firms

In 2019, the fingerprints and facial recognition information of over 1 million people was discovered on a publicly accessible database.[18]

Biometric data can, unless appropriately protected, be used to link across different databases where biometric data is stored. It can act as a unique identifier and be used to link databases that contain personal information about individuals. Where compromised this can expose individuals to a range of potential DP harms including the loss of personal control, financial and psychological harms.

2.3.2. Discrimination

Where biometric recognition systems are not trained appropriately, there is a risk of discrimination against individuals or groups. For example, fingerprint recognition is less accurate for adults over 70 and children under 12. This is because older adults' fingerprints are less distinct and young children's fingerprints are still developing so they change rapidly.

As a result, a technology may systematically perform worse for older adults and young children, causing discrimination.

Where systems are not reviewed, there is potential for other types of bias, particularly where these are used for automated decision making.

Example: Legal action over alleged facial recognition bias

In 2021, a taxi driver was dismissed due to an organisation's facial recognition

[18] Guardian (2019) *Major breach found in biometrics system used by banks, UK police and defence firms*. Available at: https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms (accessed 19 January 2024).

software not recognising him.[19] The driver alleged that the software had higher error rates for people with darker skin. This case raises concerns around the potential accuracy of biometric recognition, especially when used for automated decisions which have the potential to affect individuals' livelihoods. This highlights the need for clear guidance which prevents discrimination as a result of using biometric recognition.

2.3.3. Unwarranted intrusion, adverse effects on rights and freedoms and chilling effects

Biometric recognition systems, such as live facial recognition, can be used to monitor publicly accessible spaces. The use of this technology for surveillance creates the risk that an individual may not be aware their biometric data is being processed.

There are concerns that the use of biometric recognition systems in public spaces could result in a 'chilling effect' where people are less likely to exercise rights such as freedom of expression or freedom of assembly. Unnecessary deployment of these technologies may also result in unwarranted intrusion.

However, adoption of live facial recognition for purposes other than law enforcement is low. A recent survey of local authorities by the Biometrics and Surveillance Camera Commissioner found that while almost 99% of respondents operated public space surveillance systems, no respondents reported use of live facial recognition.[20]

2.4. Policy Context

It is important to consider the wider policy context surrounding the problem to assess where there is positive or negative alignment with the proposed intervention. This includes both internal ICO policy but also wider initiatives such as government policy.

[19] BBC News (2021) *Legal action over alleged facial verification bias*. Available at: https://www.bbc.co.uk/news/technology-58831373 (accessed 15 February 2024)

[20] Office of the Biometrics and Surveillance Camera Commissioner (2023) *The use of overt surveillance camera systems in public places*. Available at: https://assets.publishing.service.gov.uk/media/646f5bdcab40bf000c196a76/20230517_LA_survey_paper_FINAL.pdf (accessed 2 February 2024).

2.4.1. ICO strategy

ICO25 is the ICO's overarching strategic plan. The first two objectives of the plan are to:[21]

- safeguard and empower people; and
- empower responsible innovation and sustainable economic growth.

Striking a balance between the benefits of enhanced efficiency and the DP of users is imperative as technologies develop and biometric recognition becomes embedded across the economy.

2.4.2. Relevant legislation

We developed the guidance in accordance with relevant legislation on DP and employment law, in particular the UK General DP Regulation[22] (UK GDPR) and the DP Act 2018 (DPA 2018).[23] These laws control how organisations, businesses or the government use personal information. The guidance provides additional clarification to organisations on the compliant and lawful use of biometrics for recognition.

The UK government is currently working on the Data Protection and Digital Information (DPDI) Bill. Although the Bill has yet to complete its Parliamentary passage, it will likely become the most relevant legal framework when it becomes law. It is important that the guidance is flexible so it can be updated to align with the Bill.

2.4.3. Relevant external policy landscape

The most relevant external policy considerations are:

The National Data Strategy

The National Data Strategy looks at how to use the UK's existing strengths to boost the better use of data across businesses, government, civil society and people.[24]

The strategy has five main missions which set out the priority areas. These are:

---

[21] ICO (2022) *ICO25 strategic plan.* Available at: https://ico.org.uk/about-the-ico/our-information/our-strategies-and-plans/ico25-plan (accessed 15 February 2024).
[22] *UK General Data Protection Regulation.* Available at: https://www.legislation.gov.uk/eur/2016/679/contents (accessed 15 February 2024).
[23] *Data Protection Act 2018.* Available at: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted (accessed 15 February 2024).
[24] UK Government (2019) *National Data Strategy.* Available at: https://www.gov.uk/guidance/national-data-strategy (accessed 15 February 2024).

1. unlocking the value of data across the economy;
2. securing a pro–growth and trusted data regime;
3. transforming government's use of data to drive efficiency and improve public services;
4. ensuring the security and resilience of the infrastructure on which data relies; and
5. championing the international flow of data.

Providing regulatory certainty aligns well with all the missions listed. For example, assisting organisations in complying with DP legislation aligns well with the second mission, through improving trust in the data regime to enable growth.

UK Digital Strategy

Another important policy consideration is the UK Digital Strategy,[25] which sits alongside the National Data Strategy with the following objectives:

- unlocking the power of data;
- a secure digital environment; and
- enhancing the UK's place in the world.

Providing clarity and practical advice should help organisations to feel more confident about their use of personal data and assist with meeting the objectives listed.

UK digital identity and attributes trust framework

The UK digital identity and attributes trust framework aims to make it easier and more secure for people to use services that enable them to prove who they are. It is a set of rules for organisations to follow if they want to provide secure and trustworthy digital identity. The framework explains what rules organisations will need to follow to be certified against the trust framework.[26]

2.5. Market failures

The unregulated adoption of biometric recognition can result in market failures.

---

[25] DCMS (2022) *UK Digital Strategy.* Available at: https://www.gov.uk/government/publications/uks-digital-strategy/uk-digital-strategy (accessed 15 February 2024).

[26] DCMS (2023) *UK digital identity and attributes trust framework.* Available at: https://www.gov.uk/government/publications/the-uk-digital-identity-and-attributes-trust-framework/the-uk-digital-identity-and-attributes-trust-framework (accessed 15 February 2024).

Market failures in relation to biometric recognition include **imperfect information**, where feedback from our previous call for views highlighted a lack of clarity over terminology and context specific DP guidance.[27] 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. Consumers may also be unaware of the risks of handing their biometric data to organisations, or that organisations may be processing this information. A 2022 survey of UK consumers found that 60% were unaware their biometric data could be shared with other companies.[28]

The potential accuracy of biometric recognition, and the sensitivity of biometric data can also exacerbate the risk of harms (such as discrimination, and the loss of control of personal data) driving the need for intervention. The adoption of biometric recognition can also result in **negative externalities**, where organisations do not consider the invasive or sensitive nature of unnecessarily creating biometric data and the cost this may impose on individuals.

As the UK's DP regulator, the ICO is well placed to provide regulatory certainty and address these market failures.

2.5.1. Rationale for intervention

In summary, a combination of strong industry adoption and lack of regulatory input has contributed to uncertainty on how the UK GDPR and DPA 2018 apply to biometric technologies, as highlighted in a previous ICO call for views.[29] This absence of regulatory certainty has contributed to a number of DP harms and market failures, such as discrimination and the loss of personal control of personal data. Without regulatory intervention, organisations may draw their own conclusions on the lawful adoption of biometric recognition and lead to their use in inappropriate circumstances. Given the unique and sensitive nature of biometric data this creates the potential for DP harms, which in the absence of intervention is likely to grow.

---

[27] ICO (2022) *Biometrics: foresight.* Available at: https://ico.org.uk/media/about-the-ico/documents/4021971/biometrics-foresight-report.pdf (accessed 1 February 2024).

[28] Capterra (2022) *Has Covid-19 monitoring changed how UK consumers feel about sharing biometric data?* Available at: https ://www.capterra.co.uk/blog/2715/covid-monitoring-and-biometric-data-uk-consumers (accessed 2 February 2024).

[29] ICO (2022) *Biometrics: foresight.* Available at: https://ico.org.uk/media/about-the-ico/documents/4021971/biometrics-foresight-report.pdf (accessed 1 February 2024).

3. Options appraisal

Here we set out the options that were considered to address the problem identified in the previous chapter and why the preferred option was selected.

As set out in Section 1.1.2, the ICO has provided little regulatory clarity on biometric recognition to date. Although other regulatory tools are available, guidance was considered the most appropriate means to:

- improve protections for the large numbers of individuals whose data is collected by biometric technologies, including vulnerable individuals;
- create regulatory certainty to encourage responsible innovation of biometric technologies; and
- promote a lawful and responsible approach for future developments and current applications.

Additionally, the ICO's strategic plan, ICO25, commits to a 'guidance pipeline' to enhance regulatory certainty where appropriate. This includes producing guidance on emerging technology, such as AI and biometrics and a programme of guidance reviews in response to forthcoming legislative reform. Accordingly, the options presented below focus on guidance as the means of addressing the regulatory uncertainty described in Section 2.1.

3.1. Options for consideration

The following options for intervention were considered to solve the issue of regulatory uncertainly and the related harms and market failures discussed in the previous chapter:

- **Do nothing:** do not provide any additional regulatory certainty for biometric recognition.
- **Do less:** provide updates to the current guidance on special category data (see Section 1.1.2).
- **Preferred option:** provide standalone guidance covering the use of biometric data in biometric recognition systems.
- **Do more:** provide sector-specific guidance outlining specific DP considerations with all known current and emerging use cases for biometric recognition.

3.2. Assessment of options

In line with HM Treasury guidance, we qualitatively assesses options against the critical success factors (CSFs) set out below:

- **Strategic alignment:** Considers how options fit with ICO25 objectives and the wider policy landscape.

- **Affordability:** Covers the financial impacts of options, including the cost for the ICO of delivering and maintaining these (e.g. staff time and other resources).
- **Achievability:** Conders the viability of options as long-term solutions, and whether further action is likely to be required in the future.
- **Risks:** the risks posed to the ICO, including legal and reputational risks (this includes the risks of the ICO being challenged on outdated guidance).
- **Impacts –** Considers whether options have a positive or negative impact on businesses (including whether options reduce regulatory uncertainty or impose additional compliance costs on businesses).

As evidence is limited, a degree of judgement is used to score options against each of these factors. Accordingly, the assessment should be viewed as indicative rather than as a robust options appraisal. Options have been assigned a red, amber, green (RAG) rating for each CSF.

Table 1: Assessment of options

Option	Strategic Alignment	Affordability	Achievability	Risks	Impacts
Do nothing	Low	Low	High	Medium	Low (-ve)
Do less	Low	Low	High	Medium	Low (-ve)
Preferred option	High	Medium	High	Low	High (+ve)
Do more	High	Low	Low	Low	High (+ve)

Source: ICO analysis.

The preferred option has no red ratings and four out of five criteria are green. This is the highest scoring option and, as such, this is deemed the most appropriate option to progress.

The preferred option aligns with ICO25 objectives and the external policy environment. The upfront cost to the ICO of producing guidance is expected to be offset by the impact of increased regulatory certainty for organisations and the reduced potential for DP harms. The preferred option ensures that guidance on biometric recognition reflects the current state of technology and reduces the risk of the ICO being challenged on outdated guidance.

4. Detail of proposed intervention

This section provides an overview of the guidance intervention identified in the previous chapter and its objectives. It also sets out a theory of change for the guidance, which covers the change the guidance is expected to bring about and the causal chain of events that are expected to bring about that change. The section concludes by providing an overview of the main groups expected to be impacted by the guidance.

4.1. The guidance

The guidance explains how DP 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:

- the definition of biometric data under GDPR;
- what is considered biometric data;
- how this data is used in biometric recognition systems; and
- the DP requirements that must be complied with.

4.1.1. Overarching objectives

The overarching objectives of the guidance are:

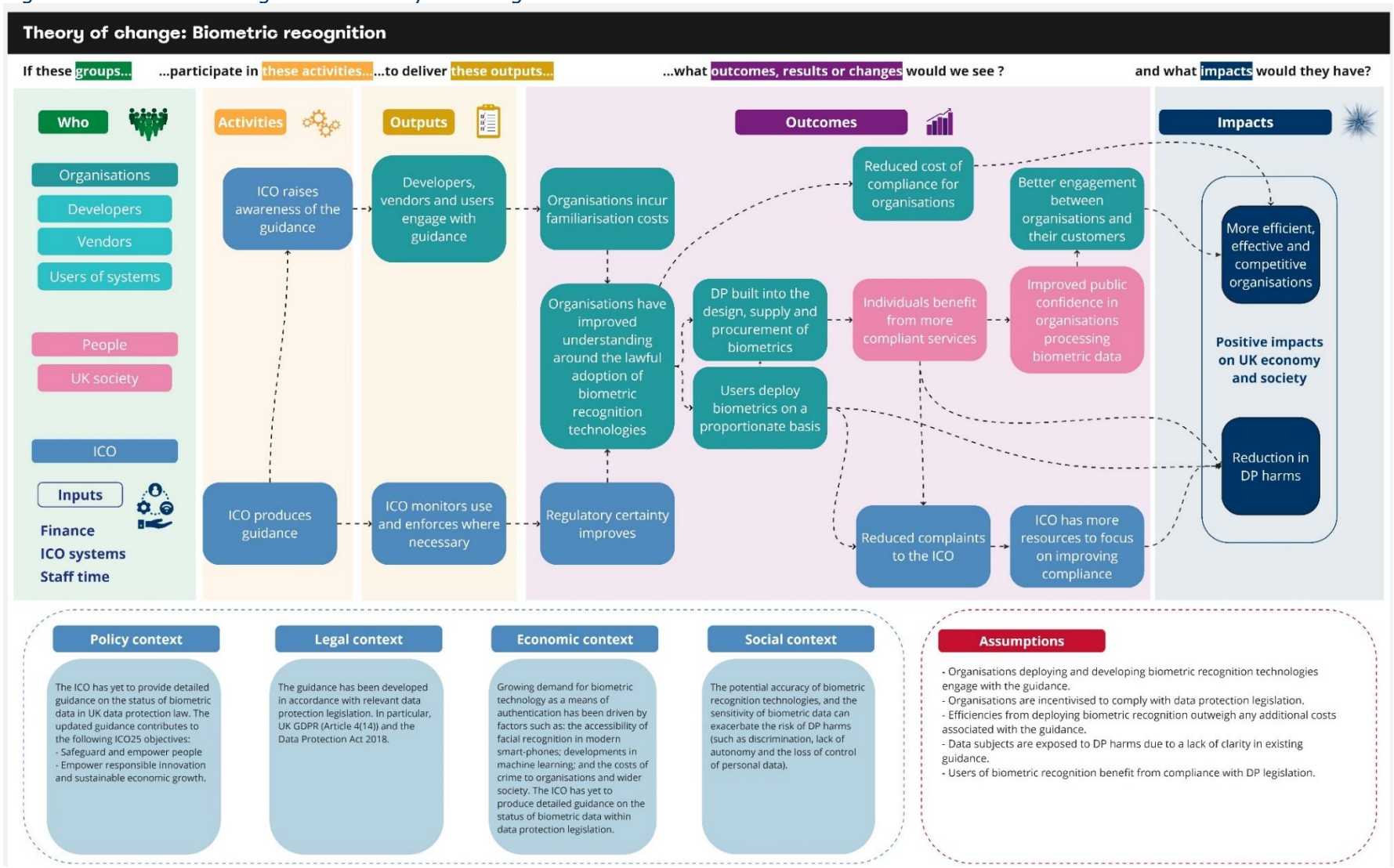
- To provide regulatory certainty to organisations processing biometric data on whether or not they are processing personal data.
- To provide regulatory certainty to organisations processing biometric data on whether or not they are processing special category personal data.
- To provide regulatory certainty to organisation regarding our expectations when they are processing special category biometric data.

These objectives align with the problem identified in Section 2, as well as with ICO25 objectives to safeguard and empower people; and empower responsible innovation and sustainable economic growth.

4.1.2. Theory of change

Our impact assessment is underpinned by an 'output to outcome to impact' methodology, called a theory of change. This shows how the guidance links to a chain of results that lead to the intended impacts. It should be noted that impact, linked to the rationale, is often the most difficult aspect to measure because it will occur over a longer period of time and can be influenced by other external factors. Our theory of change is shown in Figure 3 below.

Figure 3: Biometric recognition – theory of change



Source: ICO analysis.

4.2. Scope of guidance

The guidance is primarily aimed at organisations that use or are considering using biometric recognition systems. It is also aimed at developers and vendors of these systems.

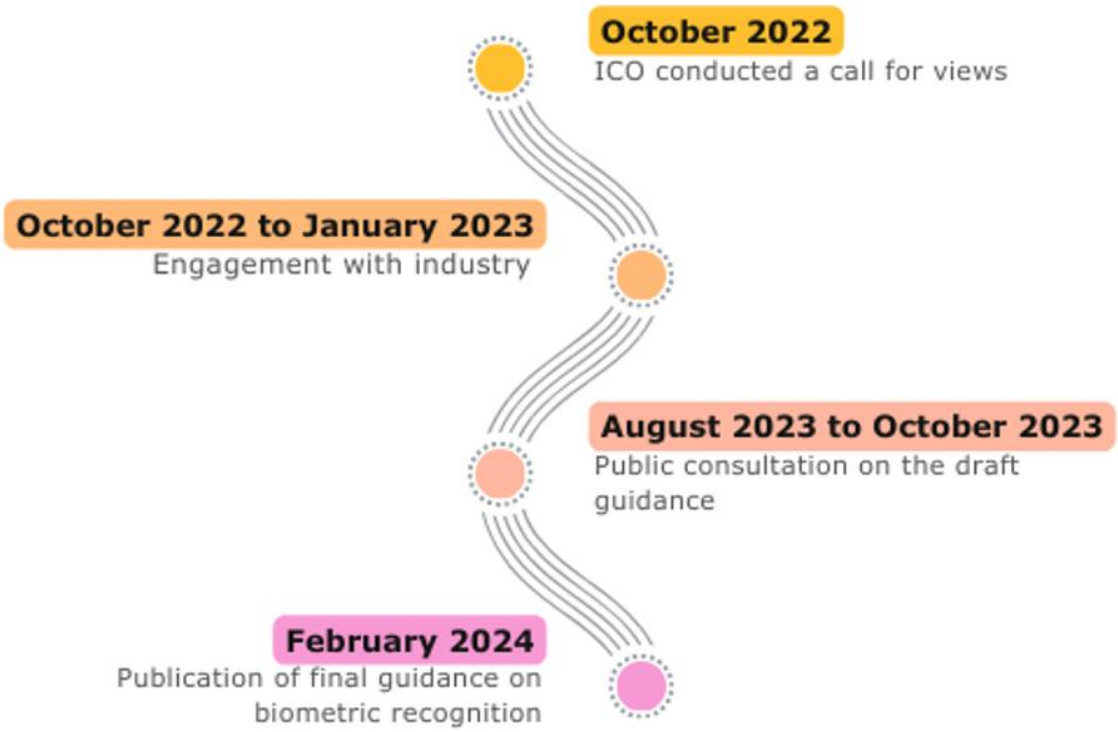
The guidance covers the definition of biometric data under the UK GDPR. It focuses on biometric recognition use cases and explains how these involve the processing of special category biometric data. It does not cover the processing of biometric data for use cases outside of biometric recognition. This will be discussed in the next phase of our guidance, due to be published towards the end of 2024.

The guidance does not cover requirements of the DP regimes for the law enforcement purposes or the security services. However, some of the principles explained in the guidance are relevant to these regimes too.

4.3. Guidance timeline

Figure 4 shows some of the key milestones in the development of the guidance.

Figure 4: Timeline of key milestones linked to the guidance



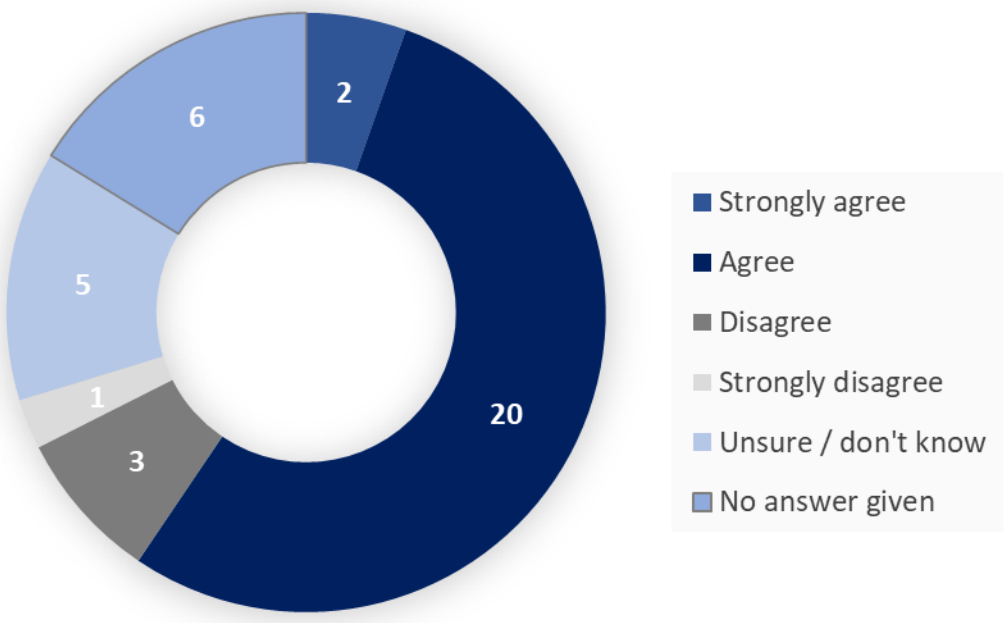
Source: ICO.

4.3.1. Public consultation

The ICO consulted on draft biometric data guidance and a summary impact assessment for eight weeks between August and October 2023.[30, 31] 37 responses were received. Around two-thirds of respondents were from organisations in the supply chain for biometric technology, the remainder were from civil society. To address some of the wider consultation feedback, additional clarification was added to the guidance.

Figure 5 shows the extent to which respondents agreed with the scope and coverage of the impact assessment presented in the consultation. 60% (22 respondents) agreed that the impact assessment summary adequately scoped the main affected groups and impacts. 30% (11 respondents) did not offer a view.

Figure 5: Extent of agreement with impact assessment's scope and coverage



Source: ICO analysis, n=37.

[30] ICO (2023) *ICO consultation on the draft biometric data guidance.* Available at: https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-consultation-on-the-draft-biometric-data-guidance/ (accessed: 24 January 2024).

[31] ICO (2023) *Annex: A summary of the Biometrics guidance impact assessment.* Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/guidance-on-biometric-data/annex/ (accessed: 24 January 2024).

The consultation touched on a range of themes and was broadly supportive of our impact approach. Areas in which respondents felt the impact assessment was not sufficient are presented below.

- A number of respondents felt the estimate of £40 for familiarisation costs was too low. In addition, respondents suggested that many staff would need to read and understand the guidance. Of the respondents representing an organisation, ten respondents indicated more than one whole department would need to read the guidance, a further four indicated one whole department (14 respondents).
- It was suggested that the ICO should explain how it determined the most appropriate regulatory action was to publish guidance rather than pursuing other regulatory approaches.

Feedback from respondents about impacts that should be reflected in the cost benefit analysis included:

- Developers and users of biometric technology welcomed the regulatory certainty that would follow the production of guidance (six respondents).
- A reduced risk of legal challenges and time spent by staff justifying directives regarding DP (one respondent).

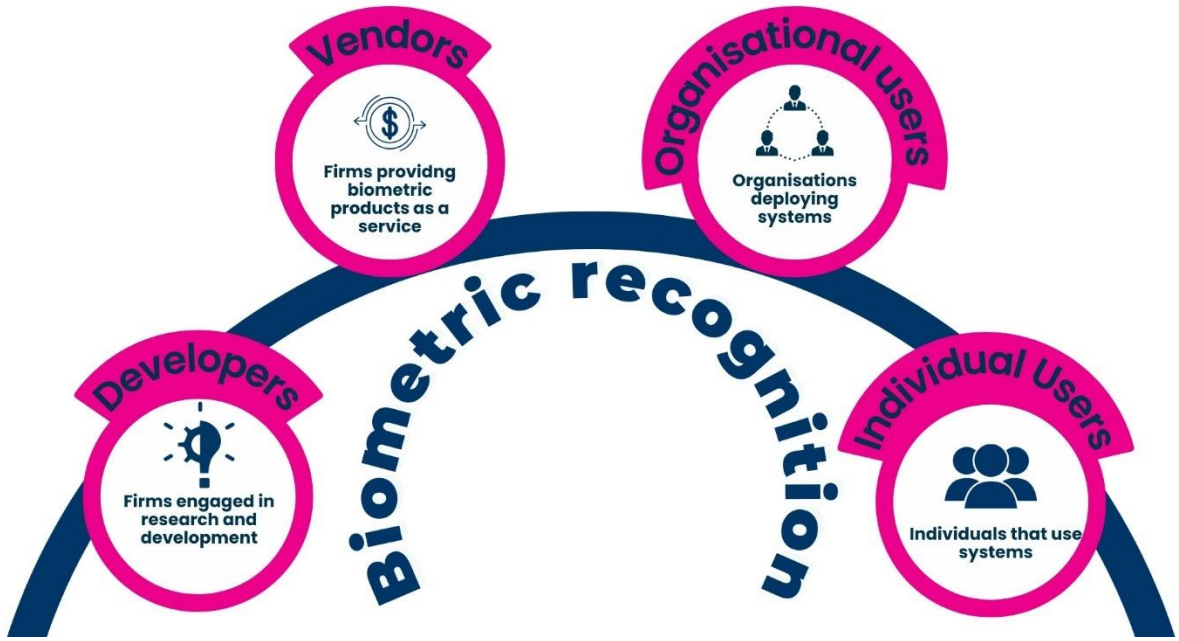
This impact assessment responds to this feedback by provided a greater level of detail on the approach and evidence used and by incorporating this input in our analysis.

4.4. Affected groups

The main groups we expect to be affected by the guidance are outlined below. The primary affected group are captured in Figure 6: showing the supply chain for biometric recognition systems from development of a product through to the end user. There are a number of challenges with quantifying the scale of affected groups, including a lack of robust data and evidence.

As biometric recognition is an established technology which is not limited to specific sectors, there are no industry SIC codes which can be used to identify market size, employment or turnover. The majority of evidence on the scale of affected groups is therefore derived from external research and surveys, or patent filings, which we have used to provide an indication of UK developer activity.

Figure 6: Supply chain for biometric recognition systems



Source: ICO analysis.

4.4.1. Developers of biometric recognition

The guidance is likely to affect developers of biometric technology and organisations involved in R&D activities. These organisations are expected to engage with the guidance to ensure that technology development complies with DP legislation.

While we have been unable to quantify the number of UK based developers, we have used patent filings as a proxy for assessing UK developer activity. It is important to note that this only offers a partial picture, as not all developers will be covered by patent filings given that biometric recognition is an established technology.

We used an online database of patents to identify those that were tagged with the following terms:[32] 'biometric recognition'; 'biometric identification'; and 'biometric verification'. In the following analysis we use 'biometric recognition' to refer to all of these terms.

To measure patent activity our analysis focusses on UK applicants who were granted patents rather than those granted by the UK Intellectual Property Office

[32] *The Lens Patent Database* Available at: https://www.lens.org/lens/search/patent/structured (accessed 2 February 2024).

(IPO).[33] This is considered a more comprehensive measure since it also captures information on UK-based applicants that seek patent protection abroad without corresponding protection in the UK.[34]

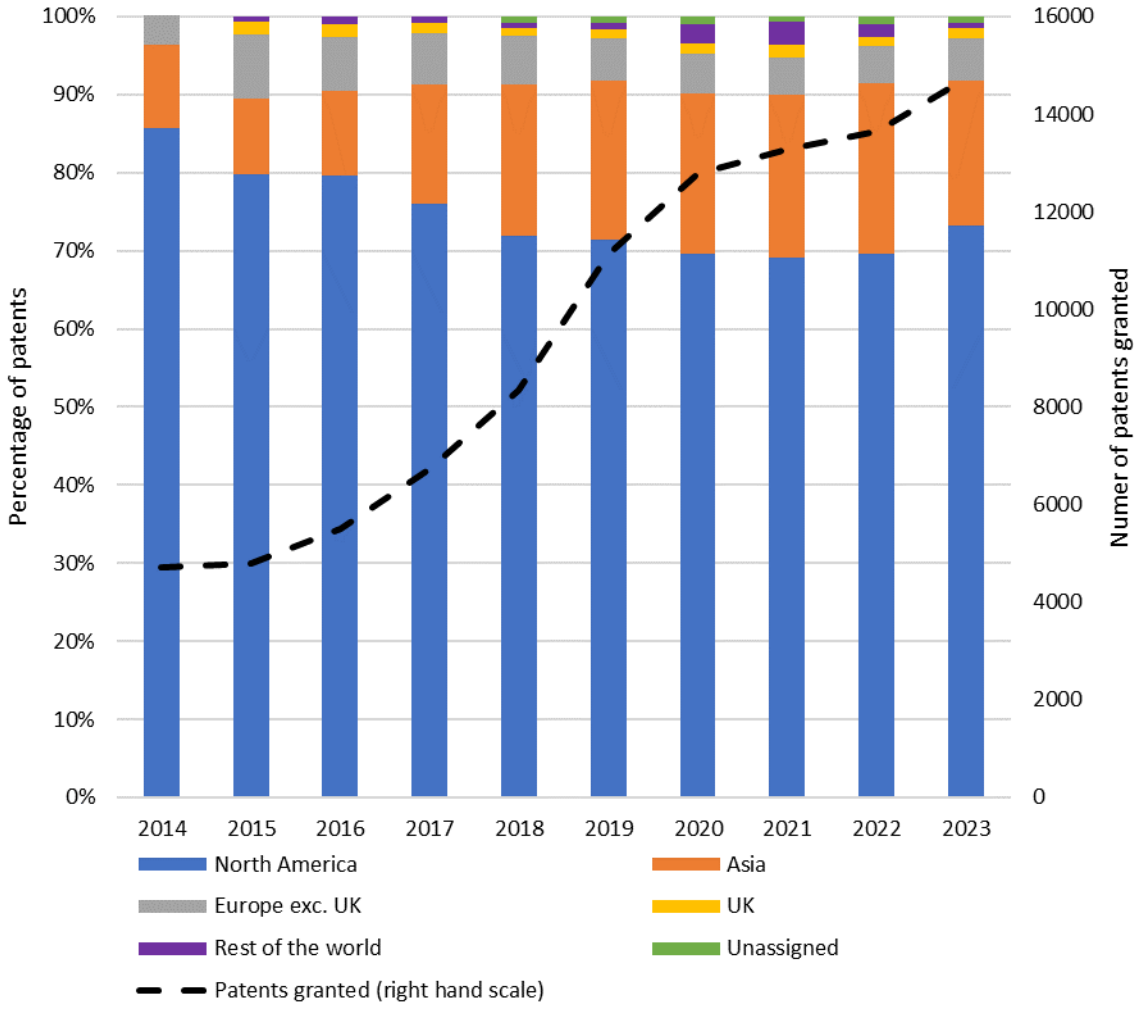
Since 2014, around 95,000 patents have been granted globally.[35] As seen in Figure 7, there has been a three-fold increase in activity, from around 5,000, patents granted in 2014 to 15,000 in 2023. UK applicants accounted for 1.4% of patents (around 1,300) granted between 2014 and 2023. By this measure, the UK ranks 6th globally.

[33] Since 2005, UK residents have not been required to make patent applications in the UK before making applications to other countries. Since 2014, just 18 patents for biometric recognition have been granted by the UK IPO, equivalent to 0.02% globally.

[34] If an applicant were to file a patent for the same innovation in multiple jurisdictions it would be counted more than once. Given the overall number of patents it was not proportionate to exclude these from our analysis.

[35] This includes patents granted by 106 national and supernational organisations listed by lens.org. These figures reflects the data available at the time of analysis (1 February 2024). Note that data is periodically revised and may be subject to change as new information is added to the database.

Figure 7: Number and share of patents granted for biometric recognition globally, 2014 to 2023



Note: Russia has been included as 'Europe'.
Source: ICO analysis of data from lens.org.

4.4.2. Vendors of biometric recognition

The guidance will also affect organisations providing biometric products as a service. There are a number of UK based suppliers that sell biometric solutions. This covers employee monitoring, and biometric recognition across a range of sectors.

Evidence on the number of UK based vendors is limited. Biometric technologies are often supplied as a package of services rather than as distinct products, and are marketed across a broad range of sectors. This makes it challenging to quantify this group of organisations.

4.4.3. Organisational users of biometric recognition

The guidance is of particular relevance to organisations that have adopted or are planning to invest in biometric recognition. These organisations need to

understand the guidance to ensure that adoption of biometric recognition is proportionate and compliant with DP legislation.

Like other groups, it is challenging to quantify the total number of users of biometric data as these technologies span a range of sectors. A non-exhaustive list of illustrative examples where biometric recognition is used is provided below.

Financial Services

Biometric data is widely used in the financial services sector for secure authentication, to reduce fraud and offer a more frictionless service to customers. Biometric data is often used for purposes including:

*Biometric payments, which are expected to reach $5.8 trillion of global purchases and cover 3 billion users by 2026.[36]

*Customer verification to allow access to a system or online account.

*Account opening and customer onboarding. A quarter of UK adults say they would abandon the process of opening a bank account if identity checks were too time-consuming or complex.

Healthcare

Biometric recognition is widely used in the healthcare sector to register and identify patients and to control access to healthcare facilities.

Some healthcare providers are also exploring the potential to link biometric data to other datasets, such as patient medical records, to increase efficiency and improve diagnosis. This might include the use of biometric recognition to accurately match patient records across different sites of care, such as multiple

[36] JP Morgan (2023) *Biometric payments get a boost.* Available at: https://www.insiderintelligence.com/content/biometric-payments-jpmorgan-targets-6b-opportunity (accessed 5 February 2024).

hospitals or clinics.

Education

Use of biometric data in the education sector largely covers access control, secure identification and cashless catering. In schools, biometric recognition is sometimes used to allow eligible pupils to claim free school meals. A study of UK schools found that 38% of primary schools and 75% of secondary schools in England used some form of biometric technology.[37]

Where biometric recognition is used schools generally offer alternative means of identification including QR codes, swipe cards or unique PIN. In an education setting fingerprint is the most common means of biometric recognition, although there is growing use of facial recognition.

4.4.4. Individual users of biometric recognition

Individuals that engage with biometric recognition are also likely to be affected by the guidance. A study by Deloitte found that 85% of UK adults own a smart-phone and around 80% of those that do have used biometric recognition features.[38] This does not cover data subjects who engage with biometric technologies through other means, and as such is likely to underestimate the number of individuals affected by the guidance.

4.4.5. ICO

The ICO will be affected, as the regulator of DP legislation and as the producer of the guidance.

---

[37] Defence Digital Me (2022) *The State of Biometrics 2022: A Review of Policy and Practice in UK Education.* Available at: https://defenddigitalme.org/research/state-biometrics-2022/#:~:text=Each%20parent%20of%20the%20child,no%20parent%20has%20withdrawn%20consent (accessed 5 February 2024).

[38] Defines UK adult population as 16-75. Deloitte (2017) *Surge in UK adoption of fingerprint recognition points way to mainstream biometric authentication at the expense of the password.* Available at: https://www2.deloitte.com/uk/en/pages/press-releases/articles/surge-in-uk-adoption-of-fingerprint-recognition.html (accessed 2 February 2024).

4.4.6. Wider society

The guidance also has the potential impact on other groups, and may have indirect impacts on wider society. This might include:

- organisations within the supply chain of developers and providers of biometric recognition;
- civil society groups; and
- the wider population.

It is difficult to estimate who the guidance would and wouldn't affect indirectly. As such, we estimate the whole population as an upper-end estimate. According to latest estimates, there are around 67 million people in the UK.[39]

[39] ONS (2022) *Population estimates time series data set 2021.* Available at: https://www.ons.gov.uk/peoplepopulationandcommunity/populationandmigration/populationestimates/datasets/populationestimatestimeseriesdataset (accessed 2 February 2024).

5. Cost-benefit analysis

In this section, we consider the potential costs and benefits of the guidance. Our aim is to understand whether there are likely to be significant impacts on affected groups (both positive and negative; and direct and indirect) and to judge the overall impact on society. We draw on a mixture of quantitative and qualitative evidence but our analysis is limited by the evidence available.

5.1.1. Counterfactual

To help us measure the impact of the guidance, we have taken as our starting point what the situation is now and how this would evolve without intervention, known as the counterfactual. The counterfactual is the baseline against which we estimate the additional impacts of introducing the guidance. If the guidance was not introduced, then the underlying DP legislation and existing guidance would continue to apply and form the counterfactual for the purposes of this assessment.

The counterfactual is the baseline against which we estimate the additional impacts of introducing the guidance. If the guidance was not introduced, then the underlying DP legislation and existing guidance would continue to apply and form the counterfactual for the purposes of this assessment (this is described in Section 1.1.2). In line with government guidance,[40] we assume compliance both with existing legislation and guidance, in the absence of specific evidence to suggest otherwise. This simplifies the assessment, but it is not intended to suggest that there is total compliance.

5.1.2. Monetising impact

Quantified analysis of the impacts is particularly challenging for this guidance because of its wide ranging scope and the difficulty in quantifying the affected groups due to a deficit of robust evidence.

Quantifying potential costs and benefits is complex because this varies considerably depending on a range of different factors. These factors include:

- the nature of activities that biometric recognition is used for;
- the processing associated with those activities; and
- the likelihood and severity of DP harms.

[40] BEIS (2017) *Business impact target.* Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/609201/b usiness-impact-target-guidance-appraisal.pdf (accessed 24th January 2024).

Our analysis therefore focuses primarily on non-monetised impacts. However, where possible, we have provided high level quantitative analysis to indicate scale.

5.1.3. Uncertainty, risk and optimism bias

As set out in the Treasury's Green Book,[41] it is necessary to consider the significant levels of uncertainty surrounding the impacts of the code. Although optimism bias is typically only considered in capital projects,[42] we understand that there can be a tendency to overestimate engagement with guidance. To account for and demonstrate the implications of any potential bias, we have provided sensitivity analysis for the impacts we have been able to quantify.[43] This tests the sensitivity of impact estimates to changes in assumptions and is provided in Annex A:A.1.

[41] HM Treasury *The Green Book: appraisal and evaluation in central government.* Available at: https://www.gov.uk/government/publications/the-green-book-appraisal-and-evaluation-in-central-government (accessed 16 February 2024)

[42] Department for Finance of Northern Ireland *Step six: assess risk and adjust for optimism bias section 2.6.27.* Available at: https://www.finance-ni.gov.uk/articles/step-six-assess-risks-and-adjust-optimism-bias (accessed 2 February 2024).

[43] See para 5.59 of HM Treasury's Green Book for more information on sensitivity analysis. HM Treasury (2022) *The Green Book: appraisal and evaluation in central government.* Available at: https://www.gov.uk/government/publications/the-green-book-appraisal-and-evaluation-in-central-govervent (accessed 2 February 2024).

5.2. Costs and Benefits

Table 2: Summary of potential impacts

Affected groups	Benefits	Costs
Developers of Biometric Recognition	Developers of biometric recognition have a better understanding of their legal obligations and the regulatory environment. Regulatory clarity over DP supports the development of biometric recognition.	Familiarisation costs of reading and understanding the guidance (estimates range from £115 for small organisations to £1,153 for a large organisation[44]). Potential loss of revenue from users switching to systems that implement a DP by design approach.
Vendors of Biometric Recognition	Vendors of biometric recognition have a better understanding of their legal obligations and the regulatory environment. Suppliers benefit from users having greater trust and confidence in products and therefore being more willing to use them.	Potential loss of revenue where users choose to adopt alternatives to biometric recognition. Familiarisation costs of reading and understanding the guidance (estimate a range from £115 per small organisations to £1,153 per large organisation.)

[44] Based on consultation feedback (as set out in Section 4.3.1) that multiple individuals will need to read the guidance, we assume medium and large organisations will read the guidance ten times resulting in a cost of £1,153. For small organisations we have assumed the guidance will be read once, resulting in a cost of £115. For further details, see Annex A.

		Potential loss of revenue from users switching to systems that implement a DP by design approach.
Organisational Users of Biometric Recognition	Greater regulatory certainty and confidence in the adoption of biometric recognition leading to safe and efficient outcomes. Increased trust and confidence amongst customers and wider society.	Familiarisation costs of reading and understanding the guidance (estimate a range from £115 per small organisations to £1,153 per large organisation.). Cost of finding and administrating alternatives, where biometric processing is not proportionate. Potential costs of applying appropriate security measures to biometric data.
Individual Users of Biometric Recognition	Reduction in potential DP harms from better understanding of the appropriate safeguards in biometric recognition. 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. 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. Reduced risk of social exclusion of individuals unable to engage with biometric technologies (e.g. finger printing in over 70s). Adoption of biometric verification systems makes it is easier to identify and correct bias and discrimination than with a human-led process.

Source: ICO analysis.

5.2.1. Developers and vendors of biometric recognition

The guidance is expected to impact developers and vendors of biometric recognition through:

- Providing greater regulatory certainty by clarifying how DP law applies. A previous ICO call for views[45] highlighted a lack of clarity over the appropriate and lawful use of biometrics for recognition. This has the potential to impede development activity, particularly where there is uncertainty over what constitutes compliant behaviour. On a global basis, a lack of sufficient regulation and governance was cited in a 2023 survey as one of the top three barriers to industry development (43% of respondents).[46]
- In becoming aware of the guidance, developers and suppliers may decide to familiarise themselves with it and incur a cost in doing so. This is discretionary and as such benefits to the providers are likely to outweigh familiarisation costs. An estimate of potential familiarisations costs for organisations that engage with the guidance is provided in Annex A.
- As a result of increased regulatory clarity, developers and suppliers may decide to make changes to how they design or implement biometric recognition solutions. This may be to correct elements of non-compliance or provide assurance to clients that biometric solutions are compliant with DP legislation.
- There may be revenue impacts where the guidance affects the adoption of biometric recognition. This could be positive, where there is increased demand for biometric recognition with enhanced security measures, or negative where users decide that adoption of biometric recognition is not proportionate. Users that are concerned about the risk of DP harms may also switch to systems that have stronger security in place to protect biometric data.

5.2.2. Organisational users of biometric recognition

- The guidance may result in increased regulatory certainty and improved confidence in organisations' adoption of biometric recognition. As highlighted earlier, a lack of global regulation is cited as one of the main barriers for industry growth. The guidance could therefore result in cost savings from not having to pay for external advice or result in efficiencies

[45] ICO (2022). Available at: https://ico.org.uk/media/about-the-ico/documents/4021971/biometrics-foresight-report.pdf (accessed 1 February 2024).

[46] Biometrics Institute (2023) *Biometrics Institute Industry Survey 2023.* Available at: https://www.biometricsinstitute.org/wp-content/uploads/SUMMARY-Biometrics-Institute-Industry-Survey-2023_FINAL.pdf (accessed 2 February 2024).

for organisations that decide to adopt biometric recognition in response to increased regulatory clarity.

- In becoming aware of the guidance, organisations using biometric recognition may decide to familiarise themselves with the guidance and incur a cost in doing so. This is discretionary and as such benefits to users is likely to outweigh familiarisation costs. An estimate of potential familiarisations costs for organisations that engage with the guidance is provided in Annex A:.
- As a result of increased regulatory certainty there may be cases where the deployment of biometric recognition is not proportionate for its intended use. This may lead to costs of finding and administering alternatives to biometric recognition. Where this is the case there are likely to be low-cost replacements available, such as passwords and pin-codes.
- Users of biometric recognition may face additional costs of putting in place appropriate security measures for biometric data. This could include the time-costs of organisational measures, such as testing and reviewing systems, as well as the additional cost of procuring security compliant systems. As organisations are likely to already undertake these measures, the additional cost is expected to be low.[47]
- Where the guidance improves compliance, there may be indirect benefits such as improved public confidence in biometric recognition systems. Survey research conducted by Frontier Economics found that improved public trust is likely to increase individuals' willingness to share data.[48] This may allow users of biometric recognition to use technologies more productively. This might involve linking biometric recognition to other datasets to offer more efficient services.

5.2.3. Individual users of biometric recognition

By providing clarity around explicit consent, individuals that engage with the guidance may be better informed and have greater capacity to exercise their DP rights. Many individuals are often unaware of their DP rights. A 2022 survey of

[47] Over half of UK organisations that have carried out activities including risk assessments and testing to identify cyber security risks in the last 12 months. Department for Digital, Cultura, Media and Sport (2022) *Cyber Security Breaches Survey 2022.* Available at: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022#chapter-4-approaches-to-cyber-security (accessed 2 February 2024).

[48] ODI (2021) *Economic Impact of Trust in Data Ecosystems.* Available at: https://theodi.org/insights/reports/the-economic-impact-of-trust-in-data-ecosystems-frontier-economics-for-the-odi-report/ (accessed 5 February 2024).

UK consumers found that 60% were unaware their biometric data could be shared with other companies.[49]

The use of biometrics increases the risk of harms resulting from biometric data being hacked or stolen, or towards individuals who may suffer discrimination from automated decision-making. Increased regulatory certainty over the lawful adoption of biometric recognition may reduce the likelihood of technology being used in inappropriate circumstances that have the potential to lead to DP harms.

The guidance may also result in minor time costs for UK data subjects from using less efficient alternatives for biometric recognition, such as passwords or pin-codes. However, these costs are expected to be minimal.

5.2.4. ICO

It is likely the ICO will incur costs in producing and raising awareness of the guidance. However, it is expected that this will be outweighed by the benefits of enhanced compliance. There may also be potential efficiency savings relating to a reduction in demand for advice and support from users of biometric recognition.

5.2.5. Wider society

Impacts of the guidance on wider society are hard to quantify but could include:

- A reduced cost of dealing with the consequences of DP harms, including to those who have their biometric data hacked or stolen.
- An increased willingness to engage with biometric recognition systems as a result of the technology being used in a clearly defined and proportionate basis.
- Reduced likelihood of 'scope creep' where the deployment of biometric recognition for one purpose may be extended to another (such as for workplace monitoring), with associated implications for public trust.
- Improved public confidence and trust in the compliant use of biometric recognition.
- Reduced risk of social exclusion for individuals unable to engage with biometric recognition systems.

The balance of these impacts is not possible to robustly assess and is largely dependent on the impacts of other affected groups.

---

[49] Capterra (2022) *Has Covid-19 monitoring changed how UK consumers feel about sharing biometric data?* Available at: https ://www.capterra.co.uk/blog/2715/covid-monitoring-and-biometric-data-uk-consumers (accessed 2 February 2024).

5.2.6. Distributional Impacts

As discussed earlier in Section 2.3.2, where biometric recognition systems are not trained sufficiently, there is a risk of discrimination against individuals or groups. Some individuals may also be unable to engage with biometric recognition (such as the over 70s with fingerprint technology). The guidance may therefore benefit those with protected characteristics through the reduced potential for DP harms.[50]

Where users are concerned about the DP harms associated with biometric recognition, the potential costs of procuring security compliant systems may impose a larger costs on smaller organisations. However, these are safeguards we expect most organisations using these technologies already undertake.

5.2.7. Key Assumptions

The impacts identified from the guidance are contingent on:

- organisations' awareness of the guidance;
- the extent that organisations engage with the guidance; and
- changes that are made to organisational practices as a result of engaging with the guidance.

While we are unable to quantify the impacts of these uncertainties, Table 3 provides an indication of the sensitivity of key impacts to these unknowns.

Table 3: Sensitivity of key impacts to identified risks

Impacts	Sensitivity
1. Increased regulatory certainty for organisations	High
2. Increased public trust and confidence in biometric recognition	Medium
3. Reduced potential for DP harms	Medium
4. Familiarisation costs	High

Source: ICO analysis.

5.2.8. Overall Assessment

As summarised in Table 4 below, our analysis has identified a number of impacts of the guidance including the reduced potential for DP harms. The guidance is expected to increase regulatory certainty for developers, vendors and users of

[50] Refers to characteristics protected by the Equality Act 2010. These include: age, disability, gender reassignment, marriage or civil partnership (in employment only), pregnancy and maternity, race, religion or belief, sex and sexual orientation.

biometric recognition and result in these technologies being used on a proportionate basis. Although there will be costs to organisations from reading, understanding and implementing the guidance, this is expected to be outweighed by the wider societal benefits of reduced DP harms. On balance we expect the guidance to have a net positive impact.

Table 4, below, presents a summary of the main impacts we expect to see from the guidance.

Table 4: Overall impacts of biometric recognition guidance

Impacts		**Attribution to the ICO**	**Direct or Indirect**
Benefits	Improved regulatory certainty for developers, vendors and users of biometric recognition	Attributable	Direct
	Increased public trust and confidence in biometric recognition	Partly Attributable	Indirect
	Increased willingness to engage with biometric recognition	Partly Attributable	Indirect
Costs	Familiarisation costs from reading and understanding guidance	Attributable	Direct
	Costs of deploying alternatives to biometric recognition for non-complaint use cases	Attributable	Direct

Source: ICO analysis.

6. Monitoring and evaluation

An appropriate and proportionate review structure will be put in place. This will follow best practice and align with our organisational reporting and measurement against ICO25 objectives.

Annex A: Familiarisation costs

This annex sets out the approach taken to estimate familiarisation costs for the guidance, which follows an approach drawn from previous impact assessments.[51, 52]

As discussed in Section 4.4, there is not enough available evidence to produce a robust estimate of the number of organisations that would be expected to familiarise themselves with the guidance. We have instead provided an estimate of familiarisation cost per organisation to give some indication of the costs that organisations may incur.

For the purposes of the assessment we assume each organisation will read the guidance in its entirety ten times. This reflects views shared by organisations at the consultation stage. This is not a recommendation on how organisations or individuals should familiarise themselves with guidance, as this will differ on a case-by-case basis.

A.1. Familiarisation costs per organisation

Drawing on impact assessment guidance,[53] we have estimated the total time for reading the guidance at 3 hours and 49 minutes. This is based on a word count of around 17,000 words and a Fleisch reading ease score of 35.

[51] ICO (2021) Data sharing code of practice – Impact assessment. Available at: https://ico.org.uk/media/2619796/ds-code-impact-assessment-202105.pdf (accessed 19 January 2024).

[52] ICO (2020) Age appropriate design: a code of practice for online services – Impact assessment. Available at: https://ico.org.uk/media/2617988/aadc-impact-assessment-v1_3.pdf (accessed 19 January 2024).

[53] BEIS (2019), Business Impact Target: Appraisal of guidance: assessments for regulator-issued guidance. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/609201/b usiness-impact-target-guidance-appraisal.pdf (accessed 19 January 2024).

Table 5: Estimate of the average time taken to read the guidance

Document	Word Count	Fleisch reading ease score	Assumed words per minute	Estimated reading time (hr:mn)
Guidance	17,169	35.0	75	3h49

Source: ICO analysis, BEIS (2019).[54]

The impact of familiarisation on organisations can be monetised using data on wages from the ONS Annual Survey of Hours and Earnings.[55]

Making the conservative assumption that the relevant occupational group is 'Managers, Directors and Senior Officials', the 2023 median hourly earnings (excluding overtime) for this group is £24.77.

This hourly cost is uprated for non-wage costs using the latest figures from the Regulatory Policy Committee guidance,[56] resulting in an uplift of 22% and an hourly cost of £30.22.

We therefore assume the cost of reading the guidance once to be approximately £115.

On the basis of evidence presented in the consultation, we assume medium and large organisations will read the guidance ten times resulting in a cost of £1,152. For small organisations we have assumed the guidance will be read once, resulting in a cost to the organisation of £115.

[54] BEIS (2019) *Business Impact Target Statutory Guidance*. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/776507/B usines__Impact_Target_Statutory__Guidance_January_2019.pdf (accessed 19 January 2024).

[55] ONS (2023) *Annual Survey of Hours and Earnings*. Available at: https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/earningsandworkinghours/datasets/ashe1997to2015selectedestimates (accessed 19 January 2024).

[56] RPC (2019) *RPC guidance note on 'implementation costs'*. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/827926/RPC_short_guidance_note_-_Implementation_costs__August_2019.pdf (accessed 19 January 2024).