Information Commissioner's Opinion:

The use of live facial recognition technology in public places

18 June 2021

ico.
Information Commissioner's Office

Contents

1. Executive Summary

Facial recognition technology (FRT) relies on the use of people's personal data and biometric data. Data protection law therefore applies to any organisation using it. Live facial recognition (LFR) is a type of FRT that often involves the automatic collection of biometric data. This means it has greater potential to be used in a privacy-intrusive way.

The Commissioner previously published an Opinion on the use of LFR in a law enforcement context. It concluded that data protection law sets high standards for the use of LFR to be lawful when used in public places. The Information Commissioner's Office (ICO) has built on this work by assessing and investigating the use of LFR outside of law enforcement. This has covered controllers who are using the technology for a wider range of purposes and in many different settings.

This work has informed the ICO's view on how LFR is typically used today, the interests and objectives of controllers, the issues raised by the public and wider society, and the key data protection considerations. The Commissioner has published this Opinion to explain how data protection law applies to this complex and novel type of data processing.

1.1 What is facial recognition technology?

Facial recognition is the process by which a person can be identified or otherwise recognised from a digital facial image. Cameras are used to capture these images and FRT software produces a biometric template. Often, the system will then estimate the degree of similarity between two facial templates to identify a match (eg to verify someone's identity), or to place a template in a particular category (eg age group). FRT can be used in a variety of contexts from unlocking our mobile phones, to setting up a bank account online, or passing through passport control. It can help make aspects of our lives easier, more efficient and more secure.

1.2 What is live facial recognition?

The uses of FRT referenced above typically involve a "one-to-one" process. The individual participates directly and is aware of why and how their data is being used. LFR is different and is typically deployed in a similar way to traditional CCTV. It is directed towards everyone in a particular area rather than specific individuals. It has the ability to capture the biometric data of all individuals passing within range of the camera automatically and indiscriminately. Their data is collected in real-time and potentially on a mass scale. There is often a lack of awareness, choice or control for the individual in this process.

1.3 Why is biometric data particularly sensitive?

Biometric data is data that allows individuals to be recognised based on their biological or behavioural characteristics, such as data extracted from fingerprints, irises or facial features.[1] It is more permanent and less alterable than other personal data; it cannot be changed easily. Biometric data extracted from a facial image can be used to uniquely identify an individual in a range of different contexts. It can also be used to estimate or infer other characteristics, such as their age, sex, gender or ethnicity. The UK courts have concluded that "like fingerprints and DNA [a facial biometric template] is information of an "intrinsically private" character."[2] LFR can collect this data without any direct engagement with the individual.

With any new technology, building public trust and confidence is essential to ensuring that its benefits can be realised. Given that LFR relies on the use of sensitive personal data, the public must have confidence that its use is lawful, fair, transparent and meets the other standards set out in data protection legislation.

1.4 How is LFR used?

The ICO has assessed or investigated 14 examples of LFR deployments and proposals (as summarised in this Opinion), as well as conducting wider research and engagement in the UK and internationally.

Controllers often use LFR for surveillance purposes, aiming to prevent crime or other unwanted behaviours in physical retail, leisure and transport settings or other public places. LFR can identify particular individuals entering the premises and allow the controller to take action (eg removing them). The ICO has also seen an increasing appetite to use LFR for marketing, targeted advertising and other commercial purposes. This can involve using an individual's biometric data to place them in a particular category.

In the longer term, the technology has the potential to be used for more advanced practices. This could include integration with big-data ecosystems which combine large datasets from multiple sources such as social media. We are investigating some examples of FRT systems where images captured from online sources are being used to identify individuals in other contexts.

Based on these examples, this Opinion focuses on the use of LFR for the purposes of identification and categorisation. It does not address verification or other "one-to-one" uses. It defines public places as any physical space outside a domestic setting, whether publicly or privately owned. But it acknowledges that

[1] The full legal definition of biometric data is contained in UK GDPR Article 4(14) and is discussed in section 4.1 of this Opinion.
[2] *R (Bridges) v Chief Constable of South Wales Police and Others [2019]* EWHC 2341, paragraph 59

the nature and context of such places may be very different, as will the public's expectations of privacy in different settings. This Opinion does not address the online environment.

1.5 What are the key data protection issues involved in LFR?

The Commissioner has identified a number of key data protection issues which can arise where LFR is used for the automatic collection of biometric data in public places. These have been identified through the ICO's investigations, our work reviewing data protection impact assessments (DPIAs) and wider research. These issues include:

- the governance of LFR systems, including why and how they are used;
- the automatic collection of biometric data at speed and scale without clear justification, including of the necessity and proportionality of the processing;
- a lack of choice and control for individuals;
- transparency and data subjects' rights;
- the effectiveness and the statistical accuracy of LFR systems;
- the potential for bias and discrimination;
- the governance of watchlists and escalation processes;
- the processing of children's and vulnerable adults' data; and
- the potential for wider, unanticipated impacts for individuals and their communities.

Other parties, including international organisations and civil society groups, have raised further issues about LFR, including ethical, equalities and human rights concerns. This Opinion sets out where such issues may be relevant to data protection analysis, for example, where bias in facial recognition algorithms could lead to unfair treatment of individuals.

It is not the role of the Commissioner to endorse or ban particular technologies. Rather, it is her role to explain how the existing legal framework applies to the processing of personal data, to promote awareness of the risks and safeguards, and to monitor and enforce the law.

1.6 What are the requirements of the law?

LFR involves the processing of personal data, biometric data and, in the vast majority of cases seen by the ICO, special category personal data. While the use of LFR for law enforcement is covered by Part 3 of the Data Protection Act 2018 (DPA 2018), outside of this context the relevant legislation is the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).

Controllers seeking to deploy LFR must comply with all relevant parts of the UK GDPR and DPA 2018. This includes the data protection principles set out in UK GDPR Article 5, including lawfulness, fairness, transparency, purpose limitation, data minimisation, storage limitation, security and accountability. Controllers must also enable individuals to exercise their rights. These requirements of UK law represent universal core principles of data protection common to many legal regimes worldwide.

While all relevant elements of the legislation apply, based on the ICO's experience the central legal principles to consider before deploying LFR are lawfulness, fairness and transparency, including a robust evaluation of necessity and proportionality. This evaluation is particularly important because LFR involves the automatic collection of biometric data, potentially on a mass scale and without individuals' choice or control.

For their use of LFR to be lawful, controllers must identify a lawful basis and a condition to process special category data and criminal offence data where required. They must ensure that their processing is necessary and proportionate to their objectives, in line with the development of these concepts in UK case law. Any processing of personal data must also be fair. This means that controllers should consider the potential adverse impacts of using LFR for individuals and ensure they are justified. They should also consider and take steps to mitigate any potential biases in their systems and ensure it is sufficiently statistically accurate. Controllers must be transparent and take a "data protection by design and default" approach from the outset so that their system complies with the data protection principles.

Controllers are accountable for their compliance with the law and must demonstrate that their processing meets its requirements. Before deciding to use LFR in public places, they should complete a DPIA. As part of this process, they must assess the risks and potential impacts on the interests, rights and freedoms of individuals. This includes any direct or indirect impact on their data protection rights and wider human rights such as freedom of expression, association and assembly.

Overall, controllers should carefully evaluate their plans with a rigorous level of scrutiny. The law requires them to demonstrate that their processing can be justified as fair, necessary and proportionate.

Together, these requirements mean that where LFR is used for the automatic, indiscriminate collection of biometric data in public places, there is a high bar for its use to be lawful. While this is the Commissioner's general assessment of what the legislation requires in this context, she emphasises that any investigation or regulatory assessment would be based on the facts of the case, considering the specific circumstances and relevant laws.

1.7 Next steps

The Commissioner will continue her investigative and advisory work. This includes completing investigations already underway, assessing DPIAs which identify high-risk processing, conducting a proactive audit of LFR systems in deployment, and, where appropriate, support data protection Codes of Conduct or certification schemes. Further next steps for the ICO and for controllers are detailed in the conclusion to this Opinion, alongside recommendations for technology vendors and the wider industry.

In considering any regulatory action or use of her enforcement powers, the Commissioner may refer to this Opinion as a guide to how she interprets and applies the law. Each case will be fully assessed on the basis of its facts and relevant laws. The Commissioner may update or revise this Opinion based on any material legal or practical developments in this evolving area, such as judicial decisions and case law, or further findings from her regulatory work and practical experience.

2. Introduction

Shaping proportionate surveillance is one of the Commissioner's regulatory priorities in protecting personal data and upholding information rights in the UK. Where new technology, including surveillance technology, relies on the use of personal data, data protection has an important role to play in building trust and confidence and protecting the public from misuse. LFR is a technology that involves the processing of personal data and biometric data, which the law recognises can be particularly sensitive. When deployed in certain ways LFR has the potential to be highly privacy intrusive. As such, the Commissioner has published this Opinion to explain how data protection law applies and the robust assessments that organisations need to make before any deployment.

2.1 Live facial recognition in public places

Facial recognition is the process by which a person can be identified or otherwise recognised from a digital facial image. Cameras are used to capture these images and FRT software measures and analyses facial features to produce a biometric template. This typically enables the user to identify, authenticate or verify, or categorise individuals.

Live facial recognition is a type of FRT which allows this process to take place automatically and in real-time. LFR is typically deployed in a similar way to traditional CCTV in that it is directed towards everyone in a particular area rather than specific individuals. It can capture the biometric data of all individuals passing within range of the camera indiscriminately, as opposed to more targeted "one-to-one" data processing. This can involve the collection of biometric data on a mass scale and there is often a lack of awareness, choice or control for the individual in this process. LFR can be used for a variety of purposes such as identifying individuals on a watchlist (see below) or commercial purposes.

2.2 The importance of biometric data

Biometric data in the form of a facial template is data of an "intrinsically private character", due to the potential to identify an individual precisely and uniquely. In *R (Bridges) v The Chief Constable of South Wales Police*, the Court of Appeal judgment noted that: "Biometric data enables the unique identification of individuals with some accuracy. It is this which distinguishes it from many other forms of data."[3] It is more permanent and less alterable than other personal data; it cannot be changed easily.

[3] *R (Bridges) v The Chief Constable of South Wales Police – Court of Appeal – [2020]* EWCA Civ 1058, paragraph 22

As such, the processing of biometric data can have a particular impact on individuals' privacy. Where LFR is used, biometric data extracted from a facial image can be used to uniquely identify an individual in a range of different contexts. It can also be used to estimate or infer other characteristics about them, such as their age, sex, gender or ethnicity. These processes can take place at significant speed and scale and can allow the controller to make a range of decisions or interventions.

Despite the sensitivity of facial biometric data, it can be collected with relative ease using LFR. Unlike a fingerprint or DNA sample, the collection process is not physically intrusive. In the Bridges case, the Court of Appeal judgment noted that "A significant difference [to fingerprints…] is that AFR [automatic facial recognition] technology enables facial biometrics to be procured without requiring the co-operation or knowledge of the subject or the use of force, and can be obtained on a mass scale."[4] Collection can take place automatically, simply because the individual comes within range of a camera.

2.3 The Commissioner's work on LFR

In 2019, the Commissioner published an Opinion on the use of LFR by law enforcement agencies. This followed the ICO's investigations into the use of LFR by South Wales Police and the Metropolitan Police Service. It concluded that Part 3 of the DPA 2018 sets a high threshold for the use of LFR to be lawful. Among other recommendations, the Commissioner called for a statutory code of practice to govern the use of LFR by police forces. Subsequently, in the Bridges judgment, the Court of Appeal also concluded that there was a need for a clearer and more specific legal framework to govern the use of LFR by the police. The Home Office and College of Policing are currently working to update the relevant guidance to reflect these developments.

The use of LFR outside of law enforcement is governed by different parts of the data protection legal framework, namely the UK GDPR and Part 2 of the DPA 2018. It is within this framework that the ICO has continued to monitor, assess and investigate emerging uses to inform our approach.

At the time of publishing this Opinion, the ICO has completed investigations of six examples of planned or actual use of LFR in public places. Some represented plans or proposals which did not progress to live processing; others involved multiple parties and multiple deployments. In some cases, the processing took place under the previous legal framework (Data Protection Act 1998).

Overall, while some of the organisations investigated had well-developed processes, others were at a relatively immature stage in their use of the technology and the associated compliance considerations. Our investigations

[4] Ibid, paragraph 23

found that controllers often gave insufficient consideration to the necessity, proportionality and fairness of the use of LFR systems and failed to be sufficiently transparent. We also found that controllers did not always do enough to demonstrate a fair balance between their own purposes and the interests, rights and freedoms of the public. These organisations have all ceased their processing of personal data using LFR. Where relevant, they have provided assurances that they have deleted all biometric data collected. As such, we have provided regulatory advice and closed these six cases with no further action. A number of further investigations into LFR are ongoing and we are yet to reach conclusions.

Alongside the six completed investigations, the ICO has also assessed nine DPIAs received from industry about the use or potential use of LFR in public places (one of which related to a completed investigation). Together these 14 examples have informed the ICO's understanding of how controllers are seeking to use LFR in public places and the key data protection compliance issues that commonly arise.

Users of LFR often purchase the technology from third party suppliers and there is significant innovation and growth in the market. This can, at times, risk creating an accountability gap where controllers rely on vendors' products and may not understand the detail of how the system operates or fully appreciate their legal obligations.

The ICO has also drawn lessons from other investigations, DPIAs and wider industry engagement about other types of FRT deployments which do not constitute LFR. In addition, the ICO's Regulatory Sandbox has collaborated closely with several organisations focused on innovation and privacy in FRT.[5] This work has helped to improve the ICO's understanding of the wider FRT environment and innovative use of biometric data.

Alongside the lessons from the ICO's practical experience as regulator, a key element in the preparation of this Opinion has been detailed legal and policy analysis. This Opinion has been informed by analysis of both the legislation and relevant case law, notably the Bridges case, but also case law including in the wider areas of privacy and human rights. In addition, we have had regard to international developments, including investigations and cases examined by similar regulators overseas and the development of the legal and policy frameworks in other jurisdictions.

Based on her assessment of the FRT environment today, the Commissioner is using this Opinion to set out how UK data protection law applies to the use of

[5] The ICO publishes a blog about its Regulatory Sandbox and in 2020 published reports on its work with Onfido, which is working to identify and mitigate bias present in biometric identity verification technology, and Heathrow Airport, which was seeking to use FRT to increase the speed, efficiency and security of passengers' journeys through airport's terminals.

LFR in public places and to emphasise that data protection by design and default principles must be at the heart of any advances.

2.4 Scope of this Opinion

Article 58(3)(b) of the UK GDPR and Section 115(3)(b) of the DPA 2018 allow the Information Commissioner to issue, on her own initiative or on request, opinions to Parliament, government, other institutions or bodies, and the public, on any issue related to the protection of personal data.

This Opinion focuses on how the UK GDPR and Part 2 of the DPA 2018 apply to the use of LFR in public places. This legislation applies to any organisation using LFR except competent authorities processing for law enforcement purposes, the intelligence services, or their processors. This processing is covered by Parts 3 and 4 of the DPA 2018. If controllers are unsure if they are processing under Part 2 or Part 3 of the DPA 2018, they can consult existing guidance on which regime applies.

The Opinion is primarily intended for Data Protection Officers and other privacy and data protection practitioners, as well as those responsible for designing, supplying and using LFR services. It may also be relevant for anyone with an interest in the development and regulation of LFR in public spaces, including government, regulators, public bodies, industry groups, technology developers and civil society groups.

What uses of LFR are within scope of this Opinion?

- This Opinion addresses the use of live facial recognition in public places. It does not address other types of FRT. Generally, it focuses on the use of LFR directed towards whole spaces (as opposed to specific individuals) and where there is automatic collection of biometric data.
- It addresses the processing of personal data, biometric data and special category data using LFR systems, which engages the UK GDPR and DPA 2018 Part 2. It does not address competent authorities (or their processors) processing for law enforcement under Part 3 of the DPA 2018.
- Public places generally include any physical space outside a domestic setting, whether publicly or privately owned. This includes anywhere providing open access to the public, such as public squares, public buildings, transport interchanges or parks. It also includes privately-owned premises such as shops, offices and leisure venues. However, the Opinion acknowledges that the nature and context of such places may be very different, as will the public's expectations of privacy in different settings. This Opinion does not address the online environment.
- It focuses on the use of LFR for the purposes of identification and categorisation, eg the use of LFR as a surveillance tool or for certain types of marketing and advertising.

- It does not address the use of LFR for verification, authentication or other "one-to-one" matching uses, eg the use of facial recognition for access control, unlocking IT devices, or digital identity checks with prior enrolment (eg where people can decide whether to share their image and provide their consent).
- LFR systems used for identification are often used in combination with a watchlist. A watchlist is a bespoke gallery of images of individuals of interest, compiled according to certain criteria, who the controller typically wishes to identify either by manual or automated means. This Opinion addresses the use of watchlists in combination with an LFR system, but does not provide comprehensive guidance on watchlists, which must also comply with data protection law in their own right. See further guidance on watchlists at section 4.9.1.

This Opinion does not focus on the use of LFR by law enforcement agencies. However, the ICO is mindful of the potential for collaboration between police and private or public sector controllers using LFR for surveillance. Where such collaboration takes place, the relationship and responsibilities must be clear. The parties must assess whether they are acting as separate controllers, or if the LFR operator is acting as a processor for the police. If a law enforcement agency is the controller for the LFR system and the processing is for a law enforcement purpose, they and their processors must meet the requirements under Part 3 of the DPA 2018. They should refer to the Commissioner's Opinion on the use of LFR in law enforcement. See more information in section 4.9.2.

In considering any regulatory action or use of her enforcement powers, the Commissioner may refer to this Opinion as a guide to how she interprets and applies the law. Each case will be fully assessed on the basis of its facts and the relevant laws, and the Commissioner will exercise her powers in line with her Regulatory Action Policy.

The Commissioner may update or revise this Opinion based on any material legal or practical developments in this evolving area, such as judicial decisions and case law, or further findings from her regulatory work and practical experience. She may add to this Opinion to address specific LFR use cases or other applications of FRT.

3. How LFR is used today

3.1 ICO analysis and key issues

3.1.1 Surveillance uses

The Commissioner's previous Opinion on the use of LFR in law enforcement described how police forces deploy LFR for surveillance purposes. Forces draw up a watchlist of individuals of interest according to certain criteria and extract a biometric template from a digital photo of their face. These biometric templates are then compared to people passing facial recognition cameras. If a match is found, an alert is generated by the system, and police officers can decide whether to intervene and apprehend the individual. Surveillance uses can generally be classed as LFR for identification.

The ICO has seen similar techniques deployed outside of law enforcement. Of the 14 examples we have examined in detail, 11 have involved some form of surveillance. Our key lessons include:

- **Setting:** The settings where LFR was used or planned include retail environments (including large, multi-site premises), open public spaces, public transport hubs, museums, conference centres and other leisure settings.
- **Processing:** In most cases, the controllers' plans involved directing LFR systems towards public areas, the blanket collection of digital facial images, and the processing of biometric data. In many cases, LFR systems were directed towards locations of high footfall such as the entrances and exits of premises. Where processing took place, most controllers deleted any 'unmatched' biometric templates within a short space of time. However, collectively the biometric data of significant numbers of people – potentially millions – is likely to have been processed during those deployments which proceeded to live processing.
- **Purposes:** All planned or actual deployments involved the use of LFR for identification. The controllers' various purposes included preventing and detecting crime, protecting the public, protecting property, identify persons of interest (eg missing persons), enforcing specific local policies (eg codes of conduct for premises), and seeking operational efficiencies for the controller.
- **Watchlists:** In most of the cases, the controller created or planned to create watchlists according to their own criteria. Some LFR systems are capable of sharing or pooling watchlists between different organisations. This means that an individual under suspicion from one company can

generate match alerts when they enter the premises of other companies using the same service.

- **Police involvement:** In some instances, watchlists involved input from law enforcement agencies, who shared images with the controller. In one case, images were provided by a local law enforcement agency to assist in locating both missing persons and persons of interest who were publicly 'wanted' for a suspected offence. Over fifty such images were provided by the law enforcement agency for this purpose.
- **Proposals, pilots and trials:** Some of the examples examined by the ICO constituted proposals only, and the controller decided not to proceed to live processing. A number of the controllers ran short-term trials or pilot deployments involving limited matching of biometric templates. However, other controllers' deployments lasted many months or even years. Any deployment which involved the processing of personal data engaged data protection law, regardless of whether it was described as a trial or pilot.

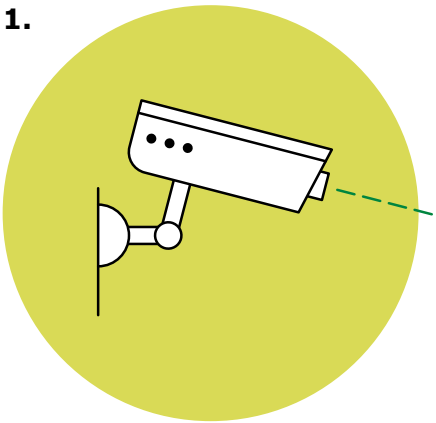
When an LFR system identifies an individual, an alert is generated for the controller. The controller will then respond according to their objectives and policies, and their intentions may include:

- controlling access to a particular set of premises or location;
- enabling further monitoring, tracking and surveillance of particular individuals;
- evicting individuals considered to be in breach of the rules of the premises or location;
- apprehending people suspected of criminal activity;
- potentially notifying law enforcement authorities; or
- taking action to identify or support individuals who may be vulnerable or at risk.

This is not an exhaustive list of possible interventions and the Commissioner notes that controllers may continue to develop new ways to use LFR for surveillance.

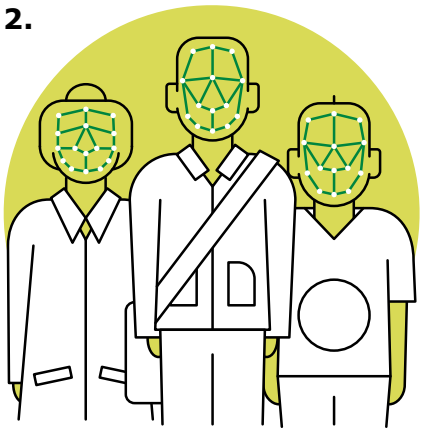
Use of LFR for surveillance

1.



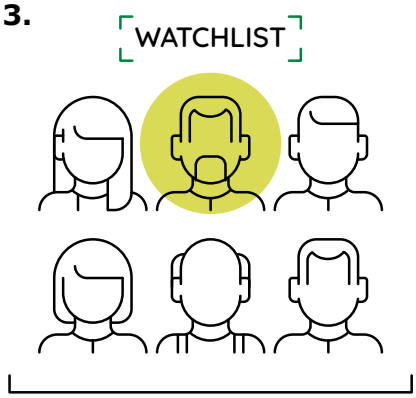
LFR is deployed in public spaces such as shopping centres, streets and convenience stores.

2.



Live video camera scans all faces and compares them with a watchlist of individuals of interest.

3.

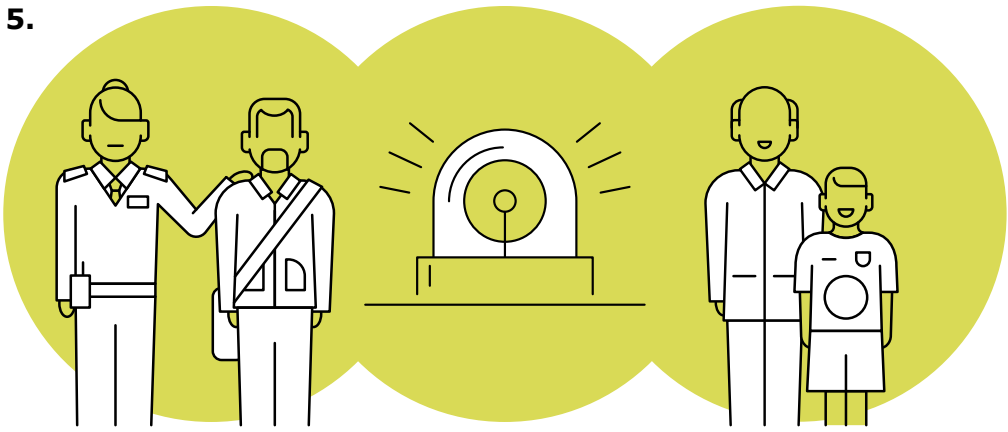


Where there is a match, the LFR system generates a 'match alert' for the organisation using the system to review.

4.

The organisation reviews the information and confirms whether or not there is a match.

5.



If there is a confirmed match, the organisation can decide on what action to take. Examples of action could include removing an individual from the premises, referring an individual to the police or protecting people at risk.

3.1.2 Marketing and advertising uses

LFR can also be deployed for marketing, advertising and other commercial purposes. The ICO has reviewed one DPIA about LFR for advertising purposes and is aware of a range of other proposals within industry and wider international consideration of such use cases. Marketing uses may be classed as LFR for categorisation or identification, or both, depending on the specific processing.

Controllers can seek to use LFR to gain marketing insights or to deliver advertising products. The ICO is aware of proposals in the digital-out-of-home advertising sector in particular. Billboards can be fitted with facial recognition cameras, enabling the controller to process biometric data for a range of purposes. This could include processing to:

- estimate footfall for advertising space (audience measurement);
- measure engagement with advertising space (dwell time at a particular location or other attention measurement);
- provide interactive experiences (eg turning on media or inviting customers to respond to it); or
- serve targeted adverts to passing individuals (demographic analytics).

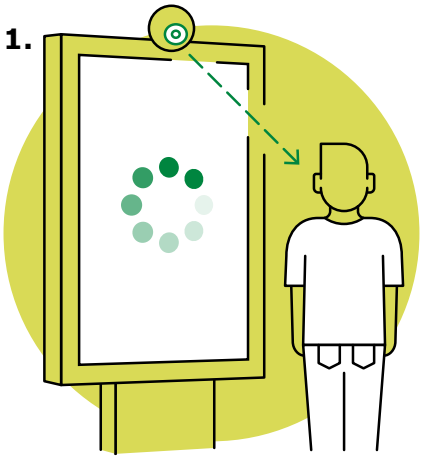
While the specific processing involved depends on the product or service in question, typically an LFR-enabled billboard can detect an "engaged" passer-by, capture an image of their face, and create a biometric template. In some examples, this can allow the individual to be categorised by estimating demographic characteristics based on their facial image. These estimated characteristics can include age, sex, gender, ethnicity, race, and even clothing styles or brands, as well as other observed data (such as dwell time). Some controllers may wish to capture this information solely for analytical purposes. However, the technology can be capable of estimating personal characteristics and attributes in real-time and displaying adverts or other content based on that information.

The European Data Protection Board has also highlighted the potential for LFR-enabled billboards or advertising systems to 'remember' customers by capturing and storing their biometric data.[6] The customer could be uniquely identified at other locations or on a return visit and served with targeted advertising. This would constitute the use of LFR for identification purposes and could also involve categorisation of individuals to allow the user to serve more targeted advertising.

[6] *Guidelines 3/2019 on processing of personal data through video devices*, European Data Protection Board, adopted 29 January 2020, paragraph 82

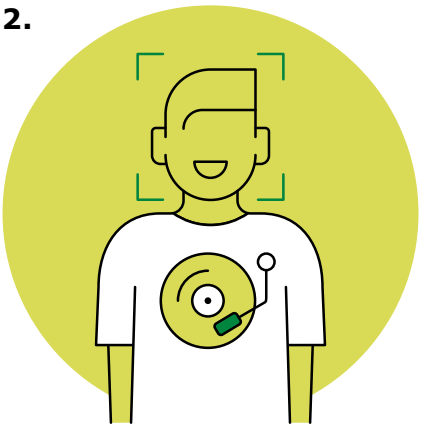
LFR for marketing and advertising

1.



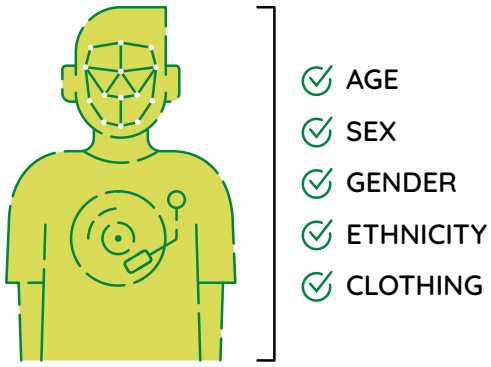
LFR systems can be used in combination with advertising billboards located in public spaces such as shopping centres or city centre streets.

2.



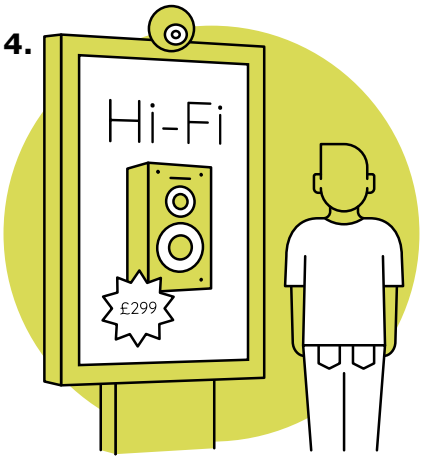
LFR-enabled billboard detects a person engaging with it or passing by and scans their features.

3.



LFR system analyses features such as age, sex, gender, ethnicity, and even clothing styles or brands to create a profile or categorise the individual.

4.



Billboard displays real-time adverts based on that profile or the data is used for other marketing purposes.

3.1.3 Other uses of LFR

The Commissioner is mindful that LFR technology could be deployed for a wider range of uses in a variety of sectors and it is not possible to anticipate all eventualities. The analysis set out in this Opinion draws on surveillance and marketing uses in particular, but the underlying legislation is the same across all uses outside law enforcement. This Opinion will therefore be a useful guide for other potential applications of LFR. Controllers should carefully assess the specific circumstances of their processing.

For example, technology developers are exploring how FRT and potentially LFR could be used for purposes such as age estimation (eg at point of sale or on entry to age-restricted premises). We have also received DPIAs from industry which assess the use of LFR for queue time monitoring and management in airports, and for photo matching at leisure attractions to allow customers to purchase their photos through an app. Such applications of FRT may involve the use of LFR for identification or categorisation, for which this Opinion sets out the key legal requirements.

As technology develops further, there is also potential that LFR systems could be used as part of big data ecosystems, which allow multiple datasets to be analysed concurrently and in real-time. For example, cloud computing capabilities could enable facial images captured by LFR systems to be cross-referenced with images from social media or immigration data. LFR could be deployed alongside artificial intelligence and machine-learning techniques, such as text extraction, object recognition, and sentiment analysis.[7] While this Opinion does not directly address this more advanced processing, the underlying requirements of data protection law remain the same.

3.1.4 Key data protection issues

Based on the ICO's investigations, our work reviewing DPIAs and wider research, the Commissioner has identified a number of key data protection issues. These can arise where LFR is used for the automatic and indiscriminate collection of biometric data in public places. They include, but are not limited to, the following:

- The automatic collection of biometric data at speed and scale without clear justification

In many of the examples examined by the ICO, the controller had not clearly made out its justification that the automatic, indiscriminate processing of biometric data was necessary and proportionate. There were no strong examples

[7] See the Biometrics and Forensics Ethics Group briefing on *Public-private use of live facial recognition technology: ethical issues,* January 2021, and the ICO's paper on *Big data, artificial intelligence, machine learning and data protection.*

of a data protection by design and default approach being taken. In the DPIAs we reviewed, there has been little consideration of the effectiveness of the LFR in achieving the controller's objective against the potential impacts for data subjects.

- The lack of control for individuals and communities

In most of the examples we observed, LFR deployed in public places has involved collecting the public's biometric data without those individuals' choice or control. This is not to say that such processing must be based on consent, but controllers need to justify the processing of biometric data without the direct engagement of the individual. Controllers must account for this lack of involvement and ensure the processing is fair, necessary, proportionate and transparent.

- A lack of transparency

Transparency has been a central issue in all the ICO investigations into the use of LFR in public places. In many cases, transparency measures have been insufficient in terms of the signage displayed, the communications to the public, and the information available in privacy notices. It may not always have been clear to data subjects when and where LFR is being used, how and why their data is being processed, and how they can exercise their rights. In some cases, transparency information was not provided at all.

A lack of transparency can also affect individuals' ability to exercise their data protection rights, such as the right of access, erasure and the right to object.

- The technical effectiveness and statistical accuracy of LFR systems

In our guidance on AI and data protection, the ICO identified some specific data protection risks which can be raised by AI systems such as LFR. These include statistical accuracy. If LFR systems are not sufficiently statistically accurate they may result in "false positives" or "false negatives". False results may have insignificant consequences in some cases. In others, they could lead to interventions such as additional surveillance, removal from the premises, or even being referred to and potentially detained by law enforcement authorities. High levels of false results would call into question whether the LFR system is necessary or fair.

In our work reviewing DPIAs, we have seen a lack of due diligence by controllers in respect of the technology they purchase from manufacturers. Some have carried out limited scrutiny of the technical effectiveness of the systems they are seeking to implement. In some cases, controllers have done too little to scrutinise vendors' statements on the accuracy of their systems, presenting accuracy rates without clear understanding of their provenance or suitability to the controller's proposed use case. The ICO has advised controllers to make further assessment of the technology they propose to use and on what

safeguards they will need to put in place to ensure their processing is compliant with data protection law.

- The potential for bias and discrimination

The potential for bias in complex AI systems is another risk highlighted in the ICO's guidance on AI and data protection.[8] Several technical studies have indicated that LFR works with less precision for some demographic groups, including women, minority ethnic groups and potentially disabled people.[9] Error rates in FRT can vary depending on demographic characteristics such as age, sex, race and ethnicity. These issues often arise from design flaws or deficiencies in training data and could lead to bias or discriminatory outcomes. Equally, there is a risk of bias and discrimination in the process of compiling watchlists (often manual) which underpin an LFR system. All these issues risk infringing the fairness principle within data protection law, as well as raising ethical concerns.

- The governance of watchlists

In the examples we have reviewed, it is not clear that watchlists were always compiled and maintained in a lawful, fair and transparent way. Data subjects must also be able to exercise their rights in relation to watchlists. These include the right to be informed, to rectification, to erasure and to object. These rights also apply to any watchlist data shared with other parties and any other LFR records held by controllers. We have concerns about the necessity and proportionality of some sharing of watchlist data between organisations. Any use of exemptions with the UK GDPR and DPA 2018 (eg from data subjects' right to be informed) need to be clearly justified.

- The governance of LFR escalation processes

We have seen varied examples of the escalation processes following an LFR match (ie what happens after someone is identified). Some organisations had defined processes, including verification of the individual's identity. Others lacked clarity on what should happen after a match. Without clear and well-governed escalation processes which fulfil the controller's purpose, LFR systems may be difficult to justify.

---

[8] See 'How should we address risks of bias and discrimination?' from the ICO's guidance on AI and data protection.

[9] See for example research from Buolamwini and Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, PMLR (2018), and studies from the U.S. Department of Commerce National Institute of Standards and Technology, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects* (December 2019) and *Ongoing Face Recognition Vendor Test (FRVT) Part 1: Verification* (August 2017). Concerns have been raised about potential discrimination towards disabled people and the need for further research to better understand the impact of LFR in, for example, the European Union Agency for Fundamental Rights paper, *Facial recognition technology: fundamental rights considerations in the context of law enforcement* (November 2019) and *Disability, Bias, and AI*, AI Now Institute NYU (November 2019).

- The processing of children's and vulnerable adults' data

In many of the examples we observed, LFR was deployed towards locations likely to be accessed by children and vulnerable adults, such as retail or public transport settings. Data protection law provides additional protections for children and adults who may be less able to understand the processing and exercise their data protection rights. This means, for example, that controllers need to pay close consideration to transparency and the necessity and proportionality of the processing. This is particularly the case when children and vulnerable adults make a significant group covered by the system.

3.2 International examples

International interest in FRT has grown significantly in recent years. Following the UK's departure from the European Union, it remains informative to consider the approach of EU regulators applying the GDPR, as well as that of non-EU countries who are also engaging with similar examples of LFR as those seen in the UK.

There are a number of examples of regulators overseas taking regulatory action against controllers using LFR. For example:

- In 2019, data protection authorities (DPAs) in France and Sweden took action against controllers using facial recognition in schools. The Swedish regulator issued a monetary penalty under the GDPR to a local authority which instructed schools to use facial recognition to track pupil attendance.[10] The school had sought to base the processing on consent. However, the Swedish DPA considered that consent was not a valid legal basis given the imbalance between the data subject and the controller. The French regulator raised concerns about a facial recognition trial commissioned by the Provence-Alpes-Côte d'Azur Regional Council, and which took place in two schools to control access by pupils and visitors. The regulator's concerns were subsequently supported by a regional court in 2020. It concluded that free and informed consent of students had not been obtained and the controller had failed to demonstrate that its objectives could not have been achieved by other, less intrusive means.[11]
- In 2020, the Dutch DPA issued a formal warning to a supermarket which had sought to use LFR to protect staff and customers and prevent shoplifting. LFR was used to scan the face of everyone who entered the store and compared these images to a database of people who had been

[10] See articles including Facial recognition: School ID checks lead to GDPR fine (BBC News, August 2019) and Facial recognition in school renders Sweden's first GDPR fine (European Data Protection Board, August 2019).
[11] See articles including Expérimentation de la reconnaissance faciale dans deux lycées (CNIL, October 2019) and Facial recognition challenged by French administrative court (Hogan Lovells, May 2020).

banned from entering the premises. The DPA stated that the use of LFR for security purposes was prohibited unless certain exceptions applied, which did not in this case.[12]

- In Canada, the Office of the Privacy Commissioner of Canada and the commissioners for Alberta and British Columbia investigated the use of LFR by a shopping mall owner to monitor footfall patterns and estimate demographic information about visitors.[13] In October 2020, the investigation concluded that the LFR processing was not within shoppers' reasonable expectations, that there were inadequacies in the transparency measures, and that the organisation had not obtained valid consent. The commissioners recommended that the organisation either obtain "meaningful express opt-in consent" and allow individuals to use malls without having to agree to their personal data being processed, or cease using the LFR system.

Governments and private organisations are also taking steps to respond to concerns raised about facial recognition used for surveillance. In 2019, San Francisco became the first US city to introduce a ban on LFR by local agencies. Public concerns have led some technology providers to pause, slow or stop offering some of their facial recognition services. In 2020, following the growth of the Black Lives Matter movement, IBM announced in the USA that it would "no longer offer general purpose" facial recognition or analysis software. IBM stated it would not condone the use of FRT "for mass surveillance, racial profiling, violations of basic human rights and freedoms, or any purpose which is not consistent with our values...".[14] Amazon and Microsoft have taken similar action to pause the sale of their facial recognition products to police forces.[15]

The Council of Europe, in its guidelines for legislators and decision-makers published in January 2021, called for strict rules to avoid the significant risks to privacy and data protection posed by the increasing use of FRT. It also recommended that certain applications of FRT should be banned altogether to avoid discrimination. In April 2021, the European Commission published its Proposal for a Regulation laying down harmonised rules on artificial intelligence. This describes the use of real-time remote biometric identification as a high risk

[12] See articles Dutch DPA issues formal warning to supermarket for use of facial recognition technology (Autoriteit Persoonsgegevens, December 2020) and Dutch DPA issues Formal Warning to a Supermarket for its use of Facial Recognition Technology (European Data Protection Board, January 2021).
13 *Joint investigation of The Cadillac Fairview Corporation Ltd by the Information and Privacy Commissioner of Alberta, the Privacy Commissioner of Canada, and the Information and Privacy Commissioner for British Columbia*, October 2020
[14] IBM CEO's Letter to Congress on Racial Justice Reform, 8 June 2020
[15] Amazon's statement on a one-year moratorium on police use of Rekognition, 10 June 2020; article on Microsoft banning the sale of Facial Recognition to police, 12 June 2020

activity and, among other proposals, proposes restrictions on its use for law enforcement.

In October 2020, the Global Privacy Assembly (GPA) adopted a resolution on FRT. This highlighted the significant risks to privacy that FRT can raise and reiterated the importance of strong data protection rules. The Commissioner is working with other GPA members to develop a set of globally agreed principles for the appropriate use of personal data in FRT and promote their application in practice by industry.

3.3 Public perceptions of LFR

In January 2019, the Commissioner instructed research firm Harris Interactive to explore the public's awareness and perceptions about the use of LFR in public spaces. This included a survey of over 2,000 adults aged 18 and above.

This research found strong support for the use of LFR by law enforcement agencies. 82% of respondents indicated that they found it acceptable for the police to deploy the technology. Use by other types of organisations had much weaker support, with entertainment venues, retailers and social media websites gaining the support of 44%, 38% and 30% of respondents respectively.

Analysis also suggested that the public care about the purpose of LFR, as well as who wields the technology. Only 31% of people found the use of FRT on dating websites acceptable. Just 26% thought it was acceptable for retailers to provide offers to customers based on their facial profile.

In July 2019, the Ada Lovelace Institute commissioned YouGov to conduct similar research, including an online survey with over 4,000 responses from adults aged 16 and above.[16] Respondents were asked for their views on a range of proposed, potential or actual uses of facial recognition technologies in a number of settings including law enforcement, education and in the private sector.

The research found that support for the use of FRT (with appropriate safeguards in place) is dependent on the purpose. There was a greater degree of approval for police use of the technology in criminal investigations (63%), than for verifying age for alcohol purchases in a supermarket (17%) or tracking shopper behaviour and targeting products (7%).

46% of respondents felt the public should be able to consent to or opt-out of facial recognition technologies. This figure was higher (56%) for respondents from minority ethnic groups. Of the respondents who answered that they were uncomfortable with the use of FRT in schools and on public transport, 64% and

[16] Ada Lovelace Institute, *Beyond face value: public attitudes to facial recognition technology*, September 2019

61% respectively cited the normalisation of surveillance as the reason for their discomfort.

When asked to consider a scenario involving police use of FRT, of those who agreed to FRT being used, 80% said that this was because they felt it was beneficial for the security of society. The research found support for the government imposing restrictions on the use of FRT by the police (55%) and in schools (68%). The Ada Lovelace Institute recommends a voluntary pause on the sale of FRT to enable public engagement and consultation to take place.

The Ada Lovelace Institute has continued its research into public attitudes towards biometrics and facial recognition through the Citizens' Biometrics Council, which published its final report and policy recommendations in March 2021.

Overall, the results of both surveys indicate that the public has a nuanced view of FRT and LFR that depends on the context in which the technology is used. The public care about who uses FRT and why, what controls are in place, and what the impact for society could be. As FRT develops, there is a strong case for further engagement and consultation, with particular attention to the concerns of minority ethnic groups. The Commissioner recommends that there is further research by industry into public attitudes as the use cases for LFR develop over time.

4. The requirements of data protection law

4.1 Why data protection law applies

Data protection law applies to the processing of personal data. LFR may involve the processing of several different types of personal data as defined by the UK GDPR, depending on the circumstances:

- **Personal data:** All LFR involves the processing of facial images, which constitute personal data as defined in the UK GDPR, even if the controller does not seek to establish the identity of the individual or single them out.[17]
- **Biometric data:** Facial images become biometric data when "specific technical processing" is carried out "which allow or confirm the unique identification" of an individual.[18] The individual does not have to be identified for this data to become biometric data - it is the type of processing that matters.
- **Special category data:** The UK GDPR singles out certain types of personal data as likely to be more sensitive, and gives them greater protection. These are referred to as special category data. Biometric data constitutes special category data whenever it is processed "**for the purpose** of uniquely identifying a natural person".[19] Any biometric data processed for this purpose will constitute special category data, regardless of whether the individual is identified. For example, all biometric facial templates collected and compared to a watchlist will constitute special category data regardless of whether there is a match. As such, biometric data will be special category data in the majority of cases. Controllers must comply with UK GDPR Article 9 when processing special category data. Special category data also includes personal data relating to race and ethnicity, health, and certain other types of demographic information, which could be derived from a facial template.

[17] It should be noted that digital images of faces constitute personal data where they are of sufficient quality to allow an individual to be identified or individuated from another person. UK GDPR Article 4(1) defines personal data as "any information relating to an identified or identifiable natural person…".
[18] UK GDPR Article 4(14) defines biometric data as "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data".
[19] UK GDPR Article 9(1) sets out the types of data which constate special category data, including "biometric data for the purpose of uniquely identifying a natural person".

- **Criminal offence data:** Processing data relating to criminal offences and convictions (including records, allegations and evidence of crime) engages UK GDPR Article 10.[20]

The types of personal data being processed will depend on how LFR is used and for what purpose.

LFR used in public spaces for identification can identify and locate individuals in real-time. The surveillance examples described above in section 3.1 all fall into this category. Using LFR for identification involves processing the personal data, biometric data and special category personal data of all individuals whose images are captured and analysed. It may involve processing criminal offence data. For example, where an individual is suspected of a crime or where local police forces have shared information with the LFR provider or user.

LFR used for categorisation will typically capture facial images, evaluate them, and categorise them based on various attributes. The marketing and advertising examples described above in section 3.1 involve categorisation. Using LFR for categorisation will usually involve processing personal data, biometric data and potentially special category data.

Identification and categorisation can take place regardless of whether the name of the individual or similar identifiers are known to the controller. What matters is whether the purpose of the processing is to identify an individual distinctly from others or to place them in a particular category.

Momentary processing

Controllers are processing personal data, biometric data and potentially special category data every time their LFR system captures a facial image, even when it is processed only momentarily. This is irrespective of whether that image is:

- matched with a person on a watchlist;
- assigned to a category; or
- unmatched and subsequently deleted within a short space of time.

This was the conclusion of the Divisional Court in the Bridges case, which was unchanged by the judgment from the Court of Appeal.[21] While the Bridges case focused on law enforcement use of LFR, this explanation of the processing applies equally to similar LFR processing outside a law enforcement context.

[20] The ICO has published detailed guidance on criminal offence data.
[21] *R (Bridges) v Chief Constable of South Wales Police and Others [2019]* EWHC 2341, paragraph 59; unchanged by the Court of Appeal [2020] EWCA Civ 1058

4.2 Legal requirements in brief

Any organisation considering deploying LFR must ensure that it will comply with data protection law before starting its processing. The legal requirements common to any deployment of LFR in a public place are summarised below.

Legal requirements in brief

Controllers deploying LFR in public places must:

- comply with the data protection principles set out in UK GDPR Article 5, namely:
  - lawfulness, fairness and transparency;
  - purpose limitation;
  - data minimisation;
  - accuracy;
  - storage limitation;
  - integrity and confidentiality (security); and
  - accountability;
- identify a lawful basis and meet its requirements, as required by UK GDPR Article 6;
- identify, where required, appropriate conditions for processing special category data under UK GDPR Article 9 and criminal offence data under Article 10;
- ensure that data subjects are able to exercise their rights, as defined in UK GDPR Articles 12 to 22, including:
  - the right to be informed;
  - the rights of access, rectification and erasure;
  - the rights to restrict processing and to object; and
  - rights in relation to automated decision making and profiling;
- ensure clarity of controller, joint controller and processor roles and responsibilities where necessary, as required by the UK GDPR Articles 24-9, and be able to demonstrate compliance;
- take a data protection by design and default approach, as required by Article 25;
- undertake a DPIA where required, as set out in UK GDPR Article 35; and
- if the DPIA identifies risks that cannot be mitigated by the controller, consult the ICO, as required by UK GDPR Article 36.

Depending on their specific circumstances, controllers may also need to fulfil additional legal requirements to comply with data protection law (eg designating a data protection officer), but the summary above represents the specific requirements when deploying LFR.

The ICO is mindful of the potential for collaboration between police and private or public sector controllers using LFR for surveillance. Where such collaboration takes place, the relationship and responsibilities (including controllership) must be clear. The key requirements are set out in section 4.9.2.

Key compliance issues

The Commissioner believes that lawfulness, fairness and transparency, including a robust evaluation of necessity and proportionality, are the crucial issues for controllers to address before deploying LFR in a public place. This is based on her assessment of current uses of LFR and her interpretation of data protection legislation. Controllers must comply with all part of the legislation, but these issues are key challenges in the context of LFR.

The concepts of necessity and proportionality run through a range of the legal requirements of the UK GDPR and the DPA 2018. They are also concepts that have been developed in UK case law and the Commissioner has reflected the conclusions of the courts in this Opinion. Controllers' assessments of necessity and proportionality will depend on the risks and potential impacts for data subjects (which the legislation requires controllers to assess in themselves).

The Commissioner focuses on these issues in the subsequent sections and in the annex to this Opinion. (The annex provides detailed advice on how controllers should approach the assessments required as part of a DPIA for LFR in public places.)

Together, these requirements mean that where LFR is used for the automatic, indiscriminate collection of biometric data in public places, there is a high bar for its use to be lawful. While this is the Commissioner's general assessment of what the legislation requires in this context, she emphasises that any investigation or regulatory assessment would be based on the facts of the case, considering the specific circumstances and relevant laws.

Interaction with the right to privacy

Much of the relevant case law is focused on the right to respect for private and family life. This is set out in Article 8(1) of the European Convention on Human Rights (ECHR), incorporated into UK law through the Human Rights Act 1998. Any interference with this right must be justified in accordance with the principles of ECHR Article 8(2).

In an LFR context, data protection legislation particularises the ECHR Article 8 right in the context of processing personal data. The legal requirements of data protection legislation and the associated assessments controllers need to make are set out in this Opinion. The Commissioner considers that satisfying these assessments and the associated aspects of data protection law will be a crucial component of ensuring that any processing of personal data through LFR is "in accordance with the law" (as required by the language in ECHR Article 8(2) and

the tests established in associated case law). In short, controllers must comply with data protection law in order to meet the requirements of the ECHR on the right to respect for private and family life.

The Commissioner may update or revise this Opinion based on any material legal or practical developments in this evolving area, such as judicial decisions and case law, or further findings from her regulatory work and practical experience.

4.3 Purposes for LFR

Key requirement: The controller must identify a specified, explicit and legitimate purpose for using LFR in a public place

The purpose limitation principle at UK GDPR Article 5(1)(b) requires controllers to identify a specified, explicit and legitimate purpose when they process personal data. Controllers should have a clear outcome or benefit in mind. A wide range of purposes or objectives may be legitimate, but they must also be sufficiently important to justify the processing of personal data in question.[22]

This obligation stems not only from the purpose limitation principle, but it is also built into the data minimisation and storage limitation principles, as well as fairness and transparency requirements.[23] Where controllers are seeking to rely on the legitimate interest lawful basis for processing, they must identify their legitimate interest to meet the first requirement of Article 6(1)(f). Likewise, many of the conditions for compliance with Article 9 are only available to controllers when they are processing for certain specific purposes.

Controllers must also comply with the purpose limitation principle and prevent any "function creep" that involves the use of the personal data for incompatible purposes.

4.4 Lawful basis and special category data

For any use of personal data to be lawful, there must be a lawful basis in place for the processing. The available bases are set out in Article 6 of the UK GDPR. In addition, when processing special category data or criminal offence data, controllers must identify an appropriate condition under Article 9 or 10 of the GDPR respectively. Controllers must identify and meet the requirements of these important gateways through the legislation for their use of LFR to be lawful.[24]

---

[22] Further guidance on what constitutes a legitimate purposes can be found in the ICO's detailed guidance on the legitimate interest lawful basis.
[23] See UK GDPR Article 5(1)(c) (data minimisation) and (e) (storage limitation).
[24] More detailed guidance on all lawful bases is provided in the ICO's Guide to GDPR, alongside detailed guidance on special category data and criminal offence data.

Key requirement: The controller must identify a valid lawful basis and meet its requirements

The ICO has encountered examples of controllers seeking to rely on the consent of the data subject as their lawful basis (Article 6(1)(a)). Under the UK GDPR:

- consent must be freely given, specific, informed and unambiguous;[25]
- it requires a statement or clear affirmative action by the data subject to signal their agreement to the processing;[26]
- the data subject must be able to withdraw their consent at any time and should be able to refuse consent without suffering detriment;[27] and
- consent needs to be collected for each data subject on an individual basis and the controller needs to be able to demonstrate that consent.[28]

Controllers also need to consider whether consent is an appropriate lawful basis for processing the personal data of children or vulnerable adults who may access the public place. As set out in ICO guidance on children's consent, controllers generally need to assess whether the individual has competence and can consent for themselves.

As stated in the ICO's guidance: "Consent is appropriate if you can offer people real choice and control over how you use their data, and want to build their trust and engagement. But if you cannot offer a genuine choice, consent is not appropriate. If you would still process the personal data without consent, asking for consent is misleading and inherently unfair."[29]

Consent can often be appropriate for uses of FRT such as authentication (eg unlocking your mobile phone or laptop), as long as the conditions set out in the law are met. However, this is more challenging when LFR is deployed towards public spaces and involves the automatic and indiscriminate collection of personal data. Consent is unlikely to be an appropriate lawful basis in these cases. It will be challenging to demonstrate that each individual has provided consent and that it has been freely given, specific, informed and unambiguous.

In many of the examples we examined, LFR-enabled cameras were proposed or used to capture the personal data of significant numbers of people as they passed through shopping centres, transport interchanges or other premises. Often, LFR systems were directed towards locations of high footfall such as the

[25] As required by UK GDPR Article 4(11) and Article 7
[26] Ibid; see also UK GDPR Recital 32
[27] UK GDPR Article 7(3) and (4) and Recital 42 which says that "Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment."
[28] UK GDPR Article 7(1), which says "Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data."
[29] See the ICO's 'in brief' guidance on consent and detailed guidance on consent.

entrances and exits of premises. In such circumstances, controllers are unlikely to be able to collect valid consent and demonstrate it for all individuals whose data they process. An individual simply choosing to enter the premises is insufficient.

In other circumstances, controllers may need to use LFR to comply with a legal obligation or to perform a public task.[30] To rely on these lawful bases, Article 6(3) of the UK GDPR requires that the legal obligation or public task must be laid down by law. Recital 41 confirms that this does not have to be an explicit statutory obligation. The law does not need to specify the use of LFR; the obligation or task could arise from common law, legislation or statutory guidance. What matters is that the law is clear and precise, its application is adequately accessible and foreseeable by the individuals subject to it (ie members of the public), and it contains appropriate safeguards against abuse. However, the controller must still demonstrate that LFR is a necessary and proportionate means of fulfilling the obligation or task.

The ICO has most often seen controllers seek to rely on the legitimate interests lawful basis. Of the 14 examples of LFR we examined in detail, eight cited legitimate interests as the basis for some or all of their processing.[31]

To rely on this basis, UK GDPR Article 6(1)(f) requires that processing is "necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data."

In line with their accountability obligations, controllers must demonstrate that they meet the three elements within Article 6(1)(f). The ICO's detailed guidance on legitimate interests underlines the importance of each component.

ICO detailed guidance on legitimate interests: What is the three part test?

Article 6(1)(f) breaks down into three parts […] It makes most sense to apply this as a test in the following order:

- **Purpose test** – is there a legitimate interest behind the processing?
- **Necessity test** – is the processing necessary for that purpose?
- **Balancing test** – is the legitimate interest overridden by the individual's interests, rights or freedoms?

[30] UK GDPR Article 6(1)(c) and (e)
[31] It should be noted that some controllers had not identified a lawful basis.

This concept of a three-part test for legitimate interests is not new. In fact the Court of Justice of the European Union confirmed this approach to legitimate interests in the Rigas case (C-13/16, 4 May 2017) in the context of the Data Protection Directive 95/46/EC, which contained a very similar provision.

This means it is not sufficient for you to simply decide that it's in your legitimate interests and start processing the data. You must be able to satisfy all three parts of the test prior to commencing your processing.

All the lawful bases, except consent, require the controller to assess whether their processing is necessary for their particular purpose (eg their specified public task or legitimate interest). Demonstrating necessity is therefore a crucial component of lawfulness.

Key requirement: The controller must identify conditions for processing special category data and criminal offence data, where required, and meet their conditions

Facial recognition involves the processing of biometric data which is likely to constitute special category data in most LFR scenarios (as discussed in section 4.1). This includes data that is processed only momentarily. Article 9 of the UK GDPR prohibits the processing of special category data unless the controller identifies a relevant condition from the legislation.

It is unlikely that controllers will be able to rely on explicit consent (Article 9(2)(a)) when collecting the public's biometric data on an automatic and indiscriminate basis for the reasons explained above. The other nine conditions in Article 9 are available to controllers processing for specific purposes (eg for employment purposes or to support legal claims). Only some of these conditions are likely to be relevant to the use of LFR in public places. To date, the ICO has only encountered controllers seeking to rely on the "substantial public interest" condition at Article 9(2)(g).

Article 9(2)(g) requires controllers to identify an additional substantial public interest condition from the DPA 2018; there are 23 such conditions set out in Schedule 1 Part 2. Each relates to a specific purpose for processing special category data, so only a limited number are applicable to LFR in public places. Examples may include "preventing or detecting unlawful acts", "safeguarding children and individuals at risk", or "statutory and government purposes".

Controllers must ensure they meet all the requirements of their chosen condition. For some of the conditions, the public interest element is built into the specified purpose (eg preventing fraud). However, 11 of the conditions explicitly

require that the controller can demonstrate that their deployment of LFR is necessary for specific reasons of substantial public interest.[32]

In addition, all but one of the 23 substantial public interest conditions require controllers to put an "appropriate policy document" (APD) in place.[33] The ICO has produced an appropriate policy document template which controllers can use.

If controllers are processing data on criminal convictions and offences (which includes records, allegations and evidence of crime), they must comply also with UK GDPR Article 10. In most cases, if the controller already has an Article 9 condition for processing special category data, this may also justify the processing of criminal offence data. However, controllers should carefully consider how to comply in their specific circumstances. The ICO has published detailed guidance on criminal offence data.

Most of the conditions for processing special category data in Article 9 also require the controller to assess whether their processing is necessary for the specified purpose. This reiterates that demonstrating necessity is a crucial component of lawfulness.

4.5 Necessity and proportionality

The legal requirement that processing must be necessary arises from several elements of the legislation. As described above, necessity is built into the data protection principles at Article 5 of the UK GDPR, lawful basis requirements at Article 6, special category data requirements at Article 9, and DPIA requirements at Article 35, among other provisions.

For the processing to be necessary, it must be "reasonably necessary". This means that the processing must be more than desirable but does not need to be indispensable or absolutely necessary. This is established in the relevant case law.[34] The processing will not be necessary if the controller's legitimate purpose could reasonably be achieved by a less restrictive or intrusive approach. Proportionality is closely related to necessity, and controllers should consider

[32] See ICO guidance "What are the substantial public interest conditions?"
[33] Under DPA 2018 Schedule 1 Part 2, condition 13 (journalism, academia, art and literature) does not require an APD. In addition, the APD requirements are different for conditions 10 (preventing and detecting unlawful acts) and 27 (anti-doping in sport). Controllers processing for these purposes do not need an APD in place to disclose data to the relevant authorities (or to prepare to disclose it). However, an APD is required for other processing activities.
[34] See *Goldsmith International Business School v The Information Commissioner and the Home Office – Upper Tribunal – [2014]* UKUT 0563 (AAC), paragraphs 33-44, upheld in *Cooper v National Crime Agency – Court of Appeal – [2019]* EWCA Civ 16, paragraphs 88-91. See also the summary of the Bank Mellat case at footnote 36. The ICO has published guidance on necessity as part of its detailed guidance on special category data and its detailed guidance on legitimate interests.

whether their purpose is of sufficient importance to justify any privacy intrusion or other impact arising for the individual.[35]

Therefore, the question of necessity and proportionality can be considered in three parts.

Key requirement: The use of LFR must be necessary and should be a targeted and effective way to achieve the controller's purpose

First, the use of LFR must be connected to the controller's purpose, making a clear, demonstrable contribution to achieving it. It should be a targeted way of achieving that purpose. To ensure that using LFR is necessary, controllers should be able to demonstrate that LFR allows them to take particular action and that this requires the collection of biometric data.

The controller should scrutinise whether the system is an effective means of achieving the intended purpose (ie realising the outcomes or benefits). If an LFR system is not effective, then it is unlikely to be necessary.

Key requirement: The controller must consider alternative measures and demonstrate that they cannot reasonably achieve their purpose by using a less intrusive measure

Secondly, if controllers can reasonably achieve the same or similar outcomes through other means which may be less intrusive, then the use of LFR is unlikely to be necessary or proportionate.

LFR does not have to be the only possible means of achieving the objective, but controllers must consider other alternative measures which are less intrusive and demonstrate that they have discounted them for adequate reasons.

Controllers should not use LFR simply because it is available, it improves efficiency or saves money, or is part of a particular business model or proffered service. While it may be justifiable in some circumstances, if the deployment of LFR is only likely to be slightly more effective than less privacy-intrusive measures (such as non-biometric measures, eg alternative types of surveillance) then it may be unnecessary.

[35] Human rights case law has established that the concepts of both necessity and proportionality are central to considering whether any interference with an individual's rights is justified (see footnote 36 on the Bank Mellat case). As such, assessing proportionality is also a key part of compliance with the fairness principle (Article 5(1)(a)). UK GPDR Article 35(7) also requires controllers to assess necessity and proportionality as part of their DPIA.

Key requirement: The use of LFR must be proportionate and the controller's purpose should be of sufficient importance to justify any privacy intrusion or other impact on individuals

A third element of the analysis involves an overall assessment of proportionality, which is closely related to necessity. Human rights case law has established that the closely-entwined concepts of both necessity and proportionality are central to considering whether any interference with an individual's rights is justified.[36] As such, assessing proportionality is a key part of compliance with the fairness principle (Article 5(1)(a)). UK GDPR Article 35(7) also requires controllers to assess necessity and proportionality as part of their DPIA.

Proportionality is particularly important when controllers are seeking to rely on the legitimate interests lawful basis. This is because controllers must demonstrate that their interest is not overridden by individuals' interests, rights and freedoms.

UK case law on proportionality, for example the *Bank Mellat* case in the Supreme Court, has set out a series of tests to assess whether an interference with an individual's rights is justified.[37] Alongside the assessment of necessity set out above, controllers should consider also:

- Whether their objective is sufficiently important to justify the processing of biometric data and interference with individuals' privacy; and
- Whether a fair balance has been struck between the interest of the controller, the rights of the individual and the interests of the community.

Assessing the importance of the controller's objective and the balance of interests is a potentially challenging issue. It involves careful evaluation and judgment based on the specific context in question. Controllers' objectives may vary significantly in their importance, from achieving small cost efficiencies or tackling petty crime, to preventing major threats to public safety.

[36] The Supreme Court set out a framework for assessing whether a particular activity amounts to an unjustified interference with a human right in *Bank Mellat v Her Majesty's Treasury (No 2) [2013]* UKSC 39 [2014] AC 700. The Court set out a four-part test to assess whether an interference with an individual's rights is justified: (1) whether the objective of the measure pursued is sufficiently important to justify the limitation of a fundamental right; (2) whether it is rationally connected to the objective; (3) whether a less intrusive measure could have been used without unacceptably compromising the objective; and (4) whether, having regard to these matters and to the severity of the consequences, a fair balance has been struck between the rights of the individual and the interests of the community. These tests were subsequently applied by the courts in *R (Bridges) v The Chief Constable of South Wales Police* (*e.g. [2020]* EWCA Civ 1058, paragraphs 44 and 131-144) in considering the proportionality of the deployment of LFR by South Wales Police. The Commissioner has incorporated parts 2 and 3 of the Bank Mellat test into her interpretation of 'necessity' in a data protection context set out in the previous sub-section above; parts 1 and 4 of the test are addressed here in the discussion of 'proportionality'.

[37] These tests are set out above at footnote 36.

However, where LFR systems are used to collect and analyse biometric data on an automatic and indiscriminate basis, potentially on a mass scale, this could represent a significant privacy intrusion. In this context, controllers must assess whether their objectives justify:

- the automatic processing of sensitive biometric data of all individuals within a given location;
- the collection of this data without individuals' choice or control; and
- any potential detriment to those individuals, whether direct or indirect. Examples could include being removed from premises, referral to law enforcement agencies, social embarrassment or stigma, or any interferences with their human rights.

As part of the DPIA process, controllers must consider the wider risks and potential impacts of their use of LFR, including for individuals' rights and freedoms.[38] (This is the focus of section 4.7.) If a controller believes that their proposed use of LFR is proportionate and the purposes of the deployment justify any impact on individuals, they must be able to demonstrate this clearly.

4.6 Fairness and transparency

Fairness and transparency are key elements of the data protection principle set out in Article 5(1)(a) of the UK GDPR. These two requirements are closely linked, and the ICO's guide to the UK GDPR advises that for processing to be fair, controllers:

- must not deceive or mislead people when collecting and processing their personal data;
- only handle people's data in ways they would reasonably expect, or can justify any unexpected processing; and
- have considered how the processing may affect the individuals and can justify any adverse impact.

Controllers should consider and justify any adverse impacts when assessing the proportionality of their processing and the risks and impact (see section 4.5 and 4.7). But when addressing the fairness of using LFR, controllers should also consider some of the specific issues which can be presented by the technology. Namely, the technical effectiveness and statistical accuracy of LFR, and the risk of bias and discrimination.

If an LFR system is not sufficiently technically effective and statistically accurate, it may lead to adverse impacts and unfair outcomes. LFR systems may also work less effectively for people from different demographic groups. This could potentially lead to unfairness in the form of discrimination and bias. These

[38] As required by Article 35(7)(c)

technological issues, and their implications for fairness, are addressed substantively in the ICO's guidance on Artificial Intelligence (AI) and data protection. The key implications of this guidance for LFR are summarised below.[39]

Key requirement: The LFR system should be technically effective and sufficiently statistically accurate

In the case of LFR, statistical accuracy refers to the proportion of predictions the system gets right (ie whether the system correctly identifies or categorises the facial biometric templates of individuals). An LFR system does not need to be 100% statistically accurate, as long as the controller treats outcomes of any LFR matches or categorisation as statistically informed estimates or predictions, as opposed to facts. [40]

Controllers should make sure the system is sufficiently statistically accurate for their purposes. An incorrect match may have an adverse impact on the individual. The greater potential detriment an inaccurate result could have on individuals, the more important it is that controllers' systems are statistically accurate. If there are too many incorrect matches, this will call into question both the fairness and the necessity of the processing.

The Commissioner expects a controller to be able to justify the accuracy threshold they have set within their LFR system, with clear reference to the purpose of their deployment and the potential consequences for individuals. The annex to this Opinion sets out some of the measures controllers can apply, including false positives, false negatives, precision and recall, to demonstrate that their system is fair.

Controllers should consider these issues during the design or commissioning of any LFR system. They should also monitor the accuracy of their system during deployment and make any improvements needed. They should stop the deployment if the accuracy of the system is not sufficiently improved.

Key requirement: The controller should address the risk of bias and discrimination and must ensure fair treatment of individuals

While LFR technology has the potential to become more accurate, some reports have concluded that it can perform with less precision for some demographic groups, such as women, minority ethnic groups and potentially disabled

---

[39] The ICO defines AI as 'the theory and development of computer systems able to perform tasks normally requiring human intelligence' (see "What do you mean by AI?"). This can include LFR technology, which functions using algorithms to perform the task of identification or categorisation usually performed by humans. Controllers should review in particular the section "How do the principles of lawfulness, fairness and transparency apply to AI?"

[40] Statistical accuracy is different to the accuracy principle within data protection law. The ICO's Guide to the UK GDPR includes guidance on the accuracy principle.

people.[41] Using such a system could potentially result in discriminatory, and therefore unfair, outcomes based on their sex, gender, ethnicity, race, impairment or disability, age or other demographic characteristics. Equally, there is a risk of bias and discrimination in the process of compiling watchlists (often manual) which underpin an LFR system. More broadly these processes risk reinforcing existing biases in society.

Controllers should take steps to mitigate these risks and the Commissioner expects to see that they:[42]

- consider the risk of bias, discrimination and the unfair treatment of different demographic groups during the design, commissioning or procurement process of any LFR system. This includes, where warranted, seeking assurances from vendors and justifying and recording their decisions on these issues;
- ensure that the LFR system has been subject to robust testing and accounted for the results of this testing in their decisions and processes;
- where applicable, fulfil their obligations under the Equalities Act 2010 and consider whether an Equalities Impact Assessment is required;
- consider whether the system is appropriate for use and, if they implement the system, what adjustments and safeguards or mitigations they need; and
- monitor the outcomes of the system, including for any evidence of bias or discrimination, and adapt their approach based on their findings.

These actions will help controllers to assess whether their system is fair and demonstrate compliance with data protection by design and default obligations.[43]

Key requirement: The controller must be transparent and provide clear information about how they are processing personal data

Transparency is a key component of fairness, as well as being a legal requirement under UK GDPR Articles 5(1)(a), 13 and 14. Controllers must provide clear information to data subjects about when, where and why they are using LFR and how individuals can exercise their data protection rights.

Controllers should generally provide such information before the processing takes place.[44] Where possible, they should therefore provide information to individuals, including prominent signage, before they enter the area covered by

[41] See footnote 9 above.
[42] More detailed recommendations are provided in the ICO's guidance on AI and data protection, "How should we address risks of bias and discrimination?"
[43] This advice does not aim to provide guidance on legal compliance with the UK's anti-discrimination legal framework, notably the UK Equality Act 2010.
[44] UK GDPR Article 13(1) requires transparency obligations to be fulfilled "at the time when personal data are obtained".

an LFR deployment and consider advance notice in the days or weeks ahead of deployment where possible.

The ICO has seen examples where the quality of information for the public and the locations and visibility of signage have been insufficient. Controllers need to take account of what people are likely to expect in public places, especially given the novel nature of LFR. Adapting standard CCTV signage is likely to be insufficient. Controllers should consider more extensive and effective measures to ensure that the public understands how their data is being processed. This should include prominent signage, clearly visible and accessible to members of the public, explaining:

- that LFR is in use and for what purposes;
- that biometric data is being processed; and
- how people can access more information and exercise their data protection rights.[45]

Controllers should consider supplementing this signage by:

- using leaflets, digital techniques (eg QR codes) and other local media, in advance where possible;
- making trained staff available to provide advice and answer questions;
- promoting information online and through social media, and otherwise using digital spaces that visitors are likely to use in advance of visiting the premises in question; and
- using other measures which are appropriate to the circumstances.

Controllers must also be transparent about watchlists, informing individuals when and why they have been added to a list unless the use of an exemption can be justified.[46] Among other information, controllers should tell individuals how their data will be used, how long it will be retained, and how they can complain or object.

The ICO has published guidance on transparency and individuals' right to be informed.

[45] In line with UK GDPR Article 12 and 13
[46] The exemptions from certain provisions of the UK GDPR, including the right to be informed, are set out in Schedules 2-4 of the DPA 2018 and the ICO has also published guidance on the use of these exemptions.

4.7 Assessing risks and impacts

It is important that controllers assess the risks and potential impacts of their use of LFR. They need to do this to demonstrate fairness and proportionality, and because assessing risk is a required part of completing a DPIA.

A DPIA is required for certain types of processing, as explained below. It is also an important way for controllers to meet their accountability obligations and demonstrate that their use of LFR complies with data protection law.[47] The annex to this Opinion provides detailed advice on how controllers should approach the assessments required as part of a DPIA for LFR in public places.

In addition, controllers seeking to rely on the legitimate interests lawful basis need to assess the risks and impacts of their processing to demonstrate that their interest is not overridden by individuals' interests, rights and freedoms. They can do this through the DPIA.

Key requirement: The controller should undertake a data protection impact assessment

Article 35(1) of the UK GDPR sets out that a DPIA is required where "a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons."

The legislation does not define "likely to result in high risk". The legal requirement in Article 35 is not focused on whether the specific processing in question is actually high risk. It is whether it constitutes a "type" of processing that is likely to be high risk. This does not mean that the type of processing in question is always high risk or always likely to cause harm, but that there is a reasonable chance that the processing could be high risk and so a DPIA is required to assess the level of risk in more detail.

Article 35(3) goes on to specify three types of processing that automatically require a DPIA.

Article 35(3) of the UK GDPR

"A data protection impact assessment […] shall in particular be required in the case of:

(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects

[47] UK GDPR Articles 5(2) and 24

concerning the natural person or similarly significantly affect the natural person;

(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or

(c) a systematic monitoring of a publicly accessible area on a large scale."

The Commissioner considers it likely that the use of LFR in public places will typically meet at least one of these criteria. Therefore controllers should carry out a DPIA for this type of processing.

Controllers may seek to argue that smaller scale deployments may not reach these thresholds. However, the use of LFR in public places may still be considered a "type of processing" likely to result in similar risks. Even smaller scale deployments are likely to hit additional criteria set out by the ICO.[48] As such, the Commissioner considers that a DPIA is still likely to be required in most cases.

If a controller decides it does not need to undertake a DPIA for its specific type of small-scale processing, it needs to justify this decision. They should refer clearly to the detailed criteria set out in the Commissioner's guidance on when a DPIA is required.[49]

A DPIA can also help demonstrate that the controller has met the legal requirement to take a data protection by design and default approach.[50] This is particularly important in the context of LFR because many issues of fairness, necessity and proportionality need to be addressed during the planning and design stage of a system.

Key requirement: The controller's assessment must consider the risks and potential impacts of the processing on the interests, rights and freedoms of data subjects

Article 35(7)(c) states that a DPIA must include "an assessment of the risks to the rights and freedoms of data subjects". When considering what risks and potential impacts controllers should assess, it is useful to refer to the ICO's existing detailed guidance on DPIAs, which explains the legislative context.

[48] Article 35(4) requires the ICO to set out other kinds of processing operations for which a DPIA is required and the ICO has provided detailed guidance on when controllers need to do a DPIA.
[49] Ibid
[50] UK GDPR Article 25

ICO detailed guidance on DPIAs: What kind of 'risk' do they assess?

There is no explicit definition of 'risk' in the UK GDPR, but the various provisions on DPIAs make clear that this is about the risks to individuals' interests. Article 35 says that a DPIA must consider "risks to the rights and freedoms of natural persons". This includes risks to privacy and data protection rights, but also effects on other fundamental rights and interests.[51]

The key provision here is Recital 75, which links risk to the concept of potential harm or damage to individuals:

> "The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data…"

The focus is therefore on any potential harm to individuals. However, the risk-based approach is not just about actual damage and should also look at the possibility for more intangible harm. It includes any "significant economic or social disadvantage".

The impact on society as a whole may also be a relevant risk factor. For example, it may be a significant risk if your intended processing leads to a loss of public trust.

A DPIA must assess the level of risk, and in particular whether it is 'high risk'. The UK GDPR is clear that assessing the level of risk involves looking at both the likelihood and the severity of the potential harm.

For more guidance on what this all means in practice, see the section on how to carry out a DPIA.

Relevant provisions in the UK GDPR – see Article 35(1) and Recitals 4, 75, 76, 84 and 90.

[51] Fundamental rights include the rights set out in European Convention on Human Rights (ECHR), incorporated into UK law through the Human Rights Act 1998. These rights include, for example, freedom of expression, assembly and association, and freedom from discrimination.

Identifying and assessing the risks and potential impacts of LFR is a highly context-specific process. The controller should pay close attention to the specific circumstances of their processing. The focus is on the potential for the deployment of LFR to cause any type of direct or indirect impact, and material or non-material damage.

Where LFR is used for the automatic collection of biometric data in public places, controllers should consider at least any potential:

- inability to exercise any legal rights;
- inability to exercise any specific data protection rights, including the right to be informed, the right of access and the right to object;
- inability to opt-out of the processing;
- loss of control over the use of personal data;
- inability to access services or opportunities; and
- direct or indirect impact on individuals' ability to exercise their rights and freedoms in this public setting, such as freedom of expression, assembly and association, including any potential inhibiting effect.

Other types of risk are considered in the annex to this Opinion on DPIAs.

In assessing the wider risks to rights and freedoms, controllers should consider the relevance of concerns about LFR raised by some academics, civil society groups, and international organisations. Some are concerned about the potential for LFR to be used to target certain individuals due to their activities, behaviours, personal attributes or beliefs. There are also concerns about the wider inhibiting effect of LFR on the free exercise of rights, such as freedom of expression and assembly.

At the time of publishing this Opinion, the Commissioner has not encountered settled evidence on the impact of LFR on communities or wider society. However, controllers should consider the relevance of these concerns in the specific context of their processing. These issues, alongside other risks, are addressed in more detail in the annex to this Opinion.

Based on their assessment of the risks and potential impacts, alongside any mitigations and compliance measure, the controller must decide if their proposed deployment of LFR can meet the legal requirements of lawfulness, fairness, necessity and proportionality. Where controllers are seeking to rely on the legitimate interests lawful basis, they must decide whether their interest is overridden by individuals' interests, rights and freedoms.

4.8 Other compliance issues

If the controller's judgment is that they can justify the use of LFR, they must also implement their system in a way which complies with the data protection principles and ensures that data subjects are able to exercise their rights. The ICO's Guide to the UK GDPR provides guidance on these obligations.

Key requirement: The controller must ensure they comply with the data protection principles

The first data protection principle, that processing must be lawful, fair and transparent (Article 5(1)(a)), has been addressed in the sections above.

Purpose limitation – Article 5(1)(b): Any data collected as part of an LFR system must not be processed for other incompatible purposes. Controllers should have controls in place to prevent any "function creep" involving new processing which has not been subject to the same assessment as the original purposes. They should fully assess and document any new purposes in line with the policy positions set out in this Opinion.

Data minimisation – Article 5(1)(c): Data processing must be adequate, relevant and limited to what is necessary. Controllers must minimise the amount of personal data they collect by ensuring that any use of LFR is as narrowly targeted as possible to achieve their stated purpose. LFR should be targeted in at least the following ways:

- Time limited: used for the shortest possible time to be effective.
- Minimum physical and spatial scope: limiting the physical area captured by the LFR system so that it is targeted to its intended purpose, as opposed to more general surveillance.
- Minimum numbers of individuals: keeping the number of people whose personal data is processed by an LFR system to a minimum, both in the size of watchlists and the total number of individuals whose facial templates are processed by the LFR system.
- Watchlist controls: ensuring that controllers compile watchlists in a compliant way, closely observing any defined criteria and having appropriate governance in place (see section 4.9.1).

Accuracy – Article 5(1)(d): Controllers must take every reasonable step to ensure data is accurate and kept up-to-date (eg images on watchlists). They should also treat data in the appropriate way. For example, ensuring that LFR results are treated as statistical estimates or predictions and not matters of fact.

Storage limitation – Article 5(1)(e): Controllers must retain any data collected through an LFR system for the shortest possible time. It is often possible to delete "unmatched" biometric templates within seconds. "Matched"

templates should also have the shortest retention period possible to achieve the controller's stated purpose.

Security – Article 5(1)(f): Controllers must ensure that appropriate technical and organisational measures are in place so that any data is captured and stored in a secure manner. Further information can be found in the ICO's guidance on security.

Accountability – Article 5(2): Controllers are responsible for complying with data protection law and must be able to demonstrate that compliance. It is crucial that controllers ensure responsibility and oversight for any LFR system is clear. This is especially important if there are multiple parties involved in its operation or broader decision-making about its use.

If there is a controller-processor arrangement, the parties must put in place a written contract which meets the minimum standards set out in UK GDPR Article 28.[52] If there are joint controllers, the parties must put in place a transparent arrangement, as required by Article 26 of the UK GDPR. In this situation, and if there is any data sharing with other, separate controllers, it is good practice to have a data sharing agreement. If there is collaboration with law enforcement authorities, controllers should consult section 4.9.2 which sets out additional considerations.

Controllers must take a data protection by design and default approach.[53] They should therefore consider privacy and data protection when procuring, purchasing or developing any LFR systems. They should also ensure LFR products or services they adopt from vendors have been designed with appropriate data protection and privacy-preserving features built-in. Controllers, not technology vendors, are responsible for this under the law. They should not deploy "off-the-shelf" solutions without adequate due diligence to understand the technical processing and associated privacy implications. Controllers also should consider whether an LFR system is designed with data subjects' rights in mind. For example, they should have the capability to isolate and extract personal data in response to a subject access request, unless valid exemptions apply.

It is especially important that controllers set out clear processes and policies governing their use of LFR, including:

- the circumstances in which the controller may activate the LFR system;
- clear criteria and governance for any watchlists;
- well-defined procedures for intervention in the event of a match and clear escalation measures;

[52] See further information in the ICO's guidance on contracts.
[53] UK GDPR Article 25

- how data subjects can complain, how controllers will handle complaints, and how they will fulfil the public's data protection rights; and
- processes to continually monitor the impact of the LFR system and assess whether it continues to be fair, necessary and proportionate.

The ICO has provided guidance on accountability and documentation requirements in the Guide to the UK GDPR, and recently published an accountability framework to help controllers fulfil their obligations. DPIAs are also a vital part of controllers' accountability obligations and are addressed in the annex to this Opinion.

Controllers may also wish to consider some of the specific data protection by design and default techniques provided within the UK GDPR, such as Codes of Conduct or Certification schemes.

4.9 Surveillance and direct marketing considerations

4.9.1 Watchlists

When controllers compile watchlists for use as part of an LFR system, this processing must also comply with data protection law and meet the same requirements of lawfulness, fairness, necessity and proportionality. Being included on a watchlist may subject individuals to direct interventions or to social stigma, and therefore places significant power over that individual in the hands of the controller. Without proper governance, this power could be exercised in unfair ways (even if not intended) which could cause detriment or distress.

The ICO has seen examples of watchlists being supplemented by law enforcement agencies. If images are received from or requested by law enforcement agencies, controllers may need to consider additional compliance issues, as discussed in section 4.9.2.

Whenever a watchlist is used for LFR, in line with the data protection principles, the Commissioner expects controllers to:

- strictly limit the images they include on the watchlist to those which are necessary and proportionate;
- ensure watchlist images are retained only as long as is necessary, in line with the data minimisation and storage limitation principles;
- include only images that are lawfully acquired and accurate, ensuring that they understand their provenance;
- process images fairly, considering possible adverse impacts for the individual;

- ensure transparency and that individuals can exercise their rights, including the right to be informed, to erasure and to object, unless relevant exemptions apply; and
- ensure watchlists are compiled and maintained by staff who have sufficient knowledge of data protection to comply with the requirements of the law.

Watchlists of individuals suspected of minor offences are less likely to satisfy the key legal tests of necessity and proportionality. Likewise, watchlists comprising images of individuals where there is no reasonable expectation that they will be in the vicinity of the LFR deployment are also less likely to meet these requirements. Watchlists based on images of uncertain provenance (eg images sourced from social media) will raise issues including lawfulness, fairness and accuracy.

4.9.2 Collaboration with law enforcement

When controllers use LFR as a surveillance tool, this is often for crime prevention purposes and may involve collaboration with law enforcement authorities. This could include several types of processing:

- organisations could refer individuals to the police after they have been identified using LFR;
- police could request information which organisations have collected as part of their LFR surveillance operations;
- police could provide organisations with images of persons of interest for use on an LFR watchlist; and
- police could direct an organisation to use its LFR system to identify individuals (the police force may become the controller and the LFR operator a processor in these circumstances).

Where there is collaboration between LFR operators and law enforcement authorities, the relationship and responsibilities must be clear.[54] The parties must assess whether they are acting as separate controllers, or if the LFR operator is acting as a processor for the police. This relationship must be set out in appropriate contracts or agreements, which clearly detail how data should be processed and limit the further processing of data for other purposes.[55] If a law enforcement agency is the controller for the LFR system and the processing is for a law enforcement purpose, they and their processors must meet the

[54] These obligations arise from UK GDPR Article 5(2) 'accountability' and the controllership provisions in Articles 24-9.
[55] The legal requirements on joint controllership and controller/processor agreements and contracts are set out in Articles 26 and 28 of the UK GDPR respectively (also see ICO guidance on contracts).

requirements under Part 3 of the DPA 2018. They should consult the Commissioner's Opinion on the use of LFR in law enforcement.

If acting as separate controllers, both parties must ensure that the processing complies with data protection law. Controllers processing under UK GDPR and Part 2 of the DPA 2018 must comply with UK GDPR Article 10 when processing criminal offence data. They can consult the Commissioner's detailed guidance on criminal offence data, on sharing personal data with law enforcement authorities, and the law enforcement sections of the Commissioner's data sharing code of practice.

Whatever the arrangement, controllers must be transparent with the public about who is processing their personal data and for what purpose. This must be communicated clearly, including through any signage, other communications and associated privacy information.

As always, controllers must assess the lawfulness, fairness, necessity and proportionality of their processing. When sharing data with police forces, they should be satisfied that the sharing is limited to what is necessary for law enforcement purposes. Therefore, they should also be prepared to obtain further clarity on any police request and ensure they record any disclosures. The user of the LFR system is responsible for the security of any data received from the police and must restrict access to the data and limit retention to what is necessary. Controllers should review any ongoing data sharing at regular intervals. It is also good practice for any sharing arrangements to be subject to a data-sharing agreement, as recommended in the ICO's data sharing code of practice.

4.9.3 Compliance issues with direct marketing

The UK GDPR contains specific provisions on direct marketing. Article 21(2) states that "Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing."

The right to object to direct marketing is absolute and there are no exemptions available within the legislation. This covers any processing "for direct marketing purposes". Therefore it is not limited to sending or displaying direct marketing to the individual, but covers controllers' use of an individual's data for direct marketing purposes more broadly.

Controllers considering using LFR need to enable individuals to exercise this right. They must also bring the right to the attention of data subjects "at the

latest at the time of the first communication with the data subject" and it must be "presented clearly and separately from any other information".[56]

However, before they use LFR for direct marketing, controllers also need to ensure that they are meeting the legal requirements for processing biometric data. This includes identifying a lawful basis and any conditions required for processing special category data, and ensuring the processing is fair, necessary and proportionate.

Based on the use cases the ICO has seen to-date, the Commissioner's view is that it would be challenging for a controller to justify the use of LFR in a public place to display direct marketing to an individual based on an analysis of their biometric data. While each case needs to be considered on its facts, it is important for controllers to be aware of the significant challenges they would face in meeting the legal conditions required for processing personal data in this way.

It may be easier for controllers to justify other less intrusive techniques. If the purpose of processing is not direct marketing but instead solely to measure footfall, dwell time, engagement with media or to activate the media, then this may be less intrusive depending on the context and the nature of the data being processed. Techniques which do not involve processing biometric data and special category data are generally likely to be less intrusive.

[56] UK GDPR Article 21(4)

5. Conclusions and next steps

This Opinion has set out the Commissioner's assessment of the LFR environment today. Through her office's investigations, assessments and wider research, she has identified the key data protection issues that LFR raises when deployed in public places and used this Opinion to set out the requirements of the law. In this document and the accompanying annex on DPIAs, she has set out how controllers considering using LFR should assess their compliance and make decisions.

Below the Commissioner summarises the key legal requirements for controllers; her recommendation to the wider industry, including technology developers and LFR vendors; and her next steps in her role as regulator.

5.1 Key requirements for controllers

Any use of personal data must be lawful, fair, necessary and proportionate. These are key requirements set by data protection law. Where the personal data in question is particularly sensitive, such as biometric data, there are stronger legal protections. Where the processing is automatic and there is a lack of choice or control for the individual, there are stronger protections. And where there are broader risks to individuals' rights and freedoms, there are stronger protections.

Together, this means that when LFR is used in public places for the automatic and indiscriminate collection of biometric data, there is a high bar for its use to be lawful. The Commissioner emphasises that any investigation or regulatory assessment by her office would be based on the facts of the case, considering the specific circumstances and relevant laws.

Summary of key requirements

- The controller must identify a specified, explicit and legitimate purpose for using LFR in a public place.
- The controller must identify a valid lawful basis and meet its requirements.
- The controller must identify conditions for processing special category data and criminal offence data, where required, and meet their conditions.
- The use of LFR must be necessary and should be a targeted and effective way to achieve the controller's purpose.

- The controller must consider alternative measures and demonstrate that they cannot reasonably achieve their purpose by using a less intrusive measure.
- The use of LFR must be proportionate and the controller's purpose should be of sufficient importance to justify any privacy intrusion or other impact on individuals.
- The LFR system should be technically effective and sufficiently statistically accurate.
- The controller should address the risk of bias and discrimination and must ensure fair treatment of individuals.
- The controller must be transparent and provide clear information about how they are processing personal data.
- The controller should undertake a DPIA.
- The controller's assessment must consider the risks and potential impacts of the processing on the interests, rights and freedoms of data subjects.
- The controller must ensure they comply with the data protection principles and are accountable for their use of personal data.

When using LFR for surveillance, controllers must:

- ensure the use of watchlists complies with data protection law and meets the same requirements of lawfulness, fairness, necessity and proportionality; and
- where there is collaboration with law enforcement, ensure roles and responsibilities (including controllership) are clear with appropriate governance and accountability measures in place. All parties must meet the specific legal requirements that apply whether under UK GDPR and DPA 2018 Part 2, or the law enforcement provisions under Part 3.

When conducting a DPIA, controller:

- should follow the guidance in the annex to this Opinion, undertaking the DPIA before the processing begins; and
- must consult the ICO if their DPIA indicates that the use of LFR would result in a high risk that the controller cannot mitigate.

Controllers should make diligent, indeed rigorous assessments against the legal requirements set out in this Opinion. The Commissioner expects controllers to be sure they can meet these requirements and to document their assessments and decisions before any deployment of LFR.

To be lawful, controllers must identify a lawful basis and a condition to process special category data and criminal offence data where required. They must meet the requirements of those key legal gateways.

In considering whether using LFR is fair, controllers must be transparent with people and protect them from any unjustified adverse impacts. They should be assured that the algorithms powering their systems produce sufficiently accurate results and address the risks of bias and discrimination. This Opinion sets out the key steps that controllers should take in designing, commissioning and operating an LFR system.

Controllers must be able to demonstrate that their use of LFR is reasonably necessary. It should be a targeted and effective way to achieve a specific purpose. Controllers must demonstrate that they have considered and, for good reasons, ruled out other less intrusive options. Controllers must not deploy LFR simply because it is available, improves efficiency, reduces costs or is part of a particular business model.

The use of LFR in public places must also be proportionate. Where LFR systems collect and analyse biometric data on an automatic and indiscriminate basis, potentially on a mass scale and without individuals' choice or control, this could represent a significant privacy intrusion. Controllers must articulate how their intended objective justifies their approach. As part of a DPIA, they need to assess the risks to the interests, rights and freedoms of individuals that could potentially arise as a result. This is not just about actual and obvious damage that could occur. It includes any potential for more intangible harm such as social disadvantage, or any inability for individuals to opt-out of the processing or access their data protection or other rights.

Controllers should consider privacy and data protection when procuring, purchasing or developing any LFR systems. They should ensure LFR products or services they adopt from vendors have been designed with appropriate data protection and privacy-preserving features built-in. Controllers, not technology vendors, are responsible for this under the law.

If the controller decides the processing can be justified, they must also comply with the data protection principles and allow individuals to exercise their data protection rights. The Commissioner expects to see high standards of governance, including clearly defined operating procedures and ongoing review processes. Any associated processing, such as compiling and maintaining watchlists, must also comply with data protection law.

5.2 Recommendations to industry

LFR is a fast-developing technology which could quickly become more widespread, without full appreciation of the long-term impacts for individuals and society. There is also potential for LFR to be used in novel ways. It could be

linked with other technological capabilities to enable more systematic monitoring and intrusive practices that could erode privacy and other rights.

The Commissioner recommends that technology developers, LFR vendors and service providers, and the wider industry should:

- put a data protection by design and default approach at the heart of any new developments;
- take steps to address and reduce the risks of bias and discrimination in LFR systems and the algorithms that power them;
- be transparent about the effectiveness of LFR systems and consider adopting common standards to assess and describe their statistical accuracy; and
- educate and advise controllers on how systems work and be transparent about the potential data obligations that controllers need to meet.

These steps will be crucial to building and maintaining the trust and confidence of the public.

5.3 The Commissioner's next steps

Following the publication of this Opinion, the Commissioner will:

- continue her investigative work. This includes cases focused on the use of LFR in retail, leisure and other public settings, the wider use of facial analytics in recruitment, and the extraction of biometric data from social media images;
- support organisations to make decisions on the compliance of LFR and FRT through advice and engagement. This includes providing advice on DPIAs where controllers identify risks which meet the threshold for prior consultation with the ICO;
- support organisations seeking to develop compliant approaches through data protection Codes of Conduct or certification schemes and, where appropriate, through the ICO's Regulatory Sandbox;
- conduct a proactive audit of LFR systems in deployment to assess compliance with UK data protection law as set out in this Opinion;
- stand ready to receive any complaints from individuals to ensure data protection rights are upheld; and
- continue to engage with Parliament, government, other regulators and industry on the application of data protection law, and collaborate with international partners on the principles governing the use of FRT worldwide.

In considering any regulatory action or use of her enforcement powers, the Commissioner may refer to this Opinion as a guide to how she interprets and applies the law. Each case will be fully assessed on the basis of its facts and relevant laws. The Commissioner may update or revise this Opinion based on any material legal or practical developments in this evolving area, such as judicial decisions and case law, or further findings from her regulatory work and practical experience. She may add to this Opinion to address specific LFR use cases or other applications of FRT.

Annex: Expectations on data protection impact assessments for live facial recognition in public places

1. Introduction

Section 4 of the Opinion sets out the key legal requirements of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA). This annex explains how organisations should assess compliance with those requirements within the framework of the data protection impact assessment (DPIA) process. It highlights some key considerations at each stage. It supplements and should be read alongside the ICO's detailed guidance on DPIAs.

2. The importance of robust evaluation

Any organisation considering the use of LFR is responsible for ensuring that its deployment complies with data protection law. They must also be able to demonstrate that compliance. This is the accountability principle, which is reflected in specific controller obligations under the UK GDPR.[57]

In effect, the law requires that organisations assess and are able to explain how their processing complies with data protection principles and obligations. They need to be able to show that they have considered all relevant issues and reached a justifiable conclusion.

In addition, the UK GDPR requires controllers to take a data protection by design and default approach.[58] This is particularly important in the context of LFR because many issues of fairness, necessity and proportionality need to be addressed during the planning and design stage of a system.

DPIAs are a key part of a controller's accountability obligations in this context. Conducting a DPIA is a legal requirement for any type of processing that is likely to result in a high risk to the rights and freedoms of individuals, in particular where it involves new technologies.[59] The UK GDPR is clear that a DPIA is required for large-scale use of special category data (including biometric data), or for systematic monitoring of a publicly accessible area on a large scale.[60]

---

[57] UK GDPR Articles 5(2) and 24
[58] UK GDPR Article 25
[59] UK GDPR Article 35(1)
[60] UK GDPR Article 35(3)

A DPIA also brings wider compliance and accountability benefits. It can be an effective way to assess and demonstrate compliance with data protection principles and obligations, and promote transparency and trust in the use of new technologies. The DPIA process supports controllers to focus on the key legal issues identified in the Opinion. These include establishing clarity of purpose, necessity and proportionality, lawfulness, fairness, and the impact on individuals.

The Commissioner therefore considers that any organisation considering deploying LFR in a public place should carry out a DPIA to decide whether or not to go ahead with a deployment.

3. Data protection impact assessments for LFR

3.1 Identify the need for a DPIA

The Commissioner's view is that any organisation considering deploying LFR in a public place should carry out a DPIA. This is because it is a type of processing which involves the use of new technologies, and typically the large-scale processing of biometric data and systematic monitoring of public areas. Even smaller scale uses of LFR in public places are a type of processing which is likely to hit the other triggers for a DPIA as set out in ICO guidance.[61]

If an organisation nevertheless considers that its intended use of LFR is a of a type which is small-scale and low-risk and does not require a DPIA, it should document this decision and the reasons for it. The Commissioner expects controllers to set out clear justifications for not carrying out a DPIA. They should refer clearly to the triggers set out in ICO guidance on when a DPIA is required.[62] The organisation also has to consider an alternative means of ensuring and demonstrating its compliance with the relevant legal requirements, as set out in the Opinion.

The DPIA should begin early in the life of the project, before any decisions are taken on the actual deployment of the LFR. It should run alongside the planning and development process. It must be completed prior to the processing, with appropriate reviews before each deployment. Controllers must consult the data protection officer (DPO) (if in post) and should clearly document their advice.[63]

Controllers should consider privacy and data protection when procuring, purchasing or developing any LFR systems. They should ensure LFR products or services they adopt from vendors have been designed with appropriate data protection and privacy-preserving features built-in. Controllers, not technology

[61] UK GDPR Article 35(4) requires the ICO to set out other kinds of processing operations for which a DPIA is required and the ICO has provided detailed guidance on when controllers need to do a DPIA.
[62] Ibid
[63] UK GDPR Article 35(2)

vendors, are responsible for this under the law. They should not deploy "off-the-shelf" solutions without adequate due diligence to understand the technical processing and associated privacy implications. For example, controllers need to consider whether an LFR system is designed with data subjects' rights in mind. They should have the capability to isolate and extract personal data in response to a subject access request, for instance. Controllers should also seek appropriate assurances from vendors on the statistical accuracy of the system and document them (see sections 3.6.1 and 3.6.2 below). These assessments are an important part of conducting a DPIA and need to be considered early in the planning process.

If and when controllers decide to deploy LFR, the Commissioner recommends that they keep their DPIA under review. The context in which the processing is taking place may change and controllers should take account of any practical experience implementing this technology. This could include any new evidence of its effectiveness, accuracy or any issues of bias, for example. Likewise, they should consider whether their supporting policies and processes are adequate and appropriate. They should continue to assess whether the use of LFR remains fair, necessary and proportionate as circumstances change. Controllers need to revise the DPIA if there is any substantial change to the processing.

3.2 Describe the processing

The controller must describe the nature, scope, context and purposes of the processing.[64] This description must be systematic and controllers should be as comprehensive as possible. It should describe the entire data lifecycle from collection to deletion. This description is crucial to properly understand the relevant legal requirements and assess the risks.

The ICO's guidance on how to describe the processing provides useful examples of the features that controllers should consider including in their description.

Controllers should pay particular attention to the nature and context of the place they propose to use LFR and the reasonable expectations of individuals accessing it.[65] They should be clear about how the technology they propose to use works in practice and highlight any relevant technical issues. They should note any current issues of public concern about the use of LFR which may be relevant to the assessment process.

---

[64] UK GDPR Article 35(1) and (7)(a)

[65] Reasonable expectations are particularly important where controllers are seeking to rely on the legitimate interests lawful basis. Recital 47 of the UK GDPR notes that: The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing.

The purpose of the processing is the specific reason why the controller plans to process the personal data. The description should include:

- the controller's purpose (including their legitimate interests where relevant);
- the intended outcome for individuals;
- the expected benefits for the controller; and
- the expected wider public benefits for society – considering both breadth (how many people benefit from the processing) and depth (the importance of that benefit).

3.3 Consider consultation

The UK GDPR requires that, where appropriate, the controller "shall seek the views of data subjects or their representatives."[66]

The Commissioner's view is that in most cases it should be possible to consult individuals in some form, and that this would be a sensible and beneficial step. An effective consultation process may help identify risks, increase transparency, and improve public engagement and trust in the deployment of LFR. Given that the deployment of LFR in public places may involve the collection of personal data of the general public (or a section of the general public), it is likely to be appropriate to carry out some form of general public consultation or targeted research. For example, this could involve market research with affected groups, contacting relevant expert, campaign or consumer groups for their views, or both.

Any consultation should be an objective process and controllers should be clear about the nature, scope, context, risks and impact of the processing. Controllers could consider adopting professional standards for any commissioned market research to help ensure quality and accuracy.[67] Controllers should also consider other sources of evidence which they have not themselves commissioned, accounting for the relevance and objectivity of those sources.

If an organisation considers that consultation is not appropriate, they should record this decision as part of the DPIA with a clear explanation. For example, if there is a valid concern that it would compromise commercial confidentiality, undermine security, or be disproportionate or impracticable.

The DPIA should include the results and outcomes of any consultation, describing the issues raised and any conclusions the controller has reached. If a controller decides to deploy LFR despite clear evidence of public objections, whether raised as part of the controller's consultation or wider public discussion,

---

[66] UK GDPR Article 35(9)

[67] For example, the Market Research Society oversees a set of professional standards for market research, including quality standards such as the Interviewer Quality Control Scheme

the DPIA should be clear about the reasons for disregarding the views of individuals.

3.4 Assess necessity and proportionality

The UK GDPR requires that a DPIA includes an assessment of the necessity and proportionality of the processing operations in relation to the purposes.[68] Key questions that controllers should consider, in order to assess the necessity of an LFR deployment in a public place, include:

- Does the LFR system operate effectively?
- Does LFR allow the controller to take particular action that otherwise would not be possible?
- Does the LFR system and subsequent action make a meaningful contribution to their overall objective?
- Does that action genuinely require the use of an LFR system and the collection of biometric data?
- What would be the impact if the LFR system was not deployed?
- Are there any reasonable alternative measures which do not require using personal data or biometric data?
- Could 'traditional' CCTV or other forms of surveillance which do not involve processing biometric data achieve the same result?
- Could alternative security measures (this could include a wide range of techniques, from electronic tags for high-value items to security staff, or access controls to certain premises) achieve the same result?
- Could alternative forms of advertising measurement or targeting achieve the same result?

Controllers must also be able to demonstrate that they have reached justifiable conclusions that their objectives could not reasonably be met by using less intrusive methods. The DPIA can be used to explain what other measures have been considered and whether they could provide a reasonable alternative method to achieving the controller's objective. If not, they should record the reasons why they have been ruled out. These reasons should be strong enough to justify the use of LFR as necessary.

To fully assess proportionality, controllers need to identify risks and assess the impact of the processing on individuals.

[68] UK GDPR Article 35(7)(b)

3.5 Identify and assess risks

The controller must assess the risks to the rights and freedoms of individuals.[69] Identifying and assessing the risks and potential impacts of LFR is a highly context-specific process. The controller should pay close attention to the specific circumstances of their proposed deployment as articulated in their systematic description of the processing.

The focus is on the potential for the deployment of LFR to cause any type of physical, material or non-material damage, and in particular any:[70]

- inability to exercise any legal rights (including but not limited to privacy rights);
- inability to exercise any specific data protection rights, including the right to be informed, the right of access and the right to object;
- inability to opt-out of the processing;
- loss of control over the use of personal data;
- inability to access services or opportunities;
- potential impact on individuals' ability to exercise their rights and freedoms in this public setting, such as freedom of expression, assembly and association, including any potential inhibiting effect (see below);
- potential impact on children, vulnerable adults, or others who may be less able to exercise their rights independently;
- potential discrimination or bias (including an assessment of the precision of the LFR system for different demographic groups, but also any other risk of discriminatory impact arising from the way the system will be used or targeted);
- reputational damage, social stigma or other non-material disadvantage that individuals may experience as a result of the use of LFR;
- financial loss or exploitation;
- physical harm; or
- any other significant economic or social disadvantage.

In assessing the wider risks and potential impacts, controllers should consider the relevance of concerns about LFR raised by some academics, civil society groups, and international organisations.

[69] UK GDPR Article 35(7)(c)
[70] See section 4.7 of the Opinion and UK GDPR Recital 75

Example concerns about the wider societal impact of LFR

Some academic studies, civil society groups, and international organisations groups have raised concerns about the potential for LFR to be used to interfere directly with human rights. For example, by targeting certain individuals due to their activities, behaviours, personal attributes or beliefs. There are also concerns about the wider inhibiting effect of LFR.

For example, in 2020 the United Nations High Commissioner for Human Rights published concerns about the effect of new technologies, and specifically facial recognition, on peaceful protests.[71] The report highlighted that facial recognition can dramatically reduce the "traditional" protections against being identified and singled out in an assembly. It highlighted that people can feel discouraged from demonstrating in public and freely expressing their views when they fear they could be identified and suffer negative consequences. The report calls for a moratorium on the use of facial recognition in the context of peaceful assemblies.

A number of studies and articles by academics have raised concerns that LFR may discourage or prevent people from exercising their rights freely and fully in public places due to fear of intervention, social stigma, or simply identification.[72] Such studies suggest that individuals may be more fearful or reluctant to participate in demonstrations, to express their political or religious views, to gather in certain groups, or even to express parts of their character. This inhibiting effect may be experienced differently and to a different extent by different social groups.[73]

At the time of publishing this Opinion, the Commissioner has not encountered settled evidence on the impact of LFR on communities or wider society, but controllers should consider the relevance of these concerns in the specific context of their processing.

---

[71] *Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests*, UN High Commissioner for Human Rights, June 2020
[72] See for example *The Watchers Assaults on privacy in America*, Jonathan Shaw, Harvard Magazine, January 2017; *Live facial recognition: the impact on human rights and participatory democracy*, Dr Daragh Murray, University of Essex, blog November 2019; and The Human Rights, Big Data and Technology Project Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology, Professor Pete Fussey & Dr.Daragh Murray, July 2019; as well as studies citing such concerns from the UK's Centre for Data Ethics and Innovation and Biometrics and Forensics Ethics Group. For wider background on the inhibiting effect of surveillance, see for example Internet Surveillance, regulation, and chilling effects online: a comparative case study, J W Penney, Internet Policy Review, May 2017. The Commissioner has had due regard to the nature and status of these studies and articles when preparing this Opinion.
[73] See for example Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data, Dr Daragh Murray and Professor Pete Fussey, Israel Law Review published online by Cambridge University Press, February 2019

To assess whether the risk is a high risk, controllers need to consider both the likelihood and severity of the possible harm. Harm does not have to be inevitable or proven to qualify as a risk or a high risk. It should be more than remote, but any significant possibility of very serious harm may still be enough to qualify as a high risk. Equally, a high probability of widespread but more minor harm may still count as high risk.

As noted above, the risks, their likelihood and severity will vary depending on the specific nature, scope, context and purpose of the processing. Controllers should consider the risks of both the ongoing operation of the LFR system (including the automatic collection and analysis of biometric data) and the risks of any interventions made based on the result of that system.

3.6 Identify measures to mitigate those risks and measures to ensure compliance

The controller must then identify specific measures to address the risks identified. These measures will vary depending on the scope and context of the processing. The controller should seek advice from the DPO (if in post) and record whether the measure would reduce or eliminate the risk.

Controllers should also identify measures to ensure compliance with data protection principles and obligations.[74] As part of accountability requirements the Commissioner expects controllers to specify:

- the lawful basis for the processing;
- the appropriate condition(s) permitting the processing of special category data and criminal conviction data, where required. This also includes an explanation of how the deployment satisfies the specific requirements of the condition (where relevant, this includes that the processing is necessary for a specific reason of substantial public interest);
- any measures taken to ensure the fairness of the processing in terms of statistical accuracy and false-positive matches, potential algorithmic biases, and other technological issues (see section 3.6.1);
- how they will ensure purpose limitation and prevent any "function creep" involving new processing which has not been subject to the same assessment as the original purposes;
- how they intend to ensure data quality;
- how they intend to ensure data minimisation;

[74] UK GDPR Article 35(7)(d)

- how privacy information will be provided to individuals (including signage and other more extensive forms communication and promotion where required);
- how they will enable individuals to exercise their rights;
- how they will ensure any processors comply;
- how any watchlists being used comply with data protection law;
- safeguards for any international transfers; and
- where applicable, any obligations under the Equalities Act 2010 (including equalities impact assessments for relevant organisations) and whether these have been met.

It is especially important that controllers set out clear processes and policies governing their use of LFR, including:

- the circumstances in which the controller may activate the LFR system;
- clear criteria and governance for any watchlists;
- well-defined procedures for intervention in the event of a match and clear escalation measures;
- how data subjects can complain, how controllers will handle complaints, and how they will fulfil the public's data protection rights; and
- processes to continually monitor the impact of the LFR system and assess whether it continues to be fair, necessary and proportionate.

3.6.1 Measuring technical effectiveness and statistical accuracy

As part of their consideration of risks and mitigations, controllers should closely consider the technical effectiveness of the LFR system they propose to use. In particular they should focus on statistical accuracy. As set out in section 4.6 of the Opinion, this is an important part of demonstrating that their use of LFR is necessary and fair.

LFR systems compare biometric templates extracted from facial images to allow the identification or categorisation of an individual. This is done by creating a similarity score between the "live" image and the watchlist or category template. This score is a numerical representation of the likelihood that two faces are the same. The algorithm which performs the matching needs to be statistically accurate to make reliable estimates. Most systems permit the user to create a threshold score, which must be met or exceeded for two images to be considered a match.

This threshold score influences the statistical accuracy of the system. This can be measured with reference to false positives and false negatives:

- A false positive result occurs when the LFR system incorrectly identifies a positive result for an individual (eg incorrectly matching an individual to someone on a watchlist, or categorising them incorrectly).
- A false negative result occurs when the LFR system incorrectly identifies a negative result when it is actually positive (eg the system fails to detect a match, or fails to categorise an individual in a relevant category).

It is important that controllers strike the balance between these two types of errors. The ICO's guidance on AI and data protection recommends two useful measures:

- Precision: the percentage of positively-identified cases that are in fact positive. For example, if nine out of 10 matches to a watchlist are correct, the precision of the LFR system is 90%.
- Recall (or sensitivity): the percentage of all cases that are in fact positive that are identified correctly. For example, if 10 out of 100 people detected by an LFR system are actually included on a watchlist, but the system only identifies seven of them, then its recall is 70%.

Precision is important so that people are not identified incorrectly and subject to any detriment as a result. However, recall is also important. If an LFR system fails to identify the individuals which it is meant to and is ultimately ineffective, then the processing of personal data may not be necessary. This could mean that the data collected is excessive and the collection of biometric data is unjustified.

The law does not stipulate a specific threshold for precision or recall. This is for the controller to establish to ensure their processing is necessary, proportionate and compliant. It is good practice to establish these thresholds in the DPIA. In the Bridges case, the ability of the police force's LFR system to accurately identify persons of interest was a factor in the Divisional Court's finding that any interference with the claimant's ECHR Article 8 rights was proportionate in those circumstances.

These issues should be considered in the design or procurement process for controllers' own LFR system or any system purchased from or outsourced to a third party. Overall, controllers should:

- ensure the statistical accuracy of any LFR system is sufficient to fulfil their purposes;
- engage, seek assurances and where necessary challenge technology vendors to provide further information on the statistical accuracy of the LFR system and how thresholds are set;
- seek assurances and make decisions on statistical accuracy, including by:
    - considering the likelihood of false positives arising from the LFR system;

- considering the potential adverse impact of false positives on individuals who are identified or categorised incorrectly;
- setting appropriate statistical thresholds for facial matches to manage the risk of false positives occurring;
- balancing the precision and the recall or sensitivity of the system; and
- setting out clear measures to mitigate the effects of false positives, such as human review of facial matches and clear processes for individuals to challenge a match or subsequent intervention; and

- record their decisions on these matters as part of the DPIA, in line with the accountability principle.

These measures will help controllers to fulfil their data protection by design and default obligations.

More broadly, the Commissioner recommends that technology vendors and wider industry considers standardisation on how accuracy is described and measured to enable controllers to make informed decisions.

3.6.2 Measures to address bias

Section 4.6 of the Opinion explains the risk that LFR systems may perform with less precision for some demographic groups, such as women, minority ethnic groups and potentially disabled people. Such biases could lead to detriment or damage to an individual or group. As part of the DPIA process, controllers should address this risk and follow the steps set out in the Opinion, namely:[75]

- consider the risk of bias, discrimination and the unfair treatment of different demographic groups during the design, commissioning or procurement process of any LFR system. This includes, where warranted, seeking assurances from vendors and justifying and recording their decisions on these issues;
- ensure that the LFR system has been subject to robust testing and account for the results of this testing in their decisions and processes;
- where applicable, fulfil their obligations under the Equalities Act 2010 and consider whether an Equalities Impact Assessment is required;
- consider whether the system is appropriate for use and, if they implement the system, what adjustments and safeguards or mitigations they need; and
- monitor the outcomes of the system, including for any evidence of bias or discrimination, and adapt their approach based on their findings.

[75] More detailed recommendations are provided in the ICO's guidance on AI and data protection, "How should we address risks of bias and discrimination?"

3.7 Outcomes and decisions

The controller must then assess whether the deployment of LFR can be justified as necessary and proportionate, fair, and lawful. They need to take into account all the factors above, including the benefits of the processing and the risks to rights and freedoms of individuals.

If relying on the legitimate interests lawful basis, the controller must be able to demonstrate that the objectives of the LFR system are not overridden by the interests or fundamental rights and freedoms of individuals. But even if the controller is relying on a different lawful basis, a similar assessment will still be required. They need to demonstrate that the deployment of the LFR is fair and proportionate in the circumstances, and that the benefits justify the risks and impact on individuals.

In reaching their decision, controllers should consider:

- all elements of data protection law which apply to their proposed processing;
- the independent advice provided by the DPO (where in post) and the controller's response to that advice;
- whether the proposals should be adapted or changed based on the findings of the DPIA;
- whether the processing should proceed based on the results of the assessment; and
- whether consultation with the ICO is required (see below).

A controller may believe that some risks are acceptable given the overall benefits of the processing and the difficulties of mitigation. However, if there is still a high risk which cannot be eliminated or significantly reduced, the controller must consult the ICO for approval before it can deploy the LFR system.[76]

Controllers can find more information about when and how to consult the ICO as part of our detailed guidance on DPIAs.

If and when controllers decide to deploy LFR, the Commissioner recommends that they keep their DPIA under review, as discussed in section 3.1. They should continue to assess whether the use of LFR remains fair, necessary and proportionate as circumstances change. Controllers need to revise the DPIA if there is any substantial change to the nature, scope, context or purposes of the processing.

[76] UK GDPR Article 36