# Facial recognition, fingerprint technology, and the GDPR: An essential pre-purchase guide for employers

IMPACT PRIVACY

Bringing privacy to life

# Foreword

Many things sound like a great idea until, with the benefit of advice (and hopefully not hindsight), the problems become obvious. The use of facial recognition technology (and other biometrics, like fingerprints) in the workplace is one of those "great ideas".

However, few (if any) biometric technology vendors provide customers with a real and honest insight into the data protection requirements that must be fulfilled in order to use their technologies. This insight should always start by making it clear the use of biometric data is prohibited under the GDPR, and that achieving lawful use is not easy.

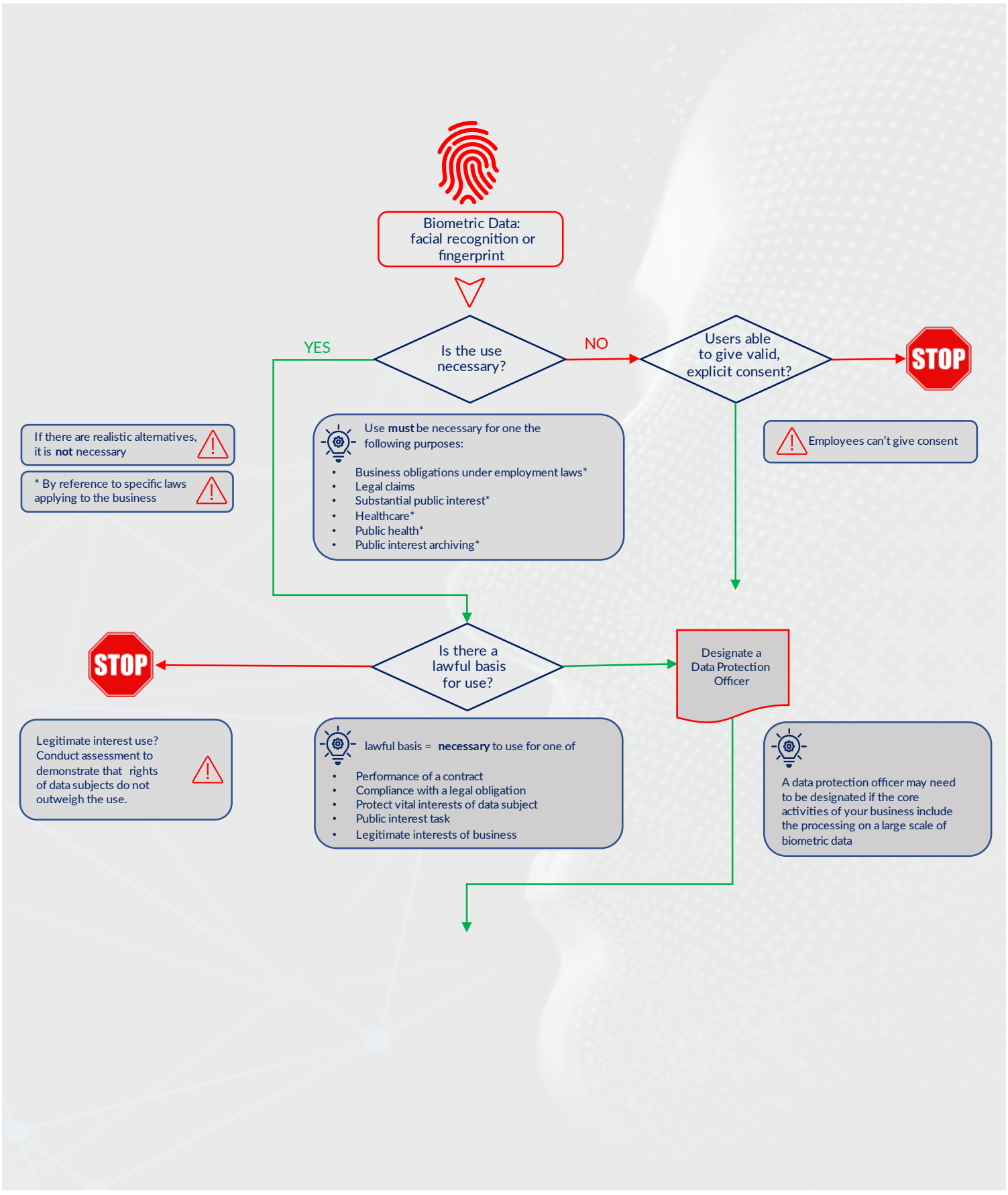
This really frustrates us, and not only because of how often we see businesses getting things wrong. We know the huge financial risks they could be facing – risks that could end up destroying their business entirely.

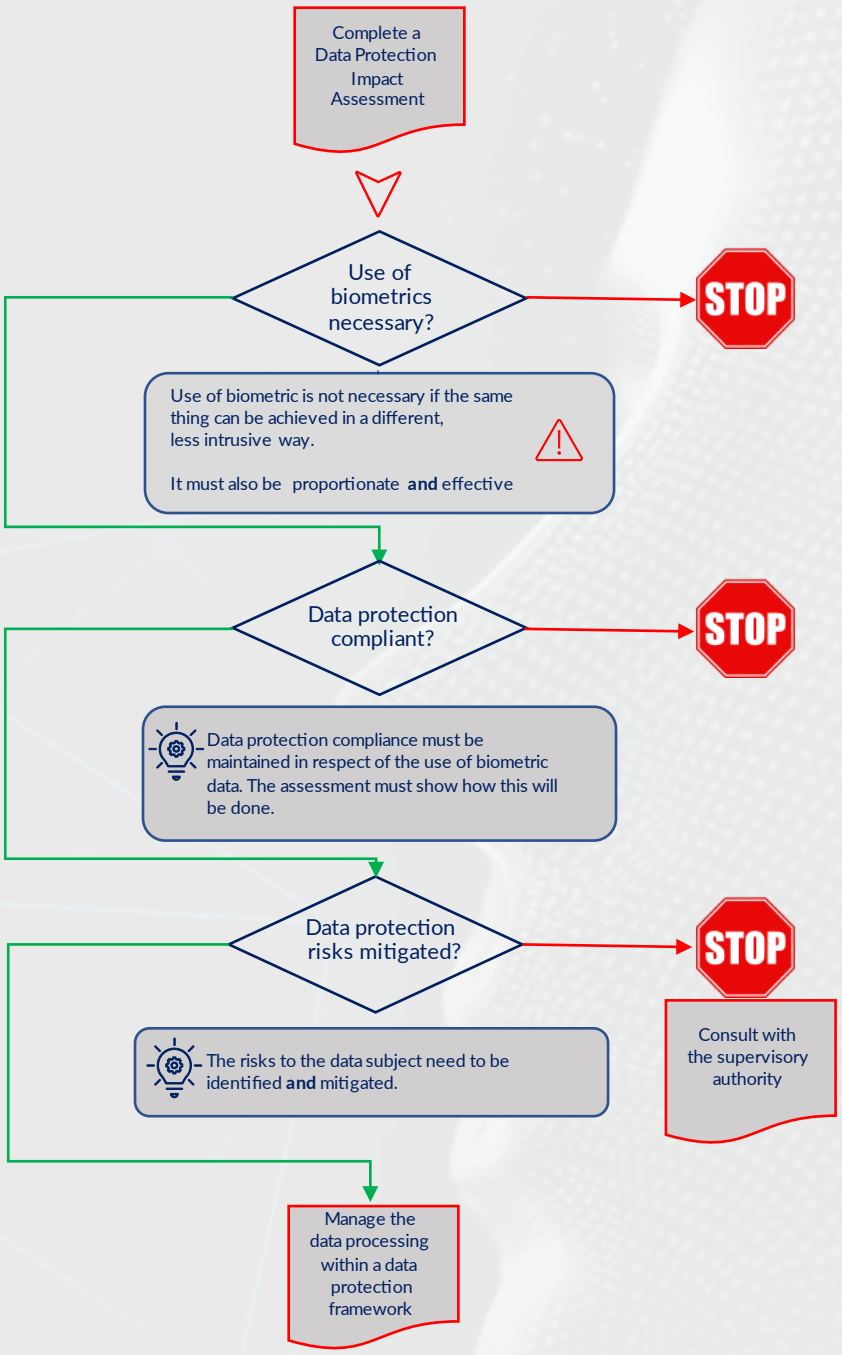
So, we want to help put things right. In this short, but essential, guide we summarise the key data protection hurdles that **must** be overcome before committing to biometrics. The aim is to help your business, as a data controller, understand the risks better and so take steps to avoid making expensive mistakes which it may quickly come to regret.

We have also included a graphic for those who want a simple overview to help them get things in perspective and ask the right questions from the outset

The Impact Privacy Team
May 2020

# Facial recognition or fingerprint technology in the workplace
# Key data protection steps for biometric data use




Complete a Data Protection Impact Assessment
Use of biometrics necessary?
STOP
Use of biometric is not necessary if the same thing can be achieved in a different, less intrusive way.
It must also be proportionate and effective
Data protection compliant?
STOP
Data protection compliance must be maintained in respect of the use of biometric data. The assessment must show how this will be done.
Data protection risks mitigated?
STOP
Consult with the supervisory authority
The risks to the data subject need to be identified and mitigated.
Manage the data processing within a data protection framework

# Hurdle #1: The use of biometric data is prohibited under the GDPR

It is worth asking your facial recognition or fingerprint technology vendor what restrictions there are on using biometric data. What they should say is that its use (or "processing") is **prohibited** by the GDPR. They should then tell you the penalty for contravening this prohibition is a fine of up to €20 million, or 4% of turnover (whichever is greater).

Of course, there are a small number of narrow exceptions to this prohibition. These are known as "conditions". However, as your vendor should tell you, these are incredibly difficult to meet, and most require the use of the biometric data to be "necessary".

## Necessary use conditions

The following conditions permit the use of biometric data, provided the processing is **necessary**:

- for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State Law;
- to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- for reasons of substantial public interest, on the basis of Union or Member State law;
- for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law;
- for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law; or
- for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law.

For most of these conditions, the purposes must **also** be authorised by law. The purpose of the processing must itself have a separate basis in law which can be specifically referred to or referenced as requiring the processing to be undertaken.

**If you cannot meet one of the necessary use conditions, you may not be able to use the biometric technology unless you get your employees' (or other data subjects') explicit consent.**

### How is necessity determined?

The necessity of processing must be determined objectively. It is not a measure of necessity from the perspective of the data controller, and the perspective of the data subject must be considered. This means necessity will not usually be a measure of desirability, convenience, or cost. Instead, necessity is considered in the context of whether there are realistic, less intrusive alternatives. If so, the processing is not necessary, and so the condition cannot be met.

## Consent condition

Whilst there are two conditions that do not carry a necessity requirement, they are irrelevant in all but the most specific circumstances. Consequently, the difficulties in demonstrating necessity mean employers often attempt to rely on the one remaining condition: that the data subjects (usually the employees) have given their explicit consent.

The standards required by the GDPR for valid consent means this is actually a far more difficult condition to meet than it might sound:

- the data subject must be told very clearly and explicitly exactly what their personal data is going to be used for before the consent is provided; and
- the consent must be related specifically to that use and only that use; and
- the consent must have been given unambiguously (without any possibility the consent was given other than deliberately); and

- the data subject cannot have been coerced, compelled, or forced into providing the consent.

Underpinning this is the requirement that data subjects must be provided with real choice as to whether to consent or not.

### Employees cannot give consent

For the use of biometric data in the workplace, the single biggest issue is that employees cannot provide consent:

"[The European Data Protection Board] *deems it problematic for employers to process personal data of current or future employees on the basis of consent as it is unlikely to be freely given. For the majority of such data processing at work, the lawful basis cannot and should not be the consent of the employees… due to the nature of the relationship between employer and employee.*"

**As an employer cannot obtain valid consent from employees, if it cannot rely on one of the other conditions to the lawful use of biometric data (including by reason of the necessity of use), then the use of the biometric data will be unlawful under the GDPR. At best, enforcement action could compel your business to cease using the technology. At worst, your business could receive a devastating fine.**

## Case study: workplace time management systems ("TMS")

An increasing number of TMS providers are promoting the benefits of facial recognition technology (or "FRT") in time and attendance management, and actively promoting FRT as a way of overcoming perceived weaknesses in traditional systems. In a recent example, an employer turned to FRT to avoid the need for employees to handle pens as part of a manual signing in process, ostensibly to reduce the risk of cross-infection from COVID-19.

As we have discussed, the first consideration must be whether there is a lawful basis for using the technology at all, in the context of the general prohibition on the use of biometrics.

Even in the case of using FRT to help avoid the risks of viral cross-infection, it is extremely difficult to see how any of the necessity conditions in the GPDR permitting the processing of biometric data could be applied. Employers might often seek to claim the following condition:

"*processing is necessary for the purposes of carrying out the obligations and exercising the specific rights of the [employer] or of the data subject in the field of employment …. law in so far as it is authorised by Union or Member State law … providing for appropriate safeguards for the fundamental rights and the interests of the data subject.*"

There are a large number of legal obligations applying to an employer requiring the accurate recording of an employee's time and attendance at work, or the protection of an employee from health & safety risks. These could be used to justify the use of FRT (or indeed any other biometric technology). However, the processing must also be: (i) necessary; **and** (ii) authorised by law.

In terms of necessity, it will only be in the rarest of cases where the use of FRT meets this high standard. In our example of seeking to avoid cross-infection, in circumstances where workers are being compelled to wear protective gloves the argument that FRT is necessary to avoid the risk associated with sharing a pen looks very weak. Where it can be demonstrated as being necessary, the processing must then be specifically authorised by law. This can be challenging.

This means the only route left open for employers wishing to use biometric data in time and attendance systems is to seek "explicit consent". However, employers are not in a position to be able to obtain valid consent from employees unless in the specific circumstances they can show the consent of the employee really was freely given. At the very least, this will require being able to show alternative means of achieving the same purpose were readily available (giving rises to issues of proportionality – which we discuss later), and that there was absolutely no detriment to an employee in using those alternative means.

## Hurdle #2: Lawfulness of processing

Even where a condition for use can be applied, users of biometric data must then ensure they can **also** apply one of six lawful bases for processing personal data set out in Article 6 of the GDPR.

### Consent

Where explicit consent is the valid condition, the corresponding lawful basis for processing will also be consent, which can be applied without any additional difficulty.

### Other lawful bases

However, if another condition has been adopted it may be difficult to decide which of the remaining five lawful bases of processing is the most appropriate to use:

- performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering the contract;
- compliance with a legal obligation to which the controller is subject;
- to protect the vital interests of the data subject;
- performance of a task carried out in the public interest; or
- for the purposes of the legitimate interests pursued by the controller or third party.

In each case a demonstration of the necessity of processing for the particular purpose will be also required.

### Legitimate interests

This is often considered an easy "catch-all" by data controllers to facilitate the use of personal data when otherwise it would not be lawful. However, apart from the processing having to be "necessary" for the legitimate interest, the interests of the data subject can override the interests of the data controller.

As the GDPR makes clear, "*the existence of a legitimate interest [needs] careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place.*"

This assessment requires a formal three-part test to be completed:

- identify the legitimate interest;
- show the processing is necessary to achieve that interest; and
- show it is not outweighed by the interests, rights and freedoms of the data subjects affected.

This is an exercise that needs incredibly careful consideration.

**Even if a condition for processing biometric data is met, if a lawful basis for processing cannot be established, the biometric data cannot be used.**

## Hurdle #3: Appointing a data protection officer

The GDPR requires a data protection officer to be designated where the core activities of your business include the processing on a large scale of biometric data. Depending on the number of employees your business intends managing using biometric data, and whether the management of those employees is a core activity, you may be required to designate a data protection officer.

If so, the person designated must have the professional qualities and expertise required to enable them to fulfil the tasks they are responsible for under the GDPR. They must report directly to the highest level of management, and they must not have a conflict of interest. The requirement cannot be met by designating a junior member of staff who has attended a one-day course on data protection. Equally, it can't be another job title for a senior member of staff.

### Case study: Business fined €50,000 for DPO appointment

A business attempted to meet the requirements of the GDPR by designating a head of department as the data protection officer. The department head was qualified as a compliance and legal professional. However, because the designation was in addition to their other duties there was a conflict of interest, in breach of the GDPR.

# Hurdle #4: The Data Protection Impact Assessment

Having determined that the particular use of biometric data is likely at least to have a lawful basis, the business (with the help of the Data Protection Officer) will also be required to complete a data protection impact assessment. The purpose of this assessment is to evaluate the risks associated with the use of biometric data through:

(i) a systematic description of the processing and its purposes including, where applicable, the legitimate interest pursued by the controller;
(ii) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
(iii) an assessment of the risks to the rights and freedoms of the affected data subjects; and
(iv) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of the personal data and to demonstrate compliance with the GDPR.

## Assessing necessity and proportionality

The necessity for the use of biometric data needs to be considered to establish the lawful basis for its use under the GDPR. However, even if necessity is not critical to lawful use (because of the reliance on consent), where the processing of biometric data is not necessary because the same thing can be viably achieved in a different, less intrusive, way the use of biometric data will be disproportionate.

### Proportionality

There must also be a balance between the intended aim, and the means used to achieve it. So, when considering proportionality, the data processing must be proportionate by reference to its effectiveness, its scale and because, overall, its benefits outweigh the privacy rights of the individual data subjects affected.

### Effectiveness

Clear evidence may be required to demonstrate objectively the use of biometric data is effective in meeting the specified purposes it is being used for. This evidence should be both quantitative and qualitative, and may require the business to go to some lengths to establish it. This is an area where your vendor should be providing help and guidance.

### Scale

The more broadly the use of biometric data is applied, the less likely it is to be proportionate. For example, the use of biometric data in access controls may be necessary and proportionate to facilitate restricted access to controlled drugs within a pharmaceutical facility, but extending the access controls to all other areas is likely to be disproportionate unless it is targeted and risk-based.

## Case study: Monitoring attendance at a school

A school used FRT as part of a pilot project to assess how it could be used to automate the class registration process and save teaching time. The school took a number of measures designed to ensure their use of FRT in the pilot complied with the GDPR and data protection legislation. However, the data protection authority compelled the school to stop the pilot and issued them with a fine of €19,000.

One specific problem was that, even with the explicit consent of the parents, the use of FRT was seen as disproportionate to the purpose. Put simply, you can easily register attendance in class in any number of ways, and the use of FRT was simply a proverbial hammer to crack a nut.

## Ensuring data protection compliance

An important step in the data protection impact assessment is documenting how data protection compliance will be maintained in respect of the use of the biometric data. This means understanding:

- the lawful basis for the processing (as already discussed);
- how function creep will be prevented;
- how data quality is assured;
- how data minimisation is attained;
- how affected individuals are provided with information about the use of their biometric data, meeting the requirements of the GDPR;
- how individuals' rights can be exercised and supported;
- how data processors (such as your technology vendor) are managed;

- the safeguards against breaches of confidentiality, availability, or integrity of the biometric data systems; and
- the safeguards to be used for international transfers.

### Assessing likelihood and severity of risks to individuals' rights and interests

Before biometric data can be used, the risks to the relevant data subjects' rights and interests need to be assessed and, where impactful risks arise, they must be mitigated or eliminated. Those risks could be physical, mental, or material, and include things such as:

- the inability to exercise rights, access services, or take advantage of opportunities;
- the loss of control over the use of personal data, or the loss of confidentiality;
- discrimination (which in the case of biometric data, depending on its intended use, can be a significant risk in the context of potential racial and gender bias);
- identity theft or fraud, or financial loss;
- reputational damage;
- physical harm; or
- other economic or social disadvantage.

The risk assessment needs to be considered, from the perspective of the data subject (the person affected), and consider the likelihood of harm arising, and the resulting severity of the harm on the individual.

### Mitigating risks

Once the risk has been assessed, mitigating measures need to be identified. These can include everything from not undertaking the processing activity at all, reducing the nature or scope of the activity, or making other changes that reduce the risk to the individuals.

What is critical is that the risks and mitigating measures are considered objectively, with consultation where appropriate. Of course, the mitigating measures then need to be documented, adopted, and implemented.

**Your technology provider must be prepared to be able to help you with the completion of the data protection impact assessment. They should know what the assessment is for, why it is needed, and should be readily able to provide you with the information you need to assess their technology, systems, and applications. If they can't do this, or simply say their systems are "GDPR compliant". find another vendor immediately.**

### Consulting the supervisory authority

Where the risks associated with the use of biometric data remain high (either because mitigating measures are not adopted, or because it is not possible to mitigate the risks), the supervisory authority must be consulted before its use commences.

The consultation process gives the supervisory authority the ability to provide written advice on the proposed use, which may include clear instructions that it cannot be used in connection with the proposed purpose, or (for example) that it can only be used in certain ways.

### Case study: Monitoring attendance at a school (2)

In addition to using FRT disproportionately, the data protection impact assessment the school undertook did not amount to a proper assessment of the risks associated with the use of FRT. Critically, had that assessment been conducted properly, the school would have consulted with its data protection authority – which it did not.

## And finally… Managing your data protection programme

Even if you are able to overcome the four main hurdles to the use of biometric technology in your workplace, this must be in the context of a well-managed data protection programme. If it is not, your business will not be able to meet the principles relating to the processing of personal data set out in the GDPR.

So, the use of biometric data should only ever be considered when the business is already capable of demonstrating compliance with these principles. This means the business should have a framework for data protection that includes:

- a documented assessment of organisational data protection risks and how the risks are addressed;

- a clear commitment to data protection compliance from the top, reflected in the resources given to managing the risk, and the awareness of everyone in the business of their responsibilities;
- a comprehensive catalogue of the personal data it processes and for each data processing activity a complete understanding of the lawful basis of compliance and the measures in place to address compliance;
- suitable policies, procedures, and systems to underpin the compliance framework, minimise the amount of personal data used, and support data subject rights;
- appropriate means for securing personal data against breaches of confidentiality, integrity, or availability, and for responding to breaches should they occur; and
- technical and organisational measures to protect personal data and ensure compliance.



*Impact Privacy delivers complete privacy and data protection solutions to micro, small and medium-sized businesses. Our services include privacy risk management, privacy solutions and the provision of privacy operations.*


info@impactprivacy.com


Europe: +353 (0)1 554 1189
Americas: +1 800-909-1189


www.impactprivacy.com