Information Commissioner’s Office

Call for views on employment practices and data protection

Summary of responses

Contents

Introduction

Between August and October 2021, the ICO ran a call for views seeking stakeholder and public input into future guidance on data protection and employment practices. This document summarises the key themes emerging from the responses we received.

Since the employment code of practice was published, the world of work has changed considerably. Technology, employment relationships, data protection law, the UK leaving the EU and the COVID-19 pandemic have all impacted on working practices. This was reflected in the responses we received.

We received 144 written responses to the call for views. We are grateful to those who took the time to comment. We received responses from a range of groups, including private, public and third sector organisations and members of the public.

We are carefully considering the responses and are using them to inform the production of the new guidance.

General themes

We received a wide variety of both general and detailed issues. It is not possible to cover every point in detail that was raised as a result of the call for views. However, several key themes did emerge from the responses, which we summarise below.

Many respondents raised general themes that cut across a range of topics. We then go on to summarise more topic-specific themes in the following sections.

Approach to updating the guidance

In the call for views document, we explained that we want to replace the existing employment practices guidance (the 2011 employment practices code, supplementary guidance and quick guide) with a new, more user-friendly online resource with topic-specific areas. We explained that we want to make sure that the new guidance:

- addresses the changes in data protection law;
- reflects the changes in the way employers use technology and interact with staff; and
- meets the needs of the people who use our guidance products.

We think the new guidance should retain the four main topic areas from the code and asked for views on this approach. The four topic areas are:

- recruitment, selection and verification;
- records;

- monitoring; and
- health.

While the vast majority of respondents generally agreed with this approach, many noted that employment practices and data protection law have changed significantly over time. Respondents thought the guidance would need to address other topic areas and focus on emerging issues and new developments. They suggested some cross-cutting topics having their own sections or giving prominence to particular content.

Several noted that the guidance should reflect the greater range of employment relationships and settings, such as the gig economy or remote working. They also thought the guidance should cover every aspect of the employment relationship where employers use personal data, as well as the different stages of employment. It was also suggested that the guidance should address the many changes in the world of work, such as:

- different recruitment methods;
- increased technological complexity; and
- the increasingly data-driven nature of work.

Others suggested a different approach, such as structuring the guidance according to the data protection principles with a focus on data protection by design.

Several respondents suggested consolidating the existing employment guidance into a single resource but retaining a quick guide for SMEs. They thought it could be beneficial to take a layered approach, with the essentials for those with less expertise in data protection but with more detail available if needed. Some noted that the guidance should not just be aimed at employers, but that it should be accessible to workers too.

Some respondents thought that the guidance should take the form of a web-based resource, keeping it consistent with other ICO guidance. This makes it easy to search and access information and can link to other relevant guidance. Some respondents also felt that it was important that the guidance is kept up-to-date, given the pace of change. They also felt that it should be made clear when we were updating the guidance. It was noted that the ability to download a document for offline use would be useful, if needed.

Several respondents felt we should establish a working group. They also believed there should be continuing consultation and engagement with stakeholders to help with the development of the guidance.

ICO’s response

We recognise there have been significant developments in both employment practices and data protection law since we published the original guidance. We also recognise there are areas and issues not previously covered that we need to address; we intend to provide guidance on these where appropriate. We set out more detail about how we intend to do this below.

Several respondents referred to the ICO needing to issue a new employment code of practice. We would like to clarify that we have no plans to issue a new code of practice in this area. This is primarily because having guidance known as a code, that is neither a ICO statutory code of practice nor an Article 40 code of conduct, would risk confusion amongst stakeholders.

Instead, we plan to create a hub of guidance covering various employment topics and issues. We intend to take a web-based approach to the hub, consistent with the format of other ICO guidance. The hub will be flexible, make relevant guidance easier to find and content can be added to over time. We will carefully consider how we present and communicate this information.

We intend to involve stakeholders in the development of new guidance products. We will do this in a variety of ways, including consultations on significant pieces of guidance as we develop them. We will provide updates on this process on the ICO website, including opportunities to provide comments on new products.

The impact of the COVID-19 pandemic

A key theme respondents reported as having generally affected employment practices is the impact of the COVID-19 pandemic. Respondents noted how addressing the pandemic has had significant consequences for many aspects of how we work, leading to:

- greater prevalence of home working for some workers;
- changing how employers keep in touch and monitor the performance of their workers remotely;
- the collection of greater amounts of health data; and
- changing recruitment practices (such as virtual interviews).

In some cases, the pandemic accelerated existing trends, such as greater use of AI and monitoring technologies. Where relevant, we discuss themes relating to the impact of the pandemic in the various topic areas below.

ICO’s response

We appreciate the pandemic has had a major impact on many aspects of working life, as well as significant implications for the use of personal data. We provide guidance on many issues, including those that affect employment practices, on our data protection and coronavirus information hub. We intend to incorporate and build on coronavirus content relevant to employment practices in our updated employment guidance.

We recognise that the pandemic is likely to have a lasting impact on employment practices, including accelerating changes that were already taking place. We intend the future employment guidance hub to reflect these trends and to provide consolidated guidance. Our aim, as far as possible, is to produce future-proof guidance that lasts beyond the pandemic.

Lawful basis and conditions for processing

Many respondents noted the need to identify valid grounds for collecting and using personal data in a variety of employment contexts and circumstances. Respondents considered that the guidance should address issues of:

- identifying a lawful basis under Article 6 of the UK GDPR;
- conditions for processing special category data under Article 9; and
- criminal offence data under Article 10.

A particular concern raised was over the role of consent, given the power imbalance between employer and worker. They would like the guidance to address these issues. More topic-specific themes on lawful bases and conditions for processing are detailed below.

ICO's response

Data protection law has changed significantly since we published the existing employment guidance, with the introduction of the UK GDPR and DPA 2018. Our guide to data protection covers in detail the requirements around lawful basis for processing personal data, as well as conditions for processing special category data and criminal offence data.

However, whilst the existing employment guidance is still useful, we recognise that it needs updating to reflect these changes in data protection law. The guidance needs to include information on identifying a lawful basis for processing personal data, as well as conditions for processing special category and criminal offence data. The new employment guidance will aim to provide further context for employers and, where appropriate, will include relevant employment case studies and examples.

Data sharing

Data sharing and disclosure of personal data was also an area that many respondents were keen for us to address in more detail.

Respondents were concerned that employers did not always make it clear that they may share personal data with third parties, such as occupational health providers, trade unions, regulators and processors. There were also concerns about personal data being transferred outside of the UK, particularly involving multinationals or third parties based in other countries.

Many respondents believed that employers should demonstrate greater transparency about who they share personal data with and their lawful basis for doing so. Some suggested that the guidance should address how data protection law interacts with other legislative requirements, such as employment law and health and safety regulations. Where employers shared special category data (such as health data) or criminal records, they also need to consider the appropriate conditions for processing.

It was felt that clear privacy information could address this issue. Some respondents suggested including examples and templates in the guidance to demonstrate best practice.

Several respondents wanted to see updated guidance on Transfer of Undertakings (Protection of Employment) Regulations 2006 as amended by the Collective Redundancies and Transfer of Undertakings (Protection of Employment) (Amendment) Regulations 2014 (TUPE), to reflect changes in data protection law.

Respondents also felt it would be beneficial to cover situations involving disclosure of worker information within an organisation.

ICO’s response

We recognise that sometimes organisations may find it difficult to know when they can share personal data in a compliant way – especially with the increased involvement of third parties in the employment relationship. Data protection should not be seen as a barrier to appropriate data sharing, including in an employment context.

In order to address some of the issues organisations face around sharing personal data, we produced a data sharing code of practice and a data sharing information hub. However, we will look to add more bespoke employment content, including relevant examples and case studies.

We intend to publish updated TUPE guidance in due course.

Data protection rights of individuals

Many respondents requested more emphasis on the rights of workers. They believed employers were not always clear as to how workers could exercise their data protection rights, such as the rights of access, erasure and objection. They felt the guidance must reflect the changing nature of the employment relationship, particularly to accommodate those working in the gig economy and other non-traditional forms of employment.

ICO's response

The introduction of the UK GDPR and DPA 2018 brought stronger data protection rights for individuals. Our new guidance will reflect these changes.

We do have existing guidance for both organisations and individuals on these rights. However, we recognise that the new guidance should cover these changes, so that employers can understand their obligations.

We will consider producing bespoke employment practices guidance, aimed at workers, to assist people to understand their information rights at work.

Data protection impact assessments (DPIAs)

Several respondents noted the importance of businesses and organisations carrying out DPIAs when processing workers' personal data. They also noted that it is a requirement, in certain circumstances, under data protection law. They identified that a DPIA provides an opportunity to consult workers before introducing new forms of processing. For example, when introducing new forms of monitoring or processing health data of workers.

Respondents would like to see guidance on DPIAs tailored to the employment context. Several trade unions noted the importance of seeking the views of workers and their representatives in the process.

ICO's response

A DPIA is an important tool, and sometimes a requirement, for organisations when they are planning on using personal data and should help build in good data protection practice from the outset. We produced detailed guidance on DPIAs, including:

- when one is required;
- what organisations need to consider;
- templates; and
- best practice advice.

We will look at how we can supplement this existing guidance with tailored, context-specific examples and case studies to help employers comply with the law.

Artificial intelligence (AI)

A key cross-cutting theme that emerged concerned the increasing use of AI and algorithmic decision-making as part of employment practices. Respondents noted this development is impacting on several areas, including the recruitment, selection and verification of candidates when applying for jobs. They also noted the use of AI in monitoring workers, including for performance management and allocation of work, as well as in aspects of processing worker health data. Several respondents raised concerns about the potential harms of using AI. We give more detail about some of the feedback provided by respondents in the relevant topic-specific themes below.

ICO’s response

We recognise the increasing role AI has to play and that there may be uncertainties in how to operate it appropriately. We previously published guidance on AI and data protection, which organisations can use to inform their considerations of using this type of technology. Our existing guidance also sets out how to explain decisions made by AI systems, as individuals have a right to know how decisions about them have been reached using AI. We are currently looking at the issue of fairness and AI.

AI is a developing area and we will continue to produce guidance and resources on this rapidly changing topic. We recognise that AI may pose particular challenges in an employment context, and we will consider how to address this in the future employment guidance.

Equal opportunities monitoring and diversity and inclusion

Many respondents noted there is a greater emphasis on collecting and recording equal opportunities data. This occurs mostly at the recruitment stage, but also during ongoing employment. Employers are also monitoring diversity and inclusion information. Respondents noted this involves processing the special category data of workers and so needs addressing in the guidance, particularly around the requirements of processing this type of data. Related themes cover these aspects in the sections on recruitment and employment records below.

ICO’s response

We recognise this is a growing area. Equality data is not static and employers can collect and use it in different ways throughout a worker’s employment relationship. Most equality data is also special category data, which can make its collection and use more complex. However, equality data can also be valuable to help employers understand their workforce better and meet their obligations under other legislations such as the Equality Act 2010.

We are keen to ensure future employment guidance considers how organisations can process diversity and equal opportunity data compliantly.

Recruitment, selection and verification themes

Applications and interviews

This was a key theme in responses on the topic of recruitment. Respondents told us about the increasing complexities in the labour market supply chain, with the end-to-end recruitment process often involving several organisations. Respondents would like guidance on special category data, data sharing, international transfers and controller-processor relationships specific to these complexities.

Respondents told us how technology enables employers and agencies to gather significantly more data about applicants since we published our code. Responses ask for guidance on what is necessary and proportionate to ask at the application stage.

It is evident that employers are increasingly using automated processes and AI in the shortlisting and selection of candidates. Respondents also told us the use of AI extends beyond sifting; employers are increasingly using it in combination with biometrics to infer personal characteristics about candidates during interviews. Many respondents were concerned about a lack of meaningful human intervention with the profiling of candidates. Some respondents perceive a general lack of awareness by organisations and individuals of the rights granted by Article 22 of the UK GDPR.

One response highlighted the value of AI in sifting large volumes of applications but stated the data protection implications require clarification. Some responses asked for lawful basis guidance for the use of AI in recruitment practices. Other respondents expressed concern about the lack of choice and transparency for candidates over the use of AI at the screening stage. Respondents would like guidance to highlight the right not to be subject to automated decision-making and the right to human intervention, and to give examples of explanatory statements.

The fairness of using AI to make recruitment decisions was another recurring issue that respondents would welcome guidance on. Respondents talked about risk of discrimination where algorithms reproduce existing biases. Respondents cited examples of both direct and indirect discrimination due to flawed automatic processes and asked for guidance on managing this risk.

Some responses asked for guidance on the use of psychometric testing. In particular, they wanted advice around transparency, purpose limitation and the use of AI to process the resulting data.

Responses showed the increasing use of online or remote interview practices, raising questions about the use and recording of video meetings for interviews.

ICO’s response

Our existing data protection guidance covers many of the key issues, including lawful basis, data sharing, controllership and international transfers. The principles for employers will be the same. However, we will consider how the updated guidance can provide further practical advice tailored to the complexities of this area.

As noted in the response to the general theme of ‘Artificial intelligence’, we recognise that this is a developing area and that there are concerns over its implementation. Again, we published guidance on AI and data protection, and we are currently looking at the issues surrounding AI and fairness. We will, however, also consider how best to address the use of AI in a recruitment context.

Pre-employment checks

This was the most commonly recurring theme within the topic of recruitment. Respondents highlighted the changes in the regimes, legislation and public bodies involved in pre-employment checks since we published our employment practices code. The responses showed the complexities of this area. These include:

- legal obligations when onboarding workers into regulated organisations;
- right to work immigration checks; and
- the varying levels of checks dependent on organisation and job role.

The area is also made complex by the widespread use of third-party verification services. Respondents would like data sharing guidance which covers this.

Several respondents noted the increase in data sources over the last decade, expressing concerns about excessive data collection. One response suggested a case study where an initial checking proposal is slimmed down, with the rationale explained.

Some respondents expressed concern about approve or deny lists and the use of these by employers during the recruitment process.

Respondents told us that, pre-pandemic, much verification work was done in person with paper documents. A lot of this work has now shifted online; respondents would like guidance which reflects this change, especially around retention of identity documents.

Respondents also asked for guidance around the stages in the recruitment process when they can gather data. They would also like guidance on the lawful basis for carrying out and then sharing verification data.

ICO’s response

We recognise that this area has developed significantly since we published the existing employment guidance. We also note the increased involvement of third-party providers and vetting services in pre-employment checks. We intend to address these changes and also changes in data protection law in the new guidance.

Criminal records

This theme came up in relation to pre-employment checks but warrants particular attention due to the sensitivity of and the special rules for criminal offence data. Respondents asked for guidance and case studies around lawful bases and the schedule conditions for processing criminal offence data. Respondents would like guidance which references the recruitment stage at which criminal records checks take place, including ‘refresh’ checks (for example, during buy outs or mergers).

Some respondents told us they would welcome guidance to cover processor-controller scenarios, where an organisation is using a third party to carry out checks. Other respondents asked for guidance and case studies which cover checks not mandated by regulation but indicated by risk. Some responses mentioned the overlapping nature of data protection law and the Rehabilitation of Offenders Act and ask for guidance which considers the relationship between these laws.

One response acknowledged our existing guidance. They asked that we draw on these resources to produce something for non-data protection practitioners.

As with the wider topic of pre-employment checks, the issue of publicly available sources (including employment tribunal decisions) ran through several responses. Respondents had concerns that these can be inaccurate, out of date or cause discrimination.

Concerns were also expressed about how to handle self-disclosure, citing risks of unnecessary or excessive disclosures. One response would like the ICO to avoid being prescriptive about the point at which employers should request self-disclosure.

Respondents raised concerns that candidates are ruled out by AI based on criminal records disclosure.

ICO’s response

We have produced guidance on criminal offence data. This is relevant to any organisation or employer that wishes to process this type of personal data, for example when recruiting workers.

However, we recognise that issues relating to criminal records have changed since we published the previous employment guidance. The future guidance will take this into account.

Social media and other publicly available sources

Respondents noted the evolution and growth of social media over the last decade means that the guidance now needs to be updated to reflect these changes.

For recruitment, employers are using publicly available sources to find candidates and to gain data to inform verification. A number of responses cited LinkedIn, noting the contrast in the use of LinkedIn and other, more personal, social media channels. There are concerns over recruiters and head-hunters using personal LinkedIn accounts to carry out corporate work. Respondents asked for case studies and guidance on controllership and purpose limitation to address this issue.

Some respondents think employers should not search through personal social media accounts. Other respondents would like guidance on how to make this area of processing fair and transparent.

Many responses were concerned with the risks of accessing sensitive data and of inaccuracy. Respondents would like us to highlight these issues in our new guidance.

ICO’s response

We recognise that this is a key development since we published the existing employment guidance. We are also monitoring developments in case law on this topic. We recognise the range of social media sources available, from services tailored specifically to employment to much less formal social media channels. There is a potential for consideration of social media by employers to blur the boundaries between work and personal life.

We will seek to address these issues in the future guidance and provide further clarity in this area.

Equality and diversity monitoring

Respondents would like guidance on best practice for gathering this data during the job application process. There is a desire to see ICO guidance which factors in other regulatory obligations, for example the Equality Act 2010. In addition, many organisations undertake inclusivity initiatives which are outside of regulatory obligations and would like guidance and case studies to assist with these.

Respondents asked for guidance on the rules for special category data in the context of collecting equality data. Best practice for retention was another recurring issue, with concerns expressed about how to handle sensitive data for unsuccessful candidates. Respondents requested case studies to illustrate how to choose a lawful basis or condition for processing, what would be considered excessive and then how to responsibly handle the data gathered.

ICO's response

As we have noted above, this is an important and complex area requiring careful consideration. In the updated guidance, we will look to provide further advice on processing diversity data, particularly in the context of special category data.

Employment records themes

Retention

Most respondents raised the issue of retention. Although the ICO currently has guidance on retention, respondents felt that more employment-related guidance would be beneficial, particularly around retention times for different types of data. Some respondents stated that more emphasis should be placed on how long organisations should retain information in an employment record. They also asked for it be made clear that different records require different retention periods.

Some of the respondents wanted the guidance to explain and make clear that data protection law was not the only legislation with obligations on retention periods.

Many respondents also stated that the guidance needed more clarity on the collection and retention of certain types of data, such as criminal records and special category data. This would ensure that employers were complying with all legislation, not just data protection law. These respondents considered this to be necessary to protect the rights of employees.

ICO's response

As our existing guidance on the storage limitation principle explains, it will be for organisations to set appropriate retention limits. These may be affected by other industry standards or legal requirements outside of data protection.

It will not be possible for the ICO, in the employment context, to set such standards given the range of data any organisation may process. However, we will ensure that the guidance is clear on what employers need to consider to comply with data protection law. We will think carefully about how to produce this guidance in the most useful format. We are considering checklists or toolkits to support employers in their decision-making process.

Subject access requests (SARs)

Many respondents raised the issue of SARs being used as part of disciplinary or grievance processes. In particular, when workers seek information to determine whether to take legal action or assist in any legal claim against their employer. These respondents felt that they needed further advice as to what information they were entitled to when asking for their employment record, for example witness statements and meeting notes. They would welcome guidance that makes clear to employers and workers what data they can disclose.

A number of respondents raised the concern that employers could not disclose references when requested through a SAR.

The inclusion of worked examples in our guidance would also be useful.

ICO’s response

We have existing detailed guidance on the right of access (subject access requests). However, we recognise there is a desire to see further guidance addressing SARs made in an employment context. We also understand that people are seeking further clarity on situations specific to employment, such as what can be shared in relation to disciplinary or grievance situations. We will consider how best to provide further clarity to address these concerns with user-friendly, tailored guidance.

We recognise there has been a change around the issue of requesting information held in confidential references. We already provide guidance on this topic.

Lawful basis and conditions for processing

Many respondents said more guidance is needed on the lawful basis for collection and retention of data held in employment records. In particular, data held in criminal and health records, as well as special category data and equality data. They also wanted guidance on how this data could be used. Respondents felt that more clarification on the lawful bases of Article 6 of the UK GDPR, particularly more detail on consent, would be helpful. They also felt that more detail on conditions for processing under Article 9 would ensure the data is processed fairly and legally.

ICO’s response

As noted above, we have existing detailed guidance on the lawful bases, and on processing special category data and criminal offence data. These resources should be helpful to employers in understanding the legislation and overarching principles. Many of the principles and considerations will be the same, regardless of what context the data is to be processed. However, we will seek to provide further clarity where appropriate, whether this includes more examples, case studies or further detailed guidance.

Security and confidentiality

Some respondents requested more guidance on security and confidentiality. In particular, guidance for multinational organisations using cloud storage and data processing solutions to store and transfer data outside of the UK and European Economic Area (EEA), to countries without adequacy decisions.

ICO’s response

We have existing guidance on security considerations, as a key data protection principle. This should provide advice for organisations on how to securely manage the personal data they hold. Security is an important topic for the ICO and we will continue to look into new systems and technologies as they develop.

In terms of international transfers, we recognise this is a complex area. We are in the process of providing updated guidance on this topic this year, which will also be relevant to employers.

Monitoring of workers themes

Data protection obligations

Many respondents asked for guidance on how to carry out monitoring in compliance with data protection law. Responses discussed the steps organisations should consider before deciding whether to deploy monitoring. These included:

- identifying a lawful basis;
- completing a legitimate interests assessment (where relevant); and
- completing a data protection impact assessment (DPIA), including consulting workers or their representatives.

Transparency was another key theme, with concerns that workers are not always adequately informed about monitoring. Some respondents asked for updated guidance on covert surveillance. Some responses referenced recent Council of Europe caselaw on covert surveillance, as well as recent action by European supervisory authorities in relation to transparency in the employment context.

Many responses concerned the question of proportionality. Several respondents were concerned about the potential for excessive monitoring. Respondents would welcome examples of compliant and non-compliant monitoring. Some respondents asked for guidance aimed at workers as well as employers, noting the power imbalance in the employment relationship.

ICO's response

We recognise that we need to update the existing guidance on monitoring workers. An updated version needs to take into account the significant developments since we originally published the guidance, both in terms of data protection law and technology. We will seek to address the general obligations an employer has and the factors they should consider in the updated guidance. Linked to this, we will be publishing updated video surveillance guidance this year. This will address some of the issues raised here.

Monitoring remote office workers

This was the most frequently recurring theme in responses about monitoring. The consensus across responses is that acceleration towards remote working, as caused by the pandemic, has increased privacy risks.

Individuals and worker representatives were concerned by the potential intrusiveness of monitoring. They noted that, even with risk-reducing measures, organisations are likely to capture private and sensitive information. Organisations want guidance around proportionality when it comes to monitoring. There is also an appetite for guidance which considers the overlap between home and work life, along with employers' desires to manage performance and track wellbeing.

ICO's response

We recognise that, particularly due to the pandemic, there has been an increase in both remote office working and monitoring of workers. This brings with it new challenges and new opportunities. In the short term, we produced guidance on data protection and working from home for our data protection and coronavirus information hub.

We intend to address the longer-term issues in our new guidance. We are keen to provide clarity on how and when employers can carry out monitoring, in a data protection-compliant way, whilst allowing workers to exercise their individual rights. This is a priority area; we are currently gathering information from our regulatory activities such as investigations, complaints, and audits to help shape future guidance in this area.

The use of non-corporate devices and applications

Many responses commented on the privacy challenges of workers using their own devices, where monitoring could intrude into non-work activities. Respondents asked for guidance on understanding employer and worker obligations where personal and work data may be accessed interchangeably between corporate and personal devices. Where monitoring occurs for data security reasons, respondents ask how to handle incidental personal data.

Several respondents expressed concerns about the use of private channels, such as WhatsApp or Facebook Messenger. Particular concern was around fulfilling subject access requests.

Respondents said they would welcome case studies and guidance around the use of non-corporate channels and private devices for work purposes. They would also welcome guidance on the extent to which employers can justify monitoring of personal social media.

ICO’s response

We previously produced guidance on Bring Your Own Device (BYOD) under the DPA 1998, which may still be useful. We also produced a checklist on BYOD in our data protection and coronavirus information hub, covering its use under current data protection law. We will consider incorporating updated guidance on this topic.

Increasing capability of technology

This was a key theme. There is an appetite for the ICO to address the new data protection challenges posed by increasingly sophisticated monitoring tools. Respondents expressed concern about excessive data collection, as technical solutions now enable organisations to collect large volumes of personal data about workers. Purpose creep and the rules for processing special category data were other recurrent themes.

Some respondents asked for guidance around the use of cloud services for handling monitoring data, and where data is handled outside of the UK. We address specific uses of technology in monitoring workers in the sections below and provide an overall response at the end of this topic.

Monitoring and artificial intelligence

Many respondents mentioned the rise in the use of AI. They cited examples where organisations apply AI tools to the datasets they gather by monitoring, then use the tools to make decisions about workers both individually and collectively. Some respondents cited new applications for this technology, including tools which analyse workers’ emotion and engagement during video meetings. Responses also noted the use of AI to identify fraudulent activity.

Respondents expressed concerns about lawfulness, fairness, transparency and the potential for algorithmic biases. Respondents would like employment-specific AI guidance, including examples on how information rights work in practice and how to use additional safeguards. Respondents told us there is a disproportionate impact on gig economy workers, where automated processes often determine work allocation and pay.

Computer activity monitoring

Keystroke monitoring involves the use of tools to capture all keyboard activity by a worker, including:

- tracking web browsing;
- emails;
- documents; and
- use of applications.

Some responses discussed the functionality of the tools used. Some 'all-in-one' packages perform a multitude of functions, including monitoring, with the capability to provide managers with granular information about workers' activities.

Respondents asked for guidance and examples on the data protection considerations for using these monitoring tools. Responses mentioned the intrusive nature of this monitoring, citing automatic screenshots and logging of all activity. Other responses discussed situations where employers deploy monitoring to prevent data loss and to comply with other obligations. Respondents would like to see guidance on what is proportionate.

Camera surveillance

Many respondents asked for up-to-date data protection guidance on the use of surveillance cameras in the workplace (including work vehicles, dashcams and body-worn cameras). In particular, respondents wanted guidance around transparency, fairness and purpose limitation. Some responses provided scenarios, for example where CCTV is deployed for crime prevention, then material is used as evidence in investigations unrelated to the original purpose.

Respondents noted challenges when subject access requests include CCTV footage, particularly when footage captures third parties. Some responses noted that technology has evolved; they would like guidance to acknowledge the use of facial recognition and audio capture in modern systems.

Vehicle or device tracking

Many responses talked about vehicle tracking, particularly in relation to gig economy workers. One response highlighted the use of tracking for protecting company assets, including when they are being used outside work time. Other responses mentioned the use of GPS tracking to locate mobile work devices.

Another issue we identified within this theme is the tracking of workers, through wearable tech, to monitor productivity. Respondents would like to see examples of good and bad practice.

Biometrics

Respondents provided examples of the use of biometrics. The most frequent uses of biometrics include:

- accessing physical places;
- using systems and applications; and
- recording start and finish times.

Some respondents expressed concern about the emerging use of biometrics which analyse worker behaviours and emotions. Respondents asked for descriptions and examples of biometric data and guidance on how to collect and process this lawfully.

Social media monitoring

Respondents raised concerns about employer monitoring of personal social media accounts. Respondents told us this is sometimes undertaken to protect against corporate reputational damage or as part of disciplinary investigations. They would like guidance on when this would be justified and proportionate. Some responses were concerned about a lack of transparency.

Respondents commented on the proliferation and the evolution of social media in the last decade and want the guidance to reflect this development.

ICO’s response

We recognise the growth in use of technology for monitoring workers. Technology is increasingly capable of processing large amounts of personal data; this can cause anxiety. Data protection law is principles-based, which means that it is flexible enough to apply to the use of different technologies as they develop. Whenever an organisation wishes to use new or more privacy-intrusive technology, they will need to consider fairness and proportionality and be able to justify the technology’s use. Our new guidance will include practical advice on how to assess and implement new technologies in a data protection-compliant way.

The ICO is currently undertaking foresight-focused research on the future of biometric technologies. We intend to publish a report on our research findings later this year. We will look to provide guidance on the use of biometrics and how it relates to employment practices in due course.

We also recognise the particular challenges involved in the use of AI in the context of monitoring workers. We will seek to address this in the updated guidance.

We will be publishing updated video surveillance guidance in due course, which addresses issues around the use of surveillance cameras in public and private sectors. This guidance will also address new applications of video surveillance technologies and provide a more comprehensive description of how the UK GDPR and DPA 2018 apply. Many of the principles and considerations will be the same in an employment context as in other circumstances. We will factor this into our planned employment guidance to produce specific employment-focused guidance where appropriate. We will also have appropriate signposting to other resources.

Health data of workers themes

Collection and use of health data

A general theme that emerged was how the collection and use of health data has changed over time. Respondents noted that organisations collect and store a greater range of health data. This includes:

- sickness and injury records;
- medical assessments and occupational health referrals;
- drugs testing;
- pre-employment screening;
- vaccination and Covid testing (see the theme 'Impact of COVID-19'); and
- mental and emotional health (see the theme 'Mental health and wellbeing').

It was noted by some that certain job roles may have a greater need for health information (such as fitness to work and for appointment to a role).

Whilst several respondents felt the existing guidance on workers' health information was still useful, some noted the changes in data protection law since its publication, particularly around processing special category data. Some respondents considered that the new guidance should make the status of health data clear under current data protection law. They suggested including what it covers and explaining what factors organisations should consider when processing it. Many suggested that the guidance should explain the appropriate lawful bases and conditions for processing health data.

Others considered that the guidance should explain what types of health data organisations can process and when. They suggested detail around when it would be appropriate to actively monitor workers' health, as well as when medical testing is acceptable.

Some suggested the guidance should address the different ways organisations collect health data and should offer best practice advice. Others would like to see guidance on:

- retention of health data;
- security and access controls;
- transparency information; and
- informing workers of their data protection rights.

It was also noted that there can be issues over data minimisation. Organisations often need to retain enough information to carry out their employment responsibilities and to keep workers safe.

A number noted the overlap between data protection law and employment law, as well as health and safety law. They wanted future guidance to recognise the interplay between these different pieces of legislation.

ICO's response

We recognise the changes in the way employers collect and use health data since the publication of the existing employment guidance. We also understand that the nature, type and sharing of health data has changed as a result of the pandemic. We intend for the upcoming guidance to address these developments and reflect changes in data protection law since then.

Lawful basis and conditions for processing health data

A cross-cutting theme was the issue of identifying a lawful basis under Article 6 of the UK GDPR and a condition for processing under Article 9. Respondents said they would value guidance on when consent can be valid and what other lawful bases employers can rely on, such as contract or legitimate interests. A number wanted guidance on the substantial public interest conditions. This issue links with many of the other general comments and the other emerging themes. Organisations want guidance on being able to meet requirements for processing worker health data in a variety of circumstances.

A common point was for guidance to include practical examples and case studies to illustrate explanations. This was also evident for the other themes.

ICO's response

We intend for the new employment guidance to address changes in data protection law. In particular, highlighting that health data is considered special category data and has stricter requirements in order to process it. Our new guidance will help employers to process and share health data in a compliant way. We will provide practical examples as to how employers can achieve this.

Impact of COVID-19

A key theme that emerged concerned the impact of the COVID-19 pandemic on employment practices, particularly on workers' health information. This led to a number of developments in the use of health information and presented new challenges around the handling of this data. These developments took place quickly, with organisations having to put in place processes at pace to deal with the pandemic.

It is clear that the pandemic led to organisations holding more health information, with some expecting this to continue going forward. Respondents reported that they are often holding information on:

- whether a worker has tested positive for COVID-19;
- whether they have Covid symptoms; and
- the vaccination status of workers.

In some instances, vaccination has been mandatory. Some employers have also requested their workers be vaccinated, with some respondents having concerns about this. This may have implications for recruitment practices as well.

Some organisations have been carrying out temperature checks to detect possible infection; others have been asking workers to answer health questionnaires. This may be required to allow access to the workplace. Depending on the nature of the employer, some need to monitor and report cases of Covid infection among their workers.

Another development linked with this is the issue of sharing information related to COVID-19. This could be with public health bodies or disclosing information internally within an organisation (such as informing colleagues if someone has tested positive).

Respondents also referred to the use of technology to track workers' health (see also the theme 'Health monitoring or tracking technologies'), which may be seen in temperature checks, testing and use of apps.

Several respondents noted concerns about the legitimacy of collecting this kind of health data. Others reported concerns about identifying the appropriate lawful basis and conditions for processing COVID-19 data, as well as problems with relying on individual consent. (see also 'Lawful basis and conditions for processing'). Concerns ranged from the collection of information related to COVID-19, particularly vaccination status, to the sharing of this data. This is also covered in the theme 'Sharing health data' below.

Respondents asked for clear guidance on these issues, along with guidance for managing health information post-Covid, and also anticipating future health emergencies. In a similar vein, many respondents thought the current ICO coronavirus guidance should be folded into future guidance on employment practices.

ICO’s response

We appreciate that the pandemic has had a major impact on the use of health data in the employment context. As noted above, the ICO has been committed to supporting organisations during the pandemic and provided guidance on many related issues. The Data protection and coronavirus information hub provides a range of guidance that may be useful for organisations who need to process worker health data. We also recognise that the pandemic is likely to have a lasting impact on employment practices and the use of health data. We intend for the future guidance to address these developments. Where appropriate, we also intend to provide consolidated existing coronavirus guidance that is relevant to worker health data.

Mental health and wellbeing

A number of respondents noted that an important development in employment practices involves the recording of information about workers’ mental health, as well as their emotional health and wellbeing.

Some organisations have assigned mental health first aiders, who may also be employees, set up employee wellness programs and provided other support for their workers’ mental health. Some of this has resulted from the impact of the pandemic, or increased in response to it, along with the growing use of health tracking technologies.

It was also recognised that psychological testing is more common, particularly in relation to the recruitment and selection of workers (see the theme ‘Recruitment’).

Respondents wanted clearer guidance on the appropriate collection and use of mental health data, including accessing it and retention periods. Another suggested it would be helpful for guidance to address dealing with mental health emergencies of workers.

ICO’s response

We acknowledge that there is a growing trend of organisations processing information about workers’ mental health and wellbeing, and that in many cases they wish to support their workforce. We produced guidance on Data sharing in an urgent situation or in an emergency, which applies to both medical and mental health emergencies.

Mental health information is special category data, and so extra safeguards need to be in place. We will look to ensure our future guidance supports employers to be more confident in how they process and share data relating to mental health.

Health monitoring and tracking technologies

A key theme that emerged concerned the use of new technology to manage and track workers' health information, particularly as a result of the pandemic. Respondents reported an increasing interest in, and in some cases use of, health monitoring technology. This may include using:

- apps;
- facial recognition systems;
- biometrics;
- wearables; and
- AI and algorithmic systems.

Some noted concerns about the deployment of such technology and the potential impacts on workers' wellbeing. They wanted clearer guidance on when and how to use these systems safely and appropriately. Some wanted guidance on the role of worker consent.

This has clear links to the themes 'Impact of COVID-19' and 'Mental health and wellbeing', as well as the general themes concerning monitoring of workers (see the section on 'Monitoring of workers').

Respondents also noted the increase in worker wellness programs and the associated collection of data.

One respondent also commented that psychological testing of workers is now quite common, linking in with developments in recruitment and verification practices.

ICO's response

We recognise that, during the pandemic, there has been an increased focus on monitoring workers' health. Organisations are using different technical solutions to meet this goal. We previously published guidance on some of these issues as part of the data protection and coronavirus information hub.

The monitoring and tracking of workers' health has clear links with more general monitoring of workers, with proportionality a key consideration. The rules around processing special category data are also important in being able to justify the processing of health data. They should provide a clear starting point for any organisation's data protection considerations or responsibilities.

The ICO will be publishing updated guidance on surveillance; many of these principles will be relevant to the use of health monitoring and tracking technologies. We will look to supplement this, where necessary, with employment-specific resources as part of our new employment guidance hub.

Sharing health data

In the context of workers' health information, another theme that was evident concerned the sharing and disclosure of this type of data. This has clear links with the general theme of 'Data sharing' found earlier in this document.

Given the sensitive nature of health data, it was noted that there are issues over confidentiality, but also sometimes a need to share it. This could be the sharing of a worker's health information between an employer and an external occupational health provider, or with public health bodies (in the context of the pandemic). It might also involve disclosure of information to colleagues within the same organisation. Others wanted to know the limits that an employer could access health records. In particular, where information about when a third party created the records, such as when a worker undergoes a medical assessment.

Some wanted to see greater emphasis on being able to share data with health and safety representatives.

Respondents noted they would like to see guidance on the sharing of health data generally, but also specifically during a pandemic and other public health emergencies. One also noted a need for clarity on when organisations can share data if a worker becomes incapacitated and is unable to make decisions.

ICO's response

We recognise there are concerns about the sharing of worker health information and who it may be disclosed to, especially given the context of the pandemic. We provided guidance on the issue of data sharing in the Data protection and coronavirus information hub, as well as more general guidance in the data sharing code of practice. We will consider how best to address this issue in the future employment guidance hub.

Occupational health and third-party providers

Another theme that emerged was the use of occupational health data and third-party providers. This has clear links with the theme of 'Sharing health data' in particular and also the general theme of 'Data sharing'. Some queried how much information organisations should share and whether this should be based on worker consent or on contract. A key issue raised was whether outsourced occupational health providers act as a controller or a processor and who can have access to the information they hold.

ICO's response

This issue clearly links with the more general theme of data sharing. As noted above, we have existing guidance that should help organisations understand when they can share personal data and their obligations.

We have existing guidance to help determine if an organisation is acting as a controller, joint controller or as a processor. This should address some of the concerns raised. It is the responsibility of organisations to properly establish their roles under data protection law. This is not always easy. We aim to provide some practical examples and guidance to help employers clearly establish their roles and the roles of third parties, so they can meet their data protection obligations.

General issues

Other points raised included:

- industrial relations and the role of trade unions and worker representatives, including sharing workforce data with unions and consulting workers;
- secondments and shared working practices;
- international transfers of personal data between multinationals and between company groups and suppliers;
- various examples and case studies that could be used in the guidance, or examples that respondents would like to be included;
- regional differences across the UK due to devolution (for example, Northern Ireland and Scotland have their own criminal record disclosure arrangements); and
- concerns over the selling or sharing of employment data due to the potential commercial value of large datasets.

ICO’s response

In the call for views there were many points raised, and where appropriate we will try to address these in future guidance. As we intend to produce a guidance hub, we will be able to address other points over time and where relevant.

Several responses included scenarios and case studies based on personal experience. We appreciate the time respondents spent to share these with us and they are valuable to informing our approach.

Next steps

We are in the process of considering the comments received in response to the call for views. These will feed into the development of the guidance. We plan to produce a hub of employment guidance with content added over time. The development of our guidance will be an iterative process with lots of opportunities for stakeholder involvement and feedback. The call for views formed the first part of that process.

We intend to run consultations on the drafts of significant pieces of guidance as we develop them. We will provide updates on this process on the ICO website, including opportunities to provide comments.