ICO'S MONITORING AT WORK DRAFT GUIDANCE

Response from the Employment Lawyers Association

18 January 2023

EMPLOYMENT LAWYERS ASSOCIATION

WORKING GROUP ON THE ICO'S MONITORING AT WORK DRAFT GUIDANCE

1 INTRODUCTION

1.1 This paper has been produced in response to the Information Commissioner's Office ("**ICO**") draft guidance on monitoring at work (the "**Draft Guidance**").

1.2 The Employment Lawyers Association (UK) ("**ELA**") welcomes the opportunity to provide its observations on the Draft Guidance. ELA is a non-political group of specialists in the field of employment law and includes those who represent employees and employers in the Courts and Employment Tribunals of the United Kingdom. Therefore, it is not ELA's role to comment on the political merits or otherwise of the Draft Guidance, rather its role is to make observations from a legal and commercial standpoint.

1.3 The ELA Working Group on the Draft Guidance is made up of both barristers and solicitors who regularly work with, and consider the impacts of, privacy and monitoring obligations on employers within the United Kingdom and abroad. The Working Group was set up by ELA's Legislative and Policy Committee under the chairmanship of Jonathan Chamberlain and Alastair Woodland to respond to the Draft Guidance. A full list of the members of the working group is annexed to this submission.

2 OUR RESPONSE

2.1 We have commented on the Draft Guidance as a whole, mindful of the specific questions the ICO have asked.

2.2 Thus, our commentary is split into four sections following the topics in the Draft Guidance: how do we lawfully monitor workers; automated processes in monitoring tools; specific data protection for different types of workplace monitoring; and, biometric data.

3 'HOW DO WE LAWFULLY MONITOR WORKERS'

3.1 Legislative Regime

(a) The ICO has provided an overview of the various legislative instruments that it has considered in its formulation of the Draft Guidance. In particular, the ICO has noted that the Draft Guidance was produced to provide clarity on the UK General Data Protection Regulation ("**UK GDPR**") and the Data Protection Act 2018 ("**DPA 2018**").[1]

(b) As part of this legislative overview, the Draft Guidance has considered the impacts of Article 6 and Article 8 of the Human Rights Act 1998 ("**HRA**"). In particular, it noted that, "[p]ublic authorities and all bodies performing public functions should also consider the right to respect for a private and family life enshrined in Article 8".[2] Whilst the primary purpose of Article 8 is to protect against arbitrary interferences by a public

[1] Information Commissioner's Office, 'Employment practices: monitoring at work draft guidance' (12 October 2022) <https://ico.org.uk/media/about-the-ico/consultations/4021868/draft-monitoring-at-work-20221011.pdf> ("**Draft Guidance**"), 5.
[2] Draft Guidance, 5.

authority with a person's private and family life, home and correspondence,[3] Member States will also have a positive obligation to ensure the protection of Article 8 rights between private parties (including private employers).

(c) This extension to Article 8 was considered in Bărbulescu v Romania [2017] ECHR 742 ("**Bărbulescu**"). In this case, the ECtHR determined that the Romanian domestic courts had failed to protect an employee's Article 8 rights where an employer had been found to be entitled to monitor the instant messaging accounts of an employee. It was held that the employee's right to private life and correspondence had been breached by the employer's monitoring and that the Romanian courts had failed to strike a fair balance between the employee's right to respect for his private life and correspondence and the employer's opposing right to ensure the smooth running of the company. As such, employees are considered to have the right to private life at work and therefore private employers need a compelling reason to restrict this right by virtue of Article 8. The right to privacy is not an absolute right; but employers should be warned that they will need to demonstrate that monitoring is justified by legitimate reasons, proportionate and necessary in order to comply with the Human Rights Act.

(d) More recently, the ECtHR in the case of Lópex Ribalda -v- Spain [2020 IRLR 60] ("**López Ribalda**") found that Spain had not failed to protect employees' rights to privacy under Article 8 of the ECHR when its courts rejected their claims of unfair dismissal in circumstances where the employer relied on covertly recorded CCTV footage of their involvement in theft as the employer was in that case justified in light of:

(i) the gravity of the scale of theft in question;

(ii) the short duration of monitoring;

(iii) the location of the monitoring being in a public area;

(iv) the limited number of people who could access/view the footage;

(v) the limited purpose for which the footage was used;

(vi) the fact that informing the employees of the monitoring may have defeated its purpose;

(vii) full disclosure of the recording were provided to the employees.

(e) If there has been a breach of HRA in obtaining evidence in disciplinary proceedings, particularly where information is covertly obtained and not (or adequately) disclosed, without sufficient justification, this is likely to have an impact on the right to a fair hearing and fair adjudication of employment related disputes.

(f) The HRA also requires all UK courts to interpret legislation so that it is compatible with the European Convention on Human Rights, so far as it is possible to do so. As such,

[3] European Court of Human Rights, 'Guide on Article 8 of the Convention: Right to respect for private and family life' (31 August 2022) <https://www.echr.coe.int/documents/guide_art_8_eng.pdf>, para 5.

UK courts should "take account" of decisions of the European Court of Human Rights in its consideration of matters. Therefore, in any employment matters UK courts are required to consider and make decisions to align with Article 8.

(g) This extended scope of Article 8 to private employers was previously considered in the ICO's commentary in the Employment Practices Code ("**EPC**").[4] Whilst the EPC was produced prior to the introduction of the DPA 2018, its guidance on the general principles of the UK GDPR and the HRA remains relevant. ELA recommends that the Draft Guidance should be amended to reflect the ICO's previous formulation of the impact of Article 8 on private employers, as per the below:

This guidance provides clarity and practical advice to help employers who are monitoring workers to comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018). The UK GDPR and the DPA 2018 do not prevent an employer from monitoring workers, but they must do any monitoring in a way which is compliant with data protection legislation. Public authorities, all bodies performing public functions and employers - especially in the public sector - should also consider the right to respect for a private and family life and for correspondence enshrined in Article 8 of the Human Rights Act 1998. This is increasingly important due to the rise of remote working. Workers' expectation of privacy are likely to be significantly greater at home than in the workplace and the risks of capturing family and private life information are higher.

3.2 **What constitutes monitoring at work?**

(a) **Systematic and occasional monitoring**

(i) The Draft Guidance has purported to cover both "systematic monitoring" and "occasional monitoring".[5] Systematic monitoring has been defined to cover circumstances "where an employer monitors all workers or groups of workers as a matter of course", whilst occasional monitoring will arise "where an employer introduces monitoring as a short-term response to a specific need".[6]

(ii) Whilst it is appropriate for the Draft Guidance to cover both categories of monitoring, the Draft Guidance should be clear that it covers systematic monitoring technologies that may only be used on an occasional basis. This type of "occasional systematic monitoring" covers circumstances where the monitoring of workers is continuous but the employer will only make use of it in select circumstances. This type of monitoring commonly occurs within email monitoring programs, in which the program will monitor all emails that employees send and receive but the output will only be used to assist in one off grievance or misconduct investigations. Whilst it is recognised that the ICO has likely intended to cover these types of monitoring, ELA recommends this category is expressly identified in the Draft Guidance to prevent any confusion from employers.

[4] Information Commissioner's Office, 'The employment practices code' (November 2011) <https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf> ("**EPC**"), 58.
[5] Draft Guidance, 6.
[6] Draft Guidance, 6.

(b) **Monitoring technologies**

(i) The ICO has provided guidance on the types of technologies that may be considered "monitoring technologies".[7] Whilst the ICO has acknowledged that the list is not exhaustive,[8] it would be beneficial for the Draft Guidance to include examples of common communication technologies that are currently used to monitor employees. In ELA's experience, these technologies include software that can track calls and emails, as well as video recording features (i.e. the recording of Microsoft Teams meetings) and swipe cards. From our experience, businesses will utilise these technologies to prevent the loss of confidential information, for security purposes as well as being used to investigate allegations of misconduct. As the monitoring of electronic communications remains the key means in which employers monitored workers, it would be prudent for the Draft Guidance to include a provision that explicitly acknowledges the application of the Draft Guidance to the monitoring of communication technologies.

(ii) For completeness we also note that the current list of monitoring technologies is duplicative, as keystroke monitoring tools are mentioned in bullet points four and six.

3.3 **Who is this guidance for?**

The ICO has noted that the Draft Guidance is aimed at "all circumstances where there is an employment relationship, regardless of the nature of the contract."[9] We understand that the ICO intends to make the scope of Draft Guidance as wide as possible and seeks to include monitoring of individuals working in the gig economy, irrespective of employment status. However, the current wording has the effect of narrowing the circumstances in which the Draft Guidance can be applied. ELA recommends that the Draft Guidance should be amended as follows:

This guidance is aimed at all organisations, both public and private sector that have employees, workers, contractors or volunteers. We use the term 'worker' throughout this guidance to refer to someone who performs work for an organisation. Business models have changed in the last decade, with the rise of the gig economy. This guidance captures these relationships too. It is aimed at all circumstances where there is an employment relationship or otherwise a relationship between an organisation and an individual where the individual performs work for the organisation, regardless of the nature of the contract.

3.4 **Lawful Basis for Monitoring**

The Draft Guidance requires that employers should identify and document all lawful bases for monitoring prior to adopting any monitoring technologies or processes.[10] ELA agrees with this in principle but recommends that the Draft Guidance be amended to provide further examples of the relevant lawful bases and identify the extent of documentation that is required for this purpose, in order to provide practical, clear and unambiguous guidance to

[7] Draft Guidance, 6.
[8] Draft Guidance, 7.
[9] Draft Guidance, 7.
[10] Draft Guidance, 10.

employers. For example, are employers required to create and maintain a separate formal record of all monitoring activity that is undertaken (and the corresponding lawful basis), or is it sufficient for this information to be reflected in privacy policies and/or the pre-existing record of processing maintained for compliance with Article 30 GDPR.

Below we set out further specific commentary on the lawful bases of "legal obligation" and "legitimate interests" described within the Draft Guidance.

(a) **Legal obligation**

(i) Employers may monitor employees where it is necessary for compliance with a legal obligation to which the employer is subject. In the employment context, this is particularly relevant to pre-employment vetting and compliance with legal obligations owed by the employer to a third party.

(ii) The Draft Guidance sets out an example of a logistics company that monitored driving time, speed and distance to comply with rules on driver's hours. In its explanation, it was noted that the company did not use the data for any other purposes. We do not consider this example to be particularly realistic of the types of obligations placed on employers in commercial settings. In these circumstances, it would be commonplace for employers to provide any information in respect of driving times and speeds to investigatory bodies where the driver has put the employer in breach of its obligations (i.e. if the employee was involved in an accident or criminal offence). In these circumstances, employers would be required to pass any information onto investigatory bodies to ensure due process. Whilst this is a minor point, for the Draft Guidance to provide as much benefit as possible to employers, we submit that this example ought to be amended to better reflect the potential pressures on employers.

(iii) It may also be helpful to have examples which address regulatory and legislative obligations, for example: monitoring of calls on trading floors at banks, and the use of data for regulatory investigations and defending liabilities; or, in discrimination/diversity monitoring, the requirement to make reasonable adjustments under the Equality Act 2010.

(b) **Legitimate interests**

(i) In the Draft Guidance, the ICO has observed that employers should avoid using the legitimate interest basis if they are monitoring in ways that workers do not understand and would not reasonably expect.[11] Whilst ELA recognises that workers should be made aware of monitoring, the Draft Guidance's commentary on this issue is not consistent with the UK GDPR.

(ii) Article 6(f) of the UK GDPR provides that the processing of data will be lawful where it is necessary for the purposes of the legitimate interests of an employer or a third party, except where those interests are overridden by the interests or fundamental rights and freedoms of the employee. This balance

[11] Draft Guidance, 12.

of the interests of employers against employee rights does not require consideration as to whether an individual has objected to, or would object to, the collection of data. Reliance on legitimate interests does allow workers to object to the processing of their data (including monitoring) under Article 21(1) GDPR. However, a data controller may continue processing such data if the data controller demonstrates "*compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims*". It is not correct therefore for the Draft Guidance to suggest that an objection by workers to monitoring is a basis for avoiding reliance on legitimate interests - compelling legitimate interests may themselves be grounds for overriding any objection.

(iii) In the Draft Guidance the ICO has further contended that employers should avoid using the legitimate interest basis if workers do not understand or would not reasonably expect the monitoring. The decision of the Irish supervisory authority regarding WhatsApp[12] requires data controllers to explain the processes they have undertaken and how the collected data may be used in their privacy policies, including monitoring. It is unclear the circumstances in which workers would not expect the monitoring, short of the exceptional circumstances where covert monitoring occurs which could still be justified by legitimate interests. In light of the above, we recommend the sentence quoted in paragraph 3.4(b)(iii) above is removed from the Draft Guidance.

3.5 **Special Category Data**

(a) **Monitoring Systems that "may" capture special category data**

(i) Throughout the Draft Guidance, the ICO has discussed the obligations of employers where the nature of monitoring means that special category data "may" be captured.[13] In these circumstances, it has been suggested that employers must identify a special category condition to cover this potential capture of special category data, which is potentially inconsistent with the UK GDPR.

(ii) Firstly, this is different from other guidance produced by the ICO (and a departure from the previous guidance). For example, the more general guidance on Special Categories of Personal Data states "*If you are processing special category data … you must identify both a lawful basis under Article 6 and a condition for processing special category data under Article 9*".

(iii) Secondly, the ICO's discussion of monitoring systems that "may" capture special category data suggests that an Article 9 condition is required even if the organisation does not actively know if it has this data. Under Article 9,

[12] Commissioner for Data Protection, Decision of the Data Protection Commission made pursuant to Section 111 of the Data Protection Act, 2018 and Articles 60 and 65 of the General Data Protection Regulation (20 August 2021) <https://edpb.europa.eu/system/files/2021-09/dpc_final_decision_redacted_for_issue_to_edpb_01-09-21_en.pdf>.
[13] Draft Guidance, 13

special category conditions will only apply in limited circumstances and will require the processing to be "necessary".

(iv) In circumstances where collection is not deliberate, it would be difficult to argue that the capture of this data is necessary, as employers are not aware of its existence nor is it needed for the monitoring program to occur (as compared to circumstances where employers are actively monitoring special category data). In any event, absent an Article 9 condition the employer may not be able to undertake what would have been justifiable monitoring previously on a legitimate interests basis. Therefore, it will be difficult for employers to satisfy any Article 9 conditions for special category data that "may" be captured. If the ICO wishes to implement such a requirement, legislative reform to the UK GDPR would be required. The current guidance seems to be unworkable in practice.

(v) In practice, many employers would cover the issue of inadvertent processing of special category data in their impact assessment or (where required) DPIA by acknowledging that there is no intention to capture special category data and identifying preventative measures to avoid the capture of such data (for example use of targeted search terms and e-discovery tools)

(b) **Purpose of monitoring**

(i) On a related note, in the selection of a special category condition, the ICO has suggested that employers must demonstrate that their "purpose for monitoring outweighs the risk of inadvertently capturing special category data". This position appears to extend the requirements of Article 9 of the UK GDPR.

(ii) As above, under Article 9, special category conditions generally require the processing of data to be "necessary", meaning monitoring must be a targeted and proportionate means of achieving a specific purpose in order to be UK GDPR compliant. However, the requirement for these programs to be "necessary" does not require that the monitoring itself has to be absolutely essential to achieve the specified purpose. For employee monitoring, it is conceivable that circumstances would arise where there was a high risk of inadvertent capture of special category data, but nevertheless the monitoring was proportionate in the surrounding circumstance i.e. due to this being a common industry practice. In these situations, the monitoring programs could be for relatively mundane purposes, such as tracking employee emails to allow for automated time recording. In these situations, whilst there may be a high risk of inadvertent capture of special category data, the monitoring itself remains proportionate in the surrounding circumstances. At present, the Draft Guidance has failed to capture these kinds of scenarios. ELA recommends that the Draft Guidance should be amended to remove references to this requirement.

(c) **CCTV**

(i) In its consideration of special category data, the ICO has indicated that CCTV footage may constitute special category data. In this discussion, the Draft

Guidance referred to the example of a bank using CCTV footage, in which it noted that the footage may capture special category data about customers and workers.[14]

(ii) It may also be useful to have the Draft Guidance in sync with the Biometric and Surveillance Cameras Commissioner's published guidance on privacy impact assessments for surveillance cameras.[15]

(iii) The approach of the Draft Guidance to CCTV is inconsistent with the ICO's previous guidance on video surveillance.[16] In this guidance it is suggested that special category data will only be obtained by video surveillance where there are additional technologies that allow users to uniquely identify individuals (i.e. facial recognition).[17] This position aligns with other ICO guidance on special category data in which it is noted [our emphasis in bold]:

If you process digital photographs of individuals, this is not automatically biometric data even if you use it for identification purposes. ***Although a digital image may allow for identification using physical characteristics, it only becomes biometric data if you carry out "specific technical processing"****. Usually this involves using the image data to create an individual digital template or profile, which in turn you use for automated image matching and identification.*[18]

…You can ***often infer an individual's religion or ethnicity with varying degrees of certainty from names or images****. For example, many surnames are associated with a particular ethnicity or religion. However, it is inappropriate to treat all such names as special category data in every instance, as this would mean you need a special category condition just to hold such names on a customer database, which is not the case. However,* ***if you process such names specifically because they indicate ethnicity or religion, for example to target services on this basis, then you are processing special category data****.*[19]

(iv) We query how CCTV footage could independently be considered to capture special category data, without an attempt to make inferences as to racial or ethnic origin, or religious beliefs or other information. ELA recommends that the Draft Guidance is amended to align with the ICO's previous guidance on this issue.

[14] Draft Guidance, 15.
[15] https://www.gov.uk/government/publications/data-protection-impact-assessments-for-surveillance-cameras
[16] Information Commissioner's Office, 'Guidance on video surveillance including CCTV' (14 October 2022) <https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-video-surveillance-including-cctv-1-0.pdf> ("**Video Surveillance Guide**").
[17] Video Surveillance Guide, 43.
[18] Information Commissioner's Office, 'Lawful basis for processing special category data' (25 April 2022) <https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data-1-5.pdf> ("**Special Category Data Guide**"), 9.
[19] Special Category Data Guide, 12.

(d) **Article 9 Conditions**

Below we set out further specific commentary on the "explicit consent" and "employment, social security and social protection" conditions:

(i) **Explicit consent**

The ICO's discussion on the introduction of access control systems that use workers' biometric data is an issue that has been considered across a range of industries. To improve the ICO's consideration of this point in its discussion of Article 9(2)(a), it would be prudent for the ICO to discuss the documentation requirements that arise out of the adoption of these systems. For instance, if employers roll out facial recognition laptops, would the ICO require them to keep a record of all workers who have consented to the use of their biometric data? This guidance would be beneficial for a range of employers given the increasing adoption of biometric systems within UK workforces.

For completeness, it would also be helpful for the Draft Guidance to make clear that for explicit consent to be given under Article 9(2) (a), the consent must be freely given and fully informed. It would also be beneficial to explicitly note that this condition does not include implied consent. Could the ICO give further examples of the "limited circumstances" in which they think explicit consent could be relied upon?

(ii) **Employment, social security and social protection**

Article 9(2) (h) provides that the processing of special category data will be acceptable where it is "necessary 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 or pursuant to contract with a health professional". This provision does not require employers to state the specific legal provision or source of advice that it relies on for the processing of the data. Rather, employers are entitled to process data where it is necessary for preventing or assessing the health, safety and welfare of workers. We consider the formulation of this condition in the Draft Guidance has unduly extended beyond the UK GDPR requirements, in particular the suggestion that employers must be able to point to a specific legal provision to justify any monitoring programs.

In any event, this requirement is unnecessary as employers will have a common law duty to take reasonable care to provide employees with a safe place of work,[20] which would often capture any monitoring programs that are aimed at worker welfare. In practice it will be difficult for employers to identify a specific legal obligation in contract or statue, given employers will underlying and accepted common law duty to provide a safe workplace. This basis for processing is often used in connection with seeking occupational health advice

[20] Wilsons & Clyde Coal Co Ltd v English [1938] AC 57.

and considering any occupational health report when, for example, determining whether an employee has a disability triggering a duty to make reasonable adjustments. Is the guidance suggesting that there needs to be a written record of the specific legal obligation relating to this, rather than (for example) referring more generally to a requirement of employment law?

3.6 **Consideration of other laws**

The Draft Guidance has provided an overview of additional laws that inform the data protection obligations outlined in the UK GDPR and DPA 2018.[21] To the extent ELA has commentary on this section of the Draft Guidance, it has been noted below:

(a) **Employment Legislation and consequential statutory instruments**

(i) The ICO's current formulation of the relevant equalities' legislation does not accurately capture the range of relevant laws across Great Britain and Northern Ireland. Furthermore, it does not consider rights arising under any consequential statutory instruments (i.e. The Maternity and Parental Leave etc. Regulations 1999).

(ii) We also note that the Draft Guidance has not addressed the impacts of employment legislation more generally on employee monitoring. As such, it is recommended the Draft Guidance is amended as follows:

In England, Wales and Scotland, the Equality Act 2010 applies to a range of organisations, including:

- *government departments;*
- *service providers;*
- *employers;*
- *education providers;*
- *transport providers;*
- *associations;*
- *membership bodies; and*
- *providers of public functions.*

In Northern Ireland, there is a range of equality-based legislation that applies similar obligations to employers. In Northern Ireland and Great Britain (i.e. England, Wales and Scotland) public authorities have obligations respectively under Section 75 of the Northern Ireland Act and Section 149 of the Equality

[21] Draft Guidance, 15.

Act 2010 to ensure that equality of opportunity and good relations are central to policy making.

These laws are relevant as monitoring which does not comply with them is likely to infringe the 'fairness' principle of the UK GDPR and associated principles in Northern Ireland equality legislation.

Where monitoring is used to make decisions about workers, you need to ensure this does not result in discrimination. Employers should also remain aware of their obligations under employment legislation more generally and their duties under any consequential statutory instruments in both Northern Ireland and Great Britain (i.e. The Maternity and Parental Leave etc. Regulations 1999).

(iii) Employers may also benefit from further guidance on the ICO's interpretation of the equal opportunities conditions for processing in Part 1 of Schedule 1 to the Data Protection Act 2018. This is a challenging issue for many employers who wish to collect diversity data to support and track the success of equal opportunities initiatives in recruitment and retention. We suggest that a case study relating to an employer who wants to provide employees the opportunity to (voluntarily) enter and maintain diversity data within a secure portal, with a link to a specific data protection notice about use of the data, and to which there would be restricted access to by senior leaders and HR managers only. The information could be used to generate diversity statistics on an aggregated basis only (and ensuring that individual employees cannot be identified by the recipient of the statistics).

(b) **Employment Relationship and implied terms**

(i) Within employment relationships, the parties will be subject to the implied term of mutual trust and confidence.[22] The duty not to undermine mutual trust and confidence has been viewed as a "general, portmanteau obligation"[23] and as such can encompass a wide range of conduct, including the adoption of employee monitoring programs.

(ii) Throughout most industries, the majority of employers will utilise some form of quality control to safeguard workers, as well as protect their own interests or the interests of their customers. With the advent of remote working and the emergence of new business structures, such as the gig economy, the methods in which monitoring occurs have continued to evolve. Despite this evolution in the types and extent of monitoring technologies, the majority of workers generally expect some level of monitoring as a consequence of their employment relationship.

(iii) Regardless of this base expectation, when monitoring technologies are inappropriately used their adoption may conflict with the relationship of mutual trust and confidence between employers and employees. This conflict is particularly apparent when monitoring captures a worker's private information.

[22] Malik and another v Bank Of Credit & Commerce International SA (in compulsory liquidation) [1998] AC 20, 47.
[23] Malik and another v Bank Of Credit & Commerce International SA (in compulsory liquidation) [1998] AC 20, 35.

As such, in the adoption of their legislative obligations, employers ought to also consider their overarching common law and implied obligations towards workers. This interrelationship with common law principles is not currently recognised in the Draft Guidance. Therefore, it is recommended that such an observation is made to make employers aware of their monitoring obligations, both under statue and at common law.

(c) **Regulation of Investigatory Powers Act 2016**

(i) It may be prudent to mention the distinction between simple monitoring and monitoring by intercepting an electronic communication, as compliance for monitoring by interception of electronic communication will be required by the employer under the Investigatory Powers Act 2016 ("**IP Act**") where it is an offence to intentionally and without lawful authority to intercept an electronic communication in the course of it transmission. This would then link to the section on 'can we use covert monitoring'. Employers are permitted to carry out an interception in certain circumstances. The relevant point is where the interception is for monitoring and record-keeping purposes, and is authorised under the Investigatory Powers (Interception by Business etc for Monitoring and Record-keeping Purposes) Regulations 2018 SI 2018/356.

(ii) At present there is reference to the Investigatory Powers (Interception by Businesses etc for Monitoring and Record-Keeping Purposes) Regulations 2018 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 and to this guidance being in line with the provisions in these regulations. The previous ICO guidance provided guidance in more detail about the impact of these statutes and the interplay.

"Electronic communications are broadly telephone calls, fax messages, e-mails and internet access. Monitoring can involve the 'interception' of such communications. The Regulation of Investigatory Powers Act, and the Lawful Business Practice Regulations made under it, set out when interception can take place despite the general rule that interception without consent is against the law. It should be remembered that - whilst the Regulations deal only with interception - the Data Protection Act is concerned more generally with the processing of personal information. Therefore when monitoring involves an interception which results in the recording of personal information an employer will need to satisfy both the Regulations and the requirements of the Data Protection Act."[24]

(d) ELA recommends it is critical for employers to be aware of the intersection between IPA and the DPA 2018.

[24] EPC, 64.

3.7 **Data Protection Principles**

To the extent ELA has queried the ICO guidance on the impact of the privacy principles in the context of employee monitoring, this has been noted below:

(a) **Transparency**

(i) In its conceptualisation of the fairness principles, the ICO noted that employers must tell workers about monitoring in a "way that is accessible and easy to understand". There is a commercial and legal need for clarification of what this requirement means for employers, in particular whether the ICO envisages that this obligation may be addressed by means of a privacy policy or whether employers are expected to engage in further communication of its monitoring programs. Post the WhatsApp decision,[25] employers may take the view that in practice they are required to explicitly detail the types of personal data that will be obtained in the employment relationship and how this data will be processed and used by the organisation. This obligation is linked with the adjacent requirement to ensure that privacy policies remain accessible to users. As the WhatsApp decision would require employers to detail any monitoring programmes, it is queried whether the ICO is suggesting an extension of this decision, such that employers must engage in further communication with employees beyond the requirements of the UK GDPR and the Data Protection Act 2018.

(ii) The ICO has previously provided specific guidance on the types of features it expects employers should consider in their privacy policy to improve the transparency of monitoring programs.[26] This level of detail would be a helpful addition to the Draft Guidance to make clear an employer's obligations in respect of transparency, in particular how these requirements may have changed in practice post the WhatsApp decision.

(iii) In respect of the transparency principle, we note that a worker's awareness will often influence their expectations of monitoring, such that where the purpose and extent of monitoring has been communicated to workers, they can often feel less negative towards these programs. This sentiment has been previously recognised by the ICO[27], and appears to be reflected in the new consultation requirements. ELA submits that it would be beneficial for this type of commentary to be included in the Draft Guidance, such that employers are reminded to consider the importance of communication prior to the adoption of monitoring programs (where such communication is appropriate in the wider circumstances). This recommendation reflects good practice from an employee relations perspective and may assist to reduce the level of employee discomfort in the adoption of workplace monitoring.

[25] Commissioner for Data Protection, Decision of the Data Protection Commission made pursuant to Section 111 of the Data Protection Act, 2018 and Articles 60 and 65 of the General Data Protection Regulation (20 August 2021) <https://edpb.europa.eu/system/files/2021-09/dpc_final_decision_redacted_for_issue_to_edpb_01-09-21_en.pdf>.
[26] EPC, 69 – 73.
[27] EPC, 65.

(b) **Accountability**

(i) In the context of its wider discussion on accountability, the Draft Guidance provides that where an employer has a data protection officer ("**DPO**"), the DPO ought to be closely involved in any monitoring plans.

(ii) In addition to this guidance, it is recommended that the ICO also notes that any individuals who monitor workers, or who can authorise such monitoring, should be briefed on the UK GDPR and DPA 2018. This obligation would expand beyond the DPO and may include members of senior management. The inclusion of this provision would also be reflective of previous guidance on this issue.[28]

(c) **Purpose Limitation**

(i) In its discussions on purpose limitation, the ICO observed that employers may change the purpose of their monitoring where the new purpose is "related to activity that no employer could reasonably ignore".[29] The types of activities that fell within this category were said to included "criminal activity at work, gross misconduct and health and safety breaches which jeopardise workers".[30] Similar to the ICO's general approach, it would be beneficial for the Draft Guidance to include a practical case study example of where any employer intends to change its purpose for monitoring in light of an activity that they could not reasonably ignore. Also, this could be extended to misuse of confidential information or evidence of unlawful behaviour when leaving employment.

(ii) One such example may include monitoring emails for emails to personal email addresses which may evidence misuse of confidential information.

(d) **Data Minimisation**

(i) In respect of the ICO's discussion of data minimisation, ELA submits that it may be beneficial to slightly amend the given example as per the below [the addition in red and underlined]:

An employer collects office ethernet connection data to monitor the use of workspace and ensure there is sufficient capacity for workers. They should not re-use this information for performance management purposes without identifying a new lawful basis and establishing the necessity and proportionality of this new purpose and being transparent with employees about the new scope.

(ii) We consider these amendments are required in order to accurately reflect other data protection principles that would arise in these circumstances.

[28] EPC, 66.
[29] Draft Guidance, 19.
[30] Draft Guidance, 19.

(e) **Accuracy of information**

(i) The Draft Guidance suggests that employers "should...provide workers with the opportunity to comment on the accuracy of any data gathered through monitoring".[31] It is firstly queried whether the ICO's use of "should" imposes a mandatory obligation on employers. If this obligation was mandatory, it would place a large administrative undertaking on both the employer and the individual. For instance, it is unlikely that employees would be willing to comment on the accuracy of all data gathered on them, for example, that was produced from email monitoring as this data could be in the thousands (in particular for employees within organisations for long periods). This is also likely to cause issues where the data amounts to opinions of the individual by others which is collected via email review monitoring. As such, this suggestion appears to be unworkable in practice.

(ii) The ICO has also suggested that "within or alongside disciplinary or grievance procedures and performance reviews or appraisals workers can see and, if necessary, explain or challenge the results of any monitoring".[32] At present, employees will have a right to appeal and comment on the results of any monitoring practices after the findings of any disciplinary and grievance procedures.[33] In light of this existing right, it is submitted that the Draft Guidance should be amended as follows [amendment in red and using strikethrough]:

Ensure that where an adverse decision is taken or is likely to be taken as part of disciplinary or grievance procedures and performance reviews or appraisals workers can see and, if necessary, explain or challenge the results of any monitoring being relied on.

(iii) As there is already a statutory framework to protect employees to ensure fairness of process within employment law, this may be seen as a separate process for the employer to take, which ELA assumes is not what is intended. That should be clarified.

(iv) The Guidance references (at page 22) briefly in very broad terms that employers should keep only the information which is relevant to the purpose being monitored, and suggests regularly reviewing the information collected and destroying that which is not necessary. We suggest expanding on this to emphasise the risk of data hoarding and the benefits of data minimisation, perhaps by further unpacking some of the principles of the Accountability Framework within the Guidance, with examples illustrating the risks.

[31] Draft Guidance, 21.
[32] Draft Guidance, 21.
[33] ACAS, "Code of Practice on disciplinary and grievance procedures" (11 March 2015), ss 27 – 29.

(f) **Security**

(i) The Draft Guidance has provided that employers should take care to identify the "most appropriate person or people to access the data collected". Whilst ELA agrees with this proposition, it would be beneficial for the ICO to provide guidance on who generally will be considered to be the most appropriate person or the types of factors that employers should consider when selecting these individuals. By way of an example, in the EPC it was noted that employers should consider whether monitoring is more appropriately carried out by security or personnel functions rather than by line managers.[34] A similar level of guidance would be beneficial in the Draft Guidance.

(ii) On the principle of security, the Draft Guidance further provides that employers should ensure that individuals are "properly trained to handle monitoring information". The guidance should be amended to provide further commentary on the type of training that would be expected under this obligation. It is recommended that this training should be provided for all workers who may come across personal information whilst monitoring and should address their data protection obligations in these circumstances. In addition to this base level of training, senior management should also be trained on the UK GDPR and DPA 2018. This standard of training is reflective of the ICO's previous guidance.[35]

3.8 **Data Protection Impact Assessment (DPIA)**

(a) In respect of DPIAs, the ICO has noted that employees "should complete a DPIA even where this is not obligatory".[36] The inclusion of this commentary in the Draft Guidance suggests that this is a set obligation on employers, however, the subsequent drafting on this issue appears contradictory to this statement. This issue is reflective of broader language issues within the Draft Guidance. It is submitted that the ICO's use of the term "should" at times appears to impose a mandatory obligation on employers whilst in other instances it merely indicates a non-binding recommendation. To prevent employers misinterpreting the Draft Guidance, it is recommended that the ICO reviews its drafting to make clear where it intends to impose bindings obligations. The Draft Guidance should also be in sync with the ICO detailed guidance on DPIAs[37] and clarification on when the requirement for a DPIA is required in alignment with the criteria in the Article 29 working party guidelines on DPIA[38] (which have been adopted by the European Data Protection Board).

(b) For completeness, ELA also notes that the Draft Guidance has not addressed circumstances where monitoring only possesses a low or medium risk to workers' data protection rights and freedoms. It is recommended that further alterations are made to the Draft Guidance to address the responsibilities of employers (if any) in these circumstances.

[34] EPC, 67.
[35] EPC, 67.
[36] Draft Guidance, 37.
[37] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/
[38] https://ec.europa.eu/newsroom/article29/items/611236

3.9 **Consultation with Workers**

(a) The Draft Guidance purports to introduce a new consultation requirement for employers to inform workers on any data that is processed via monitoring programs. At page 23 of the Guidance, the ICO states that when organisations plan on introducing monitoring, they should seek and document the views of workers or their representatives "unless there is a good reason not to".

(b) On the one hand, the addition of these words may go further than Article 35 of the UK GDPR. This states (as part of a data protection impact assessment ("DPIA")) that where appropriate], a controller shall seek the views of data subjects or their representatives on the intended processing. However, the Guidance as drafted suggests that this consultation should be carried out in advance of any form of workplace monitoring (i.e., including in cases where the employer concludes that the monitoring is low risk and a DPIA is not required). This does not necessarily reflect Article 35. On the other hand, see our query below as to whether consultation is compulsory in certain circumstances.

(c) At present, it remains unclear as to whether the ICO is in effect imposing a formal consultation requirement on employers or is merely requiring that employers have to "inform" employees about these programs. In addition to this issue, further commentary is required with respect to:

(i) with whom consultation is required;

(ii) what the consultation process should entail;

(iii) how long the consultation is needed for;

(iv) whether the employer must reach agreement with the workers as part of the consultation; and

(v) what type of information is required to be provided.

(d) In respect of who the employer should consult with, it is acknowledged that this requirement will vary depending on if the organisation is unionised. For non-unionised organisations, it is unclear whether the employer will need to create a process to appoint employee representatives or whether consultation is required across the entire workforce. Conversely, for organisations which are unionised, further guidance is needed as to an employer's obligations where there are multiple unions, or where the official unions do not represent all workers within an organisation.

(e) The Draft Guidance has suggested that as part of the consultation, employers must tell workers "how and why" they will use their personal data.[39] Further information is required on what this requirement entails in practice. In many instances, monitoring technologies will involve proprietary information and third-party providers may be reluctant or unwilling to disclose how these programs specifically work. Therefore,

[39] Draft Guidance, 23.

many employers will be unable to explain in detail "how" these programs capture and process employee data.

(f) Similarly, where employers are engaging in covert monitoring, explaining how these monitoring programs work in detail will often undermine the purpose of the monitoring. For instance, an email monitoring program may be used to track instances of insider trading. This program may have been created to flag emails with specific key words. If employees are provided with this information as part of the consultation process, it would undermine the employer's aim to capture insider trading and alert perpetrators as to attempt to avoid detection.

3.10 **Covert monitoring**

(a) The ICO's detailed consideration of the various factors that employers should consider in the adoption of covert monitoring will be beneficial to employers in overall consideration of their data obligations as in line with the **López Ribalda** case. However, for completeness we note the following points for the ICO's reflection.

(b) In respect of the authorisation requirements, the Draft Guidance has provided that these technologies should only be authorised by the "highest authority" in the workplace. In practice, it is assumed that this requirement would capture a company's board of directors, the CEO or like roles. In previous ICO guidance, authorisation for covert monitoring was merely required from "senior management".[40] ELA submits that it would be more appropriate for senior management to approve covert monitoring programs as these individuals are often closer to the issues, particularly where monitoring is used to address misconduct. Senior management can make a more informed assessment of whether covert monitoring is reasonable and proportionate in the circumstances. ELA recommends the guidance should revert to that contained in the previous version.

(c) The Draft Guidance provides that employers must not use "covert monitoring to capture communications that workers would reasonably expect to be private, such as personal emails". This example raises difficulties where covert monitoring is used in circumstances where the sending of private emails itself would constitute wrongdoing. This type of monitoring is often critical when employees are suspected of sharing confidential information or unlawful team moves or theft. For instance, employers within the banking sector may wish to monitor WhatsApp messages on employees work devices, to ensure that employees are not sharing insider information. This type of monitoring by its very nature would require employers to capture communications that workers would expect to be private. As such, it is recommended that the Draft Guidance is updated to capture the nuances of where it may be appropriate for employers to review an employee's private communications, together with further mitigations to protect employees' data protection rights – e.g., by recommending that such monitoring is covered in employee privacy notices, data minimisation principles are applied (e.g., through use of search terms and redaction) and that specific notice is given to employee data custodians at the first available opportunity.

[40] EPC, 74.

3.11 **Objections to monitoring**

(a) As part of the Draft Guidance, the ICO has discussed workers' rights to object to monitoring.[41] Whilst workers do have this right, the current drafting of the Draft Guidance suggests that this is a unique right arising from the adoption of monitoring, rather than being a reflection of Article 21 of UK GDPR. As such, it is recommended that the Draft Guidance is amended to conceptualise this right as per the below:

In common with their general right to object to the processing of personal data under Article 21 of UK GDPR, workers will have the right to object to being monitored ~~Yes~~, although this right is not absolute one. A worker can object where the lawful basis you are relying on is:

- *public task (for the performance of a task carried out in the public interest or for the exercise of official authority vested in you); or*
- *legitimate interests.*

The worker must give specific reasons why they are objecting to you collecting and processing data through monitoring. The reasons should be based upon their particular situation.

(b) Where employers reject a workers' objection to monitoring, the Draft Guidance has provided that they must inform the worker of their ability to seek to enforce their rights through a judicial remedy.[42] Whilst we understand that this comment is intended to be reflective of an employer's obligation under Article 12(4) of the UK GDPR, further guidance is needed on whether this requirement could be satisfied through this information being documented in privacy policies or whether employers must inform workers of this right in response to every monitoring complaint. Also, it would also be appropriate to remind the worker of their right to lodge a complaint with the ICO.

3.12 **Automated processes in monitoring tools**

(a) **What is meant by automated decision making?**

The ICO's current use of language in its discussion of the impacts of Article 22 of the UK GDPR raises various issues. The use of the phrase "automated decision making", a term that does not appear in the UK GDPR, appears to inadvertently extend the scope of Article 22. This arises as the use of this phrase fails to make clear that GDPR obligations will only be related to decision-making that has a legal or similarly significant effect and will only apply to solely automated decisions (i.e. without any human intervention). As such, for the purpose of clarity, it is recommended the Draft Guidance is amended to reflect the language of Article 22. Further guidance on the exceptions under Article 22 (2)-(4) should be clarified.

[41] Draft Guidance, 25.
[42] Draft Guidance, 25.

(b) **Role of Consent**

(i) For solely automated decisions with a legal or similarly significant effect on workers, the ICO has noted that employers may use this type of technology where an individual has given their explicit consent.[43] The ICO's discussion of consent is not reflective of the different conditions imposed under Article 22 of the UK GDPR. For the processing of personal data, it is sufficient for employers to rely on the contract of employment for the basis of adopting automated decision making. Conversely, these technologies are only suitable for the processing of special category data where:

(A) an employee has given their explicit consent; or

(B) the processing is necessary for reasons of substantial public interest and is proportionate.

(ii) In either circumstance, employers must ensure that there are suitable measures in place that safeguard the data subject's rights and freedoms.[44] To ensure the guidance is reflective of legislative requirements under Article 22, we recommend that it is amended to reflect the different conditions imposed for the processing of personal data and special category data.

(iii) The Draft Guidance has also failed to acknowledge the inherent difficulties in relying on Article 22 for the processing of an employee's special category data. This difficulty arises as the very nature of the employment relationship means that it is rare for processing to be needed for reasons of substantial public interest outside of the public sector. As the basis of explicit consent is difficult to rely on within employment relationships (due to the inherent power imbalance between employers and workers), Article 22 fails to provide a legitimate pathway for many employers to process special category data.

(c) **Role of Human Oversight**

The Draft Guidance has suggested that where automated decision-making tools do not have an appropriate level of human oversight, employers will be in breach of Article 22 of the UK GDPR.[45] This interpretation of Article 22 is incorrect. Article 22 only prohibits solely automated processing where the exceptions in sub clauses (2) - (4) are not satisfied. Under the UK GDPR, employees will have the right to obtain human intervention post an automated decision where the technology has merely used their personal information and the employee did not provide their explicit consent to the process. However, the UK GDPR does not inherently prevent the use of automated decision making with no human oversight. As such, it would be beneficial for the ICO to reconsider its interpretation of Article 22.

[43] Draft Guidance, 30.
[44] UK GDPR, art 22(4).
[45] Draft Guidance, 31.

(d) **Communication Requirements**

In the context of automated decision making, employees and prospective employees will have the right to be informed of the process behind any such decisions. In the Draft Guidance, it is contended that employers must provide "meaningful information about the logic involved, as well as the significant and the envisaged consequences" of the processing.[46] Similar to the approach adopted elsewhere in the Draft Guidance, ELA submitted that it would be beneficial for the ICO to provide practical examples of what "meaningful information" will involve. It would also be beneficial for the ICO to provide commentary on the particular factors employers should consider when explaining the processes behind automated decisions. As noted above, monitoring technologies will often be proprietary information and as such employers may not be aware of these programs specifically work.

4 WHAT ABOUT AUTOMATED PROCESSES IN MONITORING TOOLS

4.1 We are grateful to the ICO for the additional guidance on automated processes in monitoring tools. It represents a real improvement on the original Employment Practices Code which did not address the issues posed by automated decision making, in particular in the context of monitoring. However, as noted in previous responses on the revised draft Employment Practices Code, data protection law and market practice have undergone significant changes in the last 10 years and we believe that the current suggested draft guidance on automated processing does not quite offer the clarity of guidance required given the current state of technological capability. We recognise that this is a complex and rapidly changing area, but consider that there are a number of points where the guidance could be clarified and / or expanded. Addressing each section in turn:

4.2 ***'At a glance'***

(a) We believe it would be helpful to draw a clearer distinction between the concepts of "decision making", "automated processing" and "profiling". Under Article 22 GPDR, it is not processing or profiling itself that is potentially conflicting with data subjects' rights, but any *decision* "which produces legal effects…or similarly significant effects" (emphasis added) taken based solely on automated processing or profiling. Our experience is that automated processing is an integral part of many businesses, and something that can promote organisational efficiency. The use of automated processing has increased significantly in the last ten years, and will only continue to do so. ELA considers that it is important to recognise that they are often an important part of an organisation's commercial operations. That said, we still believe that practices of actual decision making based solely on automated processing is relatively uncommon. The introduction alludes to that, but we believe it could be made clearer that it is the decision making which should be the focus of compliance efforts in this specific context, so that protections for data subjects are appropriately targeted and preserved.

(b) A smaller point, also in the introduction we believe that the reference to 'people analytics' could be misleading. There is no set definition of ‘people analytics’, but it is typically thought to mean involving the processing of talent and people data to improve

[46] Draft Guidance, 31.

workforce processes and talent decisions. Employee monitoring is often broader than that, for example data loss prevention tools may automatically process employee data to predict loss or theft of confidential information. In effect, people analytics is a sub-category of employee monitoring and not the sole category. A small point, but it could lead readers of the guidance to conclude that only 'people analytics' fall within the scope of the remainder of the guidance, which we don't believe is the case.

4.3 ***'What do we mean by automated decision making and profiling?'***

(a) As mentioned above, Article 22 UK GDPR is a cumulative provision that requires:

(i) a decision;

(ii) that is based solely on automated processing, including profiling; and

(iii) which produces legal or similarly significant effects.

(b) It would be helpful if the guidance made this clearer, and also provided more detail on each of the elements of the Article 22 requirement, in particular:

(i) what constitutes a "decision". Is, for example, the placing of a flag on someone's IT account because suspicious activity has been detected a "decision"? In this context, it would also be helpful to understand the ICO's position on how the intersection between artificial intelligence and automated decision making operate in this space. A clearer definition of 'decision' would assist that. But, further, it would be helpful to understand the extent to which human intervention at the input phase is sufficient to take an 'automated' process outside of the scope of Article 22 UK GDPR and, if so, the degree of human intervention or design that is required at the input phase. Artificial intelligence ('AI') often requires significant human input into the design and operation of an AI solution, and the decisions reached are intended to be 'intelligent', rather than just solely automated. So whilst the 'output' is effectively automated, the 'input' is defined by human decision making. It would be helpful to understand the ICO's views on the extent to which AI could constitute a non-automated decision, if at all.

(ii) what is a "legal effect". Does it have to be a decision that affects someone's statutory or contractual rights, and is that just express rights or also implied rights? Some guidance on what is determinative of something being of legal effect would be helpful for employers and employees given this is a key threshold for determining whether Article 22 applies. Many HR related 'profiling' tools offer a range of functionalities across a spectrum of impact - from identifying training needs, to salary banding or potential candidacy for promotion - understanding where the threshold is for the application of Article 22 is critical.

(iii) equally, guidance on what is a "similarly significant effect" would also be very helpful. It is currently unclear what is similarly significant to a legal effect. Guidance from the ICO, or some examples of what it considers to be a decision of "similarly significant effect" would be helpful. The example

provided by the ICO of an automated process to calculate pay would to us appear to have a "legal" effect, as it affects how an employee is paid under their (presumably) contractual right to receive pay, whereas the example guidance from the ICO suggests it has a 'significant' effect. Clarity on that would be helpful.

4.4 ***'What do we need to consider if we are planning to make solely automated decision with legal or similar effect?'***

(a) The guidance in this section broadly replicates the provisions of Article 22, and it would be helpful to have greater clarity and guidance from the ICO on when and how the potential exceptions could apply in the UK.

(i) In the employment context, the employment contract will be the key contract between the parties so it would be helpful to understand from the ICO whether there may be circumstances where it is considered "necessary" to conduct automated decisions for the entry into or performance of an employment contract. In the example provided by the ICO, does the ICO consider that an automated process to determine an employee's level of pay be deemed "necessary" for the performance of the obligation to pay an employee under their contract? It is conceivable that there may be circumstances where it is impractical for human intervention to verify an employee's level of productivity, and that an automated process is the most accurate and efficient means.

(ii) The ICO's views on the validity of consent in this context would also be extremely helpful. Earlier in the draft guidance (at page 13) the ICO notes that consent is not usually appropriate in the employment context due to the imbalance of power between the employer and employee, and this is consistent with the ICO's guidance in other areas. However, under automated processing the guidance says it is the "most likely gateway" but that it "may be difficult". This seems to suggest that consent may be freely given in an employment context which appears inconsistent with the ICO's other guidance on consent in employment. Is it the case that to be 'freely given', an employee must simply be given an alternative which does not subject them to detriment? An example of how this would operate in practice would be helpful.

(b) We also think that it would be helpful for this section to explain briefly that if employers are relying on Article 22(2)a or c then they should also implement suitable measures to safeguard the data subject's rights and freedoms. The ICO's guidance indicates that the crucial safeguard is the ability for human oversight, but it would be helpful to understand if there are other safeguards that the ICO considers that employers should or could consider implementing.

(c) It would be particularly helpful if the ICO could provide guidance, or a worked example, in the employment context of automated processing involving special category data and the potential for justification under Article 9(2)(g) UK GDPR and Schedule 1 Part 2 of the UK DPA 2018, including the use of an 'appropriate policy document' (and what that would look like) and additional safeguards.

4.5 ***'What should we tell workers about automated decision making?'***

(a) The guidance is helpful in that it draws attention to the requirements of Article 13(2)f. UK GDPR and the standard of information required to be provided. However, it would be helpful to understand the ICO's view on what constitutes "meaningful" information. Is it the case that data subject's must simply understand that a decision may be made on the basis of automated processing, or should they also be provided with information on how the processing operates? We recognise that there is often a difficulty with 'explainability' of complex automated processing, and also that for some organisations the automated processing may be based on complex programmes, algorithms and data analytics, some of which may be proprietary information for the company or a third party provider. Either they will not be able to explain the processing in simple terms, or may be prevented from doing so as they cannot disclose details for commercial reasons.

(b) This will provide greater legal certainty for both employers and employees, and enable them to better understand the level of information that data subjects are entitled to in the context of automated decision making.

4.6 The ICO has asked responders "***Does the draft guidance cover the relevant issues about monitoring at work?***" In summary, we suggest the draft guidance may usefully expand on or address the following points in relation to this section:

(a) More detail about the definition of automated processes and AI that may be used in monitoring at work.

(b) Greater emphasis should be given on the usage of data protection impact assessments and consultation with data subjects or their representatives.

(c) Better examples should be provided in the draft guidance on how Article 22 UK GDPR applies in practice.

Dealing with each in turn:

4.7 **Definitions**

(a) It is widely known that many employers, as data controllers, are using automated processes that include Artificial Intelligence ("**AI**") to monitor their staff, as data subjects, at work[47]. For example:

(i) Sifting through job applications and CVs submitted electronically for recruitment through identification of key words and phrases.

(ii) Conducting interviews online, such as through questions generated by a chatbot.

(iii) Allocating work duties and shifts.

[47] For example, see: Jeremias Adams-Prassl 'What if your boss was an algorithm?' via IFOW

(iv) Monitoring employee output and activities against performance targets.

(v) Imposing sanctions and terminating employment.

(b) The draft guidance explains what the ICO means by 'automated decision making and profiling'[48] but query if this captures the ways in which AI is currently being used by employers to make decisions that significantly affect data subjects, particularly through machine learning and algorithms[49]. The ICO will be aware there is no single agreed definition of AI which includes algorithm or machine learning[50]. As such, our concern is that the draft guidance currently implies a narrower basis than what is required for data controllers and data subjects to understand where they stand in respect of both employment law and data protection law. Query if the ICO should seek to agree a definition with, for example, the EHRC which has in effect a supervisory or regulatory role in relation to AI in the workplace.

4.8 **Data protection impact assessments**

(a) We note that the checklist (on page 33) refers to considerations of a DPIA but we recommend that the positive requirement should be made clearer in the section **'What do we need to consider if we are planning to make solely automated decisions with legal or similar effect?'**

(b) The draft guidance does not specifically refer to any positive requirement for employers to conduct a data protection impact assessment ("**DPIA**") before it commences automated processing as such. It is arguable that solely automated decisions would necessitate "*systematic and extensive evaluation"* under Article 35(3)(a) UK GDPR therefore query if the guidance should reflect that. See also the ICO's Guidance on DPIA's generally.

(c) The draft guidance asserts, incorrectly in our view, that an individual's explicit consent is the most likely gateway for employers planning to make solely automated decisions with legal or similar effect, i.e. to monitor workers. Based on our experience, most employers would assert the lawful basis for this type of processing is necessary for the performance of a contract (namely the contract of employment) between the employer as data controller and worker as data subject under Article 6(1)(b) UK GDPR. Similarly, employers will normally assert that the requirements of Article 22(1) UK GDPR shall not apply due to the contract of employment between the employer and worker in accordance with Article 22(2)(a) UK GDPR.

(d) The draft guidance refers to Article 22 UK GDPR providing protection to workers against decision made solely by automated decision-making that has legal or similarly significant effects. However, this perhaps does not go far enough in addressing uncertainty about how Article 22(3) UK GDPR ought to be applied in practice and taking into account employment law issues. The Guidance might deal with whether employers, as data controllers, should assess the risk of algorithmic bias facilitating unlawful discrimination contravened by the Equality Act 2010 ("**EqA 2010**") or

[48] "Automated decision making is a decision made by automated means without human involvement. Automated decision making often involves profiling too."
[49] See: 'The Amazonian Era' report by IFOW
[50] Eg, compare the European Commission's proposed definition for its AI Act and what the TUC say in its survey and report.

breaching other protections, such as the right to privacy. It is because of the potential risks associated with bias and potential unlawful discrimination under the EqA 2010 against data subjects, that employers might be prudent to conduct a DPIA before commencing automated processing and/or AI to monitor workers. Query if the Guidance should reflect this caution or whether this strays too far into other policy/legislative areas.

4.9 **Consultation**

(a) The draft guidance purports to introduce a new consultation requirement – see paragraph 3.9 above for more detailed comments on this. The ICO may wish to take a view as to the ambit of the existing statutory requirements for information and consultation by employers to workers or their representatives.

(b) There are some circumstances where an employer has a free-standing obligation to carry out consultation, such as where the employer recognises an independent trade union for collective bargaining under s.178 TULRCA 1992 or where the union has appointed safety representatives or a safety committee under the Safety Representatives Safety Committee Regulations 1977 or where a non-unionised workforce is required to consult under Health and Safety (Consultation with Employees) Regulations 1996 and ICE Regulations 2004. There is a question – ELA takes no view itself – as to whether these obligations may be triggered by aspects of automated decision-taking in respect of employees and therefore query if the guidance should refer to the relevant legislation and question whether employers should consider whether it applies in their particular context. The ICO may prefer to wait for judicial guidance on the point but trades unions in particular consider this a live issue.

(c) The examples given on page 30 of the draft guidance may not accurately reflect the uncertainty about what Article 22 UK GDPR means in practice for employer data controllers. We consider the examples could be improved by addressing the extent of human involvement to trigger the 'solely' basis of decisions made by automated processing in Article 22(1) UK GDPR. This should make clear how the ICO envisages the scope of any human involvement in the automated decision-making processes, as most (if not all) automated processes require some human intervention. That intervention may, for example, become all but automatic itself as a result of consistent practice or indeed express policy. Additionally, we would appreciate greater detail about the scope of what automated processing is 'necessary' for the performance of an employment contract in Article 22(2)(a) UK GDPR. We understand there is a debate as to whether alternative methods might always be available.

(d) The relevant policy context here is that:

(i) The producers of AI may not have provided sufficient information to facilitate the requirements for employers to provide meaningful information to workers about the logic of automated processing and AI involved as well as the significance and consequences of such processing under Articles 13 and 14 UK GDPR.

(ii) There is an inherent power imbalance in the employment relationship. Employers are required to take decisions in good faith, and in a way that is lawful and rational, and employment contracts are subject to an implied term of mutual trust and confidence. However, many workers (particularly those who are not members of a trade union) will not know about their rights or how to enforce them. The ICO acknowledges (at page 23) the potential *'chilling effect on the trust between workers and employers*' of monitoring: any such effect may be even greater where monitoring is followed by automated decision-making.

Whilst it is not the ICO's role to promote the successful use of AI in the workplace, it may wish to take this into account in formulating guidance that use of the technology may win wider acceptance if mechanisms exist whereby those it affects may be given the opportunity to understand it better. Query though if (see above) this too takes the ICO into legislative and policy areas it considers currently outside its remit.

4.10 The ICO has asked whether "*there any additional examples or scenarios you'd like to see in the guidance?"*

Here are three examples the ICO may wish to consider, depending in part on whether it considers that Article 22 applies in these circumstances:

4.11 **Example 1**

(a) Applicants are given a gamified recruitment assessment as part of a recruitment process which measures their suitability for various elements of their proposed role by monitoring their reactions and/ or productivity during the assessment. Although decisions about who to progress to interview stage are taken by the talent acquisition team, candidates are pre-sorted by the software and in practice only those candidates with 85%+ suitability are taken forward.

(b) This may fall within Article 22. If it does then the employer should as a minimum:

(i) Consider whether it has a lawful basis to use the assessment tool;

(A) The employer identifies a legitimate purpose of recruiting a suitable workforce, with a focus on reaction times and/or productivity, which is a requirement of certain vacancies ("**purpose test**");

(B) The employer then completes an LIA and determines it can rely on the legitimate interest lawful basis on the grounds that:

1) the employer frequently receives hundreds of applications for certain roles, making it extremely difficult to effectively manage and shortlist suitable applicants ("**necessity test**");

2) the employer's talent acquisition team has previously attempted to observe individual applicant assessments to assess reaction times and/or productivity, however, the outcome of this has often been subjective and difficult to achieve consistently and

fairly (or otherwise has not been possible or practical because of the above bullet point) ("**necessity test**");

3) the software will not capture any special category personal data (except for the prevention of discrimination, as considered below) and will only capture inputs on the applications keyboard and mouse ("**balancing test**") [unless by 'reactions' we mean facial / body movement / verbal reactions, which may well be relevant - we think this would be an example of a failed LIA except in circumstances where facial expressions and body language etc. is extremely important, i.e., for customer-facing roles];

4) given the nature of the software, and the information provided to applicants about it and the roles advertised, the employer considers that applicants would reasonably expect such monitoring of reactions / productivity; clearly being able to work in a fast-paced environment means such skills are relevant, and the employer does not collect anything further that may be considered excessive, such as via video/audio monitoring ("**balancing test**");

5) applicants are given the opportunity to declare if they have any disability (such as dyslexia) that may disadvantage them in the assessment and are accordingly afforded extra time if appropriate. The talent acquisition team reviews such applications separately on an anonymised basis. The collection of such special category data is deemed necessary to prevent discrimination on the grounds of disability ("**balancing test**");

(ii) Document that lawful basis in its data protection policy;

(iii) Conduct a DPIA to consider and address any risks before commencing use of the assessment tool:

(A) Some of the key issues identified in the DPIA are:

1) The employer identifies scenarios where the monitoring software may not be necessary or appropriate. A decision is made not to use the software when recruiting for certain roles that do not involve fast reaction times and/or a greater focus on productivity, such as customer service positions where quality and relationships form a greater requirement of the role. Where the number of applications is relatively small and reactions / productivity is still a prevalent requirement, the talent acquisition team will consider whether they can make the assessments themselves without use the software.

2) Personal data is deleted or anonymised after one year of a decision to give applicants ample time to review or challenge any decisions taken.

3) To prevent the risk of bias, the employer allows applicants to voluntarily (with explicit consent) contribute certain sensitive information (such as race/ethnic background, disability, socio-economic background). This is anonymised by the supplier of the software and used solely to identify risk of bias to better improve its scoring system. This sensitive information is not visible by assessors during any part of the recruitment process. Applicants can freely choose to provide this information and not doing so will not affect their application. The collection of any special category data is deemed necessary to prevent discrimination.

4) The employer investigates the risks of software by making extensive enquiries with the supplier. It is discovered that the supplier has taken into account anomalies in the data which may disadvantage applicants. For example, applicants may face technical issues which mean they are diverted from the software during an assessment, suggesting a lower rate of productivity. The algorithm used is designed to detect these anomalies and flag these to the employer's talent acquisition team for human intervention. The talent acquisition team are given training to understand scenarios outside of applicant's control that may affect the scoring system.

(c) The above outcomes from the DPIA are documented as policy in the employer's data protection policy and reflect practice.

(i) Provide applicants details of how their data is processed by the assessment tool;

The privacy notice presented to applicants, amongst other things, explains that reactions / productivity is measured by recording keystrokes and movement of applicant's computer mouse. It provides an examples of how this works in practice, i.e., an example of an applicant taking long periods to react to simpler tasks yet quickly attempting complex tasks which require greater thought and planning. It explains why reaction times and productivity is relevant to certain roles of the employer.

(ii) Ensure the talent acquisition team regularly review applications for suitability for roles and cross-check the scoring provided by the assessment tool against the individual applications;

(iii) Permits applicants to challenge a decision by the assessment tool or to request human intervention;

This is reflected in the employer's privacy notice, but also on the applicant's screen prior to the assessment beginning and at the end of the assessment. An email is sent to applicants confirming completion of the assessment, once more reminding them of their ability to challenge or request human intervention.

(iv) Ensure that the assessment tool and its use of the same complies with its obligations under employment law.

(d) The employer should additionally, as a matter of best practice:

(i) Provide applicants with details of how the assessment tool will use their data and how profiles against which they are measured will be created.

4.12 **Example 2**

(a) **Call centre performance monitoring**

(i) A call centre installs worker monitoring software which tracks their workers' time records, such as login / logout times and time spent on the phone to potential customers. The call centre establishes it has a legitimate business interest after struggling to find an alternative way to monitor whilst most of its workers now work from their own homes or other remote locations away from line managers. This is notified to employees in the data protection policy.

(ii) After manual configurations are applied, the software automatically flags workers that fall below a certain standard. These flags are presented to line managers who carefully review individual reports before making a decision as to serve warnings or deduct pay.

(iii) In each instance, the line manager contacts the workers and asks for their comment, advising that they can challenge the data presented by the software if they believe it is inaccurate.

(iv) The line managers are trained to take into account various factors which could lead to inaccuracies in the automated flagged reports, such as software issues, internet connection or personal factors of workers.

(v) The management team regularly catch up on the use of the software to share their experiences and potential trends/risks, which are then updated in the call centre's DPIA and adjustments made as appropriate, such as new communications to workers about the processing or new training to line managers.

(vi) The employee privacy notice includes details of the monitoring, how data is collected and used and is regularly updated to take into account any adjustments made by the management team.

(vii) Query if this falls inside Article 22. If so, the employer has:

(A) Considered whether it has a legitimate interest;

(B) Documented that basis in its data protection policy;

(C) Conducted a DPIA and kept it regularly updated;

(D) Provided details in the privacy notice and kept it updated; and

(E) Provided the opportunity for human intervention and allowed employees to challenge the processing.

4.13 **Example 3**

(a) **Health & safety monitoring in construction/warehouse context**

(i) A construction company installs a network of cameras and a software which can, via facial recognition, automatically detect when specific workers are not using PPE, such as hard-hats and safety glasses. It automatically warns line managers of any potential health and safety risk, whilst continuously feeding live data.

(ii) In advance of the technology being utilised, workers are informed of the legitimate and substantial health and safety concerns of the employer, the employer carries out a DPIA and LIA and updates its privacy notice to explain how this data will be collected and that it will be processed for health & safety reasons. Employees are given a copy of the privacy notice by hand before the system is implemented.

(iii) However, subsequently, a line manager notices that the technology can also be used to track how long individual workers are taking on breaks which employees currently sign in and out for. The line manager repurposes the data by pulling it from the software and deducts pay for workers that took too long on their breaks, without identifying a legal basis or special category condition for doing so, and without consideration to the accuracy of that data. He helps other line managers to use the software for this purpose, with approval of the site manager.

(iv) Several workers complain to their line managers that their pay is being deducted unfairly and that they have taken shorter breaks than are being deducted from their pay. Their arguments are refused by line managers on the basis that 'the computer does not lie'. One line manager notes in passing to another that most of these workers are darker-skinned, but neither of them think this is relevant.

(v) Query if this falls within Article 22, because if so the employer has failed to comply with its obligations.

(A) Although the employer initially identified a legitimate purpose the data is now being processed for a different purpose and the employer is in breach of its obligations.

(B) There are less intrusive ways of collecting the data, such as the sign in/ out book previously used or swipe card data.

(C) There is no human intervention or cross-checking of the data collected.

(D) Although employees have challenged the assessment by the system, line managers do not consider these challenges sufficiently.

(E) There is evidence that the system may struggle to recognise darker-skinned faces, meaning there is potentially an adverse impact upon workers from certain racial groups and/ or with darker skin tones. The employer has failed to consider this and update its DPIA/ LIA accordingly.

4.14 **How do we lawfully monitor workers?**

(a) **Equal opportunities monitoring**

The Guidance explains certain conditions for processing special category data (pages 12 to 14) and touches briefly on other applicable laws, including equalities legislation (pages 15 to 16). Employers would benefit from further guidance on the ICO's interpretation of the equal opportunities conditions for processing in Part 1 of Schedule 1 to the Data Protection Act 2018. This is a challenging issue for many employers who wish to collect diversity data to support and track the success of equal opportunities initiatives in recruitment, retention and promotion. We suggest that a case study relating to an employer who wants to provide employees the opportunity to (voluntarily) enter and maintain diversity data within a secure portal, with a link to a specific data protection notice about use of the data, and to which there would be restricted access to senior HR managers only. The information could be used to generate diversity statistics on an aggregated basis only (and ensuring that individual employees cannot be identified by the recipient of the statistics).

(b) **Covert monitoring**

The Guidance makes clear that covert monitoring should only be undertaken in exceptional circumstances, such as where necessary to enable the prevention or detection of suspected criminal activity or gross misconduct. There may be some broader circumstances in which employee communications may need to be reviewed without specific advance notice to employees, such as in the context of a proposed price sensitive transaction or where regulatory (e.g., competition) clearance is required and only a limited number of individuals within the organisation are aware of the transaction. It would be useful to refer to these circumstances in the guidance, together with any further mitigations to protect employees' data protection rights - e.g.,

by recommending that such monitoring is covered in employee privacy notices, data minimisation principles are applied (e.g., through use of search terms and redaction) and that specific notice is given to employee data custodians at the first available opportunity.

5 SPECIFIC DATA PROTECTION CONSIDERATIONS FOR DIFFERENT TYPES OF WORKPLACE MONITORING

5.1 Commercially available tools

At page 35 of the Guidance, the ICO states that in some cases, a third-party that an employer engages may use personal data collected by the employer for its own purposes. The ICO states that in this case, the third-party will be a controller for this processing and the employer will become a processor. In our view, this determination does not seem to be correct. If a third-party service provider was collecting personal data either directly or from the employer to provide a service for an employer for which it would be controlling the means and purposes of processing personal data (e.g., providing training to a workforce), this would not make the employer the service provider's processor. We would expect the relationship of the two parties in this case to be that of independent controllers. It would be helpful if the ICO could correct this portion of the guidance and provide examples whereby an employer may engage a service provider as an independent controller rather than as a processor. On a practical note, it would be worthwhile for the Guidance to explicitly remind employers to update their employee privacy notices to cover this activity and update any other overlapping policies and procedures, for example, relating to the use of IT or an employer's HR procedures so that the employer is consistent across their organisation to ensure compliance.

5.2 Interception of communications

(a) At pages 36 -39 of the draft Guidance, the ICO covers monitoring calls, emails and other messages in the workplace. One example is provided where a regulated entity is required by the PRA/FCA to record calls. It would be helpful if the ICO made it more explicit that regulated entities who are required to monitor communications pursuant to a regulatory requirement may do so.

(b) While the draft Guidance does explain the data protection considerations of monitoring communications (e.g., access rights, proportionality), the existing Supplementary Guidance to the ICO's Employment Practices Code at pages 57-62[51] also explains the requirements of the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (the relevant provisions of which have been replaced by the Investigatory Powers Act 2016 and the Investigatory Powers (Interception by Businesses etc. for Monitoring and Record-keeping Purposes) Regulations 2018). The Supplementary Guidance contained helpful information setting out when an employer may record and monitor calls and other communications, when consent was required and what the notice requirements are in this context.

[51] https://ico.org.uk/media/for-organisations/documents/1066/employment_practice_code_supplementary_guidance.pdf

(c) For example, the Supplementary Guidance states at page 62: "*The requirement of the LBP Regulations is to make reasonable efforts to inform users of the system that an interception may take place. Workers, including temporary or contract staff, will be users of the system but outside callers or senders of e-mail will not be. Where, as will usually be the case, interception involves the collection, storage or use of personal information, the requirements of the Data Protection Act to provide information to those whose data are processed will come into play*." This information is useful as it demonstrates that employers need to comply with the Regulation of Investigatory Powers Act 2000 and the Data Protection Act when processing personal data and it outlines the different requirements of each regime. The law governing the interception of communications has changed since the publication of the Employment Practices Code, and there is limited information available to employers about the interception of communications. Currently, as the draft Guidance does not mention these requirements at all, employers may not be aware of the additional obligations that apply when intercepting communications.

(d) On this basis, we recommend that the ICO supplements the Guidance with information about the requirements of the Investigatory Powers Act 2016 and the Investigatory Powers (Interception by Businesses etc. for Monitoring and Record-keeping Purposes) Regulations 2018 as it relates to employers who may intercept communications. We particularly believe that a flowchart (like the one included at page 58 of the Supplementary Guidance) and specific examples would be helpful.

(e) On a practical note, there is no mention of Bring Your Own Device (BYOD) in the telephone monitoring section, yet many employers expect employees to use their own telephones, not linked to an employers' own system, to make and receive work calls. Moreover, applications like WhatsApp allow for voice calls to be made. It seems worthwhile to mention, if only in passing, that any routine monitoring of calls is impractical where BYOD is common. This might be mentioned at the foot of page 36 in the paragraph ending "*Have a policy in place for personal calls and make sure workers are aware of this*".

(f) There is no mention in the telephone / email section of Teams, Zoom or Slack etc. beyond the chat function of "collaboration tools" (not a commonly used collective noun for such apps). Certainly, anecdotally, the prevalence of video calls over such apps has largely displaced telephone calls. It seems anachronistic to devote a whole section to telephones and not mention video calls, particularly given the ease with which users of applications like Teams can record whole calls and retain chat for months totally unsystematically without reference to any policy or procedure of the employing organisation. The presumption that an employer controls recording of personal data in a central way needs to be challenged, with a reminder to DPOs of their obligation to challenge the culture of data hoarding through training for employees and awareness-raising, and to work with their IT teams / Chief Information Security Officer to look at technological solutions to limit localised storage of video calls. We suggest that the section on video or audio monitoring (foot of page 39 to top of page 40) would be the best place to reference how employers should handle recording Zoom, Teams etc. video meetings. Relatedly, employers would benefit from a reminder in the Guidance to ensure that policies and procedures about use of IT systems are updated to capture use of video calls.

5.3 **Network data and content**

At page 37 of the Guidance, the ICO states: "It would be difficult to justify monitoring the content of emails and messages where monitoring network data would meet your purpose. In exceptional circumstances where content is accessed, you must notify workers in advance that content may be monitored in relevant policy documents." In our experience, employers often need to review the content of emails in the context of an internal investigation. It would be helpful if the ICO could clarify if a DPIA would be required in such circumstances, and whether a fresh DPIA is recommended for each separate internal investigation or whether one DPIA covering communications monitoring for investigations will suffice (provided that the DPIA covers the monitoring anticipated in the specific internal investigation and is regulatory reviewed in line with Article 35 of the UK GDPR). Many employers would benefit from using one DPIA to cover monitoring for internal investigations, given that these often need to progress on an expedited basis to minimise adverse impact on the business and on the employee. Further, while the risk mitigation measures set out at page 38 are useful, further examples that:

(a) describe applying access controls when reviewing content;

(b) set out expectations for data retention; and

(c) describe the use of search terms when reviewing content in accordance with data minimisation principles, would also be useful practical measures that employers can implement - particularly when reviewing content during an internal investigation.

5.4 **DPIAs**

(a) The ICO recommends completing a DPIA in a number of places in the draft Guidance (for example, at page 37 when referring to monitoring emails and messages, at page 40 when discussing recording video and audio, at page 41 when explaining monitoring work vehicles and at page 44 when discussing data loss prevention ("**DLP**") tools).

(b) While it is accepted that each employer's proposed processing activities will be different and as such, it is not possible or appropriate for the ICO to determine whether a DPIA is required for every instance, it is not currently clear whether the ICO's statements on this issue are just good practice or strong recommendations to carry out a DPIA or at the very least, document an assessment on whether a DPIA is required.

(c) We also recommend that the ICO considers supplementing its list of specific scenarios which are likely to result in high-risk processing and consequently are likely to require a DPIA in an employee monitoring context. For example, the CNIL[52] states that tools that monitor or control working time, but without biometric devices will not require a DPIA and also that a DPIA is required when using DLP tools. While the ICO's list of examples that are likely to result in high-risk processing[53] state that "data processing at the workplace" may result in high-risk processing, this is not sufficiently

[52] See the CNIL's examples of activities that are likely and not likely to result in high-risk processing here: Decisions taken by supervisory authorities and courts on issues handled in the consistency mechanism | European Data Protection Board (europa.eu)

[53] See: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/examples-of-processing-likely-to-result-in-high-risk/

specific. While we note that the draft Guidance does state that a DPIA is required when biometric data is used at page 51, we also recommend that the Guidance is updated to include a list of employee monitoring activities that are likely to result in high-risk processing and activities that are *not* likely to result in high-risk processing, so employers can more easily identify when they should consider completing a DPIA as part of this specific Guidance.

5.5 **Remote working**

During the COVID-19 pandemic, remote working became the norm and as employers adapt to a flexible-working environment, employers need guidance on how to comply with their data protection obligations with a remote or hybrid workforce. The Guidance only contains two short paragraphs at page 47 about remote workers, stating that "*workers' expectations of privacy are likely to be higher at home than in the workplace*". We believe that employers need further information on the impact of remote working on their processing operations, and recommend adding further information within the Guidance on:

(a) the use of video-conferencing applications (such as Zoom and Teams) and when and how meetings may be recorded; and

(b) the ICO's own security guidance that discusses working from home, noting that the security risks of a remote workforce are higher - particularly if employees are using personal devices or collecting hard copy files relating to work at home[54]. The sections on monitoring time and attendance information (page 43) should be followed by monitoring device activity (middle of page 46) given the prevalence of homeworking and the rise in device activity as an alternative to the other measures mentioned at page 43. It would be useful to include headings like "working from the employer's premises" and "working from home" to enable readers to find the guidance relatively quickly. The paragraph titled "what about remote and home workers" could be moved up and positioned as an introductory paragraph to the section on monitoring device activity.

5.6 **Monitoring social media usage:**

There is no mention of social media monitoring in this section. Given the ubiquity of this medium of communication and that it often features in e.g., disciplinary cases, it would be sensible to include guidance on monitoring employees' social media activity.

6 CAN WE USE BIOMETRIC DATA FOR TIME CONTROL AND ATTENDANCE MONITORING?

We note that the current draft states that organisations must "*consider"* whether they need extra security measures in storing biometric data, as processing biometric data comes with a higher risk of harm as it cannot be reset in the event of a breach, unlike passwords. Given the section on security of biometric data page 53, it is likely that organisations will be required to do more than **consider**.

[54] See: https://ico.org.uk/for-organisations/working-from-home/

6.1 **How do we determine if using biometric data for access control is necessary and proportionate?**

The necessity and proportionality of using biometric data will be a key part of an organisations DPIA, which they will be required to carry out given the special category nature of the data. On that basis therefore it would be advisable to move the section of DPIA currently set out at page 51, so that it comes before this section on accessing the necessity and proportionality.

6.2 **How do we identify a lawful basis, and a special category condition where needed?**

(a) This section could be set out more clearly to state explicitly that in relation to the processing of biometric data, both on Article 6 and in Article 9 basis will be required. Rather than cross refer to the sections special category conditions, it would be helpful to tease out the special category conditions that can be relied on?

(b) In addition, automated decision making is a separate issue and on that basis would it preferable for it to be set out in a different section?

(c) The guidance then goes back into and focuses upon the issue of consent and use of consent in the context of the employment relationship. As consent is rarely appropriate in an employment context, would it better to also highlight the other potential grounds which can be relied on to process special category data?

(d) At the end of page 50 the last line should also make reference to the DPIA as the justification for using biometric data will be clarified within the DPIA?

6.3 **What about accuracy and fairness?**

Given the controversy in relation to use of facial recognition, it would be helpful if that could be expanded upon further as that will also be a key issue for organisations to consider in the context of the DPIA.

6.4 **Can workers object to the use of biometric data for access control?**

This section is slightly confusing and also needs to make clear that consent can be withdrawn at any time and needs to be as easy to withdraw as it is to give? It appears unlikely that companies would invest in the considerable cost of biometric technology if participation is on the basis of consent i.e. voluntary?

6.5 **What about the security of biometric data?**

The consequences of a data breach in the context of biometric data will be particularly serious and it would therefore be helpful to include an example which highlights the consequences of getting it wrong?

6.6 **What is biometric data?**

The list of examples is short, making no reference to iris scanning or retinal analysis. Consistent with the narrative in the section, no reference is made to behavioural biometric identification techniques. The reference to "monitoring" in the title appears to be restricted to

monitoring of access/entry to premises or systems. It would also be useful to explain the difference between the underlying biometric image, and the biometric template. This is not something an average member of the public would be aware of.

ELA Working Party

Jonathan Chamberlain, Gowling WLG (UK) LLP (Co-Chair)
Alistair Woodland, Clifford Chance LLP (Co-Chair)
Aisling Byrne, A&L Goodbody – Belfast
David Chalmers, Stronachs LLP
Annabel Gillham, Morrison & Foerster (UK) LLP
Shobana Iyer, Swan Chambers
Sian McKinley, Herbert Smith Freehills LLP
Ken Morrison, St. George's, University of London
David Regan, Squire Patton Boggs (UK) LLP
Bruce Robin, UNISON Legal Services
Christine Young, Herbert Smith Freehills LLP

ELA Contact Person

James Jeynes
Head of Operations

jamesj@elaweb.org.uk
01895256972