Annexe: Know your Data Protection Rights

IFOW Institute *for the* Future of Work

community

Acknowledgements

This guide has been prepared on behalf of Community and the IFOW by AWO lawyers. We are grateful for their support and guidance.

Thanks are due to:

Cassie Roddy-Mullineaux
Ravi Naik
Ben Hayes
Eric Kind
Hitesh Dhorajowala
Lucy Hannah
Edward Cooper
Professor Jeremias Adams-Prassl
Associate Professor Reuben Binns
Dr Christina J Colclough
Dr Abigail Gilbert

Introduction

It is imperative to go into negotiations with your organisation armed with a firm understanding of the basics of data protection law and other law that apply in the workplace, and the rights and obligations flowing from these. This Annexe offers a summary overview of data protection law because it is not widely understood or used.

Knowing your baseline entitlements will help you to spot gaps and areas to develop beyond what the law entitles you to.

Laws that grant you rights

UK GDPR and DPA

Processing of data in the workplace is governed by the UK General Data Protection Regulation[1] (UK GDPR) and the Data Protection Act 2018 (DPA). The employer is the data controller of the workers' personal data that it processes.[2] The worker is the data subject.

Personal data is broadly defined as *any information that relates to an identified or identifiable living individual.*

Processing is also broadly defined as *any activity involving the personal data of a living person*. This could be collecting data, using it in any way, even storing and deleting it.

[1] *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data* (the GDPR) – now the UK GDPR, i.e., the GDPR as it forms part of the law of England and Wales, Scotland, and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.

[2] The employer will also process personal data of other data subjects that you may be concerned about, such as prospective workers.

Personal data in an employment context could include:

- names and other personal details,
- payroll numbers,
- bank details,
- emails,
- browsing history; and
- CCTV footage.

Special category data includes:

- personal data relating to a worker's race, ethnic origin, politics, religion, trade union membership, biometrics e.g., fingerprint identification, and health.

Additional restrictions on processing apply to special category data.

The employer has several obligations towards workers arising from its status as a data controller of the workers' data it processes. The workers, as data subjects, have rights over their data, which they can exercise against the controller.

Legal bases

To process personal data lawfully, an employer will need:

- a legal basis (also known as lawful basis) for processing under Article 6 UK GDPR; and
- to set out the legal basis of each processing operation in the Data Protection Policy and/or Privacy Notice.

Legal bases frequently seen in the employment context include the bases of:

- performance of a contract,
- compliance with a legal obligation,
- the employer's legitimate interests*; and
- consent*.

Bases such as processing necessary to perform the employment contract or to comply with legal obligations on it (for example, legal requirements for taxation reporting) are generally uncontroversial, provided they are properly applied.

However, note that the word "necessary" is a high threshold. For example, in the case of processing for contract purposes, the processing must be more than tangentially connected with the contract, it must be necessary for its performance.

Bases like consent and legitimate interests are more problematic. In particular, consent is unlikely to be lawful in an employment situation.

Consent

- Consent is unlikely to be a valid legal basis in the employment context, outside of extremely limited circumstances (for example, if the employer conducted an opt-in anonymous survey where there were no consequences for non-participation).
- The UK GDPR provides that consent must be freely given, specific, informed, and unambiguous. It must be as easy for workers to withdraw consent as it is to give it.
- Generally, a worker cannot freely give their consent due to the power imbalance inherent in the employment relationship.

- The EDPB Guidelines[3] "*deems it problematic for employers to process personal data of current or future employees on the basis of consent as it is unlikely to be freely given.*" This is backed up by the ICO guidance.[4]

Legitimate interests

- If an employer is relying on legitimate interests (LI) as its lawful basis, then it must inform employees of this in its privacy notice/policy. Workers can object to their data being processed on the basis of LI. If this happens, an employer must stop processing the data unless it can demonstrate that its own interests outweigh those of the worker[5], which may not always be easy for it to do.
- The ICO recommends that employers always conduct a "legitimate interests assessment" (LIA) and record its outcome when processing on the basis of LIA.[6]

Special category data or criminal records data

- Where special category personal data or criminal records data is being processed an employer will need an additional lawful basis under Article 9 UK GDPR. Additional conditions and safeguards attach to some of these lawful bases under UK law and these are set out in the DPA.[7]
- The basis most often relied upon is that the data is needed to fulfil the employer's obligations under employment law. To rely on this basis, the employer must have an appropriate policy document in place which sets out how the employer will comply with the UK GDPR principles on processing this type of data, as well as its retention and erasure policies.
- Again, an employer cannot rely on "explicit consent" under Article 9 UK GDPR to process special category data of an employee, for reasons outlined above.

Transparency Obligations

The transparency and lawfulness principle[8] means that:

- processing of personal data should be lawful and fair, and it should be transparent to workers how and why their data is being collected and used by their employer.

---

[3] The European Data Protection Board (EDPB) have endorsed the Guidelines on consent adopted by WP29 under Regulation 2016/679 (WP259.01) on 10 April 2018 - https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf.

[4] *"Public authorities, employers and other organisations in a position of power may find it more difficult to show valid freely given consent"* - https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/#ib4

[5] According to Recital 47 of GDPR, *"the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing."*

[6] See, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/#:~:text=However%20an%20LIA%20is%20intended,any%20particular%20reasons%20for%20concern

[7] See Part 1 of Schedule 1 of the DPA. In many cases an appropriate policy document will be required which is described at Part 4 of the Schedule.

[8] Article 5(1)(a) UK GDPR.

Article 13 UK GDPR stipulates specific information that must be provided to data subjects, including workers, upon collection of their data by the employer. This includes:

- Information about the worker data that is being collected and processed by the employer,
- the purposes of the processing, including the lawful basis for processing,
- how long the data will be stored for,
- the rights that the worker can exercise over that data including the right of access; and
- whether the data is going to be used for automated decision-making (ADM), including profiling. If it is, then the employer needs to provide meaningful information about the logic involved to the worker.

How the information is provided may vary from organisation to organisation, e.g., it could be provided by a worker privacy notice / worker-facing data protection policy.

The important point is that the essential information is communicated to workers in an understandable way.

Purpose Limitation

The purpose limitation principle[9] says that:

- *"Personal data should only be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes."*[10]

This means that personal data cannot be used for purposes beyond the original purposes communicated to workers, unless the organisation is confident the purposes are compatible. This places a significant limitation upon the employer's ability to further process the data in any way it likes.

Data Protection Impact Assessment (DPIA)

Under Article 35 UK GDPR, employers are obliged to conduct a DPIA for types of processing likely to result in a high risk to individuals' interests.

Certain types of processing will always require a DPIA, including:

- Systematic and extensive profiling with significant effects
- Large scale use of special category data or criminal data
- Public monitoring, e.g., CCTV or video surveillance

Other factors are relevant to assessing if processing is high risk:

- The ICO has outlined certain criteria to assess if processing is high risk as has the EDPB.[11] This includes systematic monitoring. According to the ICO, if processing involves "*vulnerable data*

[9] Article 5(1)(b) UK GDPR.

[10] Recital 50 GDPR also sets out: *"The processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected."* [10]

[11] The WP29 and the ICO have produced guidance on how to assess these factors. Article 29 Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, endorsed by the EDPB. The Guidance gives the following example of systemic monitoring in the workplace that would likely require a DPIA, "*a company systematically monitoring its employees' activities including the monitoring of the employees' workstation, internet activity, etc.*" See also ICO Guidance, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/#when9

subjects", then if any one of the other criteria are met, a DPIA should be conducted. Workers are deemed *"vulnerable data subjects"*[12]. Thus, employers' monitoring of workers' activities or surveillance of workers in the workplace will always require a DPIA.

- The DPIA duty requires an employer, before conducting processing, to consider and identify the data protection and related risks (which could include risks of discrimination) that may arise from the processing, and to put measures in place to mitigate those risks, before continuing with the processing. If the employer cannot mitigate the risk, it will need to consult with the ICO before beginning the processing.

- When conducting a DPIA, there is an obligation to consult with relevant stakeholders, including workers and/or their representatives on the DPIA unless there is a good reason not to do so.

Data subject rights

The ICO provides comprehensive information about data subject rights under the UK GDPR and the DPA here.

Examples of rights that workers have include:

- a right to obtain a copy of their personal data, and other supplementary information, from their employer within a one-month period upon requesting it. Asking for a copy of your personal data is known as a Subject Access Request **(**SAR) and an employer is obliged to provide you with it**,**
- a right to have their data corrected or erased by the employer in certain instances,
- a right to object to processing, including processing based on legitimate interests; and
- a right not to be subject to automated decision-making, including profiling (see below).

Automated decision making (ADM).

- An employer is precluded from conducting ADM, including profiling, which has legal or similarly significant effects in all but extremely limited circumstances, i.e., where ADM is *necessary* (a high threshold) for entering a contract with the worker or where that employer is operating under a legal obligation.
- Note that consent will not be a valid legal basis for ADM given the power imbalance between employer and worker.
- In the limited circumstances where an employer may lawfully be entitled to use ADM, there is a right to get human intervention and to contest the decision.[13]

When rights and obligations are breached

If an organisation breaches its obligations/workers' rights, workers and their representatives have a right to:

- submit a complaint to the Information Commissioner's Office (ICO)[14],

[12] Recital 75 GDPR.

[13] Article 22(3) UK GDPR.

[14] A complaint can be submitted on the ICO's website - https://ico.org.uk/make-a-complaint/your-personal-information-concerns/ According to the ICO guidance, a complaint should be raised within three months of the last meaningful contact with the organisation in question (although note this is not a UK GDPR requirement). The ICO can give advice to the organisation concerned and ask it to solve the problem. An ICO complaint will not result in compensation.

- bring court proceedings in accordance with relevant procedural rules, i.e., seek the right to an effective judicial remedy against the organisation[15]. Under the DPA, you can:
    - ask the court to make a compliance order against the organisation/employer – this can include ordering the organisation/employer to take certain steps or to refrain from certain actions[16]; and
    - ask the court to make an order providing for compensation to be paid.[17]

Additional Legal Frameworks

Soft law

Soft law including guidance and recommendations is also relevant. This doesn't impose a legal obligation on employers,[18] but can be helpful in interpreting legal requirements such as those within the UK GDPR. These include

- the ICO Guidance and Codes of Conduct,[19]
- the Surveillance Camera Code of Practice, with respect to CCTV and other video surveillance.[20]
- Guidance of the European Commission Article 29 Working Party (WP29) (predecessor of the EDPB) and the European Data Protection Board (EDPB).[21]

The Privacy and Electronic Communications Regulations (PECR)

These regulations sit alongside the UK GDPR and DPA and complement them by providing additional privacy rights with respect to electronic communications and the accessing of information on a worker's device.

The PECR are relevant to the use of monitoring and surveillance technologies[22], and they outlaw the use of spyware and covert surveillance software because a worker will not have knowledge of these technologies which intrude on their privacy. [23]

---

[15] Article 79 UK GDPR.

[16] Section 167 DPA.

[17] Section 168 DPA.

[18] For instance, the fact that worker monitoring must be clearly signposted is set out in ICO codes of practice, but also forms part of the hard law data protection principle that data must be processed *"lawfully, fairly, and transparently"*.

[19] For example, the ICO guidance on DPIAs https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/#how7, and its guidance on AI and data protection https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/guidance-on-ai-and-data-protection/

[20] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/204775/Surveillance_Camera_Code_of_Practice_WEB.pdf - please note that it is a legal requirement for *relevant authorities* (as per the meaning given by section 33(5) Protection of Freedoms Act 2012) to comply with the code. Other authorities are merely encouraged to adopt it voluntarily.

[21] The WP29 used to deal with issues relating to the protection of privacy and personal data in EU before the GDPR entered into force. The EDPB, its successor, has since endorsed many of the WP's guidelines as well as issuing its own guidance and recommendations.

[22] See, https://ico.org.uk/for-organisations/guide-to-pecr/what-are-pecr/, and https://ico.org.uk/for-organisations/guide-to-pecr/cookies-and-similar-technologies/

[23] A full exploration of the PECR is beyond the scope of this guidance but it is important to note its application in this area.

The European Convention on Human Rights (ECHR)[24] and European Court of Human Rights (ECtHR) caselaw

Human rights laws are relevant to personal data protection as well as the broader right to privacy in the workplace which could be intruded on through technology use.

In particular, Article 8 ECHR[25] is relevant in providing that any interference with an individual's privacy, which can include their right to personal data protection, must be necessary and proportionate in order to be justified.

There are a few relevant cases on worker monitoring to be aware of:

- *Bărbulescu v. Romania*[26], in this case the ECtHR held a worker's rights under Article 8 ECHR were violated where his employer failed to inform him in advance that personal messages sent from his computer might be monitored and, in particular, that the content of those messages might be accessed.
- *López Ribalda and Others v. Spain*[27], in this case the ECtHR held the use of covert CCTV cameras to monitor workers' behaviours on the tills was justified based on the circumstances of the case due to (i) the well-founded suspicion of theft; (ii) the areas monitored were public areas and (iii) the processing had not exceeded what was reasonable to confirm a suspicion of theft.

While these two cases are difficult to reconcile, it demonstrates the case-by-case approach to determining if privacy intrusions are necessary and proportionate, based on the particular facts of the case.

[24] The rights set out in the ECHR are incorporated into UK domestic law through the Human Rights Act 1998.

[25] According to Article 8 ECHR, *"Everyone has the right to respect for his private and family life, his home and his correspondence"* and *"there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."*

[26] [2016] ECHR 61.

[27] [2018] ECHR 14.