Equal Opportunities Monitoring

Table of contents

Equal Opportunities Monitoring

1. Introduction

1.1 Under the UK General Data Protection Regulation (retained from EU Regulation 2016/679 EU) (UK GDPR), employers can gather and analyse information about employees for equality monitoring purposes, provided they have a legal basis for the processing and, where applicable, the rules relating to processing special categories of personal data are met.

2.1 While many employers have, for some time, been conducting general equal opportunities monitoring, the issue of diversity in the UK is now firmly in the spotlight and becoming increasingly important because of the implementation of the gender pay gap reporting regime and the government's plans to extend this to ethnicity pay gap reporting.

2.2 Equal opportunities monitoring and ethnicity pay gap reporting both involve the processing of 'special categories of personal data', such as information about individuals' race, ethnic origin, health, and sexual orientation. Gender pay gap reporting does not involve the processing of special category personal data, but salary information is nevertheless sensitive data.

2.3 Individuals will have a greater expectation of privacy when it comes to the processing of their special category data or salary information. In addition, they are more likely to suffer damage or distress and are more likely to take action against an employer if something goes wrong, such as if that data is lost, stolen, or unlawfully disclosed, for example.

2. Purpose

3.1 To ensure that data processing for the purpose of equal opportunities monitoring is legally compliant, employers must also be able to justify that the data they are gathering is necessary.

3.2 For example, keeping track of religious beliefs, even if done in good faith with the intent to help the employee, may not be lawful unless the organisation has legitimate organisational reasons to monitor and address any underrepresentation. In short, if an employer is not going to use the data, they should not collect it.

3.3 The UK's data protection authority, the Information Commissioner's Office (ICO), is also more likely to take a harder line in its enforcement action where special category data or other sensitive information has not being processed in accordance with UK data protection law. Fines of up to £17.5 million, or 4% of an organisation's annual global turnover, whichever is highest, can be levied under the UK's General Data Protection Regulation (UK GDPR) and UK's Data Protection Act 2018 (DPA 2018).

3. Lawful basis

4.1 Before engaging in an equal opportunity monitoring exercise, employers first need to establish that they have a lawful basis for processing the data they are seeking to collect.

4.2 Data that employers gather for the purpose of monitoring equal opportunities will often fall within the special categories of data under the UK GDPR, i.e. where it relates to employees' racial or ethnic origin, religious or philosophical beliefs, health or sexual orientation. The DPA 2018, which supplements the provisions of the UK GDPR, includes a limited provision that specifically allows these types of special category data to be processed for the purpose of monitoring equality of opportunity or treatment between different groups. An employee can require the employer to stop processing their data for that purpose by giving the employer written notice.

4.3 The provision in the DPA 2018 will not apply to all processing that an employer may wish to carry out for equality monitoring purposes. For example, employers may wish to monitor equality of opportunity based on employees' gender or whether they have taken family-related leave. This data would not fall into the special categories of data under the UK GDPR or the DPA 2018. Where the provision of the DPA 2018 does not apply, the employer could rely on the processing being necessary for its legitimate interests as its legal basis for processing. In this case, the employees would have the right to object to the processing.

4.4 Alternatively, equal opportunities monitoring is one of the rare examples of where it may be appropriate for an employer to rely on employees' consent as the legal basis for processing their data. This is because employees can have a genuine choice about whether to provide the information and there should not be any adverse consequences for those who choose not to provide it. An employer may decide to base its equality monitoring programme on consent, to give employees more control over how their data is used. Employees can withdraw their consent at any time.

4.5 Depending on the nature of an equality monitoring exercise, it may be possible to anonymise the personal data before processing it. Provided that there is no way of identifying an individual to whom the data relates, the UK GDPR would not apply. Total anonymisation when gathering equality data would not be possible for a monitoring programme where it is necessary to track individuals, for example ongoing monitoring of data on promotions or resignations with reference to race.

4.6 If an employer is processing personal data to comply with a legal obligation, such as the gender pay gap reporting regulations, then this is also a lawful ground for the processing.

4. Alternatives to consent

5.1 The ICO has commented previously that consent should be considered a last resort; and only used when one of the lawful conditions is not available. In the circumstances of equality reporting and pay gap reporting there is a legal duty to rely on. Where consent may be relevant is if the information a controller wishes to collect is wider than that required to fulfil the duty, or if they wish to share that data with a third party and so the purpose of processing is then different. In these circumstances consent could be considered – however consent can be difficult in this context.

5.2 The UK GDPR standard of consent provides that this must be 'freely given' – it has to be a decision the employee is in control of, genuinely voluntary, and such that the employee's failure to give consent will not result in any detriment to the employee.

5.3 Not just this though, the effect of consent is that it can be withdrawn, it has a shelf life in terms of duration and consent is specific to the purpose described. Any further use, widening of the use by the original collector and indeed any party with whom that data was shared would, unless such further purpose is considered 'compatible' with the original purpose, require the employer to look for additional consent.

5. Anonymisation

6.1 Best practice is to collect the data on a genuinely anonymous basis and to ensure that it is not identifiable. Data that cannot be traced back to identify a living individual is not personal data and so the DPA 2018 would not apply to its processing.

6.2 Anonymising the data would also mean that the data retention principle of not keeping data for longer than is necessary would not apply.

6. Policy

7.1 An employer can rely on this provision for equal opportunities monitoring set out in the DPA 2018 only if it has an appropriate policy document (APD) in place, setting out the safeguards it has implemented for processing special category data and its policies on for how long the data will be retained. The policy should explain to employees what the employer is doing with their data, including how the employer collects, uses, stores, and shares the data, as well as how long it is retained for.

7.2 Maintaining the policy will help employers meet their obligations on transparency under data protection law and help to reassure staff and improve employee engagement.

7. Data protection impact assessments

8.1 Employers that engage in general equal opportunities monitoring or ethnicity reporting may be under a legal obligation to carry out a data protection impact assessment (DPIA) before carrying out that activity. This is because DPIAs are mandatory under the UK GDPR where an employer is processing special categories of data on a large scale. Even if the legal obligation to carry out a DPIA under the UK GDPR is not triggered, it is best practice to conduct one when engaging in a new data processing activity.

8.2 A DPIA should consider, amongst other things, how any data will be kept secure, how long it will be kept for and who it will be shared with.

8. Outsourcing

9.1 In some cases, employers may elect to use third parties external to their business to collect and process data for equal opportunities monitoring on their behalf. This is perfectly legitimate under data protection laws, but employers must be aware that they will remain the 'controller' of the data and are responsible for ensuring it is processed in accordance with the UK GDPR.

9.2 When engaging data processors, controllers are required to have a written contract in place with those third parties to regulate their processing. Controllers must also ensure the contract commits processors to meet their legal obligations under the UK GDPR and that the processors also enable them to fulfil their own obligations. For example, it will be necessary for the contract to set out processors' duties on notifying a data breach and to prohibit them sharing data without the permission of the controller.

9.3 Employers are not relieved of their responsibilities just because someone else is processing the data for them.

9. Data sharing

10.1 Employers should also be careful about who they share the data with. They need to have a lawful basis for sharing the data as well collecting it.

10.2 It is likely to be lawful for employers to share data collected for equal opportunities monitoring purposes with their employment lawyers where it is necessary for the establishment, exercise, or defence of a legal claim. However, sharing the data in other circumstances may be more difficult to justify, even if it is just to be shared with other companies in the same group.

10.3 Transferring the data to other companies within a group of companies may not be necessary, and where the data is to be transferred outside the European Economic Area (EEA), such as to offices in the US or Australia, additional privacy safeguards, such as standard contractual clauses or binding corporate rules, will need to be in place to ensure that data benefits from equivalent protection in those jurisdictions as to what is available in the EEA.

10. Data security

11.1 Employers have an overarching duty to preserve the security of personal data they are responsible for under the UK GDPR, and further security of processing rules set out in the Regulation further explain the requirements they must meet.

11.2 Specific data security measures are not prescribed in the UK GDPR. Instead, organisations must ensure that the organisational and technical security measures they implement are 'appropriate' to address the specific risks they are presented with, considering the measures available to them at the time. In the context of equal opportunities monitoring, the sensitivity of the data collected heightens risks and therefore requires employers to put in place extra safeguards to keep data secure.

11.3 Access to the data collected should be on a 'need-to-know' basis only; it should be processed securely through, for example, password protected and encrypted systems and networks; and, unless anonymised, not kept for longer than is necessary.