

EDI data gathering: The legal issues



1 Introduction

This guidance is provided as part of the equality, diversity and inclusion (EDI) data gathering toolkit prepared by IP Inclusive in collaboration with [CIPA](#), [CITMA](#), the [IP Federation](#), the [UK Intellectual Property Office](#) and [IPReg](#). It is intended to be used by signatories to [the IP Inclusive EDI Charter](#) and other IP sector employers, in particular private practices.

Our toolkit also includes:

- A template standard EDI data gathering survey
- Practical tips for gathering and processing EDI data
- A collection of relevant resources (including benchmarking data) available elsewhere

The full toolkit can be accessed at <https://ipinclusive.org.uk/our-edi-data-gathering-toolkit/>.



BURLEY LAW

The guidance here has been kindly provided by [Burley Law Limited](#) (commercial, IP and employment law solicitors).

Please note that it is not comprehensive and it is not intended as formal advice: see the “disclaimers” in section 6. Please also note (section 5) that the guidance relates to the position under UK law; for activities in other countries and/or relating to non-UK employees, it is vital that you seek legal advice in the relevant jurisdiction(s).

We would welcome your feedback. Let us know about the legal and HR challenges you have encountered in your own EDI data gathering and processing work, and we will try to update this document to address them. The IP sector will be better equipped to gather, and to act on, meaningful EDI data if we share our experiences and our solutions to the issues we share.

2 What is EDI data and why is it relevant to organisations in the IP sector?

EDI is an umbrella term which includes equality, diversity and inclusion. These terms are widely used in employment/HR policy and practice but they are not defined in law and they mean different things.

The concept of **equality** is enshrined in [the Equality Act 2010](#), which prohibits discrimination at work – and in other areas such as public services – due to protected characteristics (race, age, sex, sexual orientation, pregnancy and maternity, marital status, disability, religion and belief, and gender reassignment). Employers must not discriminate on any of these grounds unless they have legitimate and objective justification for doing so.

Discrimination means treating someone less favourably than someone else. Less favourable treatment can be anything that puts someone with a protected characteristic at a disadvantage, compared to someone who does not have that characteristic.

It can still be discrimination even if the less favourable treatment was not intended.

Discrimination can take different forms. It can be **direct** (for example refusing to offer a job or a promotion on grounds of race) or **indirect** (for example applying policies or other workplace rules in a way that disadvantages people because of their race). It can also take the form of **harassment** where there is unwanted conduct relating to a protected characteristic which violates a person's dignity or creates an intimidating, hostile, degrading, humiliating or offensive environment for them. Victimisation is a type of discrimination that occurs when someone is treated less favourably as a result of being involved with a discrimination or harassment complaint (for example being labelled a troublemaker, being left out, or not being allowed to do something).

Employers have an additional duty to make **reasonable adjustments** for those who are disadvantaged at work because of a disability.

Diversity is defined by ACAS as¹:

“the range of people in your workforce. For example, this might mean people with different ages, religions, ethnicities, people with disabilities, and both men and women. It also means valuing those differences.”

Inclusion is described by ACAS in the following way:

“An inclusive workplace means everyone feels valued at work. It lets all employees feel safe to:

¹ See <https://www.acas.org.uk/improving-equality-diversity-and-inclusion>

- *Come up with different ideas and raise issues and suggestions to managers, knowing this is encouraged*
- *Try doing things differently to how they've been done before, with management approval."*

IP Inclusive's objectives are to promote and improve equality, diversity, inclusion and wellbeing throughout the UK's intellectual property (IP) professions. Signing up to its EDI Charter is a public endorsement of the principles of equality, diversity and inclusion. Collecting EDI data can be a way of monitoring your organisation's commitment to these principles and the effectiveness of any EDI initiatives it undertakes.

The Equality and Human Rights Commission (EHRC) Code of Practice² also recommends that all employers carry out equality monitoring and suggests that it can be used to:

- establish whether an equality policy is effective in practice
- analyse the effect of other policies and practices on different groups
- highlight possible inequalities and investigate their underlying causes
- set targets and timetables for reducing disparities, and
- send a clear message to job applicants and workers that equality and diversity issues are taken seriously within the organisation.

3 Data protection law guidance

3.1 The UK GDPR

The UK General Data Protection Regulation (UK GDPR)³ applies if you process personal data.

Personal data is any information relating to an identified or identifiable living person who can be identified either directly or indirectly, for example from their name, an identification number, location data, an online identifier, or one or more factors specific to their physical, physiological, genetic, mental, economic, cultural or social identity.

Processing includes gathering, storing, monitoring, reporting and publishing data. In this guidance we use "process" and "processing" to cover any of these types of activity.

When you process personal data from your employees you must comply with the principles set out in the UK GDPR. You must have a lawful ground for processing the data; you must provide certain

² See <https://www.equalityhumanrights.com/equality/equality-act-2010/codes-practice/employment-code-practice>

³ See <https://www.legislation.gov.uk/eur/2016/679/contents#> and <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/>

information to the employees (usually in a privacy notice); and they will have various rights such as the right of access to their data.

3.2 Lawful grounds for processing

The **lawful grounds** under the UK GDPR that are likely to be relevant to data processing in the context of EDI are:

1. That the processing is necessary for the purposes of your organisation's legitimate interests. If you want to rely on legitimate interest as your basis for processing you should carry out a legitimate interests assessment (LIA)⁴. Importantly, though, you cannot rely on this ground if in your assessment your legitimate interests are overridden by the interests or fundamental rights or freedoms of the employees whose data you are processing.
2. Consent from the employee to the processing. You should tread carefully when relying on consent as the lawful ground for processing in an employment relationship, because there are strict conditions involved (in addition, see 3.3 below regarding "special category" data). Importantly, the employee should not be in any way pressured or coerced into giving consent, and their consent can be withdrawn later.

It is unsafe to rely on any other lawful grounds under the UK GDPR (contract, legal obligation, vital interests, exercise of public function) for processing EDI data.

3.3 "Special category" data

The type of data that organisations process in the context of EDI monitoring is very likely to constitute **special category personal data** under the UK GDPR. This means that it has greater protection and must be treated more carefully. In addition to a lawful ground for the processing as set out above, you must have an additional justification for processing special category personal data.

You may rely on consent as an additional justification, but there are strict conditions to meet:

1. It must be freely given, specific and informed and you must tell employees that they can withdraw their consent at any time;
2. It must be expressly confirmed in words and not be implied by behaviour, however obvious it may be that the individual consents; and
3. The explicit element of the consent should be separate from any other consent you are seeking. So, for example, it is advisable to keep requests for employee consent to EDI data gathering completely separate from those for other types of data processing. You should not use the same form for several sets of personal data and purposes.

⁴ See <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/>, which also gives access to a sample LIA template

You should not include generic consent to the processing of special category data in an employment contract because this will not meet all of the above conditions.

Other potential justifications for processing special category personal data, which tend to be relied on in other types of processing of employee data, are problematic in the context of EDI monitoring and should not be relied on without legal advice.

There is more information on “special category” data on the ICO website⁵.

3.4 Transparency and fair processing

Your privacy notice for employees should be fully transparent about how their personal data will be used. It should set out what personal data (including special category data) will be collected, how it will be processed and who it may be shared with. The privacy notice should be easily accessible and easy to understand; clear and plain language should be used.

Additionally, you should consider if a data protection impact assessment (DPIA) may be needed. A DPIA is compulsory if you are processing special category personal data on a large scale or if your processing operations, in particular using new technologies, are likely to result in a high risk to the rights and freedoms of individuals. If you are unsure, it may be prudent to complete a DPIA before you process EDI-related data⁶.

3.5 Retaining data

Monitoring trends will inevitably involve retaining diversity data over a period of time and you should be aware of the UK GDPR requirement not to keep personal data for longer than necessary and to tell your staff how long you will keep it.

You should not retain data going further back than the period you are currently monitoring. For example, if you want to monitor data over a five-year period, you should not retain data going back more than five years. Of course, monitoring trends may not even require the retention of personal data if the data can be properly anonymised; this is considered below.

3.6 Anonymised data

The UK GDPR does not apply if the data you gather is anonymised in such a way that it does not identify a living person, directly or indirectly.

You should be careful to ensure personal data really has been properly anonymised before treating it as such. Sometimes an individual can still be identified where their name and other details have been removed. For example, they may be the only employee with a particular set of characteristics – or their job title may give away their identity. The following should also be taken into account:

⁵ See <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/>

⁶ See <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/>, which gives access to a sample DPIA template

- Encrypting personal data does not anonymise it.
- Collecting, analysing and monitoring diversity data in an entirely anonymised form is only likely to be possible for very large organisations with diverse workforces, where survey-style software is used to collect and analyse the data.
- If you want to publish the data (for example on your website) or if you are required to report it (such as to a regulator), you must consider carefully whether either can be done anonymously.

3.7 Broader GDPR considerations

The processing of personal data is likely to be involved to at least some extent in the gathering of EDI data. This should be considered as part of your overall GDPR compliance systems. Your existing policies relating to employees may need to be updated to accommodate any new processing you do. As well as the privacy policy and a possible DPIA, you should also look at the technical and organisational measures needed to keep any personal data secure, ensure it is only shared with staff who really need to have access for the intended purpose, and update any document setting out how long you hold personal data for.

Good practice is to have a data map which sets out what classes of personal data are processed, how that data is processed, the legal grounds for processing (including any special purpose data), who it may be shared with and how long it will be kept. You should continue to follow the requirements encapsulated in the concept of “data protection by design and default”⁷ by baking in the protection of personal data.

Where a third party is used to carry out any processing of EDI personal data (this could be collecting, analysing, reporting, retaining or deleting), an appropriate data processor agreement is required by law. Additional considerations also apply where personal data may be transferred abroad.

4 Employment law guidance

There is no legal obligation on employers to carry out EDI monitoring.

Workers have the right not to be discriminated against (treated unfavourably or less favourably than others) either directly or indirectly, during recruitment or employment, on the basis of any of the protected characteristics. This makes the collection and use of EDI data potentially tricky.

Protection from discrimination applies to:

- The arrangements an employer makes for deciding to whom to offer employment,

⁷ See <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/data-protection-by-design-and-default/>

- The terms on which the employer offers a person employment, and
- Situations when the employer does not offer someone employment.

Extreme caution must be exercised in the use of diversity monitoring forms, surveys or questionnaires for job applicants and employees, to ensure that decisions about offering employment, promotion and pay are not discriminatory. Particular care must be exercised over asking about disability and health in any recruitment process. Monitoring diversity in the range of job applicants for a role is allowed, but the decision makers in the recruitment process must not have access to the diversity-related data provided by candidates. Aside from some very limited exceptions, it is unlawful to take account of a person's protected characteristics in the recruitment selection process (including at the shortlisting, interviewing and offer stages).

Employers who use diversity monitoring forms must consider very carefully why they are being used, how the data will be monitored and by whom, who will have access to it, and how long it will be kept for. It is sensible to have in place a policy covering diversity monitoring and to review it regularly (at least every two years).

5 Data gathering outside the UK

This guidance covers relevant legislation in the UK. If you intend to gather, store and/or process EDI-related data outside the UK, and/or from non-UK employees, it is vital that you seek bespoke legal advice in the relevant jurisdiction(s) as the requirements may differ significantly between countries.

Note too, however, that the UK GDPR is likely to apply to UK entities processing personal data from non-UK individuals.

Also be wary if any organisation that stores or processes your data (for example a survey or marketing platform such as SurveyMonkey or Mailchimp) is likely to do so on servers outside the UK: again, please seek independent advice as appropriate.

6 The disclaimers

Whilst we hope you find it useful, please note that the guidance provided here is not intended as legal or HR advice. You should always seek independent professional advice on legal and HR aspects of your EDI and data protection policies.

Please also note that this document is tailored primarily for IP professionals in private sector organisations. Within in-house departments and teams, different constraints are likely to apply to EDI data gathering due to wider corporate EDI and data protection policies.