Bird & Bird

Equality, Diversity and Inclusivity Monitoring

A multi-country guide

HR Data Essentials

May 2022

Summary

		Is there a legal requirement to carry out equal opportunities & diversity monitoring?	Can employers actively promote diversity in the workplace?	Are there provisions in data protection law on diversity monitoring?	Is a DPIA required when an employer carries out equal opportunities & diversity monitoring?
p.5	**Australia**	🔴	🟢	🔴	⚪
p.10	**Belgium**	🟢	🟢	🟢	🟢
p.15	**China**	🔴	🟢	🔴	⚪
p.19	**Czech Republic**	🔴	🟢	🔴	🟢
p.23	**Denmark**	🔴	🔴	🔴	🟢
p.28	**Finland**	🟢	🟢	🔴	🟢
p.33	**France**	🟢	🟢	🔴	🟢
p.39	**Germany**	🔴	🟢	⚪	🟢
p.44	**Hong Kong**	🔴	🟢	🔴	⚪
p.48	**Hungary**	🔴	🟢	🔴	🟢
p.53	**Italy**	🟢	🟢	🔴	🟢
p.58	**Netherlands**	🔴	🟢	🟢	🟢
p.62	**Poland**	🔴	🟢	🔴	🟢
p.67	**Singapore**	🔴	🟢	🔴	⚪
p.71	**Slovakia**	🔴	🟢	🔴	🟢
p.76	**Spain**	🟢	🟢	🔴	🟢
p.81	**Sweden**	🟢	🟢	🔴	🟢
p.85	**UAE**	🔴	🟢	🔴	🟢
p.89	**UK**	🔴	🟢	🟢	🟢

🔴 No
🟢 Yes
⚪ Not required by law but strongly recommended or specific conditions apply

Equality, diversity and inclusivity are vital to building a strong, engaged and innovative workforce. Without monitoring, it is difficult for any organisation to know where to start. We are here to help.

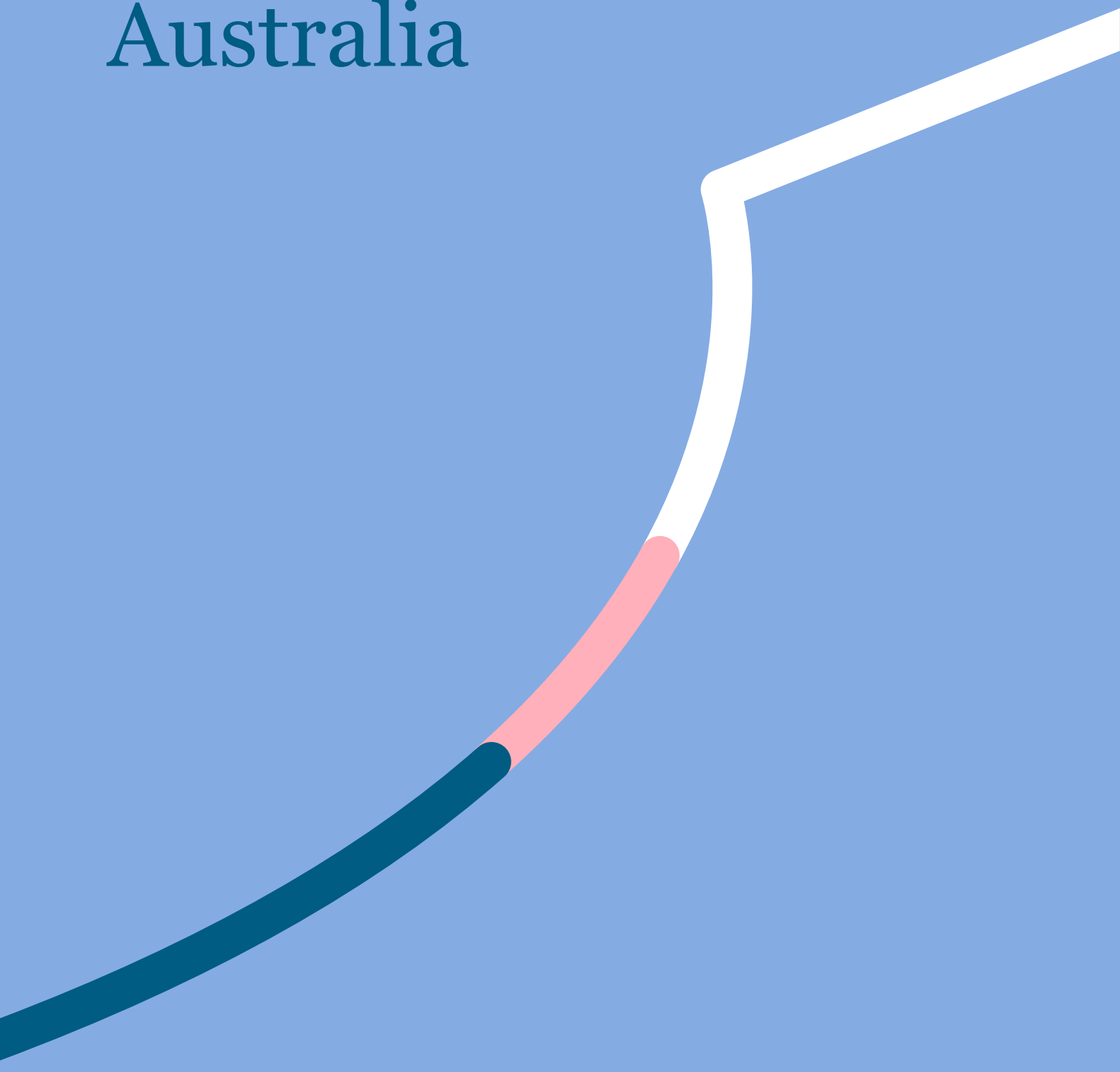
In the modern workforce, commitments to promoting equality, diversity and inclusivity ("EDI") are growing in importance. As well as ensuring that the most capable potential leaders and staff are hired, today's employees and customers place high importance on the diversity of the businesses they work with. Employers today must be able to show that they are taking proactive steps on EDI to attract the best candidates and work with the best companies.

In recent years, we have seen more and more employers try to take action to address EDI in their organisation. Many have opened up dialogue with staff members, and have started to assess what reporting, initiatives and support programmes can help develop their businesses and workforce.

The first step for most is working out what are their existing diversity challenges. This is difficult to do properly without accurate data. Collecting this data can be challenging, especially where a multi-country workforce means diverging rules across multiple jurisdictions. EDI data is usually highly sensitive, and processing this information is high-risk activity under both employment and privacy laws. There can be significant consequences of getting it wrong, from outraged staff and reputational damage to the potential for fines and legal claims.

This guide exists to help you understand these rules. Our comparative traffic-light chart and detailed country summaries have been updated to help you understand what you can collect, and how you can use the data you obtain. If you want to know more, our HR Data experts are happy to help you navigate these requirements for your workforce.

Australia



Australia

What characteristics are protected from discrimination?

- Race (including colour, national or ethnic origin and immigrant status)
- Sex
- Sexual orientation
- Age
- Physical or mental disability
- Intersex status
- Marital status
- Family or carer's responsibilities
- Pregnancy
- Gender Identity

Note also that some States have different protected attributes including religion and political opinion.

What of these are subject to additional protections/requirements under local data protection law? How does this interact with discrimination law and where do they overlap?

The *Privacy Act 1988 (Cth) (Privacy Act)* defines 'personal information' as information or an opinion about an identified individual, or an individual who is reasonably identifiable:

a whether the information or opinion is true or not; and

b whether the information or opinion is recorded in a material form or not.[1]

There are a number of different types of information which are subject to a higher level of protection under the Privacy Act:

- 'sensitive information', which includes personal information in the following categories:
  - information or opinion about an individual's racial or ethnic origin, political opinion or associations, religious or philosophical beliefs, trade union membership or associations, sexual orientation or practices, or criminal record, provided the information or opinion otherwise meets the definition of personal information); and
  - health or genetic information;
- credit information;
- employee record information (subject to exemptions); and
- tax file number information.

As can be seen from the categories above, sensitive information includes information about most of the characteristics which are protected from discrimination, including race, colour, sexual orientation, physical or mental disability, religion, political opinion and national extraction or social origin.

[1] We note that Australian data protection laws are currently undergoing a period of significant change (which will affect many of the obligations in the Privacy Act set out in this table). In late 2021, the Commonwealth Attorney-General released an extensive discussion paper proposing significant reforms to the Privacy Act (expected to be introduced later in 2022 or early 2023) (Discussion Paper), as well as an exposure draft of the Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 (OP Bill) (expected to be introduced to parliament in early 2022). One of the changes proposed in the Discussion Paper is an expansion of the definition of 'personal information' to include information that 'relates to an identified individual' as opposed to just 'about an individual'.

Is there a general legal requirement to carry out EDI monitoring?

No. There is no general requirement to carry out EDI monitoring.

Is there any specific EDI data that employers are legally required to process, e.g. to carry out EDI monitoring (such as gender pay gap reporting)?

Yes, there are specific domestic laws governing EDI in Australia:

- Employers with more than 100 employees are required to report annually on gender diversity in the workplace under the *Workplace Gender Equality Act 2012 (Cth)*. Specifically, an employer must prepare a written public report containing information relating to the employer and to gender equality indicators including:
  - gender composition of the workforce;
  - gender composition of its governing body;
  - equal remuneration between women and men;
  - availability and utility of employment terms, conditions and practices relating to flexible working arrangements for employees and to working arrangements supporting family or caring responsibilities; and
  - consultation with employees on issues concerning gender equality in the workplace.
- Employers with 500 or more employees are required to have a policy or strategy in place that specifically supports gender equality, to comply with the additional compliance requirements set out in the *Workplace Gender Equality (Minimum Standards) Instrument 2014 (Cth)*.

Can employers actively promote diversity in the workplace?

Yes. There is no positive requirement for employers to do so, however employers are obligated to prevent discriminatory practices in the workplace.

Employers with 500 or more employees must also have a formal policy or strategy in place for at least one of the Minimum Standards to comply with the Workplace Gender Equality (Minimum Standards) Instrument 2014 (Cth) in categories such as:

- workforce composition;
- gender pay gaps;
- support for carers; or
- sex-based harassment.

Does data protection law have specific provisions either permitting or prohibiting the processing of personal data for equal opportunities & diversity monitoring?

Yes. Broadly, the Privacy Act requires that personal information be managed in accordance with the Australian Privacy Principles (APPs). Further information on the basic requirements for handling personal information in accordance with the APPs is set out in the questions below.

There is an exemption in relation to the disclosure and use requirements in the APPs for “employee records” that are directly related to a current or former employment relationship; however, this exemption may not apply to an employer’s diversity monitoring initiatives as any such initiatives may not be sufficiently related to the current or former employment relationship. In addition, the employee records exemption is only available to the employing entity and not to related bodies corporate of the employing entity, noting that employee databases and EDI monitoring often involve more than one company in a group. Further, the employee record exemption does not apply to contractors, who are often included in EDI studies.

Additionally, where the employee records exemption does not apply, personal information collected as part of an EDI monitoring initiative which falls within the sensitive information category identified in question 2 above is subject to higher levels of protection than other personal information under the *Privacy Act*, including:

- a requirement to obtain employee consent to collect such sensitive information, unless an exception applies; and
- if such sensitive information is used for a secondary purpose from the primary purpose for which it was collected, a requirement that such secondary purpose be directly related to that primary purpose.

Where employers are required to, or not prohibited from, processing EDI data:

Do we have to collect and process EDI data in anonymised form?

No, but this is recommended. The *Privacy Act* does not apply to information which is sufficiently de-identified. Guidance from the Office of the Australian Information Commissioner (OAIC) indicates that this requires that there be no reasonable likelihood of re-identification occurring, for example by removing information used to re-identify an individual or through use of controls/safeguards to prevent re-identification.

If the information is not sufficiently de-identified and the employee records exemption does not apply, entities subject to the *Privacy Act* (**APP entities**) are also required to comply with the APPs. This includes APP 2 which requires that individuals have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity in relation to a particular matter unless an exception applies, for example where it is impracticable for the APP entity to deal with individuals who have not identified themselves or who have used a pseudonym. Given that EDI data is often collated and de-identified, such an exception may be difficult to argue, depending on the circumstances.

What are the key employment risks to consider?

- Employees cannot be treated less favourably as a result of a specific personal characteristic or attribute. There is an inherent risk that once EDI data has been collected and if it is not anonymised, that it could be used to engage in behaviour that would amount to unlawful discrimination.
- The collection of raw EDI data (i.e. not anonymised) will trigger the *Privacy Act* requirement in respect of collection, being the requirement that a collection notice be provided before or, if that is not practicable, as soon as practicable after an employer collects what would be considered personal information under the *Privacy Act* about an individual.
- An employee records exemption applies to the use and disclosure of personal information, but only once it has been collected and where the relevant personal information is directly related to a current or former employment relationship and employee record. The exemption will only apply to the employing entity so does not provide effective protection for company groups.

What are the key data protection compliance requirements under data protection law?

Among other obligations, employers are subject to the following key obligations in relation to personal information which is not de-identified or subject to the employee records exemption:

- APP entities that are ‘organisations’ may only collect personal information that is reasonably necessary for one or more of their functions or activities, while APP entities that are ‘agencies’ may only collect personal information that is reasonably necessary for, or directly related to, one or more of their functions or activities. Employers do not need consent from employees to collect the same, unless the information is sensitive;
- at the time of collection, employers need to take reasonable steps to provide the employee with a collection notice which includes the various matters set out in APP 5.2;
- personal information collected for a particular purpose must not be used or disclosed for a secondary purpose unless the individual to whom the information relates has consented to such use or disclosure or another exception applies;
- employers disclosing personal information to overseas recipients must take reasonable steps to ensure that the overseas recipient does not breach the APPs, unless an exception applies; and

- employers must take reasonable steps to protect the information from misuse, interference, loss and unauthorised access, modification or disclosure and to destroy or de-identify personal information that is no longer required for the purposes for which it was collected or by law.

Are there any key local considerations, such as consultation with trade union or employee representative bodies?

No. Consultation with employee representatives is only required where (1) employees' employment is covered by a Fair Work Modern Award, and (2) the workplace is introducing a "major workplace change". The processing of EDI data is highly unlikely to constitute a major workplace change and so will not trigger any consultation requirements.

What are the key risks for employers in not complying with the above?

Discriminating against another employee because of a personal characteristic or attribute may result in a general protections claim before the Fair Work Commission or a discrimination claim before the Human Rights Commission, both of which may result in monetary compensation being awarded.

The *Privacy Act* empowers the OAIC to apply to the Court to require an entity to pay a civil penalty (of up to AU$2.22mil).2 Further, the OAIC will publicly communicate information in connection with civil penalty proceedings.

[2] The OP Bill includes a proposal to increase the penalties payable under the Privacy Act. If passed, the maximum penalty applying will be an amount not more than the greater of AU$10mil, 3x the value of any benefit obtained from the contravening conduct or 10% of the company's annual turnover for the year prior to the contravening conduct.

Belgium

Belgium

What characteristics are protected from discrimination?

- Gender (this includes discrimination on the grounds of pregnancy, childbirth, breastfeeding and medically assisted reproduction, motherhood, fatherhood, co-motherhood, adoption, sex change, gender identity or gender expression, gender characteristics)
- Race (including race, skin colour, nationality, origin (e.g. Jewish), nationality or ethnicity)
- Disability
- Religious and philosophical belief
- Sexual orientation
- Age
- State of health
- Wealth
- Physical or genetical characteristics
- Civil status
- Political conviction
- Trade union beliefs
- Birth
- Social background
- Language

What of these are subject to additional protections/requirements under local data protection law? How does this interact with discrimination law and where do they overlap?

The processing of personal data is strictly regulated under Belgian law. Special categories of personal data are subject to additional protections and requirements.

The GDPR, which applies in Belgium, defines “special categories of data” as:

- personal data revealing **racial** or **ethnic origin**;
- personal data revealing **political opinions**;
- personal data revealing **religious** or **philosophical beliefs**;
- personal data revealing **trade union membership**;
- **genetic** data;
- **biometric** data (where used for identification purposes);
- data concerning **health**;
- data concerning a person’s **sex life**; and
- data concerning a person’s **sexual orientation**.

Those categories in italics above broadly overlap with the corresponding protected characteristic under discrimination law but the application of both discrimination protection and data protection requirements should be considered on a case-by-case basis.

Care should be taken where the special category data requirements overlap with other protected characteristics (e.g. gender data may include health or sexual orientation data).

Is there a general legal requirement to carry out EDI monitoring?

No. There are no general EDI data processing or monitoring requirements (under either employment or data protection law).

Is there any specific EDI data that employers are legally required to process, e.g. to carry out EDI monitoring (such as gender pay gap reporting)?

Yes. There is an obligation to monitor equal pay for men and women.

Every two years, employers who employ an average of at least 100 employees must carry out and submit a detailed analysis of their remuneration policy. A more simplified form must be submitted by companies who employ between 50 to 100 employees. Any wage disparity based on gender should therefore become transparent and should subsequently be eliminated via negotiations with employee consultation bodies (Works Council or trade union representatives).

Can employers actively promote diversity in the workplace?

Yes.

Employers can set up a diversity action plan aimed at combatting discrimination and ensuring equal opportunities in a more diverse workplace.

Does data protection law have specific provisions either permitting or prohibiting concerning the processing of personal data for equal opportunities & diversity monitoring?

Yes.

Processing of personal data, and in particular special categories of personal data, is strictly regulated (please see above).

As regards equal pay for men and women, the company is not obliged to disclose wage data if there are three or less than three workers in a specific function, as this would allow the employer to identify the workers in question and thus breach their rights under data protection legislation.

Where employers are required to, or not prohibited from, processing EDI data:

Do we have to collect and process EDI data in anonymised form?

No. Anonymisation is not required under Belgian law.

However, because there is no clear legal basis under applicable Belgian law that an employer can rely on to process ‘sensitive personal data’ for EDI purposes (see answer to Q.8 below), anonymisation of ‘sensitive personal data’ is nonetheless recommended. Please bear in mind, however, that the threshold for anonymisation is quite high and requires that personal data can no longer be linked to a specific data subject.

What are the key employment risks to consider?

The processing of EDI data increases the risk of discrimination claims, which is the key risk to be considered when contemplating such processing activity where it is not strictly required by law. The fact that an employer processes employee EDI data where this is not strictly prohibited (but not legally required) could indeed be used by employees to claim indirect discrimination, and to claim compensation on this basis.

Belgian law specifically prohibits dismissals for grounds directly or indirectly related to certain protected criteria such as:

- the exercise by an employee of his/her trade union delegate mandate, pregnancy (and childbirth);
- paternity or adoption;
- the exercise an employee of certain political mandates unrelated to his/her employment;
- having requested or being on career break or on thematic leave;
- having lodged a complaint relating to gender equality, violence or moral or sexual harassment at work;
- racism and xenophobia.
- or in relation to certain forms of discrimination.

This does not mean that employees with one of these criteria cannot be dismissed at all, but that they can only be dismissed for reasons completely unrelated to the specifically protected criterion. Generally, the burden of proof that the dismissal ground is unrelated to the protected ground lies with the employer. The flat dismissal indemnity that the law provides in case of breach of any of these specific grounds can generally not be combined with an indemnity for discriminatory dismissal, but this must be verified on a case-by-case basis.

What are the key data protection compliance requirements under data protection law?

For purposes of data protection law, organisations should draw a distinction between the processing of general (i.e. non-sensitive) **personal data** and **sensitive personal data** for EDI purposes.

The processing of personal data must rely on a legal ground. An organisation could consider relying on its legitimate interest to ensure EDI in the workplace. If so, the organisation should carry a 'legitimate interest assessment', balancing its own interests and those of the employees. The outcome for the organisation having considered all the relevant factors should be that the employee's interests do not outweigh those of the organisation. For accountability purposes, it is recommended that this 'legitimate interest assessment' is documented and kept on file.

EDI data will often include **sensitive personal data** under the GDPR (see above). In addition to identifying a legal basis for the process (see above), the processing of 'sensitive personal data' is allowed only if one of the conditions is met.

There is currently no general legal obligation or provision allowing organisations to process sensitive data for EDI purposes. In the context of EDI, the following conditions permitting the processing of sensitive personal data are potentially relevant (their application will depend on the circumstances):

- Explicit consent of the employee (noting the difficulties in obtaining valid consent in the employment context);
- Employment, social security and social protection (if authorised by law), noting that there is no general legal obligation or provisions allowing organisations to process sensitive data for EDI purposes. Organisations could possibly rely on the introduction of so-called "affirmative action" as provided for in anti-discrimination legislation.

Organisations with a registered office or at least one operational office in the Brussels Capital Region may want to consider the provisions under legislation of the Brussels Capital Region, entitling them to draw up a diversity plan and to submit it to Actiris for approval. If this diversity plan is implemented correctly, these organisations may be awarded a diversity label. Within the framework of this specific diversity plan, there is a legal authorisation to classify the workforce in the categories of beneficiary employees and therefore also a limited authorisation to process 'sensitive personal data'.

Given this position, as mentioned above organisations should consider either not processing such personal data or anonymising that data in order to minimise risk.

Are there any key local considerations, such as consultation with trade union or employee representative bodies?

Yes. Employers must consult with employee representative bodies (if they exist) in advance whenever an envisioned EDI programme is likely to impact the collective work organisation and working conditions. Although uncommon, these bodies could also ask to check these policies as part of their particular duties to monitor the social reclassification of disabled employees, vocational qualifications, or if it relates to health & safety at work.

What are the key risks for employers in not complying with the above?

Misuse or perceived misuse of staff EDI data in the context of staff management and decision-making runs a clear risk of discrimination claims as well as other related employment claims (see above).

The Belgian data protection authority has the power to impose fines of up to £17,500,000 or 4% of global annual turnover (whichever is greater), as well as to issue enforcement notices requiring changes to processing in the event of a breach of the GDPR. Employees may also have a right to seek compensation in the event of breach of the GDPR.

In addition, level 2 criminal sanctions can theoretically be imposed by the social inspection services on an employer who failed to consult or inform the employee representative bodies where it should have i.e., either an administrative fine comprised between € 200 and 2,000, or a criminal fine comprised between € 400 and 4,000, both multiplied by the number of concerned employees (capped at a maximum of 100).

In practice, any of the breaches referred to above are likely to negatively impact the social dialogue and trust between the employees and their representative bodies on the one hand, and the management at the other hand, which also has a deterrent impact for employers.

China

China

What characteristics are protected from discrimination?

- Disability
- Marriage
- Pregnancy / maternity
- Race (includes nationality, ethnicity, national origins and colour)
- Religion/belief
- Gender
- Household register (Rural or urban household registration)

What of these are subject to additional protections/requirements under local data protection law? How does this interact with discrimination law and where do they overlap?

Sensitive personal information is subject to additional protections and requirements in China. The PRC Personal Information Protection Law (**PIPL**) defines "sensitive personal information" as "personal information that, once leaked or illegally used, will easily lead to infringement of the human dignity or harm to the personal or property safety of a nature person", including without limitation:

- personal information revealing **religious beliefs;**
- information concerning **medical health;**
- personal information revealing **specific identity;**
- **financial account** information;
- **personal location** tracking;
- biometric information (where used for identification purposes);
- personal information of a **minor under the age of 14**.

The definition of sensitive information broadly overlaps with corresponding protected characteristic under discrimination law. However, the application of both discrimination protection and data protection requirements should be considered on a case-by-case basis.

Care should be taken where the sensitive personal information requirements overlap with other protected characteristics (e.g. pregnancy/maternity information may include medical health information).

Is there a general legal requirement to carry out EDI monitoring?

No.

Is there any specific EDI data that employers are legally required to process, e.g. to carry out EDI monitoring (such as gender pay gap reporting)?

No.

Can employers actively promote diversity in the workplace?

Yes.

The *PRC Employment Promotion Law* imposes obligation to promote equality of opportunities in the workplace on employers.

There is no direct broad requirement to actively promote diversity in the workplace under PRC law but employers can choose to do so.

Does data protection law have specific provisions either permitting or prohibiting the processing of personal data for equal opportunities & diversity monitoring?

No. But under the PIPL, sensitive personal information may only be processed if the employer has obtained the employee's separate consent.

Where employers are required to, or not prohibited from, processing EDI data:

Do we have to collect and process EDI data in anonymised form?

No.

Although anonymous collection is the safest way to collect and otherwise process EDI data is in anonymised form, and potentially reduces employment and data protection risks, EDI data can usually be collected and otherwise processed in a form where staff are identified, or identifiable provided steps are taken to comply with data protection law. Failure to take appropriate steps to ensure compliance will increase the risks associated with complaints, claims and sanctions under employment and data protection law.

What are the key employment risks to consider?

The collection of EDI data is sensitive and relatively high risk from an employment and data protection perspective. The unlawful processing of EDI data may result in an illegal dismissal. For example, where an employer unilaterally terminates an employee's employment as a result of employee's refusal to provide EDI data, if the employer's processing of EDI data has no legal basis or a legitimate and reasonable purpose, or is not consistent with the requirements of PIPL, such termination may be deemed as illegal dismissal. In addition, the unlawful processing of EDI data could also trigger disputes over discrimination. It should be noted that, in China, employment discrimination falls under the category of infringement of personality right, which is a right under the Civil Code rather than the employment laws.

Employers should give particular consideration to the personal information protection compliance requirements (see Q.8 below), and the management of and communications regarding EDI data programmes in order to reduce the risk of claims and sanctions, including the following.

- The EDI data must be processed in accordance with the principles of lawfulness, legitimacy, necessity, good faith, openness and transparency.
- Employers should consider carefully what data they want to collect, why, and how they want to use that data. Collection of EDI data shall be limited to the minimum scope necessary for achieving the purpose of processing and shall not be excessive.
- Employers should inform the employees of the purpose and method of processing, the type of personal information to be processed and its retention period, the way and procedure for the employees to excise their rights provided for by PIPL, etc. The employees shall be informed in a conspicuous way, in clear and easy-to-understand language, and in a truthful, accurate and complete manner.
- The employee's consent (or separate consent) should be obtained before the collection, if required by law.

What are the key data protection compliance requirements under data protection law?

The collection and analysis of EDI data in identifiable form will result in the processing of personal information. As set out above, certain types of EDI data are also "*sensitive personal information*" (see Q.2 above).

When processing any personal information, the employer must comply with the requirements set out in the PIPL. Broadly, this means employers should:

- identify and communicate a clear and legitimate purpose and legal basis for processing EDI data – where this involves sensitive personal information, the employees' separate consents should be obtained;
- only process the minimum amount of data required;
- inform the employees of the process details (see Q.7 above)
- take steps to ensure the continuing accuracy and integrity of the data;
- implement appropriate security, access and confidentiality measures, and not retain that data for longer than required for the purpose for which it was originally collected.

Additional compliance requirements under the PIPL also include:

- completion of a personal information protection impact assessment (PIPIA);
- obtaining consent (or separate consent) if required;
- updating the employer's record of processing;
- developing an internal management system and operating procedures.

Are there any key local considerations, such as consultation with trade union or employee representative bodies?

No.

What are the key risks for employers in not complying with the above?

- Equality, diversity and inclusivity is a less developed area in China's employment sphere and legislative landscape.
- Employers who misuse or are perceived to misuse EDI data may be at risk of claims in respect of illegal dismissal or discrimination under PRC employment law, with the corresponding risk of compensation or damage awards.
- Misuse or perceived misuse of staff EDI data in the context of staff management and decision-making runs a clear risk of data breach claims. In the event of a breach of the PIPL, a fine of up to CNY 50,000,000 or 5% of last year's annual revenue will be imposed on the employer. Meanwhile, the person in charge or any other individual liable for the breach will be fined up to CNY 1,000,000, and may also be banned for a certain period of time from serving as a director, supervisor, senior officer or personal information protection officer of the company.

Czech Republic

Czech Republic

What characteristics are protected from discrimination?

- Gender (this includes discrimination on grounds of pregnancy, maternity, paternity or gender identification)
- Sexual orientation
- Racial or ethnic origin
- Nationality
- Citizenship
- Socio-economic status
- Family background
- Language
- State of health
- Age
- Religion or belief
- Property
- Marital or family status
- Family relationship or responsibilities
- Political or other opinion
- Membership and activities in political parties or political movements, trade unions or employers' organizations

What of these are subject to additional protections/requirements under local data protection law? How does this interact with discrimination law and where do they overlap?

Special categories of personal data (in the meaning of Art. 9 GDPR) are subject to additional protections and requirements. The GDPR defines "special categories of data" as:

- personal data revealing **racial** or **ethnic origin**;
- personal data revealing **political opinions**;
- personal data revealing **religious or philosophical beliefs**;
- personal data revealing **trade union membership**;
- **genetic** data;
- **biometric** data (where used for identification purposes);
- data concerning **health**;
- data concerning a person's **sex life**; and
- data concerning a person's **sexual orientation**.

Those categories in italics above broadly overlap with the corresponding protected characteristic under discrimination law but the application of both discrimination protection and data protection requirements should be considered on a case-by-case basis.

Care should be taken where the special category data requirements overlap with other protected characteristics (e.g. sex/gender identity data may include health or sexual orientation data).

Is there a general legal requirement to carry out EDI monitoring?

No. There is no general legal requirement to carry out EDI monitoring. Employers are, however, required to ensure equal treatment of all employees and act in such a way so as to avoid discrimination on protected grounds.

Is there any specific EDI data that employers are legally required to process, e.g. to carry out EDI monitoring (such as gender pay gap reporting)?

Yes. As regards specific EDI requirements, employers with more than 25 employees are required to ensure at least 4% of their total employee population is comprised of people with a disability. This obligation can alternatively be fulfilled by other statutory means (e.g. by purchasing specific products or services or by payment to the state budget). To monitor the compliance with this requirement, employers are obliged to report on their fulfilment of these requirements in writing to a regional branch of the Labour Office on an annual basis.

Can employers actively promote diversity in the workplace?

Yes. Employers must ensure equal treatment for all employees as regards employee working conditions, remuneration for work and other emoluments in cash and in kind (of monetary value), professional training and opportunities for career advancement (promotion).

At the same time, the restrictions concerning the collection of the information specified below apply (see Q.5 below).

Does data protection law have specific provisions either permitting or prohibiting the processing of personal data for equal opportunities & diversity monitoring?

Yes. There are special provisions concerning the processing of certain categories of personal data under the Czech Labour Code.

The *Czech Labour Code* specifically provides that employers must not request any information from their employees that does not directly relate to performance of work and the employment relationship. In particular, employers should never request information on:

- sexual orientation;
- racial or ethnic origin;
- trade union organization membership;
- membership of political parties or movements;
- religion and confession.

The following information may be requested only where the employer has grounds to request this given the nature of work to be performed (provided that the request is reasonable), or where the employer is required to request this by law:

- information on pregnancy;
- family and property;
- clean criminal record.

Since the above restrictions under the *Czech Labour Code* are interpreted rather strictly (meaning that the information listed above should not even be collected on a voluntary basis), any collection and processing of EDI data is thereby practically prevented.

Where employers are required to, or not prohibited from, processing EDI data:

Do we have to collect and process EDI data in anonymised form?

No. That said, as discussed (see Q.5 above) the collection and other processing of most EDI data is currently prevented by the restrictions laid down in the *Czech Labour Code*.

If any EDI data is collected and processed (to the extent allowed by applicable laws), processing in an anonymised form is recommended, although not legally required.

What are the key employment risks to consider?

Please see Q.5 above.

What are the key data protection compliance requirements under data protection law?

The collection of EDI data (to the extent allowed by local laws) in identifiable form will result in the processing of personal data. As set out above, certain types of EDI data are also "special category" data (see Q.2 above).

When processing any personal data, the employer must comply with the requirements set out in the GDPR. Broadly, this means employers should:

- identify and communicate a clear and legitimate purpose and legal basis for processing EDI data – where this involves special category data, there must also be a condition for processing under Article 9 GDPR (see Q.5 above);
- only process the minimum amount of data required;
- take steps to ensure the continuing accuracy and integrity of the data,
- implement appropriate security, access and confidentiality measures, and not retain that data for longer than required for the purpose for which it was originally collected.

Are there any key local considerations, such as consultation with trade union or employee representative bodies?

Employers are required to inform their employees or Work Council/Trade Union (if relevant) regarding measures taken by the employer to secure equal treatment of male and female employees and prevention of discrimination. There is, however, no consultation obligation.

What are the key risks for employers in not complying with the above?

If an employer violates the requirement not to request information from employees not directly related to performance of work and the employment relationship, they may be fined up to CZK 1,000,000 (approx. EUR 40,000).

A fine of the same amount may be imposed for the violation of the equal treatment rules.

Denmark

Denmark

What characteristics are protected from discrimination?

- Gender
- Race
- Skin colour
- Religion / religious beliefs
- Political opinion
- Sexual orientation
- Gender identity, gender expression or gender characteristics
- Age
- Disability
- National or ethnic origin
- Socio-economic origin
- Trade union membership or activities
- Membership of associations
- Pregnancy
- Maternity/paternity/parental leave

What of these are subject to additional protections/requirements under local data protection law? How does this interact with discrimination law and where do they overlap?

Special categories of personal data are subject to additional protections and requirements in Denmark, cf. the GDPR Art. 9. There are no additional local data protection law requirements. Special categories of personal data are defined in GDPR Art. 9:

- personal data revealing **racial** or **ethnic origin**;
- personal data revealing **political opinions**;
- personal data revealing **religious** or **philosophical beliefs**;
- personal data revealing **trade union membership**;
- **genetic** data;
- **biometric** data (where used for purposes of uniquely identifying a natural person);
- data concerning **health**;
- data concerning a person's **sex life**; and
- data concerning a person's **sexual orientation**.

The categories in italics above broadly overlap (or can be derived) with the corresponding protected characteristic under discrimination law, thus the application of both discrimination protection and data protection requirements should be considered on a case-by-case basis.

Particular vigilance is required where the special category data requirements overlap with other protected characteristics, as this might not be entirely straight forward to spot (e.g. sex/gender identity data may include health or sexual orientation data).

Processing will only be allowed if local employment law, and specifically anti-discrimination law, does not prohibit such processing (e.g., the *Danish Anti-Discrimination Act*, etc., as referenced below) and a legal basis can be identified under the GDPR.

Is there a general legal requirement to carry out EDI monitoring?

No. There is no general nor specific requirement to carry out EDI processing or monitoring. Employers must act in line with regulations and legislation prohibiting of any kind of discrimination at all times.

Please note that the *Danish Anti-Discrimination Act section 4*, prohibits an employer, in connection with or during employment, from requesting, obtaining, receiving or making use of information about a worker's race, colour of skin, religion or belief, political affiliation, sexual orientation or national, socio-economic or ethnic origin.

Furthermore, it follows from the *Danish Act on the use of Health Data etc. on the Labour Market* that an employer may only request health data where the purpose is to establish whether the employee suffers from or has suffered from an illness or has had symptoms of a disease, provided that the disease will be of significant importance for the employee's capacity to perform his or her job functions.

Consequently, if any of the above-mentioned personal data covered by the scope of the Danish acts are requested and the employee is identifiable, the employer will be in violation of the *Danish Anti-Discrimination Act* and/or *Act on the use of Health Data etc. on the Labour Market*. On this basis, an approach whereby an employer gives workers the opportunity to provide or self-report EDI data on a voluntary basis might not be permitted under Danish law.

Is there any specific EDI data that employers are legally required to process, e.g. to carry out EDI monitoring (such as gender pay gap reporting)?

No, please also see above.

Can employers actively promote diversity in the workplace?

No. Employers are prohibited from applying adverse measures (terminations, demotions, rejection of applications etc.) on the grounds of one or more protected characteristic. For most of these characteristics, a split burden of proof applies. This means that if an employee who is subjected to adverse treatment can point to circumstances sufficiently supporting the notion that the protected characteristic played a role, then the burden shifts to the employer to prove that the characteristic did not play any part. The barrier for shifting the burden of proof is relatively low – for example, asking an employee or a job applicant about for information about pregnancy, ethnic origin, religious belief or another protected characteristic will normally suffice as circumstances supporting the notion that the protected characteristic played some part in the employer's decision/subsequent actions.

In addition, requesting, obtaining, receiving or making use of information about the worker's race, colour of skin, religion or belief, political affiliation, sexual orientation, gender identity, gender expression or gender characteristics or national, social or ethnic origin in connection with or during their employment is prohibited (see above).

Does data protection law have specific provisions either permitting or prohibiting the processing of personal data for equal opportunities & diversity monitoring?

Yes. Whilst there are generally no specific provisions specifically dealing with processing of EDI data under Danish data protection law, under the GDPR, processing special category data is generally prohibited unless a condition under Art. 9(2) GDPR applies.

Depending on the set up of the EDI monitoring, and provided Danish employment laws also allows for the data collection and subsequent processing, the appropriate legal basis for processing would be **explicit consent**, but only if the employer can demonstrate that this is truly voluntary. Employers must be aware of and take appropriate precautions, as there will always be an element of risk of consents not meeting all consent requirements, especially the "voluntary" requirement, due to the uneven distribution of power

inherent in the employer – employee relationship. Further, consent may be withdrawn by the employee at any point in time.

Where employers are required to, or not prohibited from, processing EDI data:

Do we have to collect and process EDI data in anonymised form?

No, to the extent the employer is allowed to collect and process such data in the first place, which as a general rule is difficult under Danish law (cf. below), there is no additional anonymisation requirement.

Under Danish law, collection and other processing of EDI data in a form where employees are identified or identifiable, can only be carried out provided steps are taken to comply with relevant (and strict) Danish employment laws (see Q.2 – 3 above) as well as data protection law. Failure to take appropriate steps to ensure compliance will increase the risks associated with complaints, claims and sanctions under employment and data protection law.

Thus, anonymous collection would generally be the safest way to collect and otherwise process EDI data and reduce the level of risk under employment and data protection laws.

Please note that no case law exists in this regard and the Danish Ministry of Employment have not provided any guidance on (anonymous) diversity surveys, or similar.

What are the key employment risks to consider?

Collecting or processing data regarding any of the characteristics, particularly in a form where employees are identifiable, will create a risk for the employer in having to "defend" any decisions under anti-discrimination laws. For example, if an employee who is subject to adverse treatment can point to circumstances sufficiently supporting the notion that the protected characteristic played a role, then the burden of proof shifts to the employer who must prove that the characteristic did not play any part.

Further, the employer should give particular consideration to the data protection compliance requirements (see Q. 8 below), and the management of and communications regarding EDI data programmes (provided they can legally be initiated under Danish employment law), in order to reduce the risk of claims and sanctions, including the following:

- the collection of EDI data should be voluntary. It is unlikely that an employer would be able to justify or enforce a mandatory requirement unless based on a legal requirement; and
- staff communication is important for managing employee perceptions, thereby reducing the risk of claims and sanctions. Employers should ensure that they carefully consider and prepare employee communications about any EDI data programmes prior to launch, and try to anticipate any resistance, concerns or potential risks.

What are the key data protection compliance requirements under data protection law?

The collection of EDI data in identifiable form will result in the processing of personal data. As set out above, certain types of EDI data are also "special category" data (see Q.2 above).

When processing any personal data, the employer must comply with the requirements set out in the GDPR, as there are no specific local data protection requirements. Broadly, this means employers should:

- identify and communicate a clear and legitimate purpose and legal basis for processing EDI data – where this involves special category data, there must also be a legal basis for processing under Article 9 (see Q.5 above);
- only process the minimum amount of data required;
- take steps to ensure the continuing accuracy and integrity of the data,
- implement appropriate security, access and confidentiality measures, and not retain that data for longer than required for the purpose for which it was originally collected.

Additional compliance requirements under the GDPR also include:

- depending on the setup of the EDI survey, completion of a data protection impact assessment (**DPIA**) and, if relevant, legitimate interests assessment;
- Provision of an appropriate notice to employees, with a clear explanation of what data they will collect, why, and how it will be used, in accordance with the GDPR, and obtaining consent if required; and
- updating the employer's record of processing.

Are there any key local considerations, such as consultation with trade union or employee representative bodies?

No.

It is not common for employers to collect EDI data in Denmark. As a rule, no categories of EDI data are routinely requested in the employment context.

As a general rule, no consultation is required with trade union or employee representative bodies. Note that there are rules on general information and employee consulting requirements in companies with at least 35 employees regarding matters of significant importance.

What are the key risks for employers in not complying with the above?

Claims for compensation under the Danish Anti-Discrimination laws can be up to 12 months' salary depending on the employee's seniority and the facts of the case. Theoretically, the employer can also be fined under the Danish Anti-Discrimination laws, but this is very rare.

Employers may also be subject to fines and other sanctions imposed by the Danish data protection authority in the event the processing in question was deemed to be a breach of Danish data protection legislation.

There are possible PR and media risks involved, but these are considered low and are rarely seen.

Finland

Finland

What characteristics are protected from discrimination?

- Age
- Origin
- Nationality
- Language
- Religion
- Belief
- Opinion
- Political activity
- Trade union activity
- Family relationships
- State of health
- Disability
- Gender
- Pregnancy / childbirth
- Maternity / parental leave
- Sexual orientation
- Gender identity
- Gender expression
- Other personal characteristics

Note: In addition to direct and indirect discrimination, harassment, denial of reasonable accommodation and an instruction/order to discriminate constitute discrimination under Finnish legislation.

What of these are subject to additional protections/requirements under local data protection law? How does this interact with discrimination law and where do they overlap?

The *Finnish Act on the Protection of Privacy in Working Life* (759/2004) applies to all personal data, including the above-mentioned characteristics. The Act also includes special provisions on processing of data concerning health, personal credit and drug use as well as provisions concerning obtaining data from personality and aptitude tests, genetic testing, camera surveillance and retrieval and opening of emails belonging to the employer (i.e. e-mails sent to or from the e-mail address provided by the employer to the employee).

Further, special categories of personal data are subject to additional protections and requirements under the GDPR in Finland. Article 9 (1) GDPR defines “special categories of data” as:

- personal data revealing **racial** or **ethnic origin**;
- personal data revealing **political opinions**;
- personal data revealing **religious** or **philosophical beliefs**;
- personal data revealing **trade union membership**;

- **genetic** data;
- **biometric** data (where used for identification purposes);
- data concerning **health**;
- data concerning a person's **sex life**; and
- data concerning a person's **sexual orientation**.

The Finnish *Data Protection Act* excludes trade union membership from the application of Article 9 (1) GDPR under certain conditions, which mean that it can be processed more easily by employers.

There is only a theoretical clash between discrimination law and data protection law, namely between the duty of keeping records to fight discrimination and the data minimization principle. This is because in Finland the duty to carry out EDI monitoring is defined very narrowly in law (see below).

Is there a general legal requirement to carry out EDI monitoring?

No, there is no general legal obligation to carry out EDI monitoring.

There is only a legal duty to promote equality in the workplace which requires assessing the realisation of equality in the workplace and this may require some monitoring in certain situations as well.

Is there any specific EDI data that employers are legally required to process, e.g. to carry out EDI monitoring (such as gender pay gap reporting)?

Employers who regularly employ at least 30 employees must have (i) an equality plan; and (ii) a gender equality plan describing the measures how, generally speaking, equality and gender equality are promoted in the workplace. More specific requirements for the plans are further laid down in the law. Employers employing at least 20 employees on a regular basis are also obliged to take measures to promote equality into account in their plan for developing a work community.

Can employers actively promote diversity in the workplace?

Yes. Please see the answer above.

Employers may take proportionate "positive actions" to promote equality under certain circumstances in the workplace.

Does data protection law have specific provisions either permitting or prohibiting the processing of personal data for equal opportunities & diversity monitoring?

Yes.

Processing of personal data, and in particular special categories of personal data, is strictly regulated (please see above).

That said, there are no specific provisions that give employers additional rights to process sensitive personal data outside of Article 9 GDPR and the Finnish *Data Protection Act*.

There are also no specific provisions prohibiting processing data for EDI purposes. The general principles under Finnish law coming from the Act on *Privacy in Working Life* will apply. This means that only strictly necessary data may be collected; generally speaking, sensitive data as defined in Article 9(1) GDPR should not be collected.

Where employers are required to, or not prohibited from, processing EDI data:

Do we have to collect and process EDI data in anonymised form?

No. There are no specific provisions requiring EDI data processing or monitoring in Finland to be anonymised (under either employment or data protection law).

That said, given the data minimization principle is strengthened in Finland by the necessity requirement, if an employer wished nonetheless to process any EDI data, in practice doing so in anonymised form is likely to be the only way to safely collect and otherwise process data for wider EDI activities beyond gender equality.

What are the key employment risks to consider?

Processing EDI data includes both employment and data protection risks. It is important to consider the data protection requirements for employers (see Q.8 below) and the management of and communications regarding EDI data programmes in order to reduce the risk of claims and sanctions. In particular, employers should:

- carefully consider the legal basis for the collection of EDI data;
- carefully determine the purposes of data processing and how data protection principles (e.g. data minimisation, accuracy of data, and confidentiality and security of data) will be followed during processing; and
- inform employees about what data and why this will be collected, and how data will be used.

An employee who has been discriminated against may be entitled to receive compensation from the employer. There is no maximum limit to such compensation, but it must be proportionate to the severity of the discriminating action. The employees may still qualify for an award of damages under the *Tort Liability Act* or other legislation even if they have been awarded compensation in court in respect of a discrimination case regarding the same set of facts. Criminal liability for the employer or its representative may also be imposed, the sanction for which may be fines or imprisonment for a term not exceeding six months.

What are the key data protection compliance requirements under data protection law?

Since collecting, analysing and otherwise using EDI data is considered processing of personal data, regular data protection requirements must be followed. In so far as EDI data belongs to the special category of personal data (see Q.2), additional requirements also apply.

The GDPR requires that when processing any personal data, employers must:

- identify and communicate to the employees a clear and legitimate purpose and legal basis for processing of EDI data (Article 6 GDPR). In so far as EDI data includes special category data, the requirements of Article 9 GDPR must also be met;
- only process the minimum amount of data required;
- take steps to ensure the continuing accuracy and integrity of the data;
- implement appropriate security, access and confidentiality measures, and not retain that data for longer than required for the purpose for which it was originally collected; and
- consider a deletion process whereby personal data that are no longer relevant are deleted in regular intervals.

In addition, the Act on the *Protection of Privacy in Working Life* requires that the employer:

- processes only personal data directly necessary for the employee's employment relationship;
- should collect personal data concerning the employee primarily from the employee themselves and if data is collected elsewhere, the employer must obtain the employee's consent.

The Act on the *Protection of Privacy in Working Life* also includes special provisions which must be considered, for example on processing of data concerning health, personal credit and drug use as well as provisions concerning obtaining data from personality and aptitude tests, genetic testing, camera surveillance and retrieval and opening of emails belonging to the employer.

Are there any key local considerations, such as consultation with trade union or employee representative bodies?

Yes.

If the employer employs regularly 30 or more employees, it must draw up an equality plan, as also mentioned above. The gender equality plan must be drawn up in cooperation with shop steward, elected representative, occupational safety delegate and other representatives the employees have appointed. Such representatives must be guaranteed real opportunities to participate in the preparations of the equality plan.

It is not very common in Finland to systematically use any other EDI data than data on gender equality.

What are the key risks for employers in not complying with the above?

Non-compliance with the GDPR can result in sanctions up to 4% of global annual turnover or EUR 20,000,000. Further, employees can make claims for compensation for example on the basis of a GDPR infringement or discrimination.

Additionally, the employer can be sentenced to a fine for violating the Act on the *Protection of Privacy in Working Life*. In addition, the *Finnish Criminal Code* (39/1889) lays down penalties for a data protection offence.

Employees may be entitled to the compensation in respect of a discrimination claim and/or damages under separate tort or other employment law and may also be at risk of criminal liability (see above).

It is also worth mentioning that the employer must make sure that the equality plan meets the demands mentioned in the Equality Act. If the requirements are not met, a fine may be enforced.

France

France

What characteristics are protected from discrimination?

The protected characteristics under French law (ss. – Article 225-1 of the *French Criminal Code*) for the purposes of protection from discrimination are the following:

- Gender
- Morals
- Sexual orientation
- Gender identity
- Age
- Pregnancy
- Marital status
- Genetic characteristics
- Particular vulnerabilities resulting from economic hardship
- Nationality
- Race / ethnic origin
- Political opinion
- Trade union membership or activities
- Religious and/or philosophical beliefs
- Physical appearance
- Name
- Place of residence
- Bank domiciliation
- Medical conditions
- Disability
- Ability to express oneself in a language other than French
- Exercising the right to strike

In addition, the following persons are protected but not specifically under discrimination legislation. This protection is set out under French Law (ss. – Article L1152-2 of the French *Labour Code* ; ss. – *Sapin II Act*):

- bullying (alleged victim or witness);
- whistle-blowers.

What of these are subject to additional protections/requirements under local data protection law? How does this interact with discrimination law and where do they overlap?

Under French law (ss. – Article 6 of the French Data Protection Act), it is forbidden to process the following categories of personal data:

- Personal data revealing **racial** or **ethnic origin**;
- Personal data revealing **political opinions**;
- Personal data revealing **religious** or **philosophical beliefs**;
- Personal data revealing **trade union membership**;
- **Genetic** data;
- **Biometric** data (for the purpose of uniquely identifying a natural person);
- Data concerning **health**;
- Data concerning a person's **sex life**;
- Data concerning a person's **sexual orientation**.

Those categories above broadly overlap with the corresponding protected characteristics under discrimination (see Q.1), but don't necessarily direct correlate with these. For example, gender identity is not explicitly included in the category of sensitive data in the French Data Protection Act. However, the gender identity constitutes one of the criteria on which a discrimination can be based (ss. – Article 95 of the French *Data Protection Act*, ss. – Article 225-1 of the *French Criminal Code*).

Employers are allowed to collect personal data revealing disabilities and gender identity only under certain circumstances. For other types of personal data, it is forbidden even with the express consent given by the employee for any such processing.

The collection of information regarding disabilities is specifically regulated by the French Labour Code (ss. – Articles L5212-2 and following of the French Labour Code). It only allows the collection of information necessary for the assessment of the employees' professional abilities and skills (ss. – Article L1222-2 of the French Labour Code).

Is there a general legal requirement to carry out EDI monitoring?

No. There are no general EDI data processing or monitoring requirements in France (under either employment or data protection law).

Is there any specific EDI data that employers are legally required to process, e.g. to carry out EDI monitoring (such as gender pay gap reporting)?

Yes. Employers may however be subject to specific requirements. Key obligations are as follows:

- All employers need to actively ensure equal pay and equal treatment of female and male employees.
- Companies with more than 50 employees must publish an annual gender pay gap indicator and to initiate negotiations with their staff representatives and in-house unions annually on this topic (sanctions include fines).
- Companies with more than 1,000 employees are also required to calculate the gender proportion amongst top executives ("cadres-dirigeants") and members of governing bodies (quota with related obligations (as from 2026) and fines (as from 2029)).
- Companies also have an obligation towards disabled workers, who must represent at least 6% of the workforce (otherwise the company will be obliged to pay a financial contribution in this respect).

Can employers actively promote diversity in the workplace?

Yes.

- Companies are required to implement actions to address their obligations with respect to equality and diversity in the workplace (e.g. diversity training, updating their internal regulations etc.).
- Employers can also promote other diversity and equality topics (ethnic diversity, LGBTQ+ rights, etc.) but there is no obligation to do so.

- Positive discrimination (treating one person in a more favourable manner because of a protected characteristic) is generally prohibited under French law, unless where prescribed by law.

Does data protection law have specific provisions either permitting or prohibiting the processing of personal data for equal opportunities & diversity monitoring?

Yes.

- The French Defender of Rights and the CNIL published a methodological handbook for cases where the processing of personal data for equal opportunities & diversity monitoring would involve sensitive data (ethnicity, sexual orientation, religious or political opinion, health, trade union membership). Please note that it was published in 2012 and was not updated to account for the GDPR. Further guidance includes a guide published by The French Defender of Rights on "Taking action against discrimination in employment on grounds of sexual orientation and gender identity" in May 2017. This guide refers to the handbook co-written with the CNIL in 2012.
- Further to the *Sapin II Act* (9 December 2016) coming into force, companies who have at least 500 employees and with annual global revenues of more than €100 million are required to report via an alert system on X if they meet the legal criteria.
- The CNIL has issued a referential concerning whistleblowing on 18 July, 2019, which is applicable for this system in France.

Where employers are required to, or not prohibited from, processing EDI data:

Do we have to collect and process EDI data in anonymised form?

Although there is no general requirement to collect and process EDI data in anonymised form, some specific directions on anonymised EDI data were adopted under French law:

- The CNIL and the French Defender of Rights stated in their methodological handbook (referenced previously) that it is necessary to ensure that sufficient measures are taken to guarantee the anonymity of the data. Such anonymity may be implemented either when collecting or processing the data, and in any event, when publishing the results. Please note that special attention should be paid to indirect identification of data subjects;
- The CNIL strongly recommends outsourcing the collection of this data to ensure the confidentiality and the impartiality of the analysis. In case of the use of an external provider, an agreement including a clause of confidentiality must be included;
- Personal data used for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes are no longer considered as personal data once they have been duly anonymized (ss. – Article 116 of the French *Data Protection Act*);
- In 2007, the CNIL published a report encouraging "a much more systematic use of encryption and anonymization techniques" of personal data, including EDI data, particularly in the field of official statistics.

What are the key employment risks to consider?

There are many employment risks to consider, including the following:

- EDI data collected for monitoring purposes should never be used to make decisions about any individual employee or applicant.
- Unless the provision or collection of EDI data is mandatory by law (e.g. gender data), and unless such the data to be provided or collected must be in identifiable form, any other EDI data should only be collected on a voluntary basis and anonymised to ensure employee privacy.
- Staff communication is key to reduce the risks when collecting EDI data or implementing EDI initiatives, in order to avoid misconceptions and prevent subsequent employee claims. This is all the more important considering that certain categories of EDI data (gender identity, sexual orientation, religious beliefs etc.) are not routinely requested in France and such requests are therefore likely to be negatively perceived by

individuals. Although the French Labour Code itself does not expressly prohibit employers from gathering such data, we generally advise against it to limit risk exposure.

- The collection and process of EDI data is highly sensitive under French law from an employment and data protection perspective. Employees and employee representatives can merely refuse to answer any EDI data programmes. We recommend that employers give particular consideration to the data protection compliance requirements (see Q. 8), and the management of and communications regarding EDI data programmes in order to reduce the risk of claims and sanctions.

What are the key data protection compliance requirements under data protection law?

In their methodological handbook, the CNIL and the French Defender of Rights recommend the following compliance requirements under the GDPR and the French *Data Protection Act*:

- The CNIL recommend outsourcing data collection to an external provider and organising the collection of such consent via the provider. The CNIL also recommend conducting pre-testing to measure the degree of acceptability of the questions, which should be formulated as open-ended questions.
- This data should be collected on a voluntary basis.
- Information notice: it is highly recommended to involve the various internal stakeholders of the company, especially the employee representatives who should be informed and consulted;
- Completion of a data protection impact assessment (DPIA) and, if relevant, legitimate interests assessment, where applicable for sensitive personal data.
- Appropriate retention periods should be set regarding the personal data collected.
- Sufficient technical, confidentiality and organisational security measures should be put in place.
- Data minimization where this is possible.
- Anonymity (**see Q.6**).
- Outsourcing (**see Q.6**).
- Record of processing activities to be maintained.
- Effective exercise of GDPR rights: the CNIL strongly insists on right of access and of rectification for data subjects.

Are there any key local considerations, such as consultation with trade union or employee representative bodies?

Yes. Regarding the recruitment process, French Labour Code specifically provides for informing the works council prior to (i) modifying recruitment methods or techniques or (ii) implementing new ones (ss. – Article L. 2323-32 of the French *Labour Code*).

- The collection of data regarding disabilities is specifically regulated by the French *Labour Code* (**see Q.2**) and the staff representative bodies, if any, must be consulted before the start of the review (ss. – Article L 2312-38 of the French *Labour Code*).
- The CNIL and the French Defender of Rights recommend in their methodological handbook consulting employee representative bodies before reviewing and disclosing results for the purposes of EDI data programmes.
- EDI initiatives should be discussed during mandatory annual negotiations (**NAO**) with trade union representatives relating to remuneration, equal pay & equal treatment.
- It would be good practice to formally inform the works council before implementing any EDI initiative, as this is a sensitive matter in France. Such information should be put on the works council's agenda and can take place during an ordinary works council meeting.
- Please note that we also recommend the consultation with trade union and work councils before commencing EDI data programmes and the processing of EDI data throughout.

What are the key risks for employers in not complying with the above?

- From a data protection perspective, the processing of personal data revealing racial or ethnic origin is a criminal offence punishable by 5 years imprisonment and a €300,00 fine (ss. – Article 226-16 of the French *Criminal Code*). The implementation of an automated processing of personal data which is non-compliant with the GDPR is subject to the same penalties.
- From a criminal law perspective, discrimination is a criminal offence punishable by 3 years of imprisonment and a €45,000 fine (ss. – Article 225-2 of the French *Criminal Code)*.
- Employees can exercise their data rights and also have a right to seek compensation in the event of a breach of the GDPR.
- The CNIL has the power to impose fines of up to €20 million or 4% of global annual turnover, whichever is higher, as well as to issue enforcement notices requiring changes to processing in the event of a breach of the French *Data Protection Act*.
- From an employment point of view, potential risks include damages and fines, in addition to adverse reputation and PR issues. EDI-related claims are difficult to deal with as they often prove to be costly as well as time-consuming to manage. Discrimination and EDI related whistleblowing claims – although not very common in France – also carry an additional financial risk as damages are uncapped.

Germany

Germany

What characteristics are protected from discrimination?

- Age
- Disability
- Ethnic origin (descent, national origin, or common language, dialect, or tradition of a particular people)
- Race (external or internal appearance characteristics, such as skin colour, physiognomy or physique)
- Nationality
- Gender (biological assignment)
- Religion or belief
- Sexual identity (sexual orientation and transsexuality)
- Political opinion
- Political or trade union activity or position
- Works council membership

What of these are subject to additional protections/requirements under local data protection law? How does this interact with discrimination law and where do they overlap?

Generally, an employer may collect and process gender data only if relevant for the administration of the employment relationship (e.g. to ensure equality in the context of pay and/or promotion). There is limited case law on whether and to what extent employers may ask for gender information for diversity goals.

In the case of an existing employment relationship, the employer is authorized to ask the employee about a possible existing disability after six months have passed (even if no probationary period has been agreed). However, there is no obligation to inform the employer about a severe disability if the disability does not affect the way work is performed. In the case of a severe disability, certain protective regulations apply, for example with regard to dismissals and leave entitlement.

Is there a general legal requirement to carry out EDI monitoring?

No. There is no general requirement to carry out EDI monitoring.

Is there any specific EDI data that employers are legally required to process, e.g. to carry out EDI monitoring (such as gender pay gap reporting)?

Yes. German employers with more than 200 employees within one business establishment are required to respond to individual enquiries by employees on gender pay equality under the German *Gender Pay Transparency Act*. Private employers with more than 500 employees are obliged to take adequate measures to ensure gender pay equality and must report on their measures.

However, in Germany, a mandatory gender quota of 30 per cent has been in force since 2016 for the supervisory boards of listed stock companies and companies with parity codetermination (where there are equal numbers of employees and company board members on the supervisory board). If a company bound by the gender quota has less than 30 per cent women on its supervisory board, it must allocate vacant positions to women until the 30 per cent mark is reached. Otherwise, the seat on the supervisory board remains unoccupied (**empty chair**).

The Act on *Equal Participation of Women and Men in Leadership Positions* also obliges about 3,500 listed or co-determined companies in Germany to set targets for increasing the proportion of women on supervisory boards, executive boards and top management levels.

Employers with 20+ employees must fulfil a mandatory quota of at least 5% of severely disabled employees (disability degree 50% or more) or equivalent persons (disability degree between 30 and 50, living or employed in Germany, and who would not be able to find work if they were not considered an equivalent person). However, on an ongoing basis, employers with an annual average of under 40 employees must employ one severely disabled or equivalent person per month on an annual average and employers with an annual average of under 60 employees must employ two severely disabled or equivalent person persons on an annual average.

Can employers actively promote diversity in the workplace?

Yes. There is no direct broad requirement to actively promote diversity and equality of opportunities in the workplace under German law but employers can choose to do so. However, it is worth bearing in mind that positive discrimination (treating one person more favourably than another because they have a protected characteristic) is generally prohibited under the law, unless there is sufficient justification for such inequality. Employers will still be subject to obligations under the law to prevent discriminatory practices in the workplace.

Employers must ensure there is equal pay for women and men for equal work of equal value.

Does data protection law have specific provisions either permitting or prohibiting the processing of personal data for equal opportunities & diversity monitoring?

Yes.

Processing of personal data, and in particular special categories of personal data, is strictly regulated (please see above).

The German *Federal Data Protection Act* (**BDSG**) does not contain any specific provisions concerning the processing of personal data for equal opportunities and diversity monitoring. However, section 26 of BDSG specifically regulates data processing in the employment context in general and also regulates and specifies processing of special categories of employee personal data. Furthermore, national guidelines and case law must be considered.

Where employers are required to, or not prohibited from, processing EDI data:

Do we have to collect and process EDI data in anonymised form?

This depends on whether or not there is a legal obligation to collect EDI data. If EDI data is collected for a purpose where there is no underlying legal obligation, the collected data must be anonymized (e.g. for internal evaluation purposes).

Through the combination of evaluation characteristics, it must never be possible to identify groups of employees smaller than three to five employees. In practice, it is common to analyse the results of groups below this threshold only in the next higher evaluation level. In this context, it is very important to clarify whether the allocation of data for groups of employees is possible in principle and whether it then makes sense for these data to remain with the external provider and not be evaluated, or not be collected at all or – by technical means – be "anonymised" right in the first evaluation step, i.e. be allocated to the next higher evaluation level. This is sometimes necessary because it is theoretically possible to calculate the demographic combinations for which there are at least three employees in a group (e.g. 30- to 34-year-old men in accounting), but these minimum quantities can actually be lower due to the participation rate. If this is not possible, only the data required by law should be collected. If there is a legal basis, non-anonymised data collection is also permissible.

What are the key employment risks to consider?

Complaints

Employees who are affected by discrimination have the right to complain firstly to their superiors, and then to equal opportunity officers (*Gleichstellungsbeauftragten*) and to company complaints offices (*betriebliche Beschwerdestelle*). The content of the complaint must be examined and the outcome communicated to the complaining employee.

Withholding of work performance

Section 14 *Equal Treatment Act* (**AGG**) provides for the right of employees to withhold their work performance without losing their salary entitlement. However, it is limited to cases of harassment and sexual harassment if the employer does not take any or no suitable countermeasures, e.g. the employer does not respond to a complaint or the harassment or sexual harassment is carried out by the employer or supervisor himself. The affected employees are entitled to stop working without loss of pay to the extent necessary for their protection.

Compensation and damages for discrimination and breach of duty

Section 15 AGG provides, as the central legal consequence of a violation of the prohibition of discrimination, a claim to appropriate compensation in money for immaterial damage (compensation for pain and suffering) and damages for material damage. The claim for material damages – unlike compensation – only arises if the employer is responsible for the breach of duty (intentionally or negligently). Immaterial damages can still be claimed against the employer regardless of fault. The amount of compensation must be appropriate but, depending on the case, must also have a deterrent effect on the employer.

Right of action for works council/trade unions

In the event of gross violations of the prohibition of discrimination by the employer, the works council or a trade union represented at the site may take legal action against the employer to cease and desist, tolerate or perform an act in order to eliminate the discrimination, even without the consent of the person concerned. However, this does not mean that the works council or the trade union can assert individual claims of the disadvantaged party by way of litigation.

What are the key data protection compliance requirements under data protection law?

Data processing must be strictly limited to what is necessary for the performance of the employment relationship (i.e. in particular where there is a legal obligation). In other cases, only anonymous and voluntarily collected data may be processed. If the data is not collected anonymously but anonymised later on, the use of service providers is recommended to ensure that only aggregated data is provided to the employer.

Are there any key local considerations, such as consultation with trade union or employee representative bodies?

Gender: Works Councils have a right to inspect the full salary list upon request. The works council can even request to inspect the salary lists once every month if they have a plausible reason to do so, to check the wages for “pay equity/wage justice”. The works council's right of inspection is limited to the site (there is no right to inspect the remuneration lists of all employees in the company) and extends to the wage and salary lists of all employees at the site (only the salaries of executive employees are excluded). In order to enforce the equality of men and women, the works council can demand that the salaries be provided in a format where the data is broken down according to gender.

Disabled Employees: When the decision is made to fill a position, i.e. before it is advertised, the obligation exists to check whether the position can be filled with a severely disabled person. The representative body for severely disabled persons must be involved in the examination and the works council must be consulted, provided that such bodies exist in the company. As soon as applications from severely disabled persons are received, the employer must inform the representative body for severely disabled persons and the works council immediately upon receipt of the application, without making its own preliminary selection. The representative body for severely disabled persons and the works council must also be involved and heard when the application is examined. The intended employer decision must be communicated to them. Important: the employer is only obliged to forward the application documents and placement proposals if the employee has disclosed his or her severe disability during the application process and not in the case of unsolicited applications.

What are the key risks for employers in not complying with the above?

Discrimination

There is a risk that employees have the right to refuse to perform their work duties, and also to bring discrimination claims seeking compensation (see Q.7 above). There is also a risk of legal action taken by trade unions or works councils (see Q.7 above).

Data privacy

The GDPR provides for the most severe penalties in respect to data protection violations in Germany (in a worst-case scenario, fines of up to EUR 20 million, or 4% of the worldwide annual revenue from the preceding financial year, whichever amount is higher). In addition, a candidate under German law may be able to claim compensation for “material” and/or “immaterial” harm.

Management positions

Companies must justify why they set a target of no women on the board. Companies that do not set a target or do not provide a reason for the zero target will be sanctioned.

Quotas

Businesses that fail to meet the quotas must pay an annual compensatory payment for each mandatory job for a disabled person which was not staffed accordingly. This is EUR 125 if the quota of disabled employees is between 3-5%, and EUR 220 per month if between 2-3% and EUR 320 per month if 2% or less. The amounts are calculated for each month according to the number of unfilled compulsory places.

However, in businesses with an average of less than 40 employees, EUR 125 must be paid if there is less than one disabled employee on average (over the year). In businesses with an average of less than 60 employees, EUR 125 (EUR 220) must be paid, if there is less than two (one) disabled employee on average. This obligation arises by operation of law if the employer does not fulfil its obligation to employ severely disabled persons or does not do so to the extent required.

Hong Kong

Hong Kong

What characteristics are protected from discrimination?

- Sex (including marital status, pregnancy and breastfeeding)
- Disability
- Race (includes race, colour, descent, national or ethnic origin)
- Family status

What of these are subject to additional protections/requirements under local data protection law?

How does this interact with discrimination law and where do they overlap?

There is no concept of "special categories of data" or "sensitive personal data" under the Personal Data (Privacy) Ordinance (Cap. 486) (**PDPO**).

However, the Privacy Commissioner for Personal Data (**PCPD**) has published and issued codes of practice and guidance notes to provide guidance on the processing of certain categories of personal data, e.g. identity card numbers, personal identifiers and biometric data.

Is there a general legal requirement to carry out EDI monitoring? Is there any specific EDI data that employers are legally required to process, e.g. to carry out EDI monitoring (such as gender pay gap reporting)?

No. There are no general or specific EDI data processing or monitoring requirements in Hong Kong (under either employment or data protection law).

Can employers actively promote diversity in the workplace?

Yes.

There is no direct broad requirement to actively promote diversity and equality of opportunities in the workplace under Hong Kong law (see above), but employers can choose to do so. Positive discrimination (treating one person more favourably than another because they have a protected characteristic) is generally prohibited under the law unless an exemption (e.g. a genuine occupational qualification) applies. The term 'discrimination' covers both direct and indirect forms of discrimination. Employers will still be subject to obligations under the law to prevent discriminatory practices in the workplace.

Does data protection law have specific provisions either permitting or prohibiting the processing of personal data for equal opportunities & diversity monitoring?

No, the PDPO does not have specific provisions concerning the processing of personal data for equal opportunities & diversity monitoring.

The processing of such data remains subject to the general data protection principles under the PDPO (see Q.8 below).

Where employers are required to, or not prohibited from, processing EDI data:

Do we have to collect and process EDI data in anonymised form?

No.

The PCPD published a guidance note titled Guidance on Personal Data Erasure and Anonymisation (revised in April 2014), which provides that anonymised data (to the extent that the individuals concerned will not be directly or indirectly identifiable), will not be considered 'personal data' under the PDPO. Anonymous collection is therefore an option for handling personal data that is no longer required for the purposes for which it was collected (other than complete erasure).

What are the key employment risks to consider?

The collection and use of EDI data, particularly in a form where staff are identifiable, is potentially sensitive from an employment and data protection perspective. Employers should give particular consideration to the data protection compliance requirements (see Q.8 below), and the management of and communications regarding EDI data programmes in order to reduce the risk of claims and sanctions, including the following:

- The collection of EDI data should ideally be voluntary. It may be difficult for an employer to justify or enforce a mandatory requirement unless extenuating circumstances apply.
- Employers should consider carefully what data they want to collect, why, and how they want to use that data. The data collected should clearly correlate to an identified business need and a specific purpose.
- Employers should provide staff with a clear explanation of what data they will collect, why, and how it will be used, in accordance with the PDPO and to limit the risk of employee complaints, grievances and claims.
- Staff communication is important for managing employee perceptions, thereby reducing the risk of claims. Employers should ensure that they carefully consider and prepare employee communications about any EDI data programmes, and try to anticipate any resistance, concerns or potential risks.

What are the key data protection compliance requirements under data protection law?

If an individual can be directly or indirectly identified from the information concerning his/her protected characteristic, such information constitutes "personal data" and the collection, processing and usage of such information will be subject to the PDPO.

The Data Protection Principles (**DPPs**) of the PDPO states that:

An employer may collect personal data from a job applicant provided that the collection of the data is necessary for a lawful purpose directly related to a function or activity of the data user (e.g. recruitment purposes and not for excluding a certain gender for a job position) and that the data is not excessive in relation to the purpose.

On or before collecting personal data, an employer must take all practicable steps to ensure the applicant is informed of: the types of personal data to be collected, the purposes for which the data are to be used, whether the supply of the data is voluntary or obligatory (and if obligatory, the consequences for failing to supply the data), the classes of persons to whom the data may be transferred, the individuals' rights of access and correction of their personal data and the contact details of the individual responsible for handling data access and correction requests (e.g. data protection officer).

If the EDI information originally collected is used for purposes other than or which are not directly related to those specified to the applicant, the employer will need to obtain prescribed consent (i.e. express consent which has not been withdrawn) from him/her before the information can be used for the "new" purposes.

Are there any key local considerations, such as consultation with trade union or employee representative bodies?

There is no general requirement for employers to consult with trade union or other employee representative bodies in Hong Kong. Employers will need to check any specific agreements with such trade unions or bodies to confirm whether any such requirements apply.

What are the key risks for employers in not complying with the above?

- Equality, diversity and inclusivity within a workplace is becoming a focus for many businesses in Hong Kong, particularly with regard to race, ethnicity and nationality.
- Misuse or perceived misuse of staff EDI data in the context of staff management and decision-making runs a clear risk of discrimination claims. EDI-related claims tend to be high-profile and sensitive, and in practice are often costly and time-consuming to manage. Discrimination claims are also dealt with separately from employment claims and are subject to its own set of compensation awards (like injury to feelings).
- Breaches of the PDPO may lead to a variety of civil and criminal sanctions including fines and imprisonment.
- The Privacy Commissioner has powers under the PDPO to initiate an investigation on its own or when it receives a complaint about an act that relates to the personal data of which the individual is the data subject and that may be a contravention of a requirement under the PDPO. Following an investigation, the Privacy Commissioner may issue warning letters, request an undertaking from the data user and/or issue enforcement notices against the parties being complained against if a contravention of the PDPO is found.
- If a data user breaches an enforcement notice issued by the Privacy Commissioner, it will be liable to a fine of HK$50,000 (on first conviction) or HK$100,000 (on a subsequent conviction) and imprisonment for 2 years. In addition, data subjects have a right to bring proceedings in court to seek compensation for damage, including damages for injury to feelings.
- Apart from issuing an enforcement notice, the Privacy Commissioner may also publish publicly available reports in respect of its investigation or inspection where the identity of the employer is disclosed. This will inevitably result in serious reputational damage to the employer.

Hungary

Hungary

What characteristics are protected from discrimination?

- Sex
- Race
- Colour
- Nationality
- Membership of a national minority
- Language
- Disability
- State of health
- Religion or belief
- Political or other opinion
- Family status
- Motherhood (pregnancy) or fatherhood
- Sexual orientation
- Gender identity
- Age
- Social origin
- Property
- Part-time or fixed-term nature of the employment relationship or other employment-related relationship
- Membership in a representative organization
- Any other status, characteristic or attribute that is suitable for protection against discrimination

What of these are subject to additional protections/requirements under local data protection law? How does this interact with discrimination law and where do they overlap?

Special categories of personal data are subject to additional protections and requirements in Hungary. The GDPR defines “special categories of data” as:

- personal data revealing **racial** or **ethnic origin**;
- personal data revealing **political opinions**;
- personal data revealing **religious** or **philosophical beliefs**;
- personal data revealing **trade union membership**;
- **genetic** data;
- **biometric** data (where used for identification purposes);
- data concerning **health**;
- data concerning a person’s **sex life**; and
- data concerning a person’s **sexual orientation**.

These categories overlap with the corresponding protected characteristic under discrimination law but the application of both discrimination protection and data protection requirements should be considered on a case-by-case basis.

Is there a general legal requirement to carry out EDI monitoring?

No. There is no general requirement to carry out equal opportunities & diversity monitoring. Employers must act in line with regulations and legislation prohibiting any kind of discrimination at all times.

Is there any specific EDI data that employers are legally required to process, e.g., to carry out EDI monitoring (such as gender pay gap reporting)?

No. There is no specific EDI data that employers are legally required to process.

Can employers actively promote diversity in the workplace?

Yes, but specific conditions apply.

Employers must ensure the principle of equal pay for equal work applies in the context of equal treatment. Employers can pursue preferential policies for disadvantaged groups, as long as the policies meet certain requirements established under the law.

Certain employers in Hungary may be subject to additional rules, particularly around equal pay, or diverse representation in the workplace, depending on the number of employees or the sector in which they are active. For example, if employers with 25 or more positions do not employ individuals with severe disabilities in at least 5 percent of those positions, they will have to pay a rehabilitation allowance. Furthermore, the remuneration policies of financial institutions must be gender-neutral and in certain cases investment firms are required to implement a strategy on gender representation in management positions.

In the case of communication to employees under the age of 18, raising awareness and providing information about LGBTQ+ topics is restricted. Under the *Family Protection Act*, "*in order to protect children, it is prohibited to make pornographic content available to children under the age of eighteen, as well as content that […] promotes or displays gender non-conformity, gender reassignment or homosexuality*."

Does data protection law have specific provisions either permitting or prohibiting the processing of personal data for equal opportunities & diversity monitoring?

Yes. Processing of personal data, and in particular special categories of personal data, is strictly regulated (please see above).

Beyond this, the processing of personal data for equal opportunities & diversity monitoring is not specifically regulated in Hungarian data protection laws.

Complying with GDPR when processing such data i.e., identifying the proper legal basis under Article 6 GDPR and the appropriate justification under Article 9 GDPR for special categories of personal data (e.g. sexual orientation) can be complicated, as consent is generally not an appropriate legal basis in the employment context.

Where employers are required to, or not prohibited from, processing EDI data:

Do we have to collect and process EDI data in anonymised form?

No. Although anonymous collection is the safest way to collect and otherwise process EDI data, and potentially reduces employment and data protection risks, EDI data can usually be collected and otherwise processed in a form where employees are identified, or identifiable provided steps are taken to comply with data protection and employment law. Failure to take appropriate steps to ensure compliance will increase the risks associated with complaints, claims and sanctions under employment and data protection law.

What are the key employment risks to consider?

The collection and use of EDI data, particularly in a form where staff are identifiable, is potentially high risk from an employment and data protection perspective. Employers should give particular consideration to data protection compliance requirements (see Q.8 below), and the management of and communications regarding EDI data programmes in order to reduce the risk of claims and sanctions.

Employers should consider carefully what data they want to collect, on which legal basis, why, and how they want to use that data. The data collected should clearly correlate to an identified business need and a specific purpose.

Employers should provide staff with a clear explanation of what data they will collect, why, and how it will be used, in accordance with the GDPR and to limit the risk of employee complaints, grievances and claims.

Staff communication is important for managing employee perceptions, thereby reducing the risk of claims and sanctions. Employers should ensure that they carefully consider and prepare employee communications about any EDI data programmes, and try to anticipate any resistance, concerns or potential risks.

What are the key data protection compliance requirements under data protection law?

The collection of EDI data in identifiable form will result in the processing of personal data. As set out above, certain types of EDI data are also "special category" data (see Q.2 above).

When processing any personal data, the employer must comply with the requirements set out in the GDPR. Broadly, this means employers should:

- identify and communicate a clear and legitimate purpose and legal basis for processing EDI data – in case of special category data, there must also be a condition for processing under Article 9 GDPR;
- only process the minimum amount of data required;
- take steps to ensure the continuing accuracy and integrity of the data;
- implement appropriate security, access and confidentiality measures, and not retain that data for longer than required for the purpose for which it was originally collected;
- satisfy additional compliance requirements, e.g., the completion of a data protection impact assessment.

Are there any key local considerations, such as consultation with trade union or employee representative bodies?

In Hungary, most large multinational companies have equal opportunities policies or communicate with employees in a positive way to support diversity & inclusion. However, promoting diversity & inclusion is typically not so evident for small and medium size companies or larger Hungary-based companies.

The employer shall consult with the works council 15 days prior to implementing any new data processing activities (including one for EDI monitoring). However, such consultation does not mean that the employer is bound by any suggestions from the works council.

What are the key risks for employers in not complying with the above?

Misuse or perceived misuse of staff EDI data in the context of staff management and decision-making runs a clear risk of discrimination claims as well as other related claims (e.g., unlawful termination and whistleblowing). Discrimination, unlawful termination, and whistleblowing claims are also subject to damages and grievance awards, therefore carrying an additional financial risk.

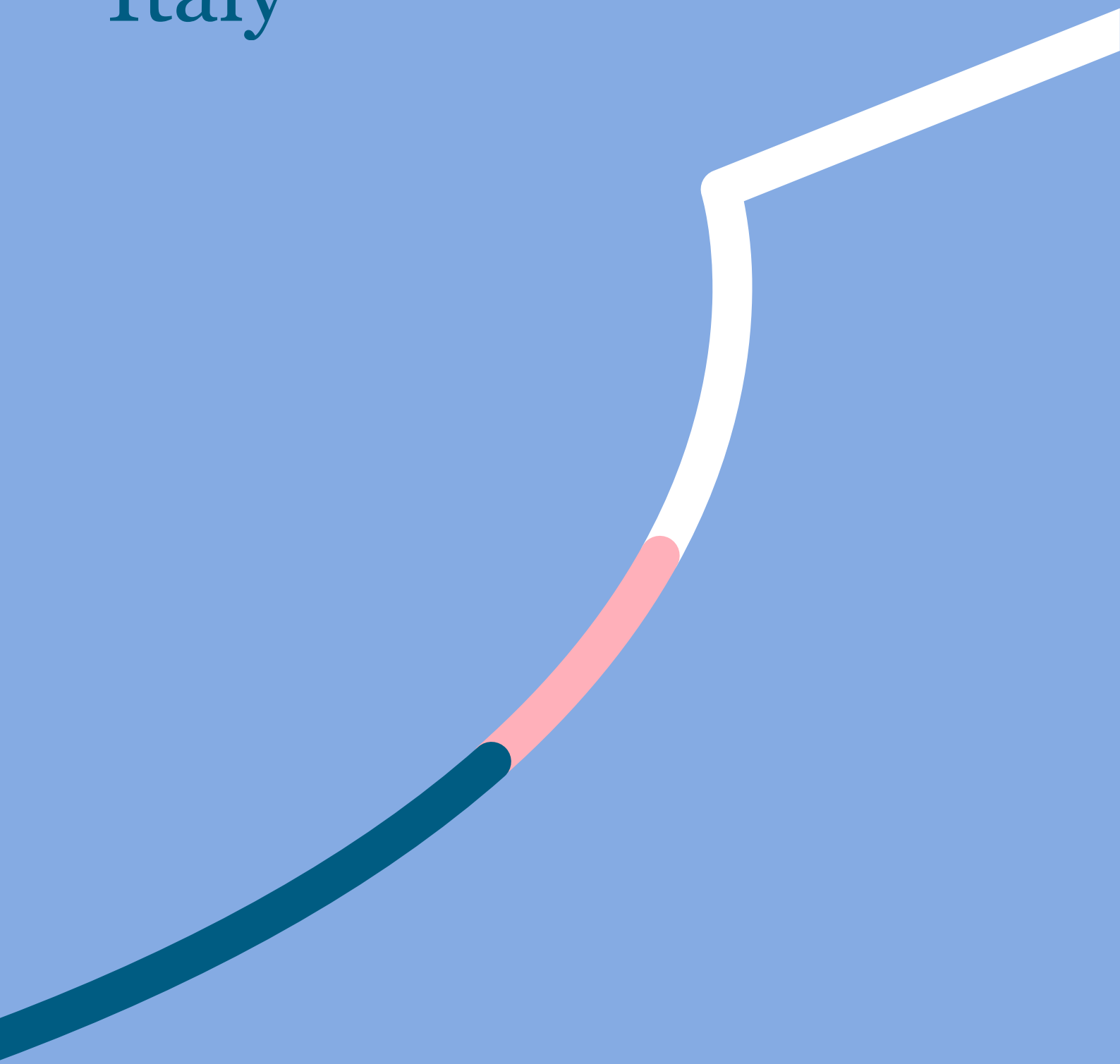
The Hungarian data protection authority has the power to impose fines of up to EUR 20 million or 4% of global annual turnover (whichever is greater), as well as to issue enforcement notices requiring changes to processing in the event of a breach of the GDPR or publish the employer's identity in its decision (potential reputation risks). The employees may also claim damages before courts in the case of breach of data protection rules.

Equality, diversity, and inclusivity remain hot topics in Hungary's employment sphere. Associated complaints, allegations and breaches often attract the attention of the press, social media, and employees themselves,

and can result in damage to an employer's reputation and brand, with other knock-on effects (e.g., difficulties with recruitment or retention of employees).

The sanctions for breaching the prohibition to display and promote gender non-conformity, gender reassignment or homosexuality to persons under the age of 18 are currently unclear. Implementing acts are expected from the Hungarian Government in this regard.

Italy



Italy

What characteristics are protected from discrimination?

- Gender
- Marital status
- Race (includes nationality, ethnicity, national origins and colour)
- Language
- Physical or mental disability
- Religion or belief
- Sexual orientation
- Age
- Trade union membership or opinion
- Politic opinion or activity
- Gender reassignment
- Pregnancy
- Maternity leave
- Physical characteristics
- Personal and social conditions

What of these are subject to additional protections/requirements under local data protection law? How does this interact with discrimination law and where do they overlap?

The processing of personal data is strictly regulated under Regulation (EU) 2016/679 (**GDPR**), applicable in Italy. Special categories of personal data are subject to additional protections and requirements. The GDPR defines "special categories of data" as:

- personal data revealing **racial** or **ethnic origin**;
- personal data revealing **political opinions**;
- personal data revealing **religious** or **philosophical beliefs**;
- personal data revealing **trade union membership**;
- **genetic** data;
- **biometric** data (where used for identification purposes);
- data concerning **health**;
- data concerning a person's **sex life**; and
- data concerning a person's **sexual orientation**.

Those categories in italics above broadly overlap with the corresponding protected characteristic under discrimination law (so information about gender, race, physical or mental disability, religion or belief, sexual orientation, trade union membership, politic opinion or activity, gender reassignment, pregnancy and ideology are or are likely to be considered as special categories of personal data under the GDPR) but the application of both discrimination protection and data protection requirements should be considered on a case-by-case basis.

There are no specific provisions in Italian data protection law affecting EDI data processing, other than the requirements for processing personal and special categories of personal data, as referred to above. However, there are binding safeguards for processing special categories of data in the employment context, i.e., health, political, philosophic, and religious beliefs, trade union membership, ethnicity, and race, etc. These types of data can be collected and processed in the context of the recruitment process, and to a more limited extent, of the employment relationship when this is necessary to comply with applicable laws, including equal opportunity laws (Register of provisions *no. 146/2019*, hereinafter, the "**Provision**").

In addition, s.8 of the Statute of Workers prohibits any investigation on facts that are not important for the evaluation of professional aptitude. The application of this provision implies that special categories information can be processed by the employer only if it is important for the evaluation of professional aptitude or required to comply with a legal obligation.

Is there a general legal requirement to carry out EDI monitoring?

No. There are no general EDI data processing or monitoring requirements (under either employment or data protection law).

Is there any specific EDI data that employers are legally required to process, e.g. to carry out EDI monitoring (such as gender pay gap reporting)?

No. There are no specific EDI monitoring requirements under Italian law.

That said, employers are permitted and/or required to process certain EDI data in order to comply with underlying legal requirements or where that EDI data is collected or otherwise processed to evaluate the professional aptitude of the employee, albeit only for the purposes of compliance with a specific legal provision – employers are not permitted to ask for information to which they are not otherwise entitled (this would be deemed a prohibited investigation).

Accordingly, employers are legally permitted/required to process the following categories of EDI data in relation to the specific rights of obligations referred to below:

- **Disability**: Employers are required to hire a minimum number of disabled persons (*sec. 9 of law no. 68/1999*) depending on the number of total employees. Note that this legal obligation does not allow the employer to ask all employees if they have any disability, but only to process data on disability of the person hired in compliance with the legal obligation.
- **Pregnancy**: Several workplace protections relate to the pregnancy status or the status of mother (it is prohibited for a mother to work from 2 months before the birth of a child, and 3 months after it; it is prohibited to dismiss a mother until the child is at least 1 year old);
- **Orphans or spouses of persons killed at work, victims of terrorism or of organized crime**: Employers are required to reserve a hiring quota for employees in these categories.
- **Trade union activity**: Union members and leaders are entitled to a certain number of paid and unpaid days off to perform union activities.
- **Specific health status/sickness**: Employers must grant specific annual leave to employees diagnosed as having with tuberculosis, cancer, HIV or who are drug addicts who participate in rehabilitation programs.
- **Religion**: Employees are entitled to take off certain religious holidays, and the employer may have access to information concerning religious beliefs in order to comply with its duties.
- **Nationality/citizenship**: Certain information may be required in connection with Italian immigration law.

Can employers actively promote diversity in the workplace?

Yes, but with tight restrictions.

Italian law protects diversity through a general prohibition on discrimination and through assigning specific rights to certain categories of subjects under law (e.g., disabled, and pregnant individuals – see below for

more detail). Promotion of diversity is lawful if it is not discriminatory for certain categories of individuals. On the other hand, the employer cannot access information not required by law or not deemed important or relevant to evaluate the professional aptitude of the employee.

Whilst Italian law protects diversity, there is no general legal obligation for an employer to promote diversity. Promotion of diversity is lawful if it is not discriminatory for certain categories of employees. Employers can promote diversity only when it is required by the law, i.e., the employer is required to hire several disabled persons which may vary depending on the total number total of employees. In principle, the employer is prohibited from collecting information that is not relevant for evaluation of professional skills (i.e., sexual orientation, religion, political opinion, etc.), and so it would not be permitted to collect information regarding a candidate's race, gender etc. when assessing their suitability for a role.

Does data protection law have specific provisions either permitting or prohibiting the processing of personal data for equal opportunities & diversity monitoring?

Yes.

Processing of personal data, and in particular special categories of personal data, is strictly regulated (please see above).

To the extent that the processing of data on diversity is relevant under employment law, this is permitted according to the revised *Legislative Decree no. 196/2003*.

Where employers are required to, or not prohibited from, processing EDI data:

Do we have to collect and process EDI data in anonymised form?

No. Employers are not legally required to only collect and otherwise process EDI data in anonymised form.

That said, given the strict limitations referred to above, we generally recommend that the collection of EDI data of employees is made voluntarily, anonymously, and in a manner such that the employer would be able to demonstrate that it has no access to data that would allow it to link EDI data to a particular employee. Such collection could therefore be done through an anonymous survey or questionnaire.

Data collected to comply with legal obligation cannot be processed as anonymised data.

What are the key employment risks to consider?

The risk is that the employee can argue that the collection of EDI data is evidence of discrimination or that they consider this to be an infringement of the prohibition for the employer to investigate on facts not important for the evaluation of professional aptitude.

In case of discrimination, employees can ask that the discriminatory act is declared void (i.e. in case of dismissal this implies the right of the employee to be reinstated). Employees can also claim compensation for damages suffered due to the discrimination.

In cases of access to “prohibited” information, the employer may be subject to criminal sanctions.

What are the key data protection compliance requirements under data protection law?

There are no explicit compliance requirements under Italian data protection law on the processing of EDI data. That said, employers should note the contents of the Provision (See above) with regard to the processing special categories data in the employment context. It expressly authorises the use of certain special categories of data (e.g., health, political, philosophical and religious beliefs, trade union membership, ethnicity and race, etc.) as part of the recruitment process and, to a more limited extent, the employment relationship when this is necessary to comply with applicable laws, including equal opportunities laws. Breaches of the requirements set out in this Provision are subject to the administrative fine provided for in Art. 83(5) of the GDPR.

Broadly, when processing any personal data, the employer must comply with the requirements set out in the GDPR and in the Legislative Decree 196/2003 and in accordance with the provisions of employment law. Employers, therefore, should:

- identify and communicate a clear purpose and legal basis for processing EDI data, where it is required by the law and only for the purposes of comply with a specific legal provision; where this involves special category data, the legal grounds are, a) an employment law obligation (however, please note that this is restricted to employer's obligations under law, such for disability and pregnancy-related information) under Art. 6(1)(c) of the GDPR, b) processing of data necessary for employment law purposes under Art. 9(2)(b) of the GDPR;
- only process the minimum amount of data required;
- take steps to ensure the continuing accuracy and integrity of the data;
- implement appropriate security, access and confidentiality measures, and not retain that data for longer than required for the purpose for which it was originally collected;
- completion of a data protection impact assessment (**DPIA**), if necessary (i.e., equal opportunities and diversity monitoring would likely require a DPIA on the basis that employers will process special category data about their employees);
- providing an appropriate notice to employees.

Are there any key local considerations, such as consultation with trade union or employee representative bodies?

There is no general requirement for employers to consult with trade union or other employee representative bodies.

What are the key risks for employers in not complying with the above?

Misuse or perceived misuse of staff EDI data in the context of staff management and decision-making runs a clear risk of discrimination claims as well as other related employment claims (see above).

Non-compliance with applicable data protection rules could lead to sanctions up to EUR 20,000,000 or 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

The infringement of the prohibition to investigation on facts not relevant for the evaluation of the professional aptitude is punished with a fine between € 154 and € 1,549 and/or imprisonment for between 15 days and 1 year (the fine can by multiplied by five by the judge in consideration of the economic conditions of the employer).

Netherlands

Netherlands

What characteristics are protected from discrimination?

- Sex (which includes discrimination on the basis of gender characteristics, gender identity and gender expression as well as pregnancy, childbirth and motherhood)
- Race
- Age
- Disability and chronic illness
- Marital or civil status
- Sexual orientation
- Religion or beliefs
- Political orientation
- Nationality
- Type of contract (i.e. fixed term or permanent)
- Working hours (i.e. full time or part-time)

What of these are subject to additional protections/requirements under local data protection law? How does this interact with discrimination law and where do they overlap?

Special categories of personal data are subject to additional protections and requirements in the Netherlands. The Dutch Implementation Act GDPR (*Uitvoeringswet Algemene verordening gegevensbescherming*, **UAVG**) defines "special categories of data" as:

- personal data revealing **racial** or **ethnic origin**;
- personal data revealing **political opinions**;
- personal data revealing **religious** or **philosophical beliefs**;
- personal data revealing **trade union membership**;
- **genetic** data;
- **biometric** data (where used for identification purposes);
- data concerning **health**;
- data concerning a person's **sex life**; and
- data concerning a person's **sexual orientation**.

Those categories in italics above broadly overlap with the corresponding protected characteristic under discrimination law but the application of both discrimination protection and data protection requirements should be considered on a case-by-case basis.

Is there a general legal requirement to carry out EDI monitoring?

No. There is no general requirement to carry out equal opportunities & diversity monitoring. Employers must act in line with regulations and legislation prohibiting of any kind of discrimination at all times.

Is there any specific EDI data that employers are legally required to process, e.g. to carry out EDI monitoring (such as gender pay gap reporting)?

Yes. The company may be subject to special legal requirements that necessitate the processing of EDI data (for example: Act Modernisation of the law on public limited companies which requires a more balanced male/female ratio in (supervisory) boards for companies that meet certain requirements).

Can employers actively promote diversity in the workplace?

Yes. However, the preferential treatment of one category must not result in discrimination against another category, unless the preferential treatment is required to comply with a specific statutory obligation.

Does data protection law have specific provisions either permitting or prohibiting the processing of personal data for equal opportunities & diversity monitoring?

Yes.

The processing of special category data is generally prohibited under the GDPR and UAVG. A limited number of derogations to this prohibition exist, most notably and relevant for this case if the data subject has given explicit consent. Please note that in employer-employee relationships valid consent is notoriously hard to obtain. This difficulty is understood to extend to applicants to a large extent. Therefore, employees will – as a rule – only be able to rely on explicit consent if appropriate and suitable safeguards are put in place (see Q.6 below).

Alternatively, the UAVG contains a narrow exemption from the general prohibition on processing data revealing racial or ethnic origin. The exemption permits processing for diversity purposes under certain circumstances but is also subject to a number of restrictions.

Where employers are required to, or not prohibited from, processing EDI data:

Do we have to collect and process EDI data in anonymised form?

No, this is not a hard requirement.

However, collection and processing of EDI data in anonymised form (potentially) is a safeguard that reduces employment and data protection risks and would make it more likely that an employer will be able to rely on the explicit consent of the employee.

EDI data may be collected and otherwise processed in a form where staff are identified or identifiable if other suitable and appropriate safeguards are put in place to comply with data protection law. Failure to put in place these safeguards will increase the risks associated with complaints, claims and sanctions under employment and data protection law.

What are the key employment risks to consider?

Apart from the requirement to comply with GPDR (in order to minimise any related employment risks in using any such data), the employer should avoid unjustified discrimination/unequal treatment (see below).

What are the key data protection compliance requirements under data protection law?

The collection of EDI data in identifiable form will result in the processing of personal data. As set out above, certain types of EDI data are also “special category” data (see Q.2 above).

When processing any personal data, the employer must comply with the requirements set out in the GDPR and the UAVG. Broadly, this means employers should:

- identify and communicate a clear and legitimate purpose and legal basis for processing EDI data – where this involves special category data a derogation to the prohibition of processing of special category data must also be identified and communicated (see Q.5 above);

- only process the minimum amount of data required;
- take steps to ensure the continuing accuracy and integrity of the data;
- implement appropriate security, access and confidentiality measures, and not retain that data for longer than required for the purpose for which it was originally collected.

Are there any key local considerations, such as consultation with trade union or employee representative bodies?

Trade unions

No consultation with trade unions required, unless prescribed in a specific and applicable *Collective Bargaining Agreement*.

Change to DP or Hiring Policy

The relevant provisions of the Dutch Works Councils Act prescribe that the company requires the consent of the Works Council (WC) for the introduction, abolition and/or change of:

- a DP policy, to the extent it relates to the processing of personal data of personnel engaged in the business; and/or
- a hiring policy.

If there is solely a Baby-Works Council (**Baby-WC**), WC with lesser prerogatives, or no WC/Baby-WC – no worker representatives' consultation is required.

No change

If there will be no change to the DP or Hiring Policy, but merely a change to the application (toepassing) of the (unchanged) DP or Hiring Policy in the day-to-day affairs of the company, there will not be a need for the WC's consent.

Compliance

If the contemplated change to the DP or Hiring Policy is required in order to (merely) comply with statutory law, there will not be a need for the WC's consent.

What are the key risks for employers in not complying with the above?

GDPR and Equal Treatment

If the company does not comply with the requirement of the GDPR or the Equal Treatment Act, enforcement action can be taken. This is done either by the Dutch Personal Data Authority (**AP**) or by the Equal Treatment Commission (**CGB**).

Employee consultation

If the company implements the (change to) policy or revokes the policy, without the WC's (or the court's substitute) consent, the WC may petition to the court for nullification (injunction) and an order to remedy.

Statute of limitation to petition to the courts: one month, calculated from the moment the entrepreneur informed the WC of its decision to implement or – if absent such notification – the moment whereon the WC demonstrably became aware of the actual implementation of the policy (change).

Poland

Poland

What characteristics are protected from discrimination?

Many EDI data categories are protected characteristics from an employment law perspective, which are subject to specific protections under Polish equal treatment law. Although the list of protected characteristics is open (i.e. not exhaustively defined), the following in particular should fall within the scope of employer interest:

- age;
- disability and chronic illness;
- gender reassignment;
- marital or civil status;
- pregnancy/maternity;
- race (includes nationality, ethnicity, national origins and colour);
- religion/philosophical beliefs;
- sex (including gender identity);
- sexual orientation;
- political beliefs;
- trade union membership;
- type of contract (i.e., fixed term or permanent);
- working hours (i.e., full-time or part-time).

What of these are subject to additional protections/requirements under local data protection law? How does this interact with discrimination law and where do they overlap?

Special categories of personal data are subject to additional protections and requirements under the GDPR and Polish Labour Code. The GDPR defines “special categories of data” as:

- personal data revealing **racial** or **ethnic origin**;
- personal data revealing **political opinions**;
- personal data revealing **religious** or **philosophical beliefs**;
- personal data revealing **trade union membership**;
- **genetic** data;
- **biometric** data (where used for identification purposes);
- data concerning **health**;
- data concerning a person’s **sex life**; and
- data concerning a person’s **sexual orientation**.

The categories in italics broadly overlap with the corresponding protected characteristic under equal treatment law, but the application of both discrimination protection and data protection requirements should be considered on a case-by-case basis.

Care should be taken where the special category data requirements overlap with other protected characteristics (e.g., sex life data may include health or sexual orientation data).

Is there a general legal requirement to carry out EDI monitoring?

No. There are no general EDI data processing or monitoring requirements in Poland (under either employment or data protection law).

The Polish Labour Code provides for the list of data that can be requested from candidates or employees. The list does not cover EDI data, except for sex (defined as male or female) and date of birth.

Is there any specific EDI data that employers are legally required to process, e.g. to carry out EDI monitoring (such as gender pay gap reporting)?

No. There are no statutory requirements (and no planned legislative changes) that would oblige employers to collect specific EDI data.

Can employers actively promote diversity in the workplace?

Yes.

There is no direct broad requirement to actively promote diversity and equality of opportunities in the workplace under Polish law (see above) but employers can choose to do so and must ensure a discrimination free workplace.

Positive discrimination (treating one person more favourably than another because their protected characteristic) is also prohibited under Polish law unless an occupational requirement applies (e.g. ensuring equal chances to personal development in a workplace for persons with disabilities). Employers will still be subject to obligations under the law to prevent discriminatory practices in the workplace.

Does data protection law have specific provisions either permitting or prohibiting the processing of personal data for equal opportunities & diversity monitoring?

Yes.

When no special category data is processed (e.g., sex: male or female), a legitimate interest under Article 6 (1)(f) GDPR can be used as the legal basis for processing data for certain purposes.

Under the GDPR, processing special category data is generally prohibited unless a condition under Art.9 GDPR applies. In most cases, the only legal basis to rely on is candidates'/employees' explicit consent under Article 9 (2) (a) of the GDPR and Article 22 [1b] of the Polish Labour Code.

Explicit consent may allow the processing of special category data, but only if:

1 the employer can demonstrate that it is truly voluntary and the lack of consent or its withdrawal does not result in unfavourable treatment of the candidate or employee and does not cause any adverse consequences for them (for examples, see the section above), and

2 such consent is provided at the initiative of the candidate or employee.

In accordance with the Polish DPA's guidelines, obtaining valid employee consent may be challenged in an employee-employer relationship context due to the imbalance of power between the employer and the employee.

Where employers are required to, or not prohibited from, processing EDI data:

Do we have to collect and process EDI data in anonymised form?

No.

Anonymous collection is the safest way to collect and otherwise process EDI data, and potentially reduces employment and data protection risks. This would involve, for example, implementing anonymous surveys, ensuring that candidates/employees are not identifiable either directly or indirectly from the data collected. Truly anonymising data in practice can be challenging. For example, if a person disclosed in a survey that she is a female and a member of a particular team, then that individual would be identifiable if only one female was in the team. Therefore, a risk of linking data to specific individuals is more prominent in a small group.

However, EDI data can usually be collected and otherwise processed in a form where staff are identified or identifiable provided steps are taken to comply with data protection law. Failure to take appropriate steps to ensure compliance will increase the risks associated with complaints, claims and sanctions under employment and data protection law.

What are the key employment risks to consider?

The collection and use of EDI data, particularly in a form where staff are identifiable, is potentially sensitive and high risk from an employment and data protection perspective. Employers should give particular consideration to the data protection and labour law compliance requirements (see Q.8 below), and the management of and communications regarding EDI data programmes in order to reduce the risk of claims and sanctions, including the following.

- The collection of EDI data should be voluntary. It is unlikely that an employer would be able to justify or enforce a mandatory requirement unless extenuating circumstances apply. Employee refusal to share EDI data may not lead to any sanctions or termination of employment (direct discrimination).
- Employers should consider carefully what data they want to collect, why, and how they want to use that data. The data collected should clearly correlate to an identified business need and a specific purpose.
- Employers should provide staff with a clear explanation of what data they will collect, why they will collect it, and how it will be used, in accordance with the GDPR and to limit the risk of employee complaints, grievances and claims.
- Staff communication is important for managing employee perceptions, thereby reducing the risk of claims and sanctions. Employers should ensure that they carefully consider and prepare employee communications about any EDI data programmes, and try to anticipate any resistance, concerns or potential risks.

What are the key data protection compliance requirements under data protection law?

The collection of EDI data in identifiable form will result in the processing of personal data. As set out above, certain types of EDI data are also “special category” data (see Q.2 above).

When processing any personal data, the employer must comply with the requirements set out in the GDPR and the Polish Labour Code. Broadly, this means employers should:

- identify and communicate a clear and legitimate purpose and legal basis for processing EDI data – where this involves special category data, there must also be a condition for processing under Article 9 GDPR (see Q.5 above);
- only process the minimum amount of data required;
- take steps to ensure the continuing accuracy and integrity of the data,
- implement appropriate security, access and confidentiality measures, and not retain that data for longer than required for the purpose for which it was originally collected,
- ensure that only persons authorized in writing (which includes electronic form) to process special category data and prior obliged to keep them secret should be allowed to process such data.

Additional compliance requirements under the GDPR also include:

- completion of a data protection impact assessment (**DPIA**) and, if relevant, a legitimate interests assessment;
- providing an appropriate notice to employees, and obtaining consent if required; and
- updating the employer’s record of processing.

Are there any key local considerations, such as consultation with trade union or employee representative bodies?

There is no general requirement for employers to consult with trade unions or other employee representative bodies in Poland. Employers will need to check any specific agreements with such trade unions or bodies to confirm whether any such requirements apply or whether the EDI policies will be inserted in other documents that require such consultation (e.g., Workplace Regulations).

Although some organizations, especially those with foreign headquarters, decide to implement such initiatives, it is not yet common in Poland to request EDI information, and it may raise concerns among some employees. Although this is changing, Poland is quite a homogenous society in terms of ethnicity and currently is heavily polarised when it comes to political and philosophical beliefs, different minorities' rights in at the centre of public discussion and subject to such polarisation (e.g. LGBT+ rights).

However, general data related to equal treatment of men and women is more often collected due to Polish anti-discriminatory laws, as well as data regarding persons with disabilities (due to statutory obligations or special schemes related thereto).

What are the key risks for employers in not complying with the above?

- EDI is becoming a topic of discussion in the Polish employment sphere, and employee activism is growing. Associated complaints, allegations and breaches that happen from time to time attract the attention of the press, social media and staff themselves, and can result in damage to an employer's reputation and brand, with other knock-on effects (e.g., difficulties with recruitment, retention of staff and wider regulatory interest).
- Misuse or perceived misuse of staff EDI data in the context of staff management and decision-making runs a clear risk of discrimination claims as well as other related claims (e.g., unfair dismissal or "mobbing"). EDI-related claims tend to be high-profile and sensitive, and in practice are often costly and time-consuming to manage. Discrimination and mobbing claims are also subject to uncapped compensation awards, so carry an additional financial risk.
- The President of the Personal Data Protection Office (the Polish data protection authority) has the power to impose fines of up to €20,000,000 or 4% of global annual turnover (whichever is greater) as well as to issue enforcement and administrative decisions requiring changes to processing in the event of a breach of the GDPR.
- Employees can exercise their data rights, including the right to access copies of their personal data. In Poland, access requests in particular are often costly and time consuming for employers to deal with and may involve the disclosure of materials the employer finds embarrassing. Employees also have a right to seek compensation in the event of breach of the GDPR.

Singapore

Singapore

What characteristics are protected from discrimination?

- Nationality
- Gender
- Marital status
- Race
- Disability
- Religion
- Age

Note: these characteristics are not protected by any national law per se, but are cited under the national guidelines under the ambit of discrimination which has been issued by the Tripartite Alliance for Fair Employment Practices (TAFEP). If an employer is found to have discriminated against an employee, there would be grounds for a complaint to TAFEP and possibly the Ministry of Manpower, who may then sanction the employer where necessary.

What of these are subject to additional protections/requirements under local data protection law? How does this interact with discrimination law and where do they overlap?

None. There are no additional protections/requirements under data protection laws specific to EDI data. EDI data comprising personal data will be subject to general data protection obligations, such as the obligations to notify individuals and obtain their consent for the collection, use and/or disclosure of their personal data for a purpose(s). There are no codified laws on discrimination in Singapore as of the time of this EDI chart.

Is there a general legal requirement to carry out EDI monitoring?

No. There is no general legal requirement to carry out EDI monitoring.

Is there any specific EDI data that employers are legally required to process, e.g. to carry out EDI monitoring (such as gender pay gap reporting)?

No. There is no specific requirement to process EDI data.

Can employers actively promote diversity in the workplace?

Yes. While there is no legal requirement to do so, employers are encouraged to promote workplace diversity in a bid to create an inclusive environment and enhance their reputation with job seekers, allowing them to attract the best workers in the market while providing fair opportunities for all.

The Ministry of Manpower has published a guide for employers on how to promote workplace diversity, signalling its support of the same.

Does data protection law have specific provisions either permitting or prohibiting concerning the processing of personal data for equal opportunities & diversity monitoring?

No.

Where employers are required to, or not prohibited from, processing EDI data:

Do we have to collect and process EDI data in anonymised form?

No. Employers can consider anonymising EDI data as a means to manage data protection risk, as anonymised data will not be considered to be personal data. However, employers that choose to do so should be mindful of the risk of re-identification. EDI data will not be considered to be anonymised if there is a serious possibility that the individual could be re-identified.

What are the key employment risks to consider?

- Employees cannot be treated less favourably as a result of specific personal characteristics or attributes, and thus collection of EDI data carries with it a discrimination risk.
- EDI data comprising personal data are subject to data protection obligations under the *Personal Data Protection Act 2012* (**PDPA**), and breaches of the PDPA may be subject to investigations and penalties imposed by the Personal Data Protection Commission (**PDPC**) (see further below).

What are the key data protection compliance requirements under data protection law?

The PDPA currently imposes 10 main data protection obligations on employers that collect, use and/or disclose personal data:

1 **Consent Obligation**: Employers must obtain an individual's consent before collecting, using or disclosing his/her personal data for a purpose.

2 **Purpose Limitation Obligation**: Employers may only collect, use or disclose personal data about an individual for purposes that are reasonable in the circumstances.

3 **Notification Obligation**: Employers must notify an individual of the purpose(s) for which they intend to collect, use or disclose his/her personal data on or before such collection, use or disclosure.

4 **Access and Correction Obligation**: Employers must, upon request: (a) provide an individual with his/her personal data in their possession/control and information about the ways in which the personal data may have been used or disclosed during the past year; and (b) correct errors or omissions in his/her personal data.

5 **Accuracy Obligation**: Employers must make reasonable efforts to ensure that personal data collected is accurate and complete if the personal data is likely to be used to make a decision that affects the individual concerned or is likely to be disclosed to another organisation.

6 **Protection Obligation**: Employers must protect personal data in their possession/control by making reasonable security arrangements to prevent: (a) unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks; and (b) the loss of any storage medium or device on which personal data is stored.

7 **Retention Limitation Obligation**: Employers must cease to retain personal data, or remove the means by which the personal data can be associated with particular individuals as soon as it is reasonable to assume that: (a) the purpose for which the personal data was collected is no longer being served by retention of the personal data; and (b) retention is no longer necessary for legal or business purposes.

8 **Transfer Limitation Obligation**: Employers must not transfer personal data to a country or territory outside Singapore except in accordance with requirements prescribed under the PDPA to ensure that transferred personal data is provided with a comparable standard of protection as under the PDPA.

9 **Data Breach Notification Obligation**: In the event of a data breach, employers must assess whether the breach is notifiable, and if so, notify affected individuals and/or the Personal Data Protection Commission.

10 **Accountability Obligation**: Employers must implement policies and procedures necessary to meet their obligations under the PDPA and make information about such policies and procedures publicly available.

Are there any key local considerations, such as consultation with trade union or employee representative bodies?

The requirement for consultation depends on whether (1) the trade union is recognised by the company and (2) whether the *Collective Bargaining Agreement* contains any requirement for employee consultation. Assuming (1) and (2) do not apply, no prior consultation is required.

The requirement with regard to any consultation or approval from trade union or other representative bodies will depend on the content of the relevant *Collective Bargaining Agreement*.

What are the key risks for employers in not complying with the above?

- **Discrimination complaints**: Complaints in relation to discriminatory practices are handled by the Ministry of Manpower (MOM). Where a complaint made by an employee is found to be substantiated, the MOM may issue a warning in the first instance, and the company will be given an opportunity to rectify its actions. Failure to adhere to the MOM's advice may result in the MOM taking administrative action, including curtailment of work pass privileges of the company.
- **Enforcement action for data protection contraventions**: Under the PDPA, the PDPC is empowered to investigate and take enforcement action against organisations for contraventions of the PDPA. In the event that a contravention is determined, the PDPC has broad discretion to issue directions to organisations to ensure compliance with the PDPA, including directing organisations to stop collecting, using or disclosing personal data, and/or to destroy personal data. In the event of intentional or negligent contraventions, the PDPC may also impose financial penalties up to a maximum of SGD 1 million (approx. USD 735,000 or EUR 670,000). The maximum limit for financial penalties is expected to be amended in due course to the higher of: (a) SGD 1 million or (b) 10% of an organisation's annual turnover in Singapore. There may also be reputational risk as infringement decisions are typically published by the PDPC and made publicly available.

Slovakia

Slovakia

What characteristics are protected from discrimination?

- Sex
- Religion or beliefs
- Race
- Nationality and ethnic group
- Disability and chronic illness
- Age
- Sexual orientation
- Marital or family status
- Political orientation or other opinion
- Colour
- National or socio-economic origin
- Property
- Lineage or other status
- Language
- Gender, including pregnancy or being a parent
- Because of a reporting of crime or other anti-social activity
- In the context of employment law relations, character of work (fixed term or flexible workers, fulltime or part-time workers, office workers or teleworkers etc.)

What of these are subject to additional protections/requirements under local data protection law? How does this interact with discrimination law and where do they overlap?

Special categories of personal data are subject to additional protections and requirements in Slovakia under the sec. 16 of the Slovak *Act No. 18/2018 Coll. on Data Protection* (**DPA**) which implements the Art. 9 of GDPR. The DPA defines "special categories of personal data" as:

- personal data revealing **racial** or **ethnic origin**;
- personal data revealing **political opinions**;
- personal data revealing **religious** or **philosophical belief**;
- personal data revealing **trade union membership**;
- **genetic** data;
- **biometric** data (where used for identification purposes);
- data concerning **health**;
- data concerning a person's **sex life**; and
- data concerning a person's **sexual orientation**.

The application of both discrimination protection and data protection requirements should be carefully considered on a case-by-case basis. Equally, the special attention shall be taken where the special category

data requirements overlap with other protected characteristics (e.g. sex/gender identity data may include health or sexual orientation data).

Is there a general legal requirement to carry out EDI monitoring?

No.

There is no general or specific legal requirement to carry out EDI monitoring in Slovakia.

Is there any specific EDI data that employers are legally required to process, e.g. to carry out EDI monitoring (such as gender pay gap reporting)?

However, employers should always act in line with the applicable legal regulation prohibiting any kind of discrimination, and therefore collection of relevant information and carrying out the EDI monitoring, incl. pay gap monitoring may happen. Any such collection and monitoring should be executed in a very sensitive and legally cautious manner subject to the applicable legal regulation.

Can employers actively promote diversity in the workplace?

Yes.

Generally, the employers must ensure that there is no discrimination and/or unfair treatment in the workplace, in other words employers must secure the equal opportunities of the employees in the workplace.

Employers with more than 20 employees are required to ensure at least 3.2 % of their total employee population is comprised of people with disabilities. This statutory obligation can be fulfilled by further allowable means (e.g. by purchasing specific products or services or by contribution to the state budget).

Does data protection law have specific provisions either permitting or prohibiting the processing of personal data for equal opportunities & diversity monitoring?

Yes.

Under the Slovak *Act No. 18/2018 Coll. on Data Protection* (**DPA**), processing of special categories of personal data is generally prohibited, unless a condition under Art. 9 of GDPR is fulfilled.

In the context of EDI, there is a potential legal basis to permit processing of special categories of personal data in Slovakia (in line with the Art. 9 of GDPR). The explicit consent of a person may allow the processing, notwithstanding the employer must demonstrate clearly that the consent of a person was truly voluntary. In practice and in the context of power imbalance inherent in the employer – employee relationship, this is difficult to obtain.

Where employers are required to, or not prohibited from, processing EDI data:

Do we have to collect and process EDI data in anonymised form?

No.

As mentioned above, EDI monitoring per se is not explicitly mandatory in Slovakia. **No**netheless, when processing, anonymous collection is the safest way to collect and otherwise process EDI data, and potentially reduces any employment and data protection risks.

However, EDI data may principally be collected and otherwise processed in a form in which the employees are identified or identifiable, provided that the necessary steps are taken in order to comply with employment law, non-discrimination law and data protection law requirements. Any potential failure to take appropriate steps (to ensure compliance) may increase the risks of complaints, claims and sanctions under employment and data protection law.

What are the key employment risks to consider?

The collection and usage of EDI data, particularly in a form where the persons are identifiable, is potentially sensitive and very risky from an employment and data protection law perspective.

Employer should focus on compliance with data protection requirements (see Q.8 below), as well as on the management and communication regarding EDI data programmes in order to reduce risk of claims and sanctions, including the following:

- The collection of EDI data should be voluntary. Subject to some exceptions, generally it is very unlikely that employer would be able to justify or even enforce a mandatory requirement, unless extenuating/facilitating circumstances apply.
- Employers should consider carefully what data they want to collect, why, and how they want to use that data. The data collected should clearly correlate to an identified business need and a specific purpose.
- Employers should provide personnel with a clear explanation of type of data they want to collect, why, and how that data will be used, in accordance with the relevant provisions of GDPR and for the purposes of minimisation of risk of employees' complaints, grievances and claims.
- Personnel communication is important for managing employees' perceptions, thereby reducing the risk of claims and sanctions. Employer should ensure that they carefully consider and prepare communication to employees about any EDI data programmes, and should try to anticipate any resistance, concerns or further potential risks.

What are the key data protection compliance requirements under data protection law?

The collection of EDI data in identifiable form will result in processing of personal data. As set out above, the certain types of EDI data appertain also to special categories of personal data (see Q.2 above).

When processing any personal data, employer must comply with the requirements set out in the Slovak *Act No. 18/2018 Coll. on Data Protection* (**DPA**) and GDPR. Broadly, this means employer should:

- identify and communicate clear and legitimate purpose and legal basis for processing EDI data – in case this involves also special categories of personal data, there must be also a condition fulfilled for processing (see Q.5 above);
- only process the minimum amount of data required;
- take steps to ensure the continuing accuracy and integrity of the data;
- implement appropriate security, access and confidentiality measures, and not to retain that data for longer than required for the purpose for which it was originally collected.

On a case-by-case basis, the additional compliance requirements under the Slovak *Act No. 18/2018 Coll. on Data Protection* (**DPA**) and GDPR may be also relevant:

- completion of data protection impact assessment (**DPIA**) and, if relevant, legitimate interests' assessment;
- provision of appropriate notice to employees, and receipt of consent, if required;
- update the employer's record of processing.

Are there any key local considerations, such as consultation with trade union or employee representative bodies?

There is no explicit general legal requirement for employer to consult the processing of EDI data with employees' representatives in Slovakia. Notwithstanding, it is advisable that employers assess if such a specific requirement applies pursuant to the collective or other agreements with the trade unions or employees' representatives.

In general, under the Slovak *Labour Code* (Slovak *Act No. 311/2001 Coll.*), employers should not infringe the employees' privacy in the workplace by monitoring the employees (including monitoring of e-mails) without serious grounds based on the specific nature of the employer's activities. Such control (monitoring) mechanisms are always subject to mandatory prior consultation with employees' representatives as well as prior notification to employees.

Also, the implementation of EDI Policy (**Programmes**) may be, under certain conditions, considered a "work procedure/regulation" which generally requires the prior consent of the employee's representatives. The process of obtaining the consent will usually involve the employer explaining the background to the policy, the reasons for its implementation, contents of the policy and proposed roll-out date. Moreover, employees shall be notified of the policy and provided with either a link to the policy or physical copy of the policy, as well as asked to either sign an acknowledgment confirming that they have read and understood the policy, or to "click to accept," electronically, to confirm that same.

What are the key risks for employers in not complying with the above?

The key risks for employers would be as follows:

- Misuse or perceived misuse of personnel EDI data in the context of personnel management and decision-making runs a clear risk of discrimination claims (including e.g. unfair dismissal claims). Sanctions may be imposed in the area of employment law sphere and the data protection sphere.
- Generally, the Slovak National Labour Inspectorate may impose fines of up to EUR 100,000 to the employer for breach of the obligations arising from employment law regulations.
- The Slovak Data Protection Authority is entitled to impose fines up to EUR 20,000,000 or up to 4 % of the total worldwide annual turnover of the preceding financial year of employer, whichever is higher, as well as to issue the enforcement notices requiring changes to processing in the event of a breach of the Slovak Act No. 18/2018 Coll. on Data Protection (**DPA**) or GDPR.
- Employees can exercise their rights related to data protection, including right to access copies of their personal data. The access requests are, in particular, often time consuming for employer to deal with. Employees have also right to seek compensation in the event of breach of data protection regulations by employer.

Spain

Spain

What characteristics are protected from discrimination?

- Gender
- Marital status
- Race
- Physical or mental disability
- Religion or belief
- Sexual orientation
- Age
- Trade union membership
- Kinship with other employees
- Gender reassignment
- Pregnancy
- Maternity/Paternity leave
- Ideology
- Socio-economic status
- Language

Conditions or circumstance:

- Working time reduction or leave to care for children;
- Any other personal or social characteristic.

What of these are subject to additional protections/requirements under local data protection law? How does this interact with discrimination law and where do they overlap?

Information regarding gender, race, physical or mental disability, religion or belief, sexual orientation, trade union membership, gender reassignment, pregnancy and ideology is or is likely to be considered as special categories of personal data under the Regulation (EU) 2016/679 (**GDPR**), applicable in Spain.

Further to the GDPR, Organic Law 3/2018, of 5 December on the Protection of Personal Data and guarantee of the digital rights (**LOPDGDD**) provides in Article 9(1) that consent shall not suffice in order to process personal information with the purpose of identifying someone's ideolo**gy, trade union membership, religion or belief, sexual orientation and/or race**. The purpose of this is to prevent discriminatory situations.

The data categories listed above clearly overlap with some of the protected characteristic under discrimination law (listed in Q.1) but the application of both discrimination protection and data protection requirements should be considered on a case-by-case basis.

Other than that, there are no specific requirements for the processing of special categories of personal data in Spain.

Note that consent would not be the appropriate lawful basis for the processing of EDI data for the purposes of said law.

Is there a general legal requirement to carry out EDI monitoring?

No. There is no general requirement to carry out equal opportunities & diversity monitoring.

Is there any specific EDI data that employers are legally required to process, e.g. to carry out EDI monitoring (such as gender pay gap reporting)?

Yes. There are requirements to collect and otherwise process specific EDI data.

1 The *Royal Decree-Law 6/2019* and *Organic Law 3/2007* provide certain equality measures.

- **Salary Record**. All companies, regardless of their size, must keep a record of the salaries of the workforce disaggregated by gender and occupational group, including management and senior positions.
  - **Minimum content of the salary record**: The arithmetic average and the median of (i) the base salaries, (ii) each of the complementary salary, and (iii) each of the extraordinary supplements of the workforce, which must be detailed by gender and distributed by professional group, professional category, level, position or any other applicable classification system.
- **Equality Plan**. Companies employing more than 50 employees must adopt an 'Equality Plan', which is a prescribed set of equality measures under Spanish law, and which must include the following minimum content:
  - Hiring process;
  - Professional classification;
  - Training;
  - Promotions;
  - Working conditions, including wage auditing between women and men;
  - Co-responsible exercise of personal, family and working life rights;
  - Under-representation of women;
  - Remuneration, and
  - Prevention of sexual and gender-based harassment.
  - For more information on discrimination under Spanish law, see our article here.

2 **Handicapped employees**. Any company with 50 employees or more must have 2% of disabled employees (i.e. 1 employee every 50 employees).

Under Spanish law, disabilities are deemed to exist when there is any kind of limitation over 33% (certificated by the Social Security through the health system).

In order to establish the number of disabled employees within the organisation, companies are permitted to issue an email asking for this workforce information as this is related to the compliance of a legal obligation. However, we do not recommend asking the employees to reply directly to such an email (in order to avoid situations where other employees inadvertently receive t personal data), but to directly contact HR (via a specific contact) if they qualify under identify as such.

It is also possible to apply for an exception from the Administration, which will then allow the organisation to fulfil this requirement through donations to foundations working with handicapped employees. Companies with less than 50 employees do not have any equivalent obligations.

Can employers actively promote diversity in the workplace?

Yes. Employers are subject to several requirements under Spanish law to promote diversity and equality of opportunity (see Q.3 above).

Does data protection law have specific provisions either permitting or prohibiting the processing of personal data for equal opportunities & diversity monitoring?

Yes.

Processing of personal data, and in particular special categories of personal data, is strictly regulated (please see above).

General requirements with regard to the processing of EDI data will apply.

Where employers are required to, or not prohibited from, processing EDI data:

Do we have to collect and process EDI data in anonymised form?

There is no statutory obligation to collect and process EDI data in an anonymised format. However, as far as possible, we advise the companies to process EDI data in an anonymised form in order to potentially reduce employment and data protection risks.

If EDI data is processed in a form where staff are identified, or identifiable, it should comply with data protection requirements (i.e. technical and organisational measures must be in place to ensure a level of security of the data appropriate to the risk, as per Article 32 of the GDPR).

What are the key employment risks to consider?

The collection and use of EDI data, particularly in a form where staff are identifiable, is potentially sensitive and high risk from an employment and data protection perspective. Employers should give particular consideration to the data protection compliance requirements (see Q.8 below), and the management of and communications regarding EDI data programmes in order to reduce the risk of claims and sanctions, including the following:

- Employers should consider carefully what data they want to collect, why, and how they want to use that data. The data collected should clearly correlate to an identified business need and a specific purpose.
- Employers should provide staff with a clear explanation of what data they will collect, why, and how it will be used, in accordance with the GDPR and to limit the risk of employee complaints, grievances and claims.
- Staff communication is important for managing employee perceptions, thereby reducing the risk of claims and sanctions. Employers should ensure that they carefully consider and prepare employee communications about any EDI data programmes, and try to anticipate any resistance, concerns or potential risks.

What are the key data protection compliance requirements under data protection law?

The collection of EDI data in identifiable form will result in the processing of personal data. As set out above, certain types of EDI data are also “special category” data. When processing any personal data, the employer must comply with the requirements set out in the GDPR and the LOPDGDD. Broadly, this means employers should:

- identify and communicate a clear and legitimate purpose and legal basis for processing EDI data – where this involves special category data, there must also be a condition for processing under Article 9 GDPR;
- only process the minimum amount of data required;
- take steps to ensure the continuing accuracy and integrity of the data;
- implement appropriate security, access and confidentiality measures, and not retain that data for longer than required for the purpose for which it was originally collected;
- completion of a data protection impact assessment (**DPIA**) and, if relevant, legitimate interests assessment;
- providing an appropriate notice to employees;
- updating the employer’s record of processing activities.

Are there any key local considerations, such as consultation with trade union or employee representative bodies?

Yes.

- **Salary record**. Workers' Representatives (if any) must be consulted with at least 10 days before the preparation of the salary record. Employees will have access to the full contents of the salary record through the Workers' Representatives (**WR**). If there are no WR in the company, employees will have limited access to the salary record information since they will only be entitled to consult the percentage differences in salary between men and women, detailed by remuneration and the applicable classification system.
- **The Equality Plan** must be negotiated with WR (failing that, with employees), and then register in the Register of *Collective Bargaining Agreements and Collective Labour Agreements*. Note that it is required to create a joint monitoring and reviewing committee.
- **Handicapped employees**. The employer must report information regarding handicapped employees or the exemptions applied from the Administration to the WR (if any).

What are the key risks for employers in not complying with the above?

Non-compliance with applicable data protection rules could lead to sanctions of up to EUR 20,000,000 or of up to the 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher. It is important to take into consideration that despite the fact that the Spanish Data Protection Authority does not tend to impose the highest fines in the EU, it is the most active EU supervisory authority (in terms of number of sanctions imposed).

Furthermore, non-compliance with the obligations regarding the non-discrimination in remuneration based on gender may result in penalties ranging from EUR 751 to EUR 7,500, and non-compliance with the obligations regarding Equality Plan would entail penalties ranging from EUR 7,501 to EUR 225,018. Additional risks apply with regard to other breaches of discrimination protections under Spanish employment law.

Where an employer does not comply with disability reporting regulations, potential risks including:

a. sanctions ranging from Eur 751 to Eur 7,500;
b. potential prevention from applying social security rebates for 2 years (for each disabled employee not hired = not receiving rebates for 1 existing employee);
c. not being able to apply in public tender process (i.e. engaging with the public authorities in Spain); and/or
d. certain private companies monitor this obligation's compliance from their service providers.

Sweden

Sweden

What characteristics are protected from discrimination?

- Sex (including individuals who have undergone, or who are planning to undergo gender reassignment surgery)
- Transgender identity or expression (include individuals who do not define themselves as a female or male)
- Religion or belief
- Disability
- Employees working part-time
- Employees on fixed-term contracts
- Employees on parental leave
- Sexual orientation
- Age
- Ethnicity

What of these are subject to additional protections/requirements under local data protection law? How does this interact with discrimination law and where do they overlap?

The following categories of personal data mentioned in question 1 constitutes special categories of personal data according to GDPR article 9 (1):

- transgender identity or expression;
- religion or belief;
- disability;
- sexual orientation; and
- ethnicity.

It is generally forbidden to process special categories of personal data unless any of the exceptions in GDPR article 9 (2) applies. Furthermore in Sweden, it is not permissible to process special categories of **personal data** to monitor equality, diversity and inclusion. Therefore, an employer needs to either refrain from processing special categories of personal data to monitor equality, diversity and inclusion and only use anonymized data or rely on any of the exceptions in GDPR article 9 (2) other than article 9 (2) (b). Explicit consent according to GDPR article 9 (2) (a) may be applicable but only if the employer can demonstrate that the consent is truly voluntary (which is difficult to do because of the power imbalance between the employer and the employee).

Whilst employers are required to counteract discrimination in the workplace and promote equal opportunities, the general consensus is that such measures can be taken without monitoring EDI data.

Is there a general legal requirement to carry out EDI monitoring?

No. Whilst employers in Sweden are required to take 'active measures' in order to prevent discrimination and promote equal rights and opportunities in the workplace, there is no general legal requirement to carry out EDI monitoring. Any EDI data collected should be made in anonymised form.

Is there any specific EDI data that employers are legally required to process, e.g. to carry out EDI monitoring (such as gender pay gap reporting)?

Yes.

- If a company in Sweden employs more than 25 employees, the active measures referred to above must be documented in writing.
- Annual gender pay-gap reports must be carried out to ensure equal opportunities/equal pay for equal work. Companies that engage 10 or more employees must ensure that the report is documented in writing.

Can employers actively promote diversity in the workplace?

Yes. Employers in Sweden are, under the Swedish *Discrimination Act (SFS 2008:567)*, are obliged to adopt active measures to prevent discrimination and promote equal rights and opportunities in the workplace. Such measures must be documented in writing if the company engage 25 or more employees. Further, if the company engage 10 or more employees, it must also carry out and document gender pay gap reports.

Does data protection law have specific provisions either permitting or prohibiting the processing of personal data for equal opportunities & diversity monitoring?

Yes.

Processing of personal data, and in particular special categories of personal data, is strictly regulated (please see above).

The Swedish prohibition on processing special categories of personal data to monitor equality, diversity and inclusion is not stipulated in law but stems from statements from the Swedish Equality Ombudsman (the competent public body in Sweden that works to promote equal rights and opportunities and to combat discrimination).

Where employers are required to, or not prohibited from, processing EDI data:

Do we have to collect and process EDI data in anonymised form?

Yes (as regards EDI data collected or otherwise processed for the purpose of promoting equal opportunities in the workplace). Please see answer to Q.5 for more information.

What are the key employment risks to consider?

Monitoring EDI in non-anonymised form would amount to a breach against employees right to privacy under data protection law (and would therefore be deemed unlawful).

If an employer subsequently used any EDI data in its management of an employee (for example, it chose to dismiss an employee based on a protected characteristic identified as part of its EDI monitoring activity, the employer would be at risk of a discrimination claim and potentially other related employment claims (such as an unfair dismissal claim), depending on the action taken by the employer.

What are the key data protection compliance requirements under data protection law?

The key requirements stipulated in the GDPR include the following:

- Ensure that an appropriate legal ground is in place for the processing of personal data;
- provide information to the employee about the personal data processing;
- only process the minimum amount of personal data required;
- ensure the continuing accuracy and integrity of the personal data processed; and

- implement appropriate security, access and confidentiality measures, and not retain personal data for longer than required for the purpose for which it was originally collected.

Are there any key local considerations, such as consultation with trade union or employee representative bodies?

If the company is bound by a collective bargaining agreement, it may need to consult with relevant trade union(s) party to the applicable agreement before implementing EDI monitoring.

What are the key risks for employers in not complying with the above?

Non-compliance with the GDPR can result in sanctions up to 4% of global annual turnover or EUR 20,000,000, whichever is higher. Further, employees can make claims for compensation for example on the basis of a GDPR infringement or due to discrimination in accordance with the Swedish Act on Discrimination (e.g. if found that the employer has not complied with its duty to take active measures or if salary discrepancies are found following a gender pay gap report).

Non-compliance with the duty to consult with trade unions (if applicable, please see comment to section 9) may render the company being held liable for damages payable to the affected trade union(s).

If an employer subsequently used any EDI data in its management of an employee (for example, it chose to dismiss an employee based on a protected characteristic identified as part of its EDI monitoring activity, the employer would be at risk of a discrimination claim and potentially other related employment claims, depending on the action taken by the employer. Further, if an employee raised concerns about the employer's EDI monitoring activities, this could form the basis for protection for the employee under Swedish whistleblowing legislation.

UAE

UAE

What characteristics are protected from discrimination?

- Race
- Colour
- Sex
- Religion
- National origin
- Socio-economic origin
- Disability

Further, under the Federal Decree Law No. 2 of 2015 on combating discrimination and hatred (**Anti-Discrimination Law**) criminalises any act of discrimination of any form by any means of expression or by any other means and therefore, broadens the scope of the protected characteristics to discrimination in 'any form'.

What of these are subject to additional protections/requirements under local data protection law? How does this interact with discrimination law and where do they overlap?

Sensitive categories of personal data are carved out in the Federal Decree Law No. 45/2021 on the *Protection of Personal Data* (**PDPL**) which defines "Sensitive Personal Data" as "*any data that directly or indirectly reveals a natural person's family, racial origin, political or philosophical opinions, religious beliefs, criminal records, biometric data, or any data related to the health of such person, such as his/her physical, psychological, mental, genetic or sexual condition, including information related to health care services provided thereto that reveals his/her health status.*"

Those categories in italics above broadly overlap with the corresponding protected characteristic under the Federal Decree-Law No. 33/2021 on *Regulation of Labour Relations* (**Labour Law**) in the UAE but the application of both discrimination protection and data protection requirements should be considered on a case-by-case basis.

Care should be taken where the special category data requirements overlap with other protected characteristics (e.g. sex/gender identity data may include sexual orientation data).

Please note that the PDPL keeps intact existing laws within the UAE's financial free zones and will operate alongside the *Data Protection Law* Dubai International Financial Centre Law No. 5 of 2020 (**DIFC DP Law**) and Abu Dhabi *Global Market's Data Protection Regulations 2021* (**ADGM DP Law**). The advice provided below is in respect of mainland UAE (and not the respective financial free zones).

Is there a general legal requirement to carry out EDI monitoring? Is there any specific EDI data that employers are legally required to process, e.g. to carry out EDI monitoring (such as gender pay gap reporting)?

No. There are no general EDI data processing or monitoring requirements in the UAE (under either employment or data protection law).

Can employers actively promote diversity in the workplace?

Yes. Whilst there is no direct broad requirement to actively promote diversity and equality of opportunities in the workplace under UAE law, employers can choose to do so provided it is not viewed as discriminatory.

Further, we note that the UAE federal employment law provides that any rules and procedures that would enhance the participation of the UAE nationals shall not be considered as discrimination.

Does data protection law have specific provisions either permitting or prohibiting the processing of personal data for equal opportunities & diversity monitoring?

Yes. The categories of data collected for equal opportunities and diversity monitoring are likely to constitute special categories of personal data under the PDPL. It is anticipated that the Executive Regulations to the PDPL which are due to be published in March 2022 will provide additional guidance on processing special categories of personal data. In the interim, explicit consent may allow the processing, but only if the employer can demonstrate that this is truly voluntary. It is unlikely that an employer would be able to justify or enforce a mandatory requirement unless extenuating circumstances apply.

Besides the general provisions in the above referenced laws, there are industry specific provisions relating to data protection and transfers, for example, the Health Data Law enacted in 2019 whereunder all health information and data related to health services provided in the UAE may not be stored, processed, generated or transferred outside of the UAE, unless otherwise prescribed by the concerned federal or local government health authority or the Ministry of Health and Prevention and subject to some exceptions.

Where employers are required to, or not prohibited from, processing EDI data:

Do we have to collect and process EDI data in anonymised form?

No. While anonymous data collection reduces employment and data protection risks, EDI data can usually be collected and processed in a form where staff are identified, or identifiable provided steps are taken to comply with data protection law. Employers should provide staff with a clear explanation of what data they will collect, why, and how it will be used. Failure to take appropriate steps to ensure compliance will increase the risks associated with complaints, claims and sanctions under employment and data protection law.

What are the key employment risks to consider?

It is important that specific consent is obtained from the employees when collecting, storing, processing or transferring any EDI data. In the event the employees do not consent or refuse to provide such data, employers cannot force such employees to provide the data unless where legally required.

In collecting EDI data, the questions should take local law aspects into consideration. For example, same sex relationships and gender reassignment (unless medically required) are not recognised in the UAE and we recommend that employers do not ask any questions surrounding such matters as employees could potentially incriminate themselves by answering such questions. Hiring any employee is subject to obtaining a work permit from competent authorities and this may have an impact who can be hired despite any diversity policy that an employer may have.

What are the key data protection compliance requirements under data protection law?

The collection of EDI data in identifiable form will result in the processing of personal data. It is prohibited to process personal data including sensitive personal data without the consent of the individual. There are cases excluded from such prohibition, however, based on the fact that this involves EDI data collection, the employer should rely on consent.

Consent needs to be specific, informed and an unambiguous indication of the employee's agreement to the processing of personal data by a statement or by a clear affirmative action, whether in writing or electronically. This means that employers can no longer rely on 'catch all' consent, which has been commonly used by UAE businesses.

In addition, the basic data protection principles under the PDPL must be observed:

- processing must be made in a fair, transparent and lawful manner.
- personal data must be collected for a specific and clear purpose.
- personal data must be sufficient and limited to the purpose.
- personal data must be accurate and correct and must be updated whenever necessary.

- appropriate measures and procedures must be in place to ensure erasure or correction of incorrect personal data.
- personal data must be kept securely and protected from any breach by establishing and applying appropriate technical and organizational measures.

The other compliance requirements under the PDPL include:

- completion of a data protection impact assessment (**DPIA**);
- providing an appropriate notice to employees, and obtaining consent if required; and
- updating the employer's record of processing.

Are there any key local considerations, such as consultation with trade union or employee representative bodies?

There are no trade union or other employee representative bodies in the UAE. However, as outlined above, specific employee consent should be obtained in collecting, storing, processing or transferring EDI data.

What are the key risks for employers in not complying with the above?

Equality, diversity and inclusivity are increasingly becoming hot topics in the UAE employment sphere. Associated complaints, allegations and breaches often attract the attention of the press, social media and staff themselves, and can result in damage to an employer's reputation and brand, with other knock-on effects (e.g. difficulties with recruitment, retention of staff and wider regulatory interest).

Misuse or perceived misuse of staff EDI data in the context of staff management and decision-making runs a clear risk of discrimination claims which in practice are often costly and time-consuming to manage.

The PDPL does not state the penalties that will apply for breaches of the law. The level of sanctions is expected to be specified in the subsequent Executive Regulations. Data subjects can file a complaint with the UAE Data Office if they have reason to believe that the PDPL has been breached by a controller or processor. Employees can also exercise their data rights, including the right to access copies of their personal data. Administrative penalties can be imposed as part of a decision by the Council of Ministers.

UK

UK

What characteristics are protected from discrimination?

- Age
- Disability
- Gender reassignment
- Marriage and civil partnership
- Pregnancy / maternity
- Race (includes nationality, ethnicity, national origins and colour)
- Religion / belief
- Sex (including gender identity)
- Sexual orientation

What of these are subject to additional protections/requirements under local data protection law? How does this interact with discrimination law and where do they overlap?

Special categories of personal data are subject to additional protections and requirements in the UK. The UK GDPR defines "special categories of data" as:

- personal data revealing **racial** or **ethnic origin**;
- personal data revealing **political opinions**;
- personal data revealing **religious** or **philosophical beliefs**;
- personal data revealing **trade union membership**;
- **genetic** data;
- **biometric** data (where used for identification purposes);
- data concerning **health**;
- data concerning a person's **sex life**; and
- data concerning a person's **sexual orientation**.

Those categories in italics above broadly overlap with the corresponding protected characteristic under discrimination law but the application of both discrimination protection and data protection requirements should be considered on a case-by-case basis.

Care should be taken where the special category data requirements overlap with other protected characteristics (e.g. sex/gender identity data may include health or sexual orientation data).

Is there a general legal requirement to carry out EDI monitoring?

No. There are no general EDI data processing or monitoring requirements in the UK (under either employment or data protection law).

Is there any specific EDI data that employers are legally required to process, e.g. to carry out EDI monitoring (such as gender pay gap reporting)?

Yes. Employers may be subject to certain specific requirements. Key requirements are as follows:

- Under the UK's Gender Pay Gap Reporting (**GPGR**) legislation, employers with 250 or more UK-based employees must collect certain gender and pay data and analyse this. Specific gender pay gap metrics must be published on their public-facing website, together with a written statement, and must be reported to the UK government (which also publishes this data).
- In **No**rthern Ireland, employers with 11 or more employees who each work more than 16 hours a week must register with the Equality Commission and then ask all staff (except contractors) to fill in an annual religious belief monitoring form (employees are not obliged to respond).
- Under the *Equality Act 2010*, public sector bodies are required to annually publish information to show compliance with the general equality duty.
- Regulatory bodies increasingly require their member employers to collect, report and publish certain EDI data on a regular basis.

Can employers actively promote diversity in the workplace?

Yes.

There is no direct broad requirement to actively promote diversity and equality of opportunities in the workplace under UK law (see above) but employers can choose to do so subject to their obligations not to unlawfully discriminate.

Positive discrimination (treating one person more favourably than another because they have a protected characteristic) is generally prohibited under the law unless an occupational requirement applies or it falls within narrow exemptions aimed at addressing underrepresentation of specific narrow groups in the workplace. Employers will still be subject to obligations under the law to prevent discriminatory practices in the workplace.

Does data protection law have specific provisions either permitting or prohibiting the processing of personal data for equal opportunities & diversity monitoring?

Yes.

Under the UK GDPR, processing special category data is generally prohibited unless a condition under Art.9 GDPR or Schedule 1 of the *DPA 2018* applies. Potential legal bases do exist to permit processing of special category in the UK in the EDI context.

- Explicit consent may allow the processing, but only if the employer can demonstrate that this is truly voluntary.
- Alternatively, the *Data Protection Act 2018* contains two substantial public interest conditions permitting employers to process specified special category data for diversity monitoring purposes, each of which will apply in respect of certain EDI data or circumstances and is subject to certain restrictions. The first condition is 'equality of opportunity or treatment' which permits certain monitoring activities but no positive action with respect to specific employees. The second condition is 'racial and ethnic diversity at senior levels of organisations' which permits some positive action without a need to seek consent, but only in respect of ethnicity data and only for certain senior positions.

Where employers are required to, or not prohibited from, processing EDI data:

Do we have to collect and process EDI data in anonymised form?

No.

Although anonymous collection is the safest way to collect and otherwise process EDI data is in anonymised form, and potentially reduces employment and data protection risks, EDI data can usually be collected and otherwise processed in a form where staff are identified or identifiable provided steps are taken to comply with data protection law. Failure to take appropriate steps to ensure compliance will increase the risks associated with complaints, claims and sanctions under employment and data protection law.

What are the key employment risks to consider?

The collection and use of EDI data, particularly in a form where staff are identifiable, is potentially sensitive and high risk from an employment and data protection perspective. Employers should give particular consideration to the data protection compliance requirements (see Q.8 below), and the management of and communications regarding EDI data programmes in order to reduce the risk of claims and sanctions, including the following.

- The collection of EDI data should be voluntary. It is unlikely that an employer would be able to justify or enforce a mandatory requirement unless extenuating circumstances apply.
- Employers should consider carefully what data they want to collect, why, and how they want to use that data. The data collected should clearly correlate to an identified business need and a specific purpose.
- Employers should provide staff with a clear explanation of what data they will collect, why, and how it will be used, in accordance with the GDPR and to limit the risk of employee complaints, grievances and claims.
- Staff communication is important for managing employee perceptions, thereby reducing the risk of claims and sanctions. Employers should ensure that they carefully consider and prepare employee communications about any EDI data programmes, and try to anticipate any resistance, concerns or potential risks.

What are the key data protection compliance requirements under data protection law?

The collection of EDI data in identifiable form will result in the processing of personal data. As set out above, certain types of EDI data are also "special category" data (see Q.2 above).

When processing any personal data, the employer must comply with the requirements set out in the UK GDPR. Broadly, this means employers should:

- identify and communicate a clear and legitimate purpose and legal basis for processing EDI data – where this involves special category data, there must also be a condition for processing under Article 9 UK GDPR (see Q.5 above);
- only process the minimum amount of data required;
- take steps to ensure the continuing accuracy and integrity of the data,
- implement appropriate security, access and confidentiality measures, and not retain that data for longer than required for the purpose for which it was originally collected.

Additional compliance requirements under the UK GDPR also include:

- completion of a data protection impact assessment (**DPIA**) and, if relevant, legitimate interests assessment;
- providing an appropriate notice to employees, and obtaining consent if required;
- updating the employer's record of processing;
- implementing an 'appropriate policy document' as described under the *Data Protection Act 2018*, if reliant on either substantial public interest condition.

Are there any key local considerations, such as consultation with trade union or employee representative bodies?

It is fairly common for employers to run EDI data programmes in the UK. That said, employees are increasingly sensitive with regard to how such data is collected and how it is used (particularly where the data is identifiable form).

There is no general requirement for employers to consult with trade union or other employee representative bodies in the UK in respect of the collection and use of EDI data but employers will need to check any specific agreements with such trade unions or bodies to confirm whether any such requirements apply.

What are the key risks for employers in not complying with the above?

- Equality, diversity and inclusivity remain hot topics in the UK employment sphere, and employee activism is growing. Associated complaints, allegations and breaches often attract the attention of the press, social media and staff themselves, and can result in damage to an employer's reputation and brand, with other knock-on effects (e.g. difficulties with recruitment, retention of staff and wider regulatory interest).
- Misuse or perceived misuse of staff EDI data in the context of staff management and decision-making runs a clear risk of discrimination claims as well as other related claims (e.g. unfair dismissal and whistleblowing). EDI-related claims tend to be high-profile and sensitive, and in practice are often costly and time-consuming to manage. Discrimination and whistleblowing claims are also subject to uncapped compensation awards, so carry an additional financial risk.
- The ICO (the UK's data protection authority) has the power to impose fines of up to £17,500,000 or 4% of global annual turnover (whichever is greater), as well as to issue enforcement notices requiring changes to processing in the event of a breach of the UK GDPR.
- Employees can exercise their data rights, including the right to access copies of their personal data. In the UK, access requests in particular are often costly and time consuming for employers to deal with and may involve the disclosure of materials the employer finds embarrassing.
- Employees may also have a right to seek compensation in the event of breach of the GDPR.

Key contacts

Pattie Walsh

Partner

+852 2248 6088
pattie.walsh@twobirds.com

Ian Hunter

Partner

+44 207 4156 140
ian.hunter@twobirds.com

Ruth Boardman

Partner

+44 207 4156 018
ruth.boardman@twobirds.com

Ariane Mole

Partner

+33 1 42 68 63 04
ariane.mole@twobirds.com

Stephanie Creed

Senior Associate

+44 207 4156 677
stephanie.creed@twobirds.com

Jeannette Tam

Senior Managing Associate

+852 2248 6089
jeannette.tam@twobirds.com

Emma Drake

Legal Director

+44 207 4156 728
emma.drake@twobirds.com

Alex Jameson

Associate

+44 207 8507 139
alex.jameson@twobirds.com

Thank you

twobirds.com

• Abu Dhabi • Amsterdam • Beijing • Bratislava • Brussels • Budapest • Casablanca
• Copenhagen • Dubai • Dusseldorf • Frankfurt • The Hague • Hamburg • Helsinki
• Hong Kong • London • Luxembourg • Lyon • Madrid • Milan • Munich • Paris • Prague
• Rome • San Francisco • Shanghai • Singapore • Stockholm • Sydney • Warsaw

The information given in this document concerning technical legal or professional subject matter is for guidance only and does not constitute legal or professional advice. Always consult a suitably qualified lawyer on any specific legal problem or matter. Bird & Bird assumes no responsibility for such information contained in this document and disclaims all liability in respect of such information.

This document is confidential. Bird & Bird is, unless otherwise stated, the owner of copyright of this document and its contents. **No** part of this document may be published, distributed, extracted, re-utilised, or reproduced in any material form.

Bird & Bird is an international legal practice comprising Bird & Bird LLP and its affiliated and associated businesses.

Bird & Bird LLP is a limited liability partnership, registered in England and Wales with registered number OC340318 and is authorised and regulated by the Solicitors Regulation Authority. Its registered office and principal place of business is at 12 New Fetter Lane, London EC4A 1JP. A list of members of Bird & Bird LLP and of any non-members who are designated as partners, and of their respective professional qualifications, is open to inspection at that address.