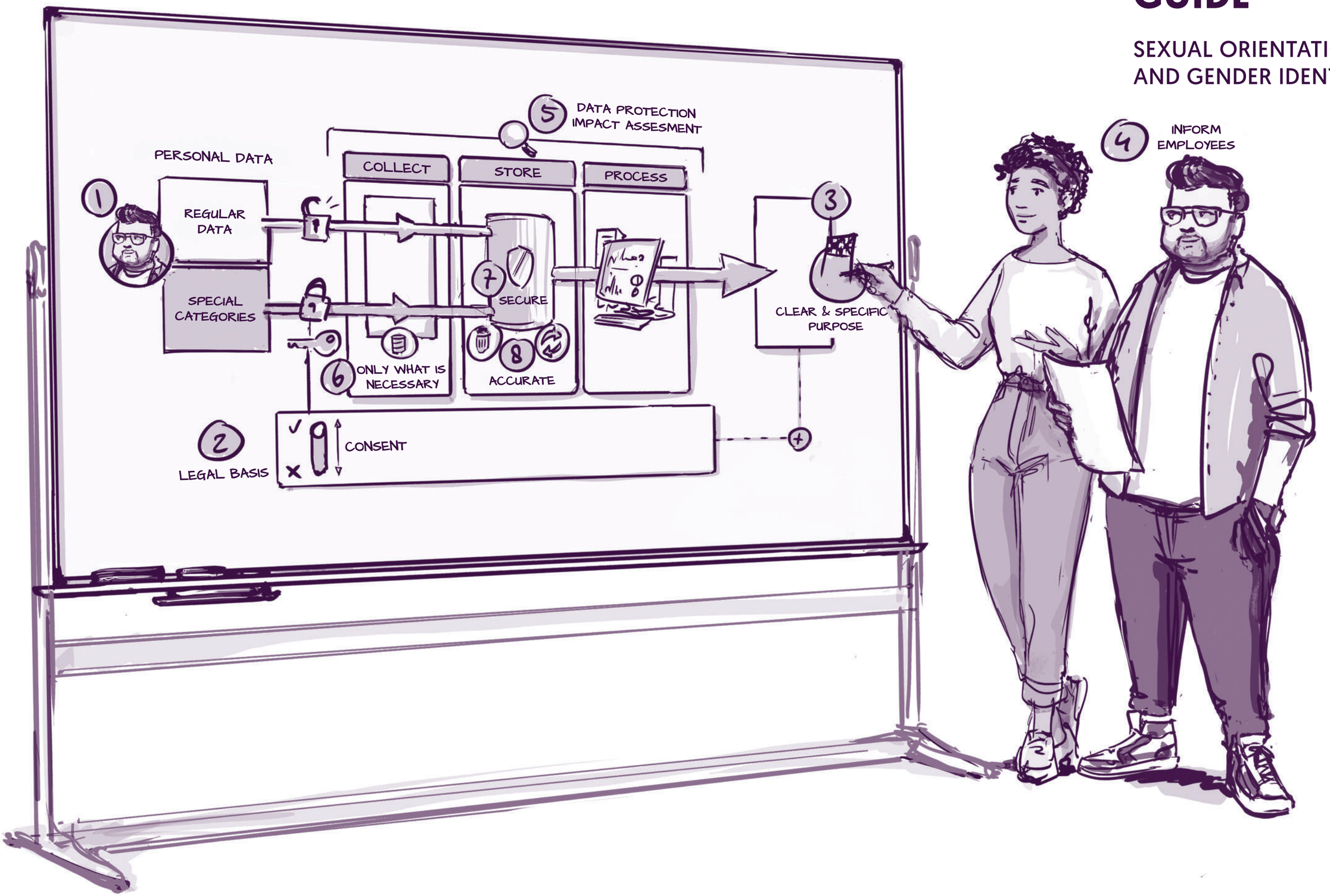
PRIVACY AND D&I POLICY GUIDE

SEXUAL ORIENTATION AND GENDER IDENTITY



PRIVACY AND D&I POLICY GUIDE

SEXUAL ORIENTATION AND GENDER IDENTITY

Information about employees' sexual orientation and gender identity is important for monitoring potential inequality at work and in developing and assessing diversity and inclusion policy.

For example, employees can be asked to register this information voluntarily in order to chart how diverse the organisation is or to determine whether efforts to improve inclusion among all employee groups have been equally effective.

At the same time, it is important to handle sensitive information about employees with care. Information about a person's sexual orientation or gender identity is personal data and subject to the General Data Protection Regulation (GDPR) and national implementation acts. This legislation is intended to protect people's privacy. When collecting and using any such data, your organisation must adhere to this privacy legislation.

A data protection officer or privacy lawyer can provide you with assistance if your organisation wishes to request and use information about employees' sexual orientation and gender identity. This document gives D&I officers an overview of the most important rules to follow in order to avoid pitfalls when developing and rolling out diversity and inclusion policy.

1. The difference between 'regular' personal data and 'special' personal data

The GDPR draws a distinction between 'regular' personal data and 'special categories' of personal data. Information about people's sexual orientation and health is in this special category of personal data. In principle, any such data should not be collected or used.[1] An exception is made if the employee has explicitly given consent for the use of the data.[2] However this is on the condition that the employee has been properly informed and knows which data will be used and for what purposes.

1 Art. 9 (1) GDPR
2 Art. 9 (2a) GDPR

The employee must also have freedom of choice in making the decision to provide data. No direct negative or positive consequences are permitted to be attached to the decision of whether or not to provide data.

2. Legal basis for use of personal data

There must always be a legal basis for processing personal data.[3] The bases that the employer is entitled to invoke are listed in the GDPR.[4] The most obvious basis for collecting and using employees' personal data is the consent of the employee.[5] This consent must be given freely.

The latter can be problematic because the employee is in a relationship of authority with the employer. It is important that the employee is not disadvantaged or misses out on an advantage if he or she is unwilling to give consent for the use of data. The employee must be informed in advance about the data being used and how and why the data will be used. In addition, it is important that employees are always able to withdraw their consent.[6] In that case, their data must be deleted insofar as this is possible.

The employer's (or other parties') 'legitimate interest' can also be a basis for processing personal data.[7] Please note, however, that this basis is not applicable for the use of special categories of personal data. In other words: consent must always be requested in order to collect and use data about sexual orientation.

3. Define a clear and specific purpose for the use of employee data

Collecting and using data about sexual orientation and gender identity is permitted for a clear and specific purpose only.[8] The use of data 'for diversity and inclusion purposes' is not sufficiently clear and specific. Collecting data about sexual orientation 'in order to assess how many LGBTIQ+ employees are employed by the organisation' is more clearly and specifically defined. It needs to be explained to employees why it is necessary for the data to be used.

In principle, it is not permitted for employees' data to be used for other purposes than that for which the data were collected.[9] However, statistical research is permitted if the data cannot be traced back to employees.

This can be done by merging or anonymising the data, for example.

3 Art. 5 (1a) GDPR
4 Art. 6 (1) GDPR
5 See Art. 4 (11) GDPR for the definition of the term 'consent'
6 Art. 7 (3) GDPR
7 Art. 6 (1f) GDPR
8 Art. 5 (1b) GDPR
9 Art. 5 (1b) GDPR

4. Inform employees

The employer must provide employees with information about the use of the data. Among other things, employees must know and understand the following:[10]

- The purposes for which the data will be used.
- The types of data that will be collected and how the data will be used. For example: combining collected data with data about employee satisfaction.
- Whether and to what extent the data will be shared with others.
- The employee's rights, such as the right to withdraw consent or to amend or correct data.

The information must be shared with the employee in understandable and clear language before the employee gives consent. This means it is important to communicate effectively and clearly with employees about the use of their data.

5. Data protection impact assessment

It is possible that a so-called 'data protection impact assessment' will need to be carried out.[11] This involves an assessment of the risks of using the data. The measures to be taken in order to limit these risks also need to be determined. This assessment must be carried out before any data are collected or used.

6. Do not collect or use more information than is necessary

It is not permitted to process more data than is necessary for the purposes determined in advance.[12] In other words: do not collect or use any more information from the employee than is necessary. It is also not permitted to store the data for any longer than necessary.[13]

7. Secure the employee data

The information about employees must be stored safely.[14] The more sensitive the data, the more is required of the employer. For example, the data must be encrypted and access to the data restricted as much as possible. When designing systems for storing and processing data, employees' privacy must also be taken into account.[15]

10 See Chapter II, Section 2 GDPR on the information to be provided
11 Art. 35 GDPR
12 Art. 5 (c) GDPR
13 Art. 5 (e) GDPR
14 Art. 5 (1f) GDPR. See also Chapter IV, Section 2 GDPR
15 Art. 25 GDPR

8. Accurate information

If information about sexual orientation and gender identity is being stored and used, it is important that the information is accurate. All employees must be offered an easy way of amending or correcting the stored information. In addition, it is advisable to give employees regular reminders of this option.

Looking for more information?

- Your organisation may have appointed a data protection officer. You can contact this officer if you have any questions or require further information.
- The Dutch Data Protection Authority website offers a reliable source of information: https://autoriteitpersoonsgegevens.nl/en
- SER Diversity at Work (a division of the Social and Economic Council of the Netherlands) offers a general charter document on the processing of personal data for diversity policy. That document (in Dutch) can be found at: https://www.ser.nl/-/media/ser/downloads/thema/diversiteitinbedrijf/publicaties/2021/Charterdocument_meten-is-weten.pdf

Utrecht University

Utrecht Young Academy

Workplace Pride — THE INTERNATIONAL PLATFORM FOR LGBTIQ+ INCLUSION AT WORK

About this document

The information in this guide is not intended as legal advice, but as assistance for D&I officers and HR professionals when dealing with the legal data protection requirements for the use of employees' data.

This document was compiled by Stefan Kulk, Marthe van der Velde, Jojanneke van der Toorn and Martine Veldhuizen as part of the P.INC project sponsored by the Utrecht Young Academy and in collaboration with Workplace Pride.

https://www.uu.nl/en/research/utrecht-young-academy/projects/privacy-and-inclusion