This document contains a brief explanation of the twelve fair information principles underpinning the EU General Data Protection Regulation (GDPR).[1]

1. Lawfulness

Any processing of personal data must be lawful. This principle carries two requirements. First, the processing of data must rest on one of the bases stated in the GDPR. Second, the processing of data must of course also comply with other legislation, such as the Constitution (*Grondwet*), the Equal Treatment Act (*Algemene wet gelijke behandeling*), and the Criminal Code (*Wetboek van Strafrecht*).

2. Fairness

Any processing of personal data must be fair. Examples of unfair processing include commercial practices that mislead consumers and terms and conditions that stipulate consumer consent to all manner of things which consumers need not reasonably expect to consent to.

3. Purpose specificity

Any processing of personal data must serve a specific purpose. This principle carries three requirements. First, a purpose must be determined before any personal data are (to be) collected. Determining a purpose after personal data have been collected is not allowed. Second, the purpose must have been explicitly documented to ensure that the compatibility of the processing with the original purpose can subsequently be easily verified. Third, the purpose must be specific. For many organizations this is a pitfall, because they have formulated their purposes in words that are far too broad and general, such as 'customer interaction', 'product improvement', 'innovation', and 'advertising purposes'. As these purposes are too broad, they are deemed unlawful.

4. Purpose limitation

Personal data must in principle only be processed for the specified purpose; using collected personal data for any new purpose is not allowed, unless it is a similar purpose.

5. Data minimization

In principle the fewer personal data are collected, the better. The GDPR data minimization principle ultimately rests on the general necessity requirement and the principle of subsidiarity. Put simply, collecting personal data must not go beyond what is strictly necessary to achieve the specified purpose(s).

6. Accuracy

The collected personal data must be accurate. In other words, collecting personal data requires carefully designing a research methodology as well as setting up safeguards for a sound data collection; arbitrarily collecting data about people and drawing some random conclusions is out of bounds. This principle has

[1] This document is an English translation of a Dutch-language explanatory document consisting almost exclusively of texts (excerpts) taken from a draft version of Bart van der Sloot's 2018 book *De Algemene Verordening Gegevensbescherming in gewonemensentaal* (The General Data Protection Regulation in plain language). Van der Sloot has given Tilburg University permission to compile these materials in an explanatory document, to translate that document into English, and to publish that document and this English translation on Tilburg University's website.

been incorporated into the GDPR to ensure that collected personal data are processed and analyzed accurately and that ensuing decisions are adequate and fair. For example, no one should suffer adverse effects of incorrectly registered data.

7. Up to date

If collected personal data are retained for a longer period, they must be kept up to date. For normal databases an annual data update will often do, but high-impact decisions and sensitive data sets require a higher update frequency, for example every month. When updating data and before taking specific decisions based on these data regarding a specific person or small group of persons, it is wise to ascertain in each individual case if the step-by-step process has been carefully followed throughout.

8. Erasure or anonymization of unnecessary personal data

If the collected personal data are no longer needed, for example because the purpose for which they were collected has been achieved, they must in principle be erased or fully anonymized. The advantage of anonymizing data sets over erasing them is that they can then still be used for general statistical analysis.

9. Storage limitation: archiving or research

Personal data that are no longer necessary for the purpose for which they were collected may only be retained if such retention serves the purpose of complying with a legal obligation, such as the duty to allow the tax authorities to inspect financial records, for the purposes of historical, scientific, or statistical research, or for complying with an obligation to archive data. Research and statistical analysis here relates to scientific and medical research; the GDPR in this regard mentions clinical trials, public health research, and research that aims to increase social knowledge.

10. Technical security

If collected personal data are stored, for example in a database, register, or filing system, technical security measures must be taken. These include:

- Encryption. Make sure that hackers cannot gain unauthorized access to databases: securely encrypt all personal data and issue alerts as soon as attempts at unauthorized access are detected.
- Automatic blocking. Make sure that if an incorrect password is entered three times, the device used to attempt access to a database is automatically blocked. When processing sensitive personal data, the default blocking response is preferably set to one incorrect password entry. The person(s) whose credentials may have been compromised must be alerted immediately.
- Raising awareness. Make sure that staff and external contacts are warned about the danger hackers pose. It is a well-known fact that many clients and staff, despite repeated warnings, are duped by fake emails that request the addressee(s) to confirm or change passwords.
- Compartmentalization. Make sure that within the organization personal data are stored in several segregated databases that run on different servers on different locations and that use different security tools. This may help prevent hackers from gaining unauthorized access to full data sets.

- Barriers. If despite all precautions something does go wrong, make sure barriers are in place that make it impossible or difficult to, for example, copy or download the entire database.
- Notification. If despite all precautions something does go wrong, make sure the incident is duly reported.

11. Organizational security

If collected personal data are stored, for example in a database, register, or filing system, organizational security measures must be taken to ensure that the only people within the organization to have access to these data are those whose access is necessary in relation to the purpose(s) for which the data were collected. These measures include:

- Authentication. Make sure that personal data, files, and databases can only be accessed by means of a personal code.
- Restriction. Make sure that authentication and access rights are only granted to people within the organization whose access is genuinely necessary. As a matter of principle, the more sensitive the personal data and the larger the data set, the fewer people have access.
- Logging. Keep track of the people within the organization who have been given access to personal data. On accessing a database, these people ideally also specify why they are doing so, but at the very least they should be able to explain why they have accessed a database when asked.
- Automatic logout. Another security measure is configuring computers to automatically log out after several minutes of user inactivity.
- Clean desk. Clean-desk policies are widely used. After office hours all documents that have not been locked away are shredded or stored to prevent sensitive information from lying around.
- Physical security. Lock rooms and special-purpose areas.

12. Transparency

One of the cornerstones of the GDPR is transparency – or openness – about processing personal data within organizations. All information must be provided free of charge and communicated in clear and understandable language. The transparency organizations must offer is of three types:

1. General transparency;
2. Information to data subjects;
3. Notification of security breaches.