Awareness raising campaign for SMEs

Quick Guide to the Principles of Data Protection

Co-funded by the Rights, Equality and Citizenship Programme of the European Union (2014-2020)

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S RIGHTS, EQUALITY AND CITIZENSHIP 2014-2019 PROGRAMME UNDER GRANT AGREEMENT N°874524.

An Coimisiún um Chosaint Sonraí
Data Protection Commission

Croatian Personal Data Protection Agency
azop
Agencija za zaštitu osobnih podataka

VUB VRIJE UNIVERSITEIT BRUSSEL

Quick Guide to the Principles of Data Protection

Principles – broad rules about conduct or desired outcomes – are an important part of data protection law, and are, in fact, at the core of the General Data Protection Regulation (GDPR). Whilst various principles can be found throughout the GDPR, Article 5 GDPR in particular sets out seven key principles related to the processing of personal data, which SMEs (an SME is a data controller as it decides how and why data are processed) need to be aware of and comply with when collecting and otherwise processing personal data:

- Lawfulness, fairness, and transparency;
- Purpose limitation;
- Data minimisation;
- Accuracy;
- Storage limitation;
- Integrity and confidentiality; and
- Accountability.

These principles are found right at the outset of the GDPR, and inform and permeate all other provisions of that legislation. They should be understood as the fundamental overarching principles which aim to ensure compliance with the spirit of data protection law and the protection of the rights of individuals ('data subjects').

The Recitals of the GDPR itself note that many of these principles are not entirely new, and that the principles found in the previous Data Protection Directive (95/46/EC) have largely been carried over or built upon. There are also other related rules and elements of the above principles which are mentioned throughout the GDPR, such as the principles of proportionality and necessity, and the principles of data protection by design and by default. More detail on these elements can be found below.

Compliance with the principles of data protection is the first and perhaps most important step that SMEs can take to ensure they comply with the requirements of the GDPR and data protection law generally; however, SMEs should also consult the provisions of the GDPR which elaborate on how these principles impact specific obligations.

SMEs should note that very similar principles of data protection apply in cases where personal data are processed for 'law enforcement purposes' under the Law Enforcement Directive (LED).

Lawfulness, Fairness, and Transparency

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.

Lawfulness means that any processing of personal data carried out by an SME must have a legal basis under the GDPR, be otherwise compliant with the requirements of the GDPR(see in particular Articles 6, 7, 8, and 9 GDPR), and not involve any otherwise unlawful processing or use of personal data.

Fairness is also a relatively broad principle, which requires that any processing of personal data must be fair towards the individual whose personal data are concerned, and avoid being unduly detrimental, unexpected, misleading, or deceptive.

Transparency is a particularly important principle of data protection within the GDPR, with various related rights and obligations seeking to ensure that processing of personal data is clear and transparent to individuals and regulators. SMEs must provide individuals with information regarding the processing of their personal data in a format that is concise, easily accessible, easy to understand, and in clear and plain language. This should be done before personal data are collected and subsequently whenever changes to the processing operation are made.

Specific rules regarding transparency obligations are found in Articles 12, 13, and 14 GDPR, including details on the specific types of information which must be provided to data subjects, and the manner in which it must be provided. In order to be transparent, SMEs must ensure the means of conveying information is the most appropriate for their platform and target audience. In particular, the principles of fair and transparent processing require that the individual be informed of the existence of the processing operation and its purposes.

Purpose Limitation

Personal data must be collected for specified, explicit and legitimate purposes, which are determined at the time of the collection of the personal data, and not be further processed in a manner that is incompatible with those purposes. However, SMEs may undertake further processing for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, as they are not considered to be incompatible with the initial purposes, where there are sufficient safeguards in place.

Further processing is only appropriate where the new purpose for processing is not incompatible with the original purpose. Whether any subsequent processing could be compatible with the original purpose will depend on any link with the original purpose, the context in which the personal data has been collected, the nature of the personal data, the possible consequences of the intended further processing for individuals, and the existence of appropriate safeguards.

The purpose of this principle is to ensure SMEs are clear and open from the outset about proposed processing of personal data and to ensure that the purposes are in line with individuals' reasonable expectations. Careful consideration of and robust compliance with this principle also assists SMEs with the principles of data minimisation and accountability.

Data Minimisation

This principle requires that SMEs only collect and process personal data that are adequate, relevant, and limited to what is necessary for the purposes for which they are processed. This essentially means that SMEs should collect the minimum amount of data they require for their intended processing operation; they should never collect unnecessary personal data. This principle complements, in particular, the principle of purpose limitation, but also supports compliance with the range of data protection principles.

Implementing data minimisation supports data protection by design and by default, limits the amount of personal data which could be lost or stolen in the event of a personal data breach, assisting with ensuring the integrity and confidentiality of personal data, and it makes it easier for SMEs to ensure that the personal data they hold are accurate and up to date, supporting compliance with the principles of accuracy.

The GDPR does not define what amount of personal data is 'adequate, relevant and limited'. This will have to be assessed by SMEs depending on the circumstances of their intended processing operations. SMEs should also periodically review the amount and nature of personal data which they process, ensuring it remains adequate, relevant, and necessary, including by deleting data which no longer fulfil these criteria.

Accuracy

This principle requires that SMEs ensure personal data are accurate and, where necessary, kept up-to-date. SMEs should take every reasonable step to ensure that personal data which are inaccurate are erased or rectified without delay, having regard to the purposes for which they are processed.

This is a straightforward requirement that all personal data collected, stored, or otherwise processed by an SME must be accurate and up to date. All reasonable steps must be taken to correct any inaccuracies promptly, including considering whether it is necessary to periodically update any personal data an SME holds. As such, SMEs that collect personal data should have clear procedures for correcting or erasing any inaccurate personal data as part of their data management activities.

In general, the reasonable steps SMEs are required to take to ensure the accuracy of personal data will depend on the circumstances and in particular on the nature of the personal data and of the processing. SMEs need to also keep in mind their obligations in relation to data subjects' right to rectification – to have inaccurate personal data rectified, or completed if it is incomplete.

Storage Limitation

SMEs must hold personal data, in a form which permits the identification of individuals, for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods where the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with the GDPR, and as long as there are appropriate technical and organisational measures to safeguard the rights and freedoms of the individual.

SMEs should therefore, in general, delete personal data as soon as it ceases to be necessary for the purposes for which it was originally collected. To this end, the GDPR recommends that time limits should be established by the SME for erasure or for a periodic review. In line with the principle of transparency, SMEs should also ensure that individuals are aware of retention periods or the criteria used to calculate them. SMEs storing personal data offline or in manual form in a filing system, even where digital versions or copies have been deleted, must still have

justifications for retaining this personal data in offline form and respond to data subject requests.

Depending on the circumstances, it may also be appropriate for SMEs to anonymise data once it is no longer necessary that the individual be identified or identifiable. Data are truly anonymous, and therefore no longer 'personal' data, only if the individual is no longer identifiable; however, if data could still be attributed to an individual by the use of additional information it would be only 'pseudonymised' and thus still considered personal data. If the process applied to supposedly anonymise personal data is not permanent and can be reversed, then the data has not been anonymised.

Integrity and Confidentiality

Personal data must be processed by SMEs only in a manner that ensures the appropriate level of security and confidentiality for the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage. To achieve this end, SMEs must utilise appropriate technical or organisational measures.

In other words, SMEs must ensure that their security measures adequately protect against accidental or deliberate harm, loss, or dissemination of the personal data they process. These security measures should cover not only cybersecurity but also physical and organisational security measures. SMEs must also routinely check that their security measures are up-to-date and effective.

The GDPR does not specify the security measures which SMEs should implement, as technological and organisational best practices are constantly evolving. SMEs should consider a range of options to determine the most appropriate measures under the circumstances, as there is no 'one size fits all' approach to data security. Relevant considerations when assessing appropriate measures include, but are not limited to: the principle of data minimisation; the principles of data protection by design and by default; transparency with regard to the functions and processing of personal data, enabling the individual to monitor the data processing; and the pseudonymisation and/or encryption of personal data.

Accountability

The principle of accountability is a new principle of data protection law, which specifically sets out that SMEs are responsible for, and must be able to demonstrate compliance with, the other principles of data protection. This means that SMEs need to ensure they comply with the principles, but also have appropriate processes and records in place to demonstrate compliance.

Compliance with the other principles of data protection will itself assist in accountability, such as by taking a data protection by design and by default approach, implementing appropriate technical and organisational measures, having concise accessible transparency information, and having clear data retention policies. Other measures to demonstrate compliance with the principles of data protection include adopting internal policies, following codes of conduct or certification schemes, recording and, where necessary, reporting personal data breaches, and implementing appropriate privacy policies and notices.

Appointing a data protection officer (DPO), where required, and ensuring that they are properly involved in all issues relating to data protection, maintaining records of processing activities, drafting clear contracts with processors acting on the SMEs 's behalf, and carrying out data protection impact assessments (DPIAs), where appropriate, are just some of the tools which can assist SMEs in complying with the principle of accountability. Obligations under the principle of accountability are ongoing and evolving, and SMEs should continually review and update their accountability measures.