The data protection principles under the General Data Protection Regulation

united-kingdom.taylorwessing.com/globaldatahub/article-the-data-protection-principles-under-the-gdpr.html

November 2016

The new General Data Protection Regulation (GDPR) is, like the Data Protection Directive (DPD), underpinned by a number of data protection principles which drive compliance. While the data protection principles under the GDPR are similar to those found in in the DPD, certain concepts are more fully developed.

Principles relating to processing of personal data (Article 5 GDPR)

Lawfulness, fairness and transparency	Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject
Purpose limitation	Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
Data minimisation	Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
Accuracy	Personal data shall be accurate and, where necessary, kept up to date
Storage limitation	Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
Integrity and confidentiality	Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures
Accountability	The controller shall be responsible for, and be able to demonstrate compliance with the GDPR

Lawfulness, fairness and transparency

The GDPR requires that the data controller provide the data subject with information about his/her personal data processing in a concise, transparent and intelligible manner, which is easily accessible, distinct from other undertakings between the controller and the data subject, using clear and plain language.

Transparency is achieved by keeping the individual informed and this should be done before data is collected and where any subsequent changes are made. It is important to remember that data is not always collected directly from individuals but may be derived from other data sets, observed by tracking or inferred using algorithms. The GDPR has a mandatory list of the information which must be given to individuals where data is obtained directly from them but also where it is obtained indirectly. How you let individuals know about what you are doing will depend both on the method of communication and on the target audience.

The UK's ICO recently updated its Code of Practice on privacy notices, transparency and control in order to assist with compliance under the GDPR. A traditional privacy policy on a website may fit the bill but the more complex the use of the data and the smaller the medium on which information is delivered, the more creative you need to be.

Delivering information in a way which can be understood by the target audience means using appropriate language and branding but it can also involve techniques such as layering of information, directing users to a 'privacy dashboard', using pop ups, tick-boxes and 'just-in-time' notices or icons in order to highlight particular issues. These are needed not only to aid transparency, but also to give the users genuine control and choice, essential to fair processing.

Conversely, pages of small print which the user will never read are much less likely to qualify. The more unusual your use of data or the more risk there is to the individual, the more you have to do to bring it to the user's attention. In this respect, the issues are very similar to those under consumer law.

Purpose limitation

Processing personal data is only permissible if and to the extent that it is compliant with the original purpose for which data was collected. Processing “for another purpose” later on requires further legal permission or consent. The only exception to this requirement is where the “other purpose” is “compatible” with the original purpose. Indications for this will be 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 data subjects or the existence of appropriate safeguards.

Data minimisation

Data controllers shall ensure that only personal data which is necessary for each specific purpose is processed (in terms of the amount of personal data collected, the extent of the processing, the period of storage and accessibility). Under the GDPR, data must be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed". This links back to the purpose limitation. Controllers need to make sure that they collect enough data to achieve their purpose but not more than needed.

Accuracy

Personal data must be accurate and kept up to date – this will be familiar from the DPD. Inaccurate or outdated data should be deleted or amended and data controllers are required to take "every reasonable step" to comply with this principle.

Storage limitation

Once you no longer need personal data for the purpose for which it was collected, you should delete it unless you have other grounds for retaining it. This means there should be a regular review process in place with methodical cleansing of databases.

Integrity and confidentiality

Under the GDPR, like the DPD, personal data must be protected against unauthorised access using appropriate organisational and technical measures. This goes to the heart of protecting the privacy of individuals. Data controllers and processors need to assess risk, implement appropriate security for the data concerned and, crucially, check on a regular basis that it is up to date and working effectively. There are strict breach reporting provisions in the GDPR. High profile data breaches can cause significant embarrassment and expense for businesses. TalkTalk was recently fined a record £400,000 for failing to keep data secure and this amount will look paltry once the new sanctions under the GDPR apply, under which fines for data breaches will be up to 2% of annual global turnover or 10m Euros, whichever is higher.

Accountability

The final principle under the GDPR states that data controllers must be able to demonstrate compliance with the other principles. This is a short sentence with major implications. One of the notable changes under the GDPR

compared with the DPD, is the increased compliance burden, much of which is sparked by the accountability principle. It is not enough to comply, you have to be seen to be complying. The range of processes that organisations have to put in place to demonstrate compliance will vary depending on the complexity of the processing but may include:

- assessing current practice and developing a data privacy governance structure which may include appointing a Data Protection Officer;
- creating a personal data inventory;
- implementing appropriate privacy notices;
- obtaining appropriate consents;
- using appropriate organisation and technical measures to ensure compliance with the data protection principles;
- using Privacy Impact Assessments; and
- creating a breach reporting mechanism.

Read more on key compliance issues.

If you have any questions on this article or would like to propose a subject to be addressed by the Global Data Hub please contact us.