CHAPTER 4: SIX DATA PROTECTION PRINCIPLES

The Regulation stipulates that infringements of "the basic principles for processing, including conditions for consent" are subject to the highest possible administrative fines – up to €20,000,000 or 4% of global annual turnover, whichever is higher. If any detail can get the attention of the people who need to understand this, it's likely that potential fines of that scale will do the job.

The GDPR lays down a set of data protection principles to guide how organisations manage personal data. The principles can be seen as an overview of your most important duties in complying with the Regulation, and anyone reading the Regulation should keep them in mind when interpreting other requirements.

The six data protection principles can be found in Article 5 of the Regulation and are as follows:

1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Data minimisation
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality

For organisations already complying with relevant legislation based on the Data Protection Directive (DPD)[66], these principles will doubtless look familiar. Although the principles are the direct successors of those outlined in the DPD, the Regulation notes that "the objectives and principles of [the Data Protection Directive] remain sound, but it has not prevented fragmentation in the implementation of data protection across the Union, legal uncertainty or a widespread public perception that there are significant risks to the protection of natural persons, in particular with regard to online activity"[67]. Because of this, organisations should have two primary concerns when ensuring they comply with the principles:

1. Understanding the full scope of the principles under the GDPR.
2. Ensuring that any distinctions between the previous principles and the new ones are identified and understood.

In the first instance, organisations need to appreciate that the scope of the GDPR is not the scope of the DPD. The Regulation applies more broadly and has a different scope from the laws that were developed in response to the DPD. (See Chapter 1 for a discussion of the GDPR's scope and that of the privacy compliance framework.)

[66] This would include laws such as the UK's Data Protection Act, Germany's Bundesdatenschutzgesetz, France's Loi informatique et libertés, and so on.

[67] GDPR, Recital 9.

In the second instance, organisations need to take care that their compliance programmes are sufficiently updated. Too often updating compliance programmes results in little change; people are set in their habits, they assume the current practices are still "good enough", and the people interpreting the Regulation may suffer from "fatigue of repetition" and miss salient points.

Principle 1: Lawfulness, fairness and transparency

The three components of this principle are clearly linked: the data subject must be told what processing will occur (transparent), the processing must match this description (fair), and the processing must be for one of the purposes specified in the Regulation (lawful). The data subject should also be "informed of the existence of the processing operation"[68].

Fairness

Drawing on existing practice, "Fairness" requires that the controller:

- Is open and honest about its identity;
- Obtains data from someone who is legally authorised/required to provide it;
- Only handles data in ways the data subject would reasonably expect;

[68] GDPR, Recital 60.

- Does not use the data in ways that might unjustifiably have a negative effect on them.

Transparency

"Transparency" requires the data controller to tell people clearly and openly how (unless it is obvious) they intend to use any personal data that has been collected. These two are regularly linked in the Regulation, most notably in the statement that "the principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and its purposes"[69]. The UK's ICO offers a relevant example of fair and transparent processing:

When an individual enters into a mobile phone contract, they know the mobile phone company will keep their name and address details for billing purposes. This does not need to be spelt out. However, if the company wants to use the information for another purpose, perhaps to enable a sister company to make holiday offers, then this would not be obvious to the individual customer and should be explained to them.[70]

[69] GDPR, Recital 60.

[70] *https://ico.org.uk/for-organisations/guide-to-data-protection/principle-1-fair-and-lawful/*.

Lawfulness

The final component of this first data protection principle, "lawfulness", describes processing that meets one of the tests set out in Article 6. This is a complex area and most organisations are likely to need specific legal advice in respect to the lawful basis on which they are processing data. Remember that, if there is no lawful basis, then by definition the processing will be illegal.

> Processing shall be lawful only if and to the extent that at least one of the following applies:
>
> (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
> (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
> (c) processing is necessary for compliance with a legal obligation to which the controller is subject;
> (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
> (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
> (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are

> overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.
>
> Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

Note that this only requires *one* of the conditions to have been met for the processing to be lawful. The Regulation makes it clear that lawfulness "does not necessarily require a legislative act adopted by a parliament", but that "such a legal basis or legislative measure should be clear and precise and its application should be foreseeable to persons subject to it"[71]. Organisations that process personal data in the public interest or as a public authority must ensure that the processing has "a basis in Union or Member State law"[72].

Point (a) – that the data subject has given consent to the processing of his or her personal data for one or more specific purposes – means that the data subject cannot reasonably be expected to consent without being in possession of the facts, nor can those facts be implicit (such as in fulfilment of a contract or compliance with a law). This is consistent with the Regulation's statement in Recital 50 that:

---

[71] GDPR, Recital 41.

[72] GDPR, Recital 45.

> The processing of personal data for purposes other than those for which the personal data were originally collected should be allowed only where the processing is compatible with the purposes for which the personal data were originally collected. In such a case, no legal basis separate from that which allowed the collection of the personal data is required.[73]

In Chapter 10 we deal, at some length, with the practical issues around consent. In short, consent should not necessarily be the first option selected to be the basis of lawful processing. The test for consent is relatively high: consent "*must be freely given, specific, informed and unambiguous indication of the data subject's wishes in which he or she by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.*"

"Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment."[74]

"Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations."[75]

These tests mean that employers are unlikely to be able to rely on consent in relation to the processing of most personal

[73] GDPR, Recital 50.

[74] GDPR Recital 42

[75] GDPR Recital 43

data relating to their employees. Any such consent would be invalid and the processing would therefore be unlawful.

Consent is accompanied by the right to withdraw consent, and by the rights of rectification and data portability. There may be circumstances in which organisations therefore wish to identify alternative lawful bases for processing, and these come from the other options set out in Article 6.

Organisations should use privacy notices and terms and conditions to give relevant context and transparency, provided that these are clear and accessible. The Regulation explicitly states that "the principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used"[76]. Simply including a link to detailed terms and conditions may not be adequate.

Clause 4 of Article 6 applies additional requirements for determining whether personal data can be processed without the data subject's consent. This essentially balances transparency (the data subject's knowledge of the processing) with lawfulness (providing exemptions for valid purposes) by applying a doctrine of fairness.

Where consent has not been gained for the specific processing in question, the organisation must address additional conditions to determine the fairness and

[76] GDPR, Recital 58.

transparency of the processing. These conditions include, but are not limited to, the below[77]:

(a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
(b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;
(d) the possible consequences of the intended further processing for data subjects;
(e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

While such safeguards may make processing more onerous, expensive or difficult, you should always consider a minimum level of security for personal data. Decisions on this matter should result from risk assessments and data protection impact assessments (DPIAs), which are discussed in Part 2 of this manual.

When processing data without consent, the organisation should determine further considerations appropriate to the

[77] GDPR, Article 6, Clause 4.

processing, including the types of personal data involved, the specific reasons that consent is not available, and so on. The UK's ICO provides the following example:

> Personal data will be obtained fairly by the tax authorities if it is obtained from an employer who is under a legal duty to provide details of an employee's pay, whether or not the employee consents to, or is aware of, this.[78]

In this instance, the personal data has been acquired without consent and without the subject being aware. However, this is wholly fair and legal because it is entirely reasonable for an employer to facilitate people paying their taxes.

Processing personal data without consent is also allowable under specific or extraordinary conditions, such as when national security or the protection of other data subjects is relevant to the processing[79].

Demonstrating that processing of personal data is lawful, fair and transparent will not be simple for many organisations. Your first consideration, however, should be to clearly document how you describe your processing when the data subject offers consent. Assuming you then do exactly as you say – and can prove it – and you are not in contravention of any other requirements of the GDPR or other laws, you should be confident that your processing is lawful, fair and transparent.

---

[78] *https://ico.org.uk/for-organisations/guide-to-data-protection/principle-1-fair-and-lawful/.*

[79] GDPR, Article 23, Clause 1.

The supervisory authority might offer relevant information about the sort of proof they require to demonstrate compliance[80] but you shouldn't rely on this; you have an obligation to keep appropriate records and evidence.

Principle 2: Purpose limitation

The Regulation states that personal data can only be collected for "specified, explicit and legitimate purposes"[81]. That is, to comply with the purpose limitation principle, you must define up front what the data will be used for and limit the processing to only what is necessary to meet that purpose.

Privacy notices, terms and conditions, and consent forms should provide the data subject with unambiguous information about the extent of processing involved. These public statements should be reflected in the actual processing and the documentation of that processing.

For instance, many supermarkets collect personal information so that they can provide customers with targeted offers that match up with their usual spending habits. It would be a breach of this principle for those supermarkets to then hand this data to a sister company that sells holidays, as this is beyond the scope of the purpose for which the data was collected.

[80] The UK's ICO, for instance, has a number of articles and tools for determining whether your organisation complies with the law, as well as guidance on the implementation of the law. Cf. *https://ico.org.uk/for-organisations/guide-to-data-protection/*.

[81] GDPR, Article 5, Clause 1 (b).

The Regulation does permit some further processing "for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes" [82]. Safeguards for processing this sort of information are laid out in Article 89, and you will need to examine both technical and organisational options in order to become compliant. Pseudonymisation and encryption, for instance, would be valid measures, as would restricting access to such information on the basis of role and the requirements of a given set of procedures.

Principle 3: Data minimisation

The Regulation states that personal data you collect and/or process should be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed"[83]. This means that you should hold no more data beyond what is strictly required. After all, it is difficult to lose information that you don't have.

Some organisations are more prone to carrying excess information than others, particularly those in the healthcare industry or the financial services sector. The UK's ICO offers this example:

> A recruitment agency places workers in a variety of jobs. It sends applicants a general questionnaire, which includes specific questions about health conditions that are only relevant to particular manual occupations. It

[82] GDPR, Article 5, Clause 1 (b).

[83] GDPR, Article 5, Clause 1 (c).

> would be irrelevant and excessive to obtain such information from an individual who was applying for an office job[84].

In this instance, the purpose for processing is to ensure that the applicant is placed into an appropriate role for which they are qualified. As the indicated medical conditions are not relevant to office jobs, there is no need to collect this information, and the principle of data minimisation says that it should not be collected or processed.

Complying with this data protection principle will be facilitated by data mapping, which is discussed in Chapter 7 of this manual, and by review of your procedures. Ensuring you know how data is used is critical to minimising the data that you collect and process, and should be integrated into the way your organisation works as part of a privacy-by-design approach[85].

Data minimisation should also be taken into account in agreements with suppliers and data processors. This may include stripping out certain data before passing information over for external processing, and then reattaching the data when it returns from the processor. Ensuring that data minimisation is accounted for in supplier agreements and binding corporate rules should be included in procurement and supply procedures.

[84] *https://ico.org.uk/for-organisations/guide-to-data-protection/principle-3-adequacy*

[85] GDPR, Article 25.

Principle 4: Accuracy

The Regulation requires personal data to be "accurate and, where necessary, kept up to date"[86]. Besides being good practice for any business, this protects the data subject from a number of threats, such as identity theft. It also ensures that any automated profiling decisions made regarding the data subject use accurate data.

The Regulation clearly aims to regulate when, how and under what conditions profiling can be conducted[87]. If your organisation indulges in profiling of any kind – and especially if there are material impacts for the data subject – you need to ensure that you have processes in place to keep all personal data accurate and up to date.

The corollary to this principle is the data subject's right to rectification. This grants the data subject the right to "rectification of inaccurate personal data" and "the right to have incomplete personal data completed"[88]. You should ensure not only that personal data is accurate, but also that you have a process by which data subjects can request correction or completion of their personal data. This could be linked to whatever method you use to provide data

[86] GDPR, Article 5, Clause 1 (d).

[87] Recital 71 of the Regulation makes this abundantly clear: "The data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention".

[88] GDPR, Article 16.

subjects' access to their data (which will be covered more fully in Chapter 11).

Maintaining personal data to ensure accuracy should be built into your regular processes. For instance, in a monthly process to archive redundant data, you could include steps to identify out-of-date or incorrect data, which then automates sending the data subject a request to provide accurate information. Alternatively – and more simply, perhaps – regular emails to data subjects could include the request that they log in to check and update any information. Other types of information or organisations in different relationships with the data subjects may require different solutions with potentially greater complexity.

It is not necessary to correct some forms of inaccuracy. For instance, if a customer places an order with an organisation and that order is fulfilled, it is not necessary to maintain an accurate record of the customer's address unless the customer makes other orders, in which case the order process should ensure that the address is accurate.

Other forms of inaccuracy may be valuable to retain. The ICO's *Guide to data protection* provides this example:

> A mis-diagnosis of a medical condition continues to be held as part of a patient's medical records even after the diagnosis because it is relevant for the purpose of explaining treatment given to the patient, or to additional health problems.[89]

[89] *https://ico.org.uk/for-organisations/guide-to-data-protection/principle-4-accuracy/*.

In this case, the original error is corrected (replacing the misdiagnosis with the correct diagnosis) but the record of the misdiagnosis is retained because it is information for the data subject's benefit.

Principle 5: Storage limitation

The Regulation requires that personal data is "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"[90]. The phrase "kept in a form" refers not to the medium on which it is stored (although that may be a factor) but to the way it is stored; whether, for instance, it is encrypted or split into separate databases to prevent identification of the data subject.

In simpler terms: if you no longer need the data, get rid of it. As you should be defining a purpose for all data collection, it should be quite simple to determine when the data is no longer required. Some organisations, however, may need to retain personal data for long-term purposes with intermittent processing – in healthcare, for instance – and in such cases summarily deleting data may not be possible.

Pseudonymisation – splitting personal data into sets that do not individually permit identification of the data subject – is one solution to secure storage of personal data, but presents its own issues with regard to usability. If that personal data

[90] GDPR, Article 5, Clause 1 (e).

must be regularly processed, the time spent reversing the pseudonymisation may be onerous or represent a poor ROI.

Wherever possible, it will be preferable to simply delete or destroy all personal data immediately following processing, and this will save having to implement additional measures.

Your approach to storage limitation should be enshrined in a data retention policy and supporting procedures. This must take into account legal and contractual requirements for retention periods – both minimum and maximum – and then trigger a process by which data is either securely disposed of or secured at the end of this period.

Many organisations approach the GDPR with substantial quantities of old personal records. Unless there is a lawful basis for continuing to process this data, organisations should make arrangements to delete them (and to do so securely) as soon as possible. Remember that storing and archiving of data falls within the definition of processing and, therefore, any data subject access request can legitimately require copies of stored, archived or backed-up data. Seek guidance from local supervisory authorities as to available options for demonstrating that archived digital data is not actually still being processed.

Principle 6: Integrity and confidentiality

This principle is perhaps the most important from a financial perspective. While breaches of the other data protection principles can be damaging to data subjects, the impact is usually limited. Breaches of this principle, however, tend to result in data breaches, which make it very easy for supervisory authorities to prove that data has not been held

securely – the fact that a data breach has occurred is compelling evidence in itself.

This final principle requires organisations to process personal data "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"[91].

In the parlance of information security, confidentiality is the "property that information is not made available or disclosed to unauthorized individuals, entities, or processes"[92]. This means that personal data must be classified as confidential even within the organisation, as it is extremely unlikely that every single person in the organisation needs to have access to personal data. In many cases, there may be no requirement for anyone to access personal data.

Integrity is the "property of accuracy and completeness"[93]. This clearly links to Principle 4 and is necessary for the same reasons: the data subject should not be jeopardised by inaccurate information. This also includes ensuring that personal data is correctly linked – such as keeping the correct address associated with the data subject – and making sure that data is not corrupted over time or by poor storage practices.

Meeting requirements for integrity and confidentiality are, mercifully, quite straightforward. Assuming you follow the

[91] GDPR, Article 5, Clause 1 (f).

[92] ISO/IEC 27000:2016, Clause 2.12.

[93] ISO/IEC 27000:2016, Clause 2.40.

advice of this manual, you will implement an information security solution such as an ISO 27001 information security management system to protect the confidentiality, integrity and availability of your organisation's information assets.

These processes and frameworks will naturally link up with any necessary DPIAs or risk assessment activity (see Part 2 of this manual) in order to identify the critical risks to personal data and other sensitive information.

Accountability and compliance

Clause 2 of Article 5 is brief but extremely important:

> The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

This is a sort of 'seventh' principle, which asserts that the data controller is responsible for ensuring compliance with the previous six data protection principles and for being able to demonstrate this compliance. As such, the data controller needs to ensure that the data protection principles are met wherever the personal data goes: external processors and internal organisations/divisions must be required by contract and binding corporate rules to adhere to the data protection principles. There should be additional processes built into third party service agreements to demonstrate that the personal data is processed in compliance with these principles at every stage.

Failure to ensure that your suppliers meet the requirements of the principles can have a considerable impact. Even under the UK's DPA, which is often seen as lacking teeth, the ICO has levied notable fines. For instance, in November 2015, the ICO fined the Crown Prosecution Service £200,000 after

laptops storing police interviews were stolen from a private film studio. This was obviously bad for the film studio's business, but financially and reputationally worse for the Crown Prosecution Service.

Embedding accountability into your organisation if you are the data controller may be difficult: you are asking your employees to be accountable for the suppliers' actions. Building a corporate culture that believes in the virtue of data protection, and in which responsibility and accountability are corporate values, will often be the difference between success and failure. An employee who feels they have ownership of the corporate relationship with the processor, or a duty to protect the information in question, should be encouraged to feel it a matter of professional pride to ensure personal data is protected.

A culture of accountability must be fed from the top down. It is very simple for an employee to feel no sense of responsibility if senior managers and the compliance manager don't show the same level of dedication. Training and staff awareness programmes should be developed to ensure that all staff understand their various duties and responsibilities in relation to privacy and data protection.

The GDPR makes explicit provision for codes of conduct. The expectation is that, over the course of the next few years, trade associations and representative bodies will prepare codes of conduct that are then put forward for approval, registration and publication by a national supervisory authority, or, where processing activities take place across Member States, by the European Data Protection Board. It is possible that the EU Commission may then declare one or more of the codes recommended by EDPB to have general validity within the EU. Codes may be approved in relation to

a wide range of topics and adherence to codes will, like implementation of and compliance with national or international management system standards, help controllers and processors demonstrate compliance with their GDPR obligations. Compliance with such codes will, of course, be subject to monitoring, carried out by suitably qualified and accredited bodies. Controllers and processors who are found to have infringed a relevant code may be blocked from claiming compliance with the code and reported to the relevant supervisory authority.

The UK's ICO recommends that codes of conduct should cover:

- fair and transparent processing;
- legitimate interests pursued by controllers in specific contexts;
- the collection of personal data;
- the pseudonymisation of personal data;
- the information provided to individuals and the exercise of individuals' rights;
- the information provided to and the protection of children (including mechanisms for obtaining parental consent);
- technical and organisational measures, including data protection by design and by default and security measures;
- breach notification;
- data transfers outside the EU, or;
- dispute resolution procedures.

There is nothing stopping an organisation adopting its own code of conduct immediately and then adapting and

improving it once more formal codes appear in the market place. A code of conduct is a solid starting point to inculcate a culture of accountability. It depends on the exact nature of your business, its third-party suppliers and the industry in which you work, but a holistic approach is necessary to ensure the six data protection principles of the GDPR are understood and implemented across the organisation.

Of course, a good starting point is simply that: a starting point. In practice, organisations should establish a full suite of policies and procedures to ensure and demonstrate compliance with the Regulation and other relevant laws. This might include documentation around governance, management structures, roles and responsibilities, risk management, training and awareness, records management, physical and logical safeguards, data sharing agreements, or compliance and assurance programmes. In other words, an organisation will need to demonstrate it has records to prove that it is doing what it says it is. These are necessary to show that the principles and associated behaviours are fully embedded in the business.

Part 2: Data protection impact assessments and risk management