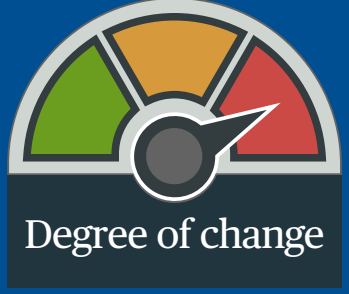
# Data governance obligations

## At a glance

- The GDPR requires all organisations to implement a wide range of measures to reduce the risk of their breaching the GDPR and to prove that they take data governance seriously.
- These include accountability measures such as: Privacy Impact Assessments, audits, policy reviews, activity records and (potentially) appointing a Data Protection Officer a ("DPO").
- For those organisations which have not previously designated responsibility and budget for data protection compliance these requirements will impose a heavy burden.




## To do list

| | |
|---|---|
| ☐ | Assign responsibility and budget for data protection compliance within your organisation. Whether or not you decide to appoint a DPO (or have to) the GDPR's long list of data governance measures necessitates ownership for their adoption being allocated. |
| ☐ | Be clear as to whether those to whom you have designated responsibility are a DPO (for GDPR purposes) or not, given the conflict of interest rules and protected employment status which will apply to DPOs under the GDPR. |
| ☐ | Consider reporting lines –supervisory authorities will expect a line direct to the board – and the job specification for those designated with data protection responsibilities. |
| ☐ | Ensure that a full compliance program is designed for your organisation incorporating features such as: PIAs, regular audits, HR policy reviews and updates and training and awareness raising programs. |
| ☐ | Audit existing supplier arrangements and update template RFP and procurement contracts to reflect the GDPR's data processor obligations. |
| ☐ | Monitor the publication of supervisory authorities / EU and industry published supplier terms and codes of practice to see if they are suitable for use by your organisation. If you are a supplier, consider the impact of the GDPR's provisions on your cost structure and responsibility for signing off the legality of your customer's activities. |
| ☐ | Implement measures to prepare records of your organisation's processing activities. If you are a supplier develop your strategy for dealing with customer requests for assisting with the development of such records. |

*The GDPR enshrines a number of "data governance" concepts the virtues of which law makers and supervisory authorities have extolled for some time. These concepts will create significant new operational obligations and costs for many public and private sector organisations.*

*A general obligation is imposed upon controllers to adopt technical and organisational measures to meet their GDPR obligations (and to be able to demonstrate that they have done so.) Operating a regular audit program, plus the other measures detailed below (PIAs in particular), seem likely to be regarded in a favourable light by supervisory authorities in their enforcement of the obligations of the GDPR.*

*Key obligations include the following:*

# Privacy by design

Organisations must implement technical and organisational measures to show that they have considered and integrated data compliance measures into their data processing activities.

Adopting appropriate staff policies is specifically mentioned, as is the use of pseudonymisation (to ensure compliance with data minimisation obligations).

# Privacy Impact Assessments (PIAs)

A Data Protection Impact Assessment, also known as a PIA, is an assessment to identify and minimise non-compliance risks. The concept is not a new one - current regulator guidance recommends their use and Bird & Bird has run PIAs for a number of its clients - but the GDPR formalises a requirement for PIAs to be run.

Specifically, controllers must ensure that a PIA has been run on any *"high risk"* processing activity before it is commenced – measured by reference to the risk of infringing a natural person's rights and freedoms.

High risk processing encompasses (i) systematic and extensive processing activities, including profiling and where decisions have legal effects – or similarly significant effects – on individuals, (ii) large scale processing of sensitive data or criminal convictions or offence details or (iii) large scale, systematic monitoring of public areas (CCTV).

Draft guidance from the Article 29 Working Party indicates that other factors may increase risk, including the presence of vulnerable data subjects (e.g. children and, notably, employees), matching or combining data sets in unexpected ways from the perspective of the affected individuals, daily transfers outside the EU, and processing designed to deny an individual a right or access to a contract or service.

As a minimum, the GDPR requires that a PIA include:

- A description of the envisaged processing operations and the purposes of the processing;
- An assessment of (i) the need for and proportionality of the processing and (ii) the risks to data subjects (as viewed from the perspective of data subjects) arising; and
- A list of the measures envisaged to (i) mitigate those risks (including non-data protection risks, such as infringements on freedom of thought and movement) and (ii) ensure compliance with the GDPR.

If a DPO has been appointed (see below), his/her advice on the carrying out of the PIA must be sought.

There is no mandated form for a PIA and as noted by the Article 29 Working Party numerous templates already exist. Interestingly, draft guidelines on this topic take account of two relevant ISO documents - one on risk management and one on PIAs in an information security context.

Draft guidance from the Article 29 Working Party considers that a PIA is only required for processing initiated after the GDPR comes into force. However, a similar review would have to be carried out for existing processing if there is a change in risk.

Consulting the supervisory authority is required whenever risks cannot be mitigated and remain high - such as where individuals may encounter significant or even irreversible consequences, or when it is obvious that a risk may occur. The GDPR contains specific procedural directions for this process.

Controllers are directed to seek the views of affected data subjects *"or their representatives"* in conducting a PIA, if appropriate. In the context of HR data processing this is likely to be interpreted as an obligation to consult with works councils or Trade Unions.

# Data Protection Officer (DPO)

Controllers and processors are free to appoint a DPO but the following must do so:

- Public authorities (with some minor exceptions);
- Any organisation whose core activities require:
  - *"regular and systematic monitoring"* of data subjects *"on a large scale"*; or
  - *"large scale"* processing of Sensitive Data or criminal records; and
- Those obliged to do so by local law (countries such as Germany are likely to fall into this category).

Guidance from the Article 29 Working Party are here to help organisations interpret the terms "core activities", "regular and systematic monitoring" and "large scale". This guidance included the following points:

- *"Core activities":* Activities which are 'an inextricable part' of the controller's/processor's pursuit of its goals are cited. Reassuringly the guidance confirms that an organisation's processing of its staff information (which is highly likely to include sensitive data) is ancillary to its activities, not core. Examples of core activities given include, a security company's surveillance where it is hired to safeguard a public space, a hospital's processing of patient health data and an outsourced provider of occupational health services' processing of its customer's employee data.
- *"Regular and systematic monitoring":* All forms of on-line tracking and profiling are called out as examples by the Article 29 Working Party, including for the purpose of behavioural advertising and email retargeting. Other examples cited include: profiling and scoring (e.g. for credit scoring, fraud prevention or for the setting of insurance premiums); location tracking; fitness and health data tracking; CCTV; processing by connected devices (smart meters, smart cars etc); and data-driven marketing activities (i.e. big data).
- "Large scale": In its guidance the Article 29 Working Party says that it is not currently keen on precise numbers being used as a benchmark for this term, but that plans are afoot to publish thresholds in the future. Instead, the December 2016 guidance lists some fairly obvious generic factors to be considered in defining large scale (e.g. the number of individuals affected and geographic extent of processing). Examples of large scale processing cited include: a bank or insurance company processing customer data; and processing of an international fast food chain's customer geo-location data in real time for statistical purposes by a specialist processor.

The Article 29 Working Party's guidance confirms that where a DPO is appointed on a voluntary basis the same requirements as set by the GDPR to mandatory DPOs will apply to them (i.e. the points which are summarised below). Moreover, once an organisation opts to appoint a DPO, it cannot circumscribe the scope of the DPO's review – the DPO must have the authority to review *all* data processing. In response to an uncertainty in the GDPR, guidance from the Article 29 Working Party confirms that nothing prevents an organisation from assigning the DPO with the task of maintaining the records of processing operations.

Interestingly, the Article 29 Working Party also recommends that an organisation which decides not to voluntarily appoint a GDPR DPO documents why it thinks that it is not subject to the mandatory DPO appointment criteria (as summarised above). Such assessments should be kept up to date and revisited when new activities or services are contemplated.

If a DPO is not mandatory and a DPO is not appointed voluntarily, staff or consultants can be appointed to carry out similar tasks, but the Article 29 Working Party says that to avoid confusion they should not be called DPOs.

Where appointed, a DPO must be selected by reference to their professional qualities and expert knowledge (which employers are obliged to help maintain). Critically, while they may be supported by a team, there can only be one DPO per organisation and that person should preferably be located in the EU. The Article 29 Working Party guidance notes that the more sensitive or complex an organisation's data processing activities are, the higher the level of expertise that its DPO will be expected to have.

Organisations must ensure that their DPO's primary objective is ensuring compliance with the GDPR. Their tasks should as a minimum include: advising their colleagues and monitoring their organisation's GDPR/privacy law/policy compliance, including via training and awareness raising, running audits, advising regarding PIAs and cooperating with supervisory authorities. The above mentioned Article 29 Working Party guidance stresses that DPOs will not be personally liable for their organisation's failure to comply with the GDPR. Liability will fall upon the organisation, including if it obstructs or fails to support the DPO in meeting his/her primary objective.

Adequate resources must be provided to enable DPOs to meet their GDPR obligations, and they should report directly to the highest level of management.

Group companies can appoint a single DPO. A DPO can be a member of staff or a hired contractor. The Article 29 Working Party guidance notes that key features of a DPO's skillset include that they must be knowledgeable about the organisations they represent and accessible – including that they are able to easily communicate with supervisory authorities and data subjects (e.g. customers and staff) in countries in which the organisation operates. So it seems that the Article 29 Working Party expects DPOs to be multi linguists as well as data protection experts – or at least to have easy access to good translation facilities.

Controllers and processors must ensure that their DPO is involved in all material matters regarding data protection (including, according to the Article 29 Working Party's guidance, following a security breach), and can operate independently of instruction and is not dismissed or penalised for performing their task. It remains to be seen how the employment laws will interpret this provision. Organisations must ensure there is a secure and confidential channel by which employees can communicate with the DPO.

The Working Party's guidance also states that if an organisation's management do not agree with and decide not to follow a DPO's recommendation then they should formally record this and the reasons for their decision. The guidance also warns that instruction must not be given to the DPO regarding how to deal with a matter, what results should be achieved or whether or not to consult with a regulatory authority, which is likely to give rise to some interesting potential interchanges following a data breach.

The GDPR does not restrict DPOs from holding other posts but expressly requires that organisations ensure that such other tasks do not give rise to a conflict of interest for the DPO. The Article 29 Working Party's guidance goes further. It says that a DPO cannot hold senior positions in management (i.e. as a CEO, COO or CFO). Other senior managers, including Head of HR, Marketing or IT, or lower level employees who make decisions about the purposes and means of processing are also barred from the position. If an external DPO (e.g. a lawyer) provides day-to-day DPO services to controllers or processors, this may prevent this individual from representing those entities before courts in cases involving data protection issues.

The DPO's contact details must be published and also notified to an organisation's supervisory authority as the DPO is to be a point of contact for questions about data protection compliance matters.

## Using service providers (data processors)

The GDPR imposes a high duty of care upon controllers in selecting their personal data processing service providers which will require procurement processes and request for tender documents to be regularly assessed.

Contracts must be implemented with service providers which include a range of information (e.g. the data processed and the duration for processing) and obligations (e.g. assistance where a security breach occurs, appropriate technical and organisational measures taken and audit assistance obligations). Likewise where a service provider hires a sub-processor.

The Commission and supervisory authorities are likely to publish approved form service provider contract clauses. It seems likely that, from a service provider's point of view, these will be onerous. Providers' approach to pricing contracts will therefore need to be reviewed.

## Record of processing activities

Organisations are obliged to keep a record of their processing activities (the type of data processed, the purposes for which it is used etc) similar to that which under current laws controllers are required to register with DPAs.

Data processors are also required to maintain such a record about personal data which controllers engage them to process, a requirement which will challenge many cloud and communications service providers.

Whilst an exemption from the above obligations applies to organisations employing fewer than 250 people this exemption will not apply where sensitive data are processed, which seems likely to nullify its usefulness.

### *Where can I find this?*

| | | |
|---|---|---|
| *Privacy by Design* | *Article 25* | *Recitals 74-78* |
| *PIAs* | *Articles 35-36* | *Recitals 89-94* |
| *DPOs* | *Articles 37-39* | *Recital 97, WP 243* |
| *Using data processors* | *Article 28 and 29* | *Recitals 81* |
| *Record of processing activities* | *Article 30* | *Recital 82* |