Rollits LLP

Compliance with the General Data Protection Regulation

Is your organisation ready?

Hull +44 (0) 1482 323239
York +44 (0) 1904 625790
rollits.com

The overarching objective of the GDPR is the same as the Data Protection Act 1998: to protect individuals' personal data. It makes significant changes to the way in which organisations are required to obtain, hold and handle information about people. This guide summarises some of the steps organisations should be taking to ensure compliance with the GDPR.

Set out below are some of the key components of the GDPR and initial suggestions for organisations seeking ways to aid compliance. GDPR definitions used in this guide (which are broadly the same as under the Data Protection Act 1998 ("DPA")) are:

- "**controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;
- "**personal data**" means any information relating to an identified or identifiable natural person ("data subject"). It includes information such as online identifiers (for example, an IP address) and other personal identifiers. Personal data that has been pseudonymised may also fall within scope of the GDPR. Sensitive personal data is now referred to as "special categories of personal data" and the definition has been expanded to include genetic and biometric data;
- "**processor**" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

In very broad terms this means that if you deal with information about an individual you are probably a controller processing information about data subjects, and therefore have to comply with the GDPR. You will also have compliance obligations if you process personal data on behalf of someone else.

1. Principles

The general principles of the GDPR remain much the same as those set out in the DPA, but there are a number of new elements and requirements which organisations should familiarise themselves with.

Personal data must be processed **lawfully, fairly and in a transparent manner** in relation to the data subject. The transparency requirement is new under the GDPR and means that information must be provided to data subjects on why their personal data is being collected, used or otherwise processed in a manner which is easily accessible and easy to understand.

Personal data should **only be collected for specified, explicit and legitimate purposes**, and should **not be processed in any manner incompatible with those purposes**. Personal data should be collected and processed only to the extent that is **adequate, relevant, and limited to the minimum extent necessary** in relation to the purposes for which they are processed ("data minimisation"). The data minimisation principle expands the requirements under the DPA and is designed to ensure that controllers do not engage in unnecessary processing activities.

Personal data held must be **accurate and kept up-to-date**. Data should be **anonymised or deleted** after it has been processed for the purposes for which it was obtained and time limits should be established for erasure or periodic review of personal data. Every reasonable step should be taken to ensure that any inaccurate personal data is rectified or deleted.

With effect from May 2018, controllers are under a legal duty to comply with the principles of the GDPR and **have to be able to demonstrate compliance** with specific requirements set out in the GDPR (the "accountability principle", which is discussed further in point 3).

Key action points

- Organisations should determine and document the legal basis for their processing of personal data. In order to do this, organisations should examine when and how they obtain personal data from data subjects and ensure that sufficient information is provided to such data subjects at the time their personal data is obtained. Any existing notices and information provided to data subjects should be examined to determine whether they comply with the comprehensive and detailed requirements of the GDPR (and, if not, they should be updated and re-sent to existing data subjects).
- Organisations should adopt appropriate technical and organisational measures to ensure that personal data is only processed for the purposes for which it is obtained.
- Organisations should periodically review any personal data held and ensure that any historic, unnecessary personal data is erased and any inaccurate personal data is updated as appropriate.

2. Consent

Under the GDPR, where consent is being used for the basis of fair and lawful processing, controllers have to demonstrate that such consent was "freely given, specific, informed and unambiguous indication of the data subject's wishes by 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". Silence, pre-ticked boxes or inactivity are not capable of constituting consent. If the processing has multiple purposes, consent is required for each purpose.

The controller bears the burden of proof to demonstrate that it has obtained the data subject's consent and the controller can only process special categories of personal data (for example, race, political opinions, religious beliefs etc.) if it has explicit consent.

If a child's personal data is being processed then, if the child is below the age of 16, parental consent is required. Individual member states may lower this age so long as such lower age is not below 13. The controller is required to make reasonable efforts to verify that consent is given or authorised by the child's parent or custodian.

The data subject has the right to withdraw consent at any time and consent must be as easy to withdraw as it is to give.

Key action points

- Organisations should consider the consent mechanisms they currently have in place and ensure that such mechanisms are compliant with the GDPR. If not, they will need to be adapted accordingly.
- Organisations should consider how they will discharge the evidential burden of demonstrating that consent has been obtained, and (if necessary) review what systems are in place for obtaining parental consent if processing children's personal data.
- Organisations should ensure that an individual can withdraw consent at any time and that the process for withdrawing consent is as easy as the process for giving consent.

3. Accountability and governance

The GDPR introduces an accountability principle requiring controllers and processors to demonstrate that they comply with the data protection principles. This can be achieved through implementing appropriate governance measures. Organisations with 250 or more employees are also required to maintain additional internal records in respect of processing activities. This additional obligation also applies to organisations with less than 250 employees in respect of activities relating to high risk processing (for example, the processing of personal data that could result in a risk to the rights of the individual).

The GDPR introduces the concept of "**data protection by design and default**". This imposes a general obligation on organisations to implement appropriate technical and organisational measures to demonstrate that data protection has been considered in respect of any processing activities. Furthermore, in certain circumstances (such as when new technologies are being used, or when processing is likely to pose a high risk to the data subjects) privacy impact assessments need to be carried out to identify and address any potential issues.

All public authorities, and any other organisations carrying out large scale systematic monitoring of individuals or large scale processing of special categories of data, are required to appoint a data protection officer ("DPO"). The DPO must operate independently and cannot be dismissed or penalised for performing their role. The DPO is required to have professional experience and knowledge of data protection law. The role of DPO can be contracted out externally.

Key action points

- Organisations should take steps to implement appropriate technical and organisational measures, such as data protection policies, staff training, internal audits and reviews of HR policies.
- Organisations should ensure that all data processing activities are documented and should conduct privacy impact assessments when appropriate.
- Organisations should implement measures such as data minimisation and pseudonymisation in order to comply with the concept of data protection by design and default.
- Where required, steps should be taken to appoint a DPO who is appropriately qualified to inform and advise the organisation on its obligations under the GDPR and monitor compliance with the GDPR.

4. Expanded territorial reach

Controllers and processors which offer or provide goods or services to, or monitor the behaviour of, data subjects in the EU (which will include most businesses with an online presence) are required to comply with the GDPR irrespective of whether or not they themselves are based in the EU.

"Offering goods or services" does not have to be in return for payment, however it requires more than mere access to a website, email address or other contact details. Additional factors, such as the language or currency used and any mentioning of customers or users in the EU on the website, are also relevant and may make it apparent that the organisation envisages offering goods or services to data subjects in the EU. "Monitoring the behaviour of a data subject in the EU" includes tracking and profiling that data subject (for example, through use of cookies).

Where the controller or processor offers or provides goods or services to, or monitors the behaviour of, data subjects in the EU but is not located in the EU, the non-EU controller or processor is required to designate in writing a representative in the EU.

This requirement does not, however, apply to a public authority or body, or to processing which is occasional and does not include large scale processing of special categories of data (i.e. sensitive personal data).

This means that many non-EU organisations that were not required to comply with the Directive will now fall within the scope of the GDPR.

Key action points

- Organisations carrying out activities which previously fell outside the scope of the Directive should take steps to establish whether such activities will be subject to the GDPR and (if they are) ensure that such activities are compliant with the GDPR.
- Organisations should note that, following Brexit, it may be necessary to appoint a representative in the EU.

5. Individuals' rights

The GDPR strengthens individuals' data rights (compared to the DPA) and creates new rights which organisations should familiarise themselves with. These are summarised below.

(a) The right to be informed

Controllers are required to provide concise, transparent, intelligible and easily accessible information relating to the personal data obtained from the data subject and the purpose of the processing. This can typically be achieved through a privacy notice. The GDPR sets out the information which must be supplied to data subjects and the point at which the information must be provided.

(b) The right of access

Data subjects have the right to obtain confirmation that their personal data is being processed and the right to access their personal data. However, under the GDPR, organisations are not be able to charge a fee for dealing with a subject access request and any request must be complied with in a shorter period of time (without delay and no later than one month of receipt).

(c) The right to rectification, the right to restrict processing and the "right to be forgotten"

Data subjects have the right to have their personal data rectified if it is inaccurate or incomplete as well as further rights to restrict the processing of their personal data. Furthermore, data subjects have the right to have their personal data erased in certain circumstances, such as where the personal data is no longer necessary for the purpose for which it was originally collected.

(d) The right to data portability

Data subjects have the right under the GDPR to have their data moved, copied or transferred safely and securely from one controller to another where technically feasible. The right to data portability impacts on online service providers in particular and it is intended to promote interoperability between online systems.

(e) The right to object

Data subjects have the right under the GDPR to object to the processing of their personal data for processing based on legitimate interests or for the performance of a task in the public interest or exercise of official authority. The controller must comply with the request unless the controller can demonstrate compelling legitimate grounds for the processing that overrides the data subject's interests. This is a significant change. The data subject can also object to the processing of personal data for direct marketing purposes and the controller must explicitly offer this right to the data subject.

The GDPR also provides safeguards against, and limits the extent to which data subjects can be subjected to, decisions based on automated processing.

Key action points

- Organisations should re-examine and, where necessary, amend their privacy notices (or implement privacy notices if they are not already in use) to ensure that they comply with the detailed requirements of the GDPR.
- Staff should be trained to recognise subject access requests and appropriate policies should be implemented for responding to requests (including any requests to have data rectified, erased, restricted or transferred) on time and without delay. All requests should be documented, along with any action taken in respect of that request.
- If any processing of personal data by an organisation would constitute automated decision making, that organisation should review and update their procedures in order to comply with the requirements of the GDPR.

6. Breach and enforcement powers

Under the GDPR, organisations are required to notify the relevant supervisory authority (the ICO in the UK) and, in some cases, the individual concerned, if there has been a data protection breach. This only applies if the breach is likely to result in a risk to the rights and freedoms of an individual (for example, if data is lost which could lead to identity theft, although it could be interpreted widely by the ICO and the Courts). If there has been a notifiable breach, it must be reported to the relevant supervisory authority within 72 hours.

Under the DPA the maximum fine that can be imposed for a data protection breach in the UK is £500,000. The GDPR significantly increases this. Under the GDPR the ICO can impose a fine of:

- up to 2% of the organisation's annual worldwide turnover for the preceding financial year or EUR10 million (whichever is greater) for data protection breaches relating to internal record keeping, DPOs, processor contracts, data security and breach notifications and data protection by design and default; or
- up to 4% of annual worldwide turnover for the preceding financial year or EUR20 million (whichever is greater) for data protection breaches relating to the data protection principles, conditions for consent, data subjects rights and international data transfers.

Furthermore, the GDPR gives the ICO the power to carry out audits, require information to be provided and obtain access to premises.

Key action points

- Staff should be made aware of what would constitute a breach and an internal policy should be implemented for reporting and investigating a breach.
- Any organisation considering data protection breaches to be low-risk would be advised to re-examine its position in light of the increased enforcement powers under the GDPR and take steps to ensure compliance.

7. Processors

The GDPR introduces direct, statutory data protection obligations on processors. In addition, processors may be liable to pay a fine of up to 4% of their annual worldwide turnover of the preceding financial year or EUR20 million (whichever is the greatest) for breaching any such obligation. Under the DPA, processors are generally not subject to direct obligations, fines or other penalties and so this represents a significant change.

Processors are required to provide guarantees to controllers that they have implemented appropriate technical and organisational measures to ensure that their processing of personal data meets the requirements of the GDPR.

Processing by a processor needs to be governed by a contract with the controller which sets out certain information including the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data, categories of data subjects and the obligations and rights of the controller.

Other obligations imposed on processors under the GDPR include requirements to: (1) maintain a record of all processing operations under their responsibility; (2) designate a DPO if required; (3) conduct an impact assessment before undertaking any processing (although this only applies in certain circumstances); and (4) notify the controller on becoming aware of a data protection breach without undue delay.

Key action points

- Organisations should consider if they are, or use, a processor.
- Processors should conduct a risk assessment to identify any gaps in their current data protection practices and procedures and take appropriate steps to ensure compliance with the GDPR.
- Controllers and processors should identify any agreements (or lack thereof) governing the processing of personal data and ensure that any data processing agreements comply with the GDPR.
- As a result of the increased compliance obligations and risk, processors may wish to review the cost of the data processing services they offer.

Information

If you have any queries on any issues raised in this document please contact David White on 01482 337209.

This is for the use of clients and will be supplied to others on request. It is for general guidance only. It provides useful information in a concise form. Action should not be taken without obtaining specific advice. We hope you have found this useful. If, however, you do not wish to receive further mailings from us, please write to Pat Coyle, Rollits, Citadel House, 58 High Street, Hull HU1 1QE.

Hull Office
Citadel House, 58 High Street,
Hull HU1 1QE
Tel +44 (0)1482 323239

York Office
Forsyth House, Alpha Court,
Monks Cross, York YO32 9WN
Tel +44 (0)1904 625790

rollits.com

June 2017