
How to be GDPR Compliant
invenias

Disclaimer

GDPR - How to be Compliant

- This guide is not exhaustive and is not intended to be a substitute for legal advice relevant to the individual circumstances of the reader.
- Legal advice should be sought for all areas before assuming or expecting to satisfy compliance with legislation
- Legislation may change or be open to new interpretations
- Invenias gives no warranty or guarantee as to the suitability or reliability of this data

GDPR

How to be Compliant

- Preparation
- Data Privacy Impact Assessments
- GDPR Policies
- Geography
- Data Protection Principles
- Lawful Basis for Processing
- Rights of Data Subjects
- Data Protection Officers

Compliance Activities

- The GDPR is still evolving and, although the underlying legislation has been published, this is still subject to interpretation and application within specific country legislations.
- Whilst this presentation outlines the main key actions that should be undertaken, some key documentation to be prepared and the overall considerations that have to be taken into account there may be additional requirements for individual circumstances depending on activities, location, size and past history.

Preparation

What do you need to do first?

- Determine who is going to be responsible in your company
  - Identify and engage the relevant people in your organisation & ensure they are familiar with GDPR
- Create, review and update your Technical & Organisational measures
  - How is your business structured, technically and operationally, to protect data privacy and comply with GDPR requirements?
- Create a GDPR File
  - Maintain a central repository for all your GDPR policies, training, reviews and relevant documentation.
- Assess and record the Data Streams you are processing
  - Collate all the areas in which you hold Personal Data (e.g. Placement, Coaching, Assessment, Employment, Sales) and create an analysis table to review the compliance and security actions required in relation to that data
- Determine and record the Purpose of that processing
  - For each stream of data record the type of data you collect, process and store and the purpose for which you do so

Data Privacy Impact Assessments

As a first stage, following on from identifying the data streams you process and separating our the purposes, you should undertake Privacy Impact Assessments for each stream.

- Templates are available at https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

These assess the risks associated with that data stream and importantly, the harm that could ensue in relation to that data. This shows you have duly considered the underlying issues and risks

GDPR Policies

These are the key policy statements recommended for minimum GDPR compliance. If templates or pro-formas are used, these must be reviewed and considered by the Company Officers to ensure they are appropriate and relevant to the business and Legal Advice should be taken to ensure they are fully compliant and lawful.

The list is not exhaustive and individual businesses may require additional policies.

Template Documents

To assist Invenias customers with the creation of policy statements, we have provided a number of Templated Documents which can be downloaded and amended to assist with fulfilling this requirement.

These can be accessed and downloaded through the Invenias Help Centre here.

A review of these items will ensure that the process and policies you have in place will minimise risk of non-compliance.

GDPR Policies

- Technical and Organisational Measures statement
  - Explanation of how your technology and business operations ensure appropriate levels of data security and protection
- GDPR Purpose Statement
  - Default Purposes – Title and description of the purposes for which you process and hold data
- Default Lawful basis
  - The Lawful basis on which you are processing and holding data for each purpose (the descriptions are defined in the legislation)
- Data Retention Policy
  - Set policies on how long you will hold data for each purpose before either reviewing, refreshing or deleting it
- Privacy Policy
  - To cover all these elements you will need to consider the following issues when planning a privacy notice: What information is being collected?; Who is collecting it?; How is it collected?; Why is it being collected?; How will it be used?; Who will it be shared with?; What will be the effect of this on the individuals concerned?; Is the intended use likely to cause individuals to object or complain?
- Data Transfer Policy
  - A statement considering how you will handle data transfers (e.g. to clients) with special consideration of transfers to other countries and how you will ensure the protection and security of the personal data.
- Legitimate Interest Assessment (LIA)
  - If you are relying on Legitimate Interest as a lawful basis then you should perform an LIA for each Purpose to determine whether the balance of LI is outweighed by the data subjects rights, freedoms and interests. Templates can be found here https://www.dpnetwork.org.uk/dpn-legitimate-interests-guidance/
- Data Breach Process
  - A documented process for how you would handle a data breach, from first becoming alert to notification of Supervisory Authority and Data Subjects
- Information Security policy
  - A document explaining your approach to information security that can be shared with staff
- DSAR process policy (including identity verification policy)
  - A process explaining how you will handle a Data Subject Access request

Geography

Each country in the EU is required to enshrine the GDPR in it's own local Data Protection legislation

The requirements of the GDPR may not be reduced but countries can add additional compliance requirements in their own region

Outside of the EU countries are implementing their own Data Privacy legislation which in many cases mirrors the GDPR

The local Data Protection Authority in each country will become the Supervisory Authority for that location

You will need to determine your Lead Supervisory Authority which will be based on where your main establishment resides (where decisions about the purposes and means of processing are taken)

Data Protection Principles

At it's heart compliance with GDPR is about compliance with the Data Protection Principles and you will need to consider your data processing activities with these in mind

- Personal data shall be processed **lawfully**, **fairly** and in a **transparent** manner. Lawful processes include "consent", "contractual necessity" and "legitimate interest";
- And shall be collected for **specified**, explicit and **legitimate purposes;**
- And shall be **adequate**, **relevant** and **limited** to what is **necessary** and kept for no longer than is **necessary;**
- And be **accurate** and **up to date;**
- And be processed in a manner that ensures **appropriate security** of the personal data

Lawful Basis for Processing

The GDPR sets out the conditions the must be met for the processing of personal data to be lawful. Any processing of data must be based on at least one of these lawful bases. They are:

- processing is **necessary for the purposes of the legitimate interests pursued by a controller**, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data;
- the **data subject has given consent** to the processing of their personal data for one or more specific purposes;
- 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;

These conditions are all equally valid and organisations should assess which of these grounds are most appropriate for different processing activities and then fulfil any further requirements the GDPR sets out for these conditions.

Lawful Basis for Processing

Additional lawful bases that could be used are:

- processing is **necessary for compliance with a legal obligation** to which the controller is subject;
- processing is **necessary in order to protect the vital interests of the data subject**;
- 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;

Rights of Data Subjects

GDPR confers a number of specific rights on data subjects:

- The Controller must state what the data subjects rights are, in a concise, transparent, intelligible and easily accessible form, using clear and plain language (in writing or by electronic means)
- The rights conferred include:
  - The right to be informed
  - The right of access
  - The right to rectification
  - The right to erasure
  - The right to restrict processing
  - The right to data portability
  - The right to object
  - Rights in relation to automated decision making and profiling.

Each of these rights will be considered in turn and organisations will need to ensure that their policies, processes and activities are sufficient to satisfy these rights.

Rights to be informed

Controller has to inform data subject with the following information (either at time of first contact or within 30 days of obtaining data):

- identity and the contact details of the controller (including DPO);
- purposes of processing;
- legal basis for processing; categories of personal data concerned;
- recipients or categories of recipients of the personal data; Intended transfers to a third country;
- period for which the personal data will be stored;
- legitimate interests pursued by the controller;
- existence of the right to request access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;
- if consent has been obtained, the existence of the right to withdraw consent at any time;
- right to lodge a complaint with a supervisory authority;
- from which source the personal data originate;
- the existence of automated decision-making, including profiling

Right of Data Access

Under the GDPR, individuals will have the right to obtain:

- confirmation that their data is being processed;
- access to their personal data; and
- other supplementary information – this largely corresponds to the information that should be provided in a privacy notice

Such data should be provided in electronic format and for no fee (unless requests are excessive or repetitive). Information must be provided without delay and at the latest within one month of receipt

You must verify the identity of the person making the request, using "reasonable means".

Right to Rectification

- Individuals are entitled to have personal data rectified if it is inaccurate or incomplete.
- If you have disclosed the personal data in question to third parties, you must inform them of the rectification where possible. You must also inform the individuals about the third parties to whom the data has been disclosed where appropriate.
- You must respond within one month.
- Where you are not taking action in response to a request for rectification, you must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy.

Right to erasure

The right to erasure (the right to be forgotten) allows an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

- The right to erasure does not provide an absolute 'right to be forgotten'. Individuals have a right to have personal data erased and to prevent processing in specific circumstances:
  - Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
  - When the individual withdraws consent.
  - When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
  - The personal data was unlawfully processed (ie otherwise in breach of the GDPR).
  - The personal data has to be erased in order to comply with a legal obligation.
- You can refuse to comply with a request for erasure where the personal data is processed for the following reasons:
  - to exercise the right of freedom of expression and information;
  - to comply with a legal obligation or for the performance of a public interest task or exercise of official authority;
  - for public health purposes in the public interest;
  - archiving purposes in the public interest, scientific research historical research or statistical purposes; or
  - the exercise or defence of legal claims.

Right to restrict processing

- An individual has a right to block or restrict. When processing is restricted, you are permitted to store the personal data, but not further process it. You can retain just enough information about the individual to ensure that the restriction is respected in future.
- You will be required to restrict the processing of personal data in the following circumstances:
  - Where an individual contests the accuracy of the personal data, you should restrict the processing until you have verified the accuracy.
  - Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and you are considering whether your organisation's legitimate grounds override those of the individual.
  - When processing is unlawful and the individual opposes erasure and requests restriction instead.
  - If you no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.
  - If you have disclosed the personal data in question to third parties, you must inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.
  - You must inform individuals when you decide to lift a restriction on processing.

Right to data portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services and move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

The right to data portability only applies:

- to personal data an individual has provided to a controller (this would include data from interactions such as interviews);
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means.
- You must provide the personal data in a structured, commonly used and machine readable form (e.g. CSV files).
- The information must be provided free of charge.
- If the individual requests it, you may be required to transmit the data directly to another organisation if this is technically feasible. However, you are not required to adopt or maintain processing systems that are technically compatible with other organisations.
- You must respond without undue delay, and within one month.

Right to object

Individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

If you process personal data for the performance of a legal task or your organisation's legitimate interests, Individuals must have an objection on "grounds relating to his or her particular situation".

You must stop processing the personal data unless:

- you can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
- the processing is for the establishment, exercise or defence of legal claims.

You must inform individuals (explicitly and clearly) of their right to object "at the point of first communication" and in your privacy notice.

Rights in relation to automated decision making and profiling

The GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention. You must identify whether any of your processing operations constitute automated decision making and consider whether you need to update your procedures to deal with the requirements of the GDPR.

Individuals have the right not to be subject to a decision when:

- it is based on automated processing; and
- it produces a legal effect or a similarly significant effect on the individual.

You must ensure that individuals are able to:

- obtain human intervention;
- express their point of view; and
- obtain an explanation of the decision and challenge it.

The right does not apply if the decision:

- is necessary for entering into or performance of a contract between you and the individual;
- is authorised by law (e.g. for the purposes of fraud or tax evasion prevention); or
- based on explicit consent.

Furthermore, the right does not apply when a decision does not have a legal or similarly significant effect on someone.

Rights in relation to automated decision making and profiling

The GDPR defines profiling as any form of automated processing intended to evaluate certain personal aspects of an individual, in particular to analyse or predict their:

- performance at work; economic situation; health; personal preferences; reliability; behaviour; location; or movements.

When processing personal data for profiling purposes, you must ensure that appropriate safeguards are in place. You must:

- Ensure processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the envisaged consequences.
- Use appropriate mathematical or statistical procedures for the profiling.
- Implement appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.
- Secure personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

Automated decisions taken for the purposes listed in Article 9(2) must not:

- concern a child; or
- be based on the processing of special categories of data unless:
- you have the explicit consent of the individual; or
- the processing is necessary for reasons of substantial public interest on the basis of EU / Member State law. This must be proportionate to the aim pursued, respect the essence of the right to data protection and provide suitable and specific measures to safeguard fundamental rights and the interests of the individual.

Data Protection Officer (DPO)

You should have someone in your organisation who has responsibility for Data Protection under GDPR but you don't necessarily require a DPO.

A DPO must be appointed when:

- The processing is carried out by a 'public authority'.
- The 'core activities' require regular and systematic monitoring of data subjects on a 'large scale'.
- Where 'core activities' involve 'large scale' processing of 'special categories' of personal data and relating to criminal convictions and offences.

The DPO is the data protection expert within the organisation and acts as the person that data protection queries are directed to. The DPO, who can be a staff member or contractor, shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the following tasks:

- Informing and advising the controller or the processor and their employees of their data protection obligations.
- Monitoring compliance with the Regulation, including the assignment of responsibilities.
- Awareness-raising and training of staff involved.
- Providing advice where requested as regards the data privacy impact assessments (DPIAs) and monitoring compliance and performance.
- Engaging with the relevant Supervisory Authority.

The Regulation also stipulates that the DPO reports directly to top level management and must be given all resources necessary to carry out their functions.