GDPR Self-Assessment
HONcode Certification

Data protection is the fair and proper use of personal information

• What is the GDPR?

The GDPR is the General Data Protection Regulation (EU) 2016/679. It sets out the key principles, rights and obligations for most processing of personal data. The GDPR came into effect on 25 May 2018.

• Does the GDPR apply to me?

The GDPR applies to:[1]

- organisations located within the EU
- organisations located outside of the EU if they offer goods or services to, or monitor the behaviour of, EU data subjects.
- all companies processing and holding the personal data of data subjects residing in the European Union, regardless of the company's location.

• What is 'personal data'?[2]

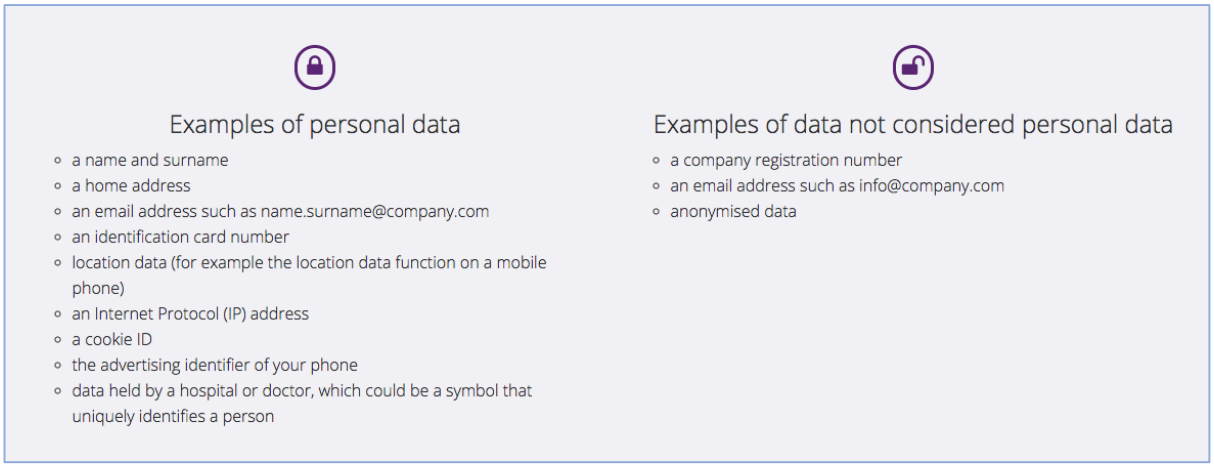
In short, personal data means information about a living individual. This might be anyone, including a customer, client, employee, partner, member, supporter, business contact, public official or member of the public.

It does not need to be 'private' information – even information which is public knowledge or is about someone's professional life can be personal data.

Personal data only includes information relating to natural persons where:

- They can be identified or who are identifiable, directly from the information in question; or
- they can be indirectly identified from that information in combination with other information.
- the data falls into a special category of personal data or criminal conviction and offences data. These are considered to be more sensitive and you may only process them in more limited circumstances.

[1] https://eugdpr.org/the-regulation/gdpr-faqs/
[2] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/



• What is 'processing'?[3]

Almost anything you do with data counts as processing; including collecting, recording, storing, using, analysing, combining, disclosing or deleting it.

• What is a 'controller'?

A controller is the person that decides how and why to collect and use the data. This will usually be an organisation, but can be an individual (eg a sole trader). If you are an employee acting on behalf of your employer, the employer would be the controller. The controller must make sure that the processing of that data complies with data protection law.

• What is a 'processor?

A processor is a separate person or organisation (not an employee) who processes data on behalf of the controller and in accordance with their instructions. Processors have some direct legal obligations, but these are more limited than the controller's obligations.

[3]: https://ico.org.uk/for-organisations/guide-to-data-protection/introduction-to-data-protection/some-basic-concepts/

SELF ASSESSMENT - INTRODUCTION

The GDPR sets out seven key criteria[4]

1. **Lawfulness, fairness and transparency**: *Data should be processed **lawfully**, **fairly** and in a **transparent manner** in relation to individuals.*
2. **Purpose limitation**: *Data should be collected **for specified, explicit and legitimate** purposes and **not further** processed in a manner that is incompatible with those purposes*
3. **Data minimization**: *Data collection should be **adequate, relevant and limited** to what is necessary in relation to the purposes for which they are processed.*
4. **Accuracy**: Data should be **accurate** and **up to date**.
5. **Storage limitation**: Data shouldn't be kept for longer than **necessary**.
6. **Integrity and confidentiality**: Data should be processed in a manner that ensures **appropriate security** of the personal data
7. **Accountability**: The controller shall be **responsible** for and be **able to demonstrate** compliance with these criteria. A controller is the person that decides how and why to collect and use the data.

We will go through every principle, step by step, to help you ensure that you comply with the GDPR, thanks to a form.
Do not hesitate to contact us if you have any questions about this regulation, our team is at your disposal to help you.

SELF ASSESSMENT FORM

In order to check if your service is compliant with the GDPR, we will go through the 7 principles of the Regulation.

Step 1 – Determine your eligibility to process personal data

1. What is / are your *eligibility(s):*[5]

You need to identify your eligibility before you can process personal data. At least one of these should apply to your service if you process personal data. Otherwise, you are not authorized to process personal data.

☐ **Consent**[6]: the individual has given clear consent for you to process their personal data for a specific purpose.

☐ You have a separate and understandable request for consent for the use of your service.

☐ You have a record of when and how you got consent from the individual.

☐ The user has the right to withdraw his or her consent at any time.

[4] https://gdpr-info.eu/art-5-gdpr/
[5] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/
[6] https://gdpr-info.eu/art-7-gdpr/

☐ If your business relies on consent to offer online services directly to children, you have systems in place to manage it.

Consent means offering people genuine choice and control over how you use their data.

- You should keep your consent requests prominent and separate from other terms and conditions.
- Seek a positive opt-in such as unticked opt-in boxes or similar active opt-in methods.
- Avoid making consent a precondition of service.
- Be specific and granular. Allow individuals to consent separately to different purposes and types of processing wherever appropriate.
- Name your business and any specific third party organisations who will rely on this consent.
- Keep records of what an individual has consented to, including what you told them, and when and how they consented.
- Tell individuals they can withdraw consent at any time and how to do this.[7]

You need to have a lawful basis for processing a child's personal data.

- If you are offering online services to children, only a child aged 13 or over will be able to provide their own consent.
- You will therefore need to make reasonable efforts to verify that anyone giving their own consent is old enough to do so.
- For children under 13 you need to get consent from whoever holds parental responsibility for the child.

☐ **Contract**: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.[8]

You can rely on this lawful basis if you need to process someone's personal data: to fulfil your contractual obligations to them; or because they have asked you to do something before entering into a contract (eg provide a quote).

☐ **Legal obligation**: the processing is necessary for you to comply with the law (not including contractual obligations).

You can rely on this lawful basis if you need to process the personal data to comply with a common law or statutory obligation.[9]

☐ **Vital interests**: the processing is necessary to protect someone's life.

The processing of personal data should also be regarded as lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. Processing of personal data based on the vital interest of another natural person

[7] https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/controllers-checklist/
[8] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/contract/
[9] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legal-obligation/

should in principle take place only where the processing cannot be manifestly based on another legal basis.[10]

☐ **Public task**: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

You can rely on this lawful basis if you need to process personal data:

- 'in the exercise of official authority'. This covers public functions and powers that are set out in law;
- or to perform a specific task in the public interest that is set out in law.

It is most relevant to public authorities, but it can apply to any organisation that exercises official authority or carries out tasks in the public interest.[11]

☐ **Legitimate interests**: the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, unless interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data. (This cannot apply if you are a public authority processing data to perform your official tasks.)

If you choose to rely on legitimate interests, you are taking on extra responsibility for considering and protecting people's rights and interests.

[10] https://gdpr-info.eu/recitals/no-46/
[11] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/public-task/

Step 2 – Comply with the 7 GDPR criteria

Criteria 1 - Lawfulness, fairness and transparency

Personal data shall be: processed lawfully, fairly and in a transparent manner in relation to the data subject[12]

Your business has identified your eligibility for processing and documented them.

The first principle requires that you process all personal data lawfully, fairly and in a transparent manner. If no lawful requirement for the processing, your processing will be unlawful and in breach of the first principle.

☐ Yes

☐ No

If you answered Yes, continue the self-assessment.

If you answered No, you're back to Step 1. You can use this link to help you identify your eligibility:

https://ico.org.uk/for-organisations/resources-and-support/lawful-basis-interactive-guidance-tool

☐ You don't do anything generally unlawful with personal data (Lawfulness)

Lawfulness also means that you don't do anything with the personal data which is unlawful in a more general sense. This includes statute and common law obligations, whether criminal or civil. If processing involves committing a criminal offence, it will obviously be unlawful. However, processing may also be unlawful if it results in:

- a breach of a duty of confidence;
- your organisation exceeding its legal powers or exercising those powers improperly;
- an infringement of copyright;
- a breach of an enforceable contractual agreement;
- a breach of industry-specific legislation or regulations; or
- a breach of the Human Rights Act 1998.[13]

☐ You only handle people's data in ways they would reasonably expect (Fairness)

The principle of fairness means that the personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed[14]

In general, fairness means that you should only handle personal data in ways that people would reasonably expect and not use it in ways that have unjustified adverse effects on them. You need to stop and think not just about how you can use personal data, but also about whether you should.

[12] https://gdpr-info.eu/art-5-gdpr/

[13] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/

[14] https://gdpr-info.eu/recitals/no-39/

☐You comply with the transparency obligations of the right to be informed.

The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used.

Criteria 2 - 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; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes.[15]

☐ You have clearly identified why you are collecting personal data and what you intend to do with it.

The specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data.[16]

☐ You specify these purposes in an appropriate and understandable Privacy Policy for individuals

If you plan to use personal data for a new purpose, you have to check that this is compatible with your original purpose or get specific consent for the new purpose[17]

Criteria 3 - Data minimisation

The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed.[18]

☐ You only collect personal data you actually need for our specified purposes. (Relevant)

☐ You have sufficient personal data to properly fulfil those purposes. (Adequate)

☐ You periodically review the data you hold, and delete anything you don't require. (Limited)

This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review.[19]

Criteria 4 - Accuracy

[15] https://gdpr-info.eu/art-5-gdpr/
[16] https://gdpr-info.eu/recitals/no-39/
[17] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/purpose-limitation/
[18] https://gdpr-info.eu/art-5-gdpr/
[19] https://gdpr-info.eu/recitals/no-39/

Personal data should be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, be erased or rectified without delay.

☐ You ensure that the personal data you hold is accurate and up to date and of any personal data you create.

Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted.

In practice, this means that you must:

- take reasonable steps to ensure the accuracy of any personal data;
- ensure that the source and status of personal data is clear;
- carefully consider any challenges to the accuracy of information; and
- consider whether it is necessary to periodically update the information.

Criteria 5 - 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')

☐ You do not keep personal data for longer than you require it.

Even if you collect and use personal data fairly and lawfully, you cannot keep it for longer than you actually need it. Apart from helping you to comply with the data minimisation and accuracy principles, this also reduces the risk that you will use such data in error – to the detriment of all concerned.[20]

☐ You have established and documented standard retention periods for different categories of information you hold wherever possible.

In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review.[21]

Criteria 6 - Integrity and confidentiality (Security)

Personal data should 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[22]

☐ You process personal data in a manner that ensures appropriate security to prevent the personal data you hold being accidentally or deliberately compromised.

[20] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation/
[21] https://gdpr-info.eu/recitals/no-39/
[22] https://gdpr-info.eu/art-5-gdpr/

In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption.
Those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected[23]

☐ You use encryption and/or pseudonymisation where it is appropriate to do so.

The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: the pseudonymisation and encryption of personal data.[24]

☐ In case of a data breach, we notify, in clear comprehensible language, the supervisor authority within 72 hours and users without undue delay.

Therefore, as soon as the controller becomes aware that a personal data breach has occurred, the controller should notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it[25]

The controller should communicate to the data subject a personal data breach, without undue delay, where that personal data breach is likely to result in a high risk to the rights and freedoms of the natural person in order to allow him or her to take the necessary precautions.[26]

Criteria 7 - Accountability

The controller shall be responsible for, and be able to demonstrate compliance with, previous principles.[27]

☐ You take responsibility for complying with the GDPR, and review your accountability measures at appropriate intervals

Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.[28]

[23] https://gdpr-info.eu/recitals/no-83/
[24] https://gdpr-info.eu/art-32-gdpr/
[25] https://gdpr-info.eu/recitals/no-85/
[26] https://gdpr-info.eu/recitals/no-86/
[27] https://gdpr-info.eu/art-5-gdpr/
[28] https://gdpr-info.eu/art-24-gdpr/

Step 3 – Last Step – 8 Rights for individuals

1- Right to be informed

☐ You provide all the necessary information about your organization and the personal data you collect, in your Privacy Policy.

More details about the information you need to provide: https://gdpr-info.eu/art-13-gdpr/

2-Right of access

☐ You can respond to individuals' requests to access their personal data

The data subject shall have the right to obtain from the controller, confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data.[29]

3- Right to rectification

☐ You comply with the individual's right to rectification without undue delay and carefully consider any challenges to the accuracy of the personal data.

Remember that individuals have the absolute right to have incorrect personal data rectified[30]

The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.[31]

4- Right to erasure / Right to be forgotten

☐ You have appropriate processes in place to comply with individuals' requests for erasure under 'the right to be forgotten

User shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay[32]

5- Right to restriction of processing

☐ You can respond to individual's request to restrict the processing of their personal data.

The data subject shall have the right to obtain from the controller restriction of processing. A data subject who has obtained restriction of processing shall be informed by the controller before the restriction of processing is lifted.[33]

6- Right to data portability

☐ You have processes to allow individuals to move, copy or transfer their personal data from one IT environment to another in a safe and secure way, without hindrance to usability.

[29] https://gdpr-info.eu/art-15-gdpr/
[30] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy/
[31] https://gdpr-info.eu/art-16-gdpr/
[32] https://gdpr-info.eu/art-17-gdpr/
[33] https://gdpr-info.eu/art-18-gdpr/

The data subject should be allowed to receive personal data concerning him or her which he or she has provided to a controller in a structured, commonly used, machine-readable and interoperable format, and to transmit it to another controller.[34]

7- Right to object

☐ You have appropriate methods in place to erase, suppress or otherwise cease processing personal data, upon the right to object of the user.

Where personal data might lawfully be processed because 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, or on grounds of the legitimate interests of a controller or a third party, a data subject should, nevertheless, be entitled to object to the processing of any personal data relating to his or her particular situation.[35]

8- Right to lodge a complaint

☐ You took measures such as providing a complaint submission form, so your users can submit a complaint to a supervisory authority

Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.[36]

DPO : Data Protection Officer

☐ You are a public authority (except for courts acting in the judicial capacity);

☐ You carry out large scale regular and systematic monitoring of individuals (eg online behaviour tracking);

☐ You carry out large scale processing of special categories of data or data relating to criminal convictions and offences.

☐ None of these propositions

You may find it useful to designate a DPO on a voluntary basis even when the GDPR does not require you to.[37]

If one of the first three:

DPO Recommendation: You shall designate a data protection officer, a person with expert knowledge of data protection law and practices should assist the controller or processor to monitor internal compliance with this Regulation[38]

[34] https://gdpr-info.eu/recitals/no-68/
[35] https://gdpr-info.eu/recitals/no-69/
[36] https://gdpr-info.eu/art-77-gdpr/
[37] https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/controllers-checklist/
[38] https://gdpr-info.eu/recitals/no-97/

DPIA : Data protection impact assessments

☐ You use a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural persons;

☐ You process special category or criminal offence data on a large scale;

☐ You systematically monitor publicly accessible places on a large scale.

☐ None of these propositions

If one of the first three:

DPIA Recommendation: In such cases, a data protection impact assessment should be carried out by the controller prior to the processing in order to assess the particular likelihood and severity of the high risk, taking into account the nature, scope, context and purposes of the processing and the sources of the risk. That impact assessment should include, in particular, the measures, safeguards and mechanisms envisaged for mitigating that risk, ensuring the protection of personal data and demonstrating compliance with this Regulation.[39]

[39] https://gdpr-info.eu/recitals/no-90/