Legitimate interest as a lawful base for personal data processing

What does legitimate interest mean?

According to article 6 (f) of the GDPR, data processing is lawful if it is necessary for the legitimate interests of a controller or 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. Therefore, data controllers can claim legitimate interest as legal ground for processing personal data.

Example: A company/organisation has a legitimate interest when the processing takes place within a client relationship, when it processes personal data for direct marketing purposes, to prevent fraud or to ensure the network and information security of your IT systems.

How is legitimate interest different from other lawful basis for processing?

According to ICO, "Legitimate interests is different to the other lawful bases as **it is not centred around a particular purpose** (eg performing a contract with the individual, complying with a legal obligation, protecting vital interests or carrying out a public task), and it is not processing that the individual has specifically agreed to (consent). Legitimate interests is more flexible and could in principle apply to any type of processing for any reasonable purpose. Because it could apply in a wide range of circumstances, it puts the onus on you to balance your legitimate interests and the necessity of processing the personal data against the interests, rights and freedoms of the individual taking into account the particular circumstances. This is different to the other lawful bases, which presume that your interests and those of the individual are balanced." (ICO, A)

When does legitimate interest apply?

Thus, the GDPR states that legitimate interest of a data processor might serve as a lawful basis for processing. However, what does legitimate interest mean in practice? How can we determine whether a concrete circumstance can be considered a legitimate interest? This question is hard to answer, since the GDPR does not provide concrete advice. The processing of the data may be in your own interests or indeed those of a third party. In addition, it must be noted that the expression 'third party' not only applies to other legal entities such as companies, organizations or institutions, but more importantly it may also be applied to another person or individual. It is also important to point out that the general public's legitimate interests in the data processing may also play a part in determining the order of preference of legitimate interests. (ICO, A),

It must be highlighted that legitimate interest must be understood in a very wide sense. Indeed, such interest can range from trivial to compelling, and be straightforward or more controversial. For instance, starting a new business can be considered perfectly as such. However, according to the criterion expressed by the Court of Justice of the European Union (CJEU) in the Rigas case (C-13/16, 4 May 2017) in the context of the Data Protection Directive 95/46/EC, which contained a very similar provision, in order to process data on the basis of Letigitimate Interest**, "three cumulative conditions must be fulfilled:**

- first, the pursuit of a legitimate interest by the data controller or by the third party or parties to whom the data are disclosed;
- second, the need to process personal data for the purposes of the legitimate interests pursued; and
- third, that the fundamental rights and freedoms of the person concerned by the data protection do not take precedence"

Therefore, the use of the concept of legitimate interests as a legal ground for data processing needs to **balance the interests of the data controller** or **any third parties to whom the data are disclosed, against the rights and freedoms of the individual; only** if the latter do not take precedence will the data processing be lawful.

The balancing test

According to a quite old (but still useful) opinion of the Article 29 Working Party on legitimate interests under the current Data Protection Directive (A29WP, 2014, hyperlink https://www.dataprotection.ro/servlet/ViewDocument?id=1086) a balancing test is an excellent tool to make a decision on whether legitimate interest applies as a lawful basis for data processing. Carrying out a balancing test involves considering several key factors:

- the **nature and source** of the legitimate interest: whether the data processing is **necessary** for the exercise of a fundamental right, is otherwise **in the public interest**, or **benefits from recognition** in the community concerned

- **the nature of the data and the impact of the processing on the data subjects** and their reasonable expectations about what will happen to their data

- **additional safeguards which could limit undue impact on the data subject**, such as data minimisation, privacy by design and by default, privacy-enhancing technologies; increased transparency, general and unconditional right to opt-out, data portability, etc.

The Opinion by the Article 29 Working Party details how to assess these factors and carry out the balancing exercise (Annex I). Its model includes **seven steps:**

Step 1: Assessing which legal ground may potentially apply under Article 7(a)-(f)

Step 2: Qualifying an interest as 'legitimate' or ‘illegitimate’

Step 3: Determining whether the processing is necessary to achieve the interest pursued

Step 4: Establishing a provisional balance by assessing whether the data controller’s interest is overridden by the fundamental rights or interests of the data subjects

Step 5: Establishing a final balance by taking into account additional safeguards

Step 6: Demonstrate compliance and ensure transparency

Step 7: What if the data subject exercises his/her right to object?

Does Legitimate Interest raise any special issue that must be considered by data controllers?

It is essential to highlight that the legitimate interests condition **might be very dangerous** as a legal ground for processing for the data controllers, due to the fact that **the duty of correct behaviour is placed on the organization** (the data controller). This means that, for example, a company dealing in big data would have to demonstrate that it has implemented an appropriate value system that enables it to carry out a correct and regular evaluation of the data processing taking place.

In addition, this system must be open to review by an external interested party, such as a data subject or regulator. Moreover, GDPR Articles 13(1)(d) and 14(2)(b) expressly state that **the data controller must make its legitimate interests public in a privacy notice that is clearly accessible to the data subjects**. It is quite clear that this will be harder for SMEs.

Indeed, if the data controller is willing to rely on legitimate interest they need to be confident about taking on the responsibility of protecting the interests of the individual. If it is more appropriate to put the onus on individuals to take responsibility for the use of their data, then the controller may wish to consider whether informed consent would be a more appropriate lawful basis (ICO B). Data controllers must also know that if they decide to use legitimate interest rather than another lawful basis, **individuals need to be told about those legitimate interests along with the obligation to advise individuals about their right to object.** It important to keep always in mind that the use of legitimate interest as legal ground for data processing requires a risk assessment based on the specific context and circumstances to demonstrate that processing is appropriate.

Legitimate interest and public authorities

Finally, a very important reminder: **public authorities cannot use legitimate interests as a lawful basis if the processing is in the performance of their tasks as public authorities!** "The GDPR explains the reason for this exclusion is because it is for the legislature to give public authorities the legal authority to process personal data; i.e. if you are a public authority you should only be able to process personal data in performance of your tasks if the law has given you authorisation." (ICO B). Indeed,

under the GDPR the legitimate interests condition will not be available to public authorities, since it will not apply to processing they carry out "in performance of their tasks", according to Recital 47 and Article 6(1). However, this restriction on the use of legitimate interests is about *the nature of the task*, not the nature of the organisation. Thus, if the data controller is a public authority, legitimate interests could serve as legal ground for data processing **if the controller is not playing the role of a public authority.**

Tools related to legitimate interest

- Legitimate interest balancing test
- Risk assessment
- DPIA
- Data processing records

For further questions such as:

- Are there cases when legitimate interests is likely to apply?
- Can we use legitimate interests for employee or client data?
- Can we use legitimate interests for intra-group transfers?
- Can we use legitimate interests for our marketing activities?
- Can we use legitimate interests for our business to business contacts?

  Please, follow the links (they all direct to ICO B)

DO

- Identify a legitimate interest (what interest are you pursuing?), perform a Necessity test: is the processing necessary for that purpose? And then perform a Balancing test: do the individual's interests override the legitimate interest
- Perform a risk analysis and a DPIA (this is not always compulsory but much recommendable)

- Keep detailed records about all the initiatives performed and all data processing and especially about the legitimate interest that served as a lawful basis for processing
- Advise individuals about their right to object.
- Use another lawful basis that more obviously applies to a particular purpose if possible be.

DON'T

DON'T USE legitimate interests as an appropriate lawful basis for your processing **IF** (based on a non-exhaustive list provided by the ICO (B)):

- You are a public authority and the processing is to perform your tasks as a public authority, or the processing does not comply with broader legal, ethical or industry standards if you are not a public authority
- You don't want to take full responsibility for protecting the interests of the individual, or would prefer to put the onus onto the individual
- You intend to use the personal data in ways people are not aware of and do not expect (unless you have a more compelling reason that justifies the unexpected nature of the processing), or there's a risk of significant harm (unless you have a more compelling reason that justifies the impact)
- The outcome of the balancing test in negative or non-conclusive
- Another lawful basis more obviously applies to a particular purpose. Although in theory more than one lawful basis may apply to your processing, in practice legitimate interests are unlikely to be appropriate for any processing purpose where another basis objectively applies.

Check list (based on ICO, C)

Data controllers should check that:

☐ They have checked that processing personal data is necessary and there is no less intrusive way to achieve the same result.

☐ They have ensured that legitimate interests is the most appropriate basis for processing by comparison with other possible bases.

☐ They have identified the relevant legitimate interests.

☐ They are taking responsibility to protect the individual's interests and implements concrete measures to guarantee it.

☐ They have conducted a legitimate interests assessment (LIA) and kept a record of it, to ensure that they can justify their decisions.

☐ They have performed a balancing test, and are confident that the individual's interests do not override those legitimate interests that justify data processing.

☐ They use individuals' data in ways that individuals would reasonably expect, unless there is a very good reason not to.

☐ They are not using other people's data in ways that people would find intrusive or which could cause those people harm, unless there is a very good reason.

☐ If they process children's data, they take extra care to make sure that they protect the children's interests.

☐ They have included safeguards to reduce the impact where possible.

☐ They have considered whether they can offer an opt out.

☐ If the LIA identifies a significant privacy impact, They have considered whether they also need to conduct a DPIA.

☐ They keep their LIA under review, and repeat it if circumstances change.

☐ They have included information about their legitimate interests in their privacy information.

Additional Information Sources

- An exhaustive analysis of the rulings by the Court of Justice of the European Union (CJEU) can be found here: Future of Privacy Forum, Processing Personal Data on the Basis of Legitimate Interests under the GDPR, at: http://www.ejtn.eu/PageFiles/17861/Deciphering_Legitimate_Interests_Under_the_GDPR%20(1).pdf
- Article 29 Working Party, "Opinion 6/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46", April 9, 2014, at: https://www.dataprotection.ro/servlet/ViewDocument?id=1086
- Charities Institute Ireland, Information and Guidance Notes General Data Protection Regulation (GDPR). Legitimate Interest 'Balancing Test' Assessment Template, https://static1.squarespace.com/static/57ff6b30bebafba9d10c7dcd/t/5a5f3336ec212d22697ba776/1516188471440/CII+Guidance+Notes+Legitimate+Interest+%27Balancing+Test%27+Assessment+Template+%281%29.pdf
- ICO A, What is the 'legitimate interests' basis? https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/
- ICO B, When can we rely on legitimate interests?, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/when-can-we-rely-on-legitimate-interests/
- ICO C, Legitimate Interest, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/