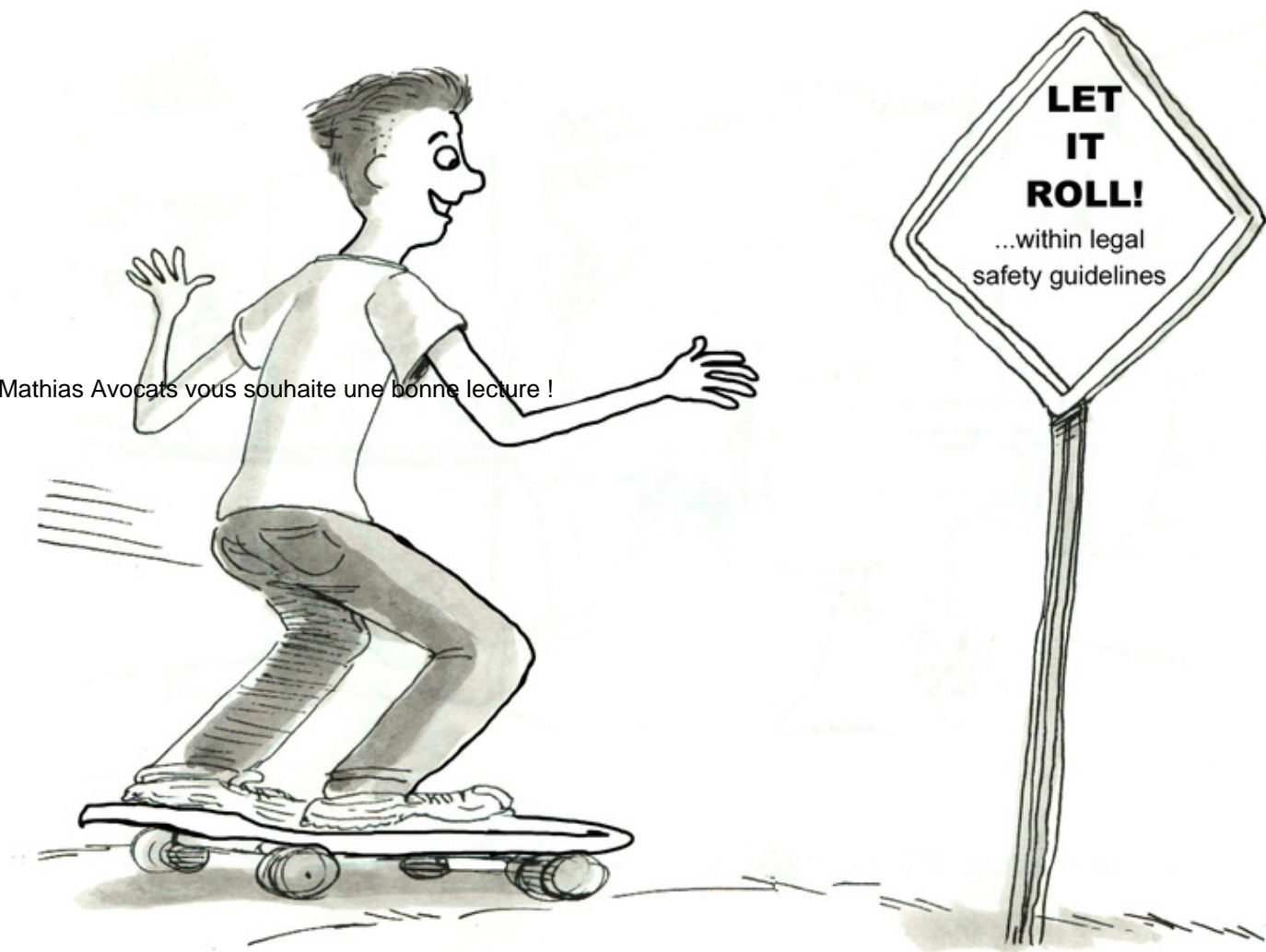


The ICO's guide on legitimate interest

Date : 18 avril 2018



Mathias Avocats vous souhaite une bonne lecture !

[Regulation n°2016/679](#), also known as the General Data Protection Regulation, will be coming into application in just a few months on the 25th of May 2018. The Information Commissioner's Office (ICO) – data protection authority in the United Kingdom – with its [guidelines](#) on the notion of legitimate interest.

To prepare, many Member States are currently drafting Bills to modify their legislation concerning the protection of personal data and to be in conformity with the GDPR (ex: [France](#), [Belgium](#)...). Moreover, certain data protection authorities have also published guidelines in conjunction with Article 29 Working Party ([WP29](#)) to explain certain articles or notions of the GDPR. This is namely the case for the ICO.

Mathias Avocats gives an overview of ICO's guidelines.

What is legitimate interest under the GDPR?

Under [Article 6, f\) of the GDPR](#), processing “shall be lawful only if and to the extent that (...) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party” (ex : fraud detection and prevention, intra-group transfers, IT security...). The legitimate interests of the data controller or of a third party are thus a lawful basis for data processing. Let us underline that there are also five other lawful basis.

However, the legitimate interests of the data controller or third party will be overridden by the interests and fundamental rights and freedoms of the data subject ([Article 6, f\) of the GDPR](#)). It is not a “catch-all basis” and is subject to strict case-to-case scrutiny.

The ICO [states](#) that “legitimate interests is most likely to be an appropriate basis where you use data in ways that people would reasonably expect and that have a minimal privacy impact. Where there is an impact on individuals, it may still apply if you can show there is an even more compelling benefit to the processing and the impact is justified”.

Although the GDPR gives further indications namely in [Recital 47](#), the notion of legitimate interests remains vague. It is a very flexible lawful basis for processing. Data controllers must take particular caution when their processing activities are based on a legitimate interest.

It is important to note that the legitimate interests must be explained clearly and simply to data subjects in order to comply with the transparency requirement under the GDPR ([Article 12 of the GDPR](#)). It is not enough for the data controller to simply state that he or she or it has a legitimate interest.

Mathias Avocats vous souhaite une bonne lecture !

How does the ICO interpret them?

The ICO does not give a list of legitimate interests which may apply to the data controller’s processing activities. It has instead created several helpful tools to determine whether legitimate interests is an appropriate lawful basis.

Considering the definition of legitimate interests basis under [Article 6, f\) of the GDPR](#), the ICO has drawn a three part test to determine whether legitimate interests are an appropriate basis for the data processing :

- Purpose test: is the controller pursuing a legitimate interest?
- Necessity test: is the processing necessary for that purpose? In other words, is the processing a targeted and proportionate means of achieving the purpose?
- Balancing test: do the data subject’s interests override the legitimate interest? The data controller must proceed to a balancing test to determine whether the data subject would reasonably expect the use of his or her data in that way and whether the processing activity is likely to cause unwarranted harm.

In practice, if there is another reasonable and non-intrusive way to carry out the personal data processing activity, the data controller will most likely not be able to rely on legitimate interests as a lawful basis.

The ICO refers to this test as legitimate interests assessment (LIA) which must be undertaken before the processing activity is implemented. In practice, this will help the controller comply with its accountability obligation and may be part of a [data protection impact assessment](#) and/or the records of processing activities.

Moreover, the ICO has also created a [lawful basis interactive guidance tool](#) to help data controller determine the appropriate legal basis for their personal data processing activities.

Mathias Avocats remains at your disposal to answer any questions you may have regarding your conformity and will accompany you in your conformity procedure.