



Legitimate Interest Assessment (LIA)

A GUIDE TO WHEN AND HOW TO USE THEM EFFECTIVELY





Businesses may find Legitimate Interest to be more flexible than consent for some data processing activities. However, you need to meet some basic criteria and must complete a Legitimate Interest Assessment (LIA).

GDPR, PECR AND LIAS

A whole lot of acronyms; a whole lot of regulations for you to think about.

It's easy to see where the confusion lies. Since the introduction of the GDPR (General Data Protection Regulation) in May 2018, reports of data breaches have been rife, and the mishandling of people's personal data has seen offenders being fined, or formally threatened with fines, which are higher than ever before throughout the EU.

As a business, you undoubtedly have plans for your profits that don't involve shelling out thousands for contravening the new data regulations, but you also have a need to market your services beyond your own walls. And if you're confused about how to balance the two, you're not alone.

A focus for business since the introduction of the GDPR has been centred, both rightly and wrongly, on obtaining explicit consent before processing personal data. The PECR (Privacy and Electronic Communications Regulations, the latest version of which came into effect at the start of 2019) sets out more specific rights on electronic communications – requiring individuals to consent to marketing calls, emails, texts and faxes.

However, what still alludes a number of businesses is the ability to apply Legitimate Interest for business to business (B2B) marketing communications. It can also apply to communications with individuals, where you already have a customer relationship, or enquiry regarding a similar product or service. For Legitimate Interest Grounds to apply, you need to meet some basic criteria and must complete a Legitimate Interest Assessment (LIA).

There are six lawful basis set out in the GDPR to justify the processing of personal data – Legitimate Interest being one of them. But what exactly is Legitimate Interest, when can you use it, and how do you make sure you still comply with PECR?

This guide is intended to provide an overview of Legitimate Interest – and Legitimate Interest Assessments – but it should be remembered that LIAs are not an exact science, and circumstances will vary from business to business.

WHAT IS LEGITIMATE INTEREST?

Put simply, Legitimate Interest is more flexible than consent but comes with its own hoops to jump through. This involves conducting a formal assessment of the impact of any data processing activity – an LIA. This ensures that there is no adverse impact upon the individuals concerned.

Legitimate Interest can be a sensible option where the level of sensitivity and risk to data subjects is low. It's often used by companies to support the processing of personal data for marketing purposes – but it is by no means a 'get out of jail free card'.

For both electronic and paper forms of marketing you need to meet obligations under clauses 13 and 14 of GDPR. These describe the information to be communicated to individuals when their data is gathered, including:

- **The right to opt-out:** of further electronic marketing communications.
- **The source of their data:** if you obtained their information from 3rd party or public sources.
- **Sharing:** who their data will be shared with if not used solely by your organisation, and the conditions under which it is shared.
- **The obligation to inform individuals:** If you plan to rely on Legitimate Interest, you're obliged to inform the data subject of those Legitimate Interests.
- **The right to object:** If relying on Legitimate Interest, you're also obliged to inform the data subject of their right to object to such processing.

To help you comply with the rules laid out by the GDPR, it is essential that you maintain an inhouse opt-out file, and act on any requests as soon as practicable – regardless of which basis you're relying on to justify data processing.

WHEN CAN YOU USE LEGITIMATE INTEREST?

Businesses are encouraged to use Legitimate Interest as their basis for processing data when:

- There is clear benefit to the business
- There is limited privacy impact on the data subject
- The data subject should reasonably expect you to use their data in this way (your privacy notice should establish reasonable expectation)
- No Legal Requirements or Consent are required

To give you a clearer idea of how and when Legitimate Interest may be applied in commercial settings, we've included an insightful (but non-exhaustive) list of examples.

EXAMPLES OF LEGITIMATE INTEREST

- **FRAUD:** An insurance company needs to process personal data in order to meet critical anti-fraud measures; whilst this is clearly in the interests of the data controller, it is also in its customers' interests, as the cost of fraud can raise insurance premiums for all.
- **INDIVIDUAL RIGHTS:** A data subject has objected to the processing of their personal data, and exercised their right to erasure; the business in question needs to retain basic data – purely for suppression purposes – to prevent the data subject from further unwanted processing.
- **NETWORK SECURITY:** As specified in its IT governance policies, a mail order company monitors access to accounts containing Personal Data by named users within the organisation, in order to prevent theft of data by employees
- **PROFILING:** In carrying out its risk modelling, an insurance company captures and uses a range of personal data in order to assess factors affecting those risks, such as age, location and claims history.
- **EVIDENTIAL PURPOSES:** A hotel logs customer entries and exits to their hotel rooms, as well as employee access to customers' rooms, using key card data. This information is used to manage disputes with guests, investigate staff misconduct, and improve customer experience. The data is limited and normally only retained for 31 days, then deleted.
- **EMPLOYEE RELATIONS:** A financial services company processes an employee's contact details in order to arrange business travel, and ensure the employee receives benefits and training.
- **HUMAN RESOURCES RECORDS:** A distribution company processes the personal data of its employees in order to provide optional staff benefits, such as health plan and gym membership.
- **DIRECT MARKETING:** A charity sends a postal mailshot to existing supporters providing an update on its activities and details of upcoming events.
- **POSTAL MARKETING FROM THIRD PARTIES:** A catalogue company adds details to its online order forms which suggests it shares data with other cataloguers. The purchaser can object to this sharing this sharing, and the cataloguers are listed in the privacy statement.

Reference: Examples from IAPP/Data Protection Network Guidance

Be aware that the right to object to direct marketing, regardless of its format, is an absolute right. You must stop marketing activities immediately if you receive an objection to processing an individual's data for marketing purposes.

If you do hope to rely on Legitimate Interest, you will need to demonstrate that your interests are not overridden by the interests or fundamental rights and freedoms of the individuals in question. And you demonstrate that by carrying out a Legitimate Interest Assessment.

You will need an LIA for each new processing activity, and must give the data subject the option to opt out of processing each time.

LEGITIMATE INTEREST ASSESSMENTS (LIA)

A Legitimate Interest Assessment is essentially a balancing test. You can't just assume that you have a Legitimate Interest because you're a business that needs to reach out to customers. For your own protection (as well as that of your data subjects), it's essential to carry out – and document – LIAs whenever you plan to use Legitimate Interest as your legal basis for data processing. And we mean whenever. New direct marketing campaign? New LIA.

We've provided a template for you to follow; filling this out for each LIA will help you to meet the accountability and transparency requirements that are pivotal to GDPR and PECR. But briefly, the LIA is split into three different stages.

THREE STAGES OF AN LIA

- 1. Identify a Legitimate Interest:** An LIA is designed to make you think. So consider, why are you processing personal data? What's the purpose, and why is that important to you as the data controller? This needs to be clearly articulated to the data subject.
- 2. Carry out a Necessity Test:** Whatever your commercial or business objectives, is the processing of personal data necessary to achieve them? Or is there another way to achieve those same objectives?
- 3. Carry out a Balancing Test:** You can only rely on Legitimate Interest when, after evaluation, the rights and freedoms of the data subject do not override your (the Controller's) Legitimate Interest. The balancing test must be conducted fairly.

When planning to rely on Legitimate Interest, it's important to consider the individual's 'reasonable expectations': would (or should) that individual expect their data to be processed in this way?

For example, just because you purchased a car, you would not necessarily expect to be marketed a caravan. However, if you purchased a tow bar with that car, it may be reasonable to expect some follow-up marketing information about caravans. As part of your privacy notices at the point of sale, the marketing of related products or services should be listed as processing under legitimate interest – particularly if this marketing may come from a third party like a sister organisation.

The outcome of your LIA should be documented as evidence and reviewed periodically. You must also provide your data subject with a clear opportunity to opt out every time you process their data. And if you fall foul of the regulations? Some stats to bear in mind...

Since the introduction of the GDPR in May 2018, there have been:



144,376

queries and complaints
from all data protection
authorities in Europe



89,271

data breach notifications
from all data protection
authorities in Europe

And for those found breaking the rules?



£400k

Bounty (UK) fined for sharing
data for unlawful marketing



£500k

In December 2018, it was ruled that
Directors of companies who make
nuisance phone calls now face
personal fines of up to **£500,000**



In September 2018, the first
employee was **jailed** for **computer
misuse** in contacting people
unlawfully for **marketing purposes**

*So whether you're a business, company Director, or a single employee,
your LIA must be robust enough to protect you.*

IN SUMMARY

Legitimate Interest can be a great option for organisations that rely on digital marketing or processing to meet their business aims, but you need to follow the proper steps to protect yourself, your business, and the rights and freedoms of your data subjects.

SOME IMPORTANT POINTS TO REMEMBER:

- Ensure you meet the criteria to be able to use Legitimate Interest as opposed to consent for marketing activities;
- Make sure your privacy policy is clear, accessible, and underlines the fact that you're relying on Legitimate Interest for marketing purposes;
- When you collect data or communicate with a data subject, you need to provide them with a clear and simple opportunity to opt out of marketing communications;
- If an individual does exercise their right to opt out, act on the request immediately – removing them from both communications and any profiling activities;
- Refrain from spam, be sure to always send relevant content, and never communicate anything that can be deemed inappropriate;
- Even if your LIA balances in your favour, you can still be guilty of the 'nuisance factor' with overly frequent communications;
- Your LIA should identify risks with contacting anyone that could be considered 'vulnerable' (such as offering high interest loans to those in financial trouble);
- Always clearly document your assessment of how Legitimate Interest applies and be prepared to justify this if necessary.



Legitimate Interest Assessment		Assessment No.
		0000
Legitimate Interest		
Data Description	(Established in the Data Mapping and Discovery)	
Data Processing Activity	(Established in the Data Mapping and Discovery)	
Processing Purpose	(What is the purpose of the processing activity?)	
3rd Party Sharing and disclosure	(Who else may the data be shared with and for what purpose?)	
Organisational Objectives	(Clearly state how company objectives are achieved through this processing activity?)	

Balancing Test	
Data Subject Expectation	(Is the Data Subject Expecting or have an expectation that the Processing Activity will Take Place?)
Value/Benefit	(Does the processing benefit or add value to a product or service used by the data subject?)
Data Subject Impact	(Will the processing negatively impact the Data Subjects Rights?)
Distress / Harm	(Could the processing result in distress or harm to the data subject?)
Data Subject Interest	(Is the processing in the interests of the Data Subject?)
Existing Relationship	(What is the existing connection between the organisation and the Data Subject?)
Data Category	(What is the category (type/sensitivity) of the data being processed?)
Data Source	(Has the data been obtained directly from the data subject?)

Now you're ready, refer to our Legitimate Interest Assessment Template to complete and review your own assessment. If you're unsure, you can also view the Legitimate Interest Assessment Example to view how they can be completed.

Whilst we've provided an LIA template to help you determine whether Legitimate Interest can reasonably be relied upon, you should bear in mind that conclusions are subjective and must always be based on the judgment and experience of those conducting the assessment.

This template should also be completed alongside the ICO's guidance on Legitimate Interests, and modified to suit your own business.

GET IN TOUCH

If you would like to discuss LIAs – or the GDPR at large – in more detail, and how the Regulations relate to your campaigns, please get in touch.

Avoid creating biased, self-serving LIA's in order to 'justify' data processing activities. They might tick the box for demonstrating you have a documented LIA, but they are a complete waste of time.

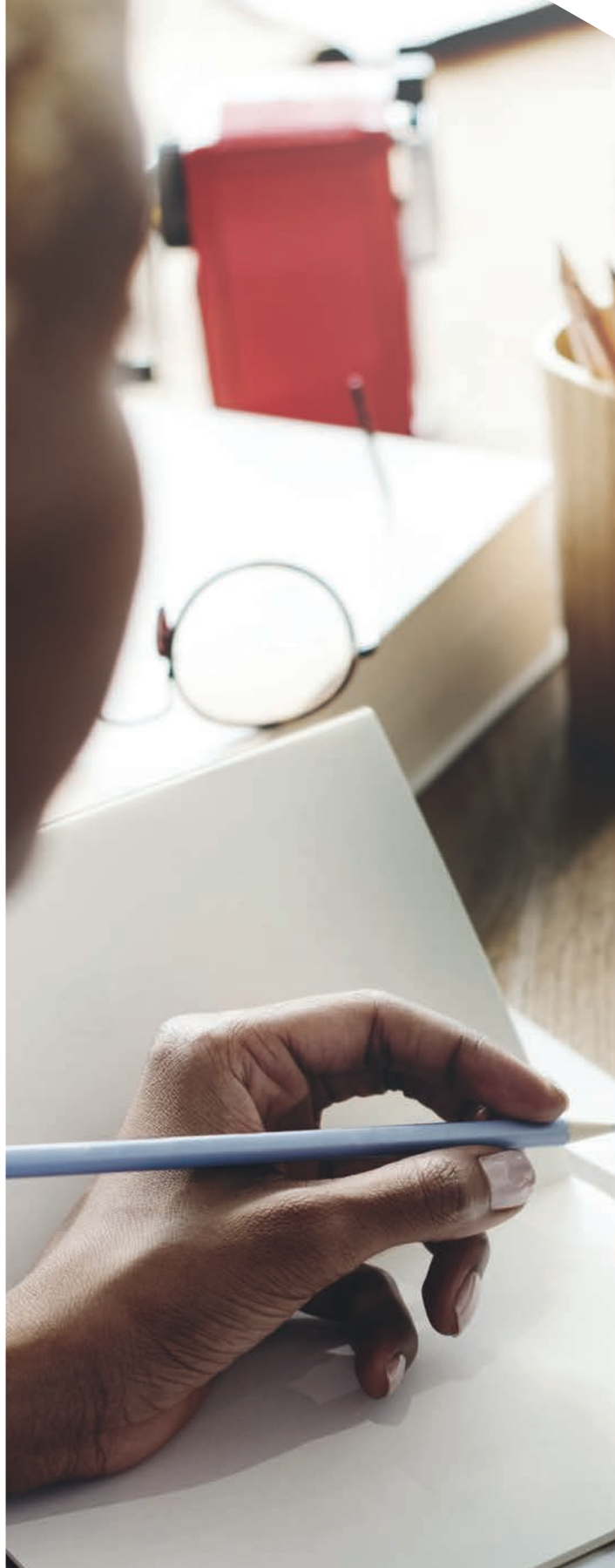
ABOUT KPM

EFFECTIVE DIRECT MAIL, PRINT AND FULFILMENT

We are a print production company based in Swanley, Kent, established in 2001. We are known for delivering high quality print management, from multichannel campaigns to complex fulfilment. From direct mail that gets noticed to navigating cost effective postage options, we'll help your campaigns to make an impact.

- ✓ Direct mail design, copy and campaign production
- ✓ Full Print Management
- ✓ Online portals for Print on Demand and Web2Print
- ✓ Fulfilment, packaging and VAT advice
- ✓ Best postage options

We can design, copy write and produce campaigns on your behalf, working with clients across a range of industry sectors. We also advise on GDPR, VAT guidelines and pack design to ensure that mailings are fully compliant.







COMPLIANT CAMPAIGNS

Optimise multichannel marketing with effective direct mail, print and fulfilment.



T: 01322 663328

E: sales@kpmgroup.co.uk

www.kpmgroup.co.uk



Print Management | Personalisation | Web2Print | Print Production | Fulfilment & Mailing
