# Sample LIA template

This legitimate interests assessment (LIA) template is designed to help you to decide whether or not the legitimate interests basis is likely to apply to your processing. It should be used alongside our legitimate interests guidance.

## Part 1: Purpose test

You need to assess whether there is a legitimate interest behind the processing.

| |
|---|
| • Why do you want to process the data?<br>• What benefit do you expect to get from the processing?<br>• Do any third parties benefit from the processing?<br>• Are there any wider public benefits to the processing?<br>• How important are the benefits that you have identified?<br>• What would the impact be if you couldn't go ahead with the processing?<br>• Are you complying with any specific data protection rules that apply to your processing (eg profiling requirements, or e-privacy legislation)?<br>• Are you complying with other relevant laws?<br>• Are you complying with industry guidelines or codes of practice?<br>• Are there any other ethical issues with the processing? |
| • Why do you want to process the data?<br>We want to process the data to improve our email marketing strategy, improve the accuracy of audience engagement levels, and enable more personalised and effective communications.<br><br>• What benefit do you expect to get from the processing?<br>We expect to:<br>  • Improve audience engagement<br>  • Boost revenue through more targeted and effective communications<br>  • Maintain an up-to-date and accurate database<br>  • Keep our audience updated with relevant information<br><br>• Do any third parties benefit from the processing?<br>While the primary beneficiary is Proctor + Stevenson, our partners may indirectly benefit from improved targeting for joint initiatives. However, they will not have direct access to the enhanced data.<br><br>• Are there any wider public benefits to the processing?<br>Fundamentally, this processing exercise is purely to meet the business requirements of our clients so there is no direct benefit to the wider public. |

- How important are the benefits that you have identified?
  N/A

- What would the impact be if you couldn't go ahead with the processing?
  - Have less accurate audience data, potentially leading to less effective communications
  - Miss opportunities to encourage businesses to invest in their marketing to increase their own success
  - Be limited in our ability to personalise services and recommendations

- Are you complying with any specific data protection rules that apply to your processing (eg profiling requirements, or e-privacy legislation)?
  Yes, we are complying with GDPR requirements, including:
  - Complying with UK GDPR and the Privacy and Electronic Communications Regulations (PECR) for email marketing
  - Sending marketing emails only where there is a lawful basis (consent or "soft opt-in" for existing customers)
  - Providing clear and simple opt-out (unsubscribe) options in all communications
  - Maintaining records of consent where required and regularly review/update marketing lists
  - Ensuring transparency, fairness, and purpose limitation in line with internal Data Protection and GDPR policies
  - Carrying out limited, proportionate profiling/segmentation only to improve relevance (no automated decision-making with legal or significant effects)
  - Applying ISO 27001-certified controls to protect marketing data (e.g. access control, secure storage, defined retention periods)
  - GDPR compliance independently verified by an external data protection partner

- Are you complying with other relevant laws?
  - Yes — we comply with all relevant UK data protection and business legislation applicable to our processing activities
  - This includes UK GDPR, the Data Protection Act 2018, and PECR (for electronic marketing)
  - We adhere to contractual, confidentiality, and intellectual property obligations where applicable
  - Our ISO 27001-certified Information Security Management System ensures compliance is embedded through policies, controls, and regular audits

- Are you complying with industry guidelines or codes of practice?
    - Yes — we align with recognised industry standards and best practice frameworks for information security and data protection
    - We are accredited to ISO 27001, demonstrating adherence to internationally recognised information security management standards
    - Our policies and controls are structured in line with ISO 27001 requirements, including risk management, access control, encryption, and incident management
    - We follow ICO guidance and best practice recommendations for GDPR compliance and responsible data handling
    - Our processes reflect established principles such as data minimisation, purpose limitation, and security by design and default
    - Staff operate under a formal Data Protection Code of Conduct, reinforcing consistent application of these standards
    - Compliance is regularly reviewed through internal audits and independently verified by an external data protection partner

- Are there any other ethical issues with the processing?
  We have considered potential ethical issues, such as:
    - Ensuring fair treatment of all customer segments
    - Maintaining transparency about data usage

  We are addressing these by:
    - Regularly reviewing our data
    - Providing clear information about data usage in our privacy notices
    - Offering opt-out options for customers who prefer not to have their data processed in this way

## Part 2: Necessity test

You need to assess whether the processing is necessary for the purpose you have identified.

| |
|---|
| • Will this processing actually help you achieve your purpose?<br>• Is the processing proportionate to that purpose?<br>• Can you achieve the same purpose without the processing?<br>• Can you achieve the same purpose by processing less data, or by processing the data in another more obvious or less intrusive way? |
| • Will this processing actually help you achieve your purpose?<br>  ○ Yes — the processing is necessary and effective in achieving our purpose of delivering relevant email marketing communications<br>  ○ It enables us to communicate with individuals about services, updates, and content that are relevant to their interests or existing relationship with us<br>  ○ Limited profiling and segmentation help ensure communications are targeted and meaningful, improving engagement and reducing irrelevant messaging<br>  ○ The processing supports maintaining accurate and up-to-date contact records, ensuring individuals' preferences are respected<br>  ○ It allows us to manage consent and opt-out requests effectively, ensuring ongoing compliance with GDPR and PECR<br><br>• Is the processing proportionate to that purpose?<br>  ○ Yes — the processing is proportionate to the purpose of delivering relevant email marketing communications<br>  ○ We only process the minimum personal data necessary (e.g. contact details and limited preference or engagement data)<br>  ○ Any segmentation or profiling is kept simple, relevant, and non-intrusive, solely to improve communication relevance<br>  ○ We do not use excessive, sensitive, or unrelated data for marketing purposes<br>  ○ Individuals retain full control through clear consent mechanisms and easy opt-out options at any time<br>  ○ Data is retained only for as long as necessary in line with our retention policies<br>  ○ Appropriate technical and organisational controls (aligned with ISO 27001) ensure data is handled securely and responsibly<br><br>• Can you achieve the same purpose without the processing?<br>  ○ No — the purpose cannot be effectively achieved without this processing |

- Email marketing inherently requires the use of personal data (e.g. contact details) to deliver communications to individuals
- Without processing this data, we would be unable to send relevant updates, services information, or manage ongoing client/prospect relationships
- Alternative approaches (e.g. generic, non-targeted advertising) would be less effective, less relevant, and potentially more intrusive
- The limited use of segmentation ensures communications remain appropriate and reduces unnecessary or unwanted contact
- Processing is therefore necessary to achieve the intended purpose in a targeted, controlled, and compliant manner

- Can you achieve the same purpose by processing less data, or by processing the data in another more obvious or less intrusive way?
  - We already apply data minimisation and only process the minimum personal data necessary (e.g. name, contact details, and limited preference data)
  - The purpose cannot be achieved with significantly less data, as basic contact information is essential to deliver email communications
  - Any segmentation is deliberately simple and non-intrusive, avoiding excessive or detailed profiling
  - We do not process special category data or unnecessary personal information for marketing purposes
  - Processing is conducted in the least intrusive way, with clear transparency, lawful basis, and easy opt-out mechanisms
  - Individuals are given control over their data and communication preferences at all times
  - Our approach ensures the purpose is met in a way that is proportionate, privacy-conscious, and aligned with GDPR principles

# Part 3: Balancing test

You need to consider the impact on individuals' interests and rights and freedoms and assess whether this overrides your legitimate interests.

First, use the DPIA screening checklist. If you hit any of the triggers on that checklist you need to conduct a DPIA instead to assess risks in more detail.

| **Nature of the personal data** |
| --- |
| • Is it special category data or criminal offence data?<br>• Is it data which people are likely to consider particularly 'private'?<br>• Are you processing children's data or data relating to other vulnerable people?<br>• Is the data about people in their personal or professional capacity? |

- Is it special category data or criminal offence data?
    - No, we are not processing any special category data or criminal offence data. The data being appended is general demographic and lifestyle information, not sensitive personal data as defined under GDPR.

- Is it data which people are likely to consider particularly 'private'?
    - The data being processed is unlikely to be considered particularly 'private'. It includes:
        - Which of our ads they have engaged with
        - The company and industry they work in
        - Job title
        - Location (as available on LinkedIn)

- Are you processing children's data or data relating to other vulnerable people?
    - We are not processing children's data and the data being processed would not identify someone as being vulnerable

- Is the data about people in their personal or professional capacity?
    - The data is primarily about people in their professional capacity. However, some of the data may indirectly relate to someone's personal capacity i.e. their country location (as taken from LinkedIn)

**Reasonable expectations**

- Do you have an existing relationship with the individual?
- What's the nature of the relationship and how have you used data in the past?
- Did you collect the data directly from the individual? What did you tell them at the time?
- If you obtained the data from a third party, what did they tell the individuals about reuse by third parties for other purposes and does this cover you?
- How long ago did you collect the data? Are there any changes in technology or context since then that would affect expectations?
- Is your intended purpose and method widely understood?
- Are you intending to do anything new or innovative?
- Do you have any evidence about expectations – eg from market research, focus groups or other forms of consultation?
- Are there any other factors in the particular circumstances that mean they would or would not expect the processing?

- Do you have an existing relationship with the individual?
    - Yes — in many cases, we have an existing relationship with the individual (e.g. current clients, previous clients, or individuals who have engaged with our services or content)

- Where this relationship exists, we may rely on the "soft opt-in" under PECR to send relevant marketing communications
- Where no direct relationship exists, individuals are identified via two primary channels:
  - Intent-Based: Individuals who have engaged with our digital assets (e.g. our website, tracked via Leadfeeder). In these instances, there is a reasonable expectation of contact, as the individual has demonstrated an active interest in our services. Communication is strictly limited to the specific area of interest shown during their visit.
  - Sector-Based: Professionals identified via Clay who operate within sectors directly relevant to our services. While no prior relationship exists, the processing is restricted to professional contact data used in a business-to-business (B2B) context. The communication is highly targeted to their specific job role, ensuring the outreach is relevant and provides professional value, thereby minimising any perceived intrusiveness.
- We ensure that all communications are relevant to the individual's interaction with us and aligned with their reasonable expectations
- Regardless of the relationship, individuals are always provided with clear information and the ability to opt out at any time

- What's the nature of the relationship and how have you used data in the past?
  - The relationship is typically that of a client, prospective client, or individual who has engaged with us (e.g. enquiries, downloads, event attendance, or subscription to communications)
  - In the past, we have used personal data to respond to enquiries, deliver requested services, and provide relevant information about our offerings
  - Where appropriate, we have also used contact details to send marketing communications in line with consent or soft opt-in rules under PECR
  - Data has been used in a transparent and limited way, aligned with the individual's expectations at the point of collection
  - We have maintained accurate records, respected preferences, and honoured opt-outs at all times
  - All processing has been carried out in accordance with our Data Protection Policy, ensuring fairness, security, and compliance with UK GDPR
  - Our ISO 27001-certified controls ensure that personal data has always been handled securely and responsibly throughout the relationship

- Did you collect the data directly from the individual? What did you tell them at the time?

- In most cases, personal data is collected directly from the individual (e.g. via website forms, enquiries, or event registrations)
  - At the point of collection, individuals are provided with clear privacy information explaining how their data will be used
  - This includes the purpose of processing (e.g. responding to enquiries, delivering services, and/or sending marketing communications)
- For intent and sector-based channels, data was collected indirectly.
  - For website visitors, data was sourced via Leadfeeder, which identifies business IPs and associated professional profiles.
  - For sector-specific prospecting, data was sourced via Clay, utilising publicly available professional records and business directories.
  - As the data was not collected directly, individuals were not informed at the point of collection. However, in compliance with Article 14 of the UK GDPR, we provide a link to our Privacy Notice in the first point of communication. This notice clearly outlines the categories of data processed, the source of the data, and the individual's right to object (opt-out) at any time.
- For all communication:
  - We inform individuals of the lawful basis for processing, including consent or legitimate interests where applicable
  - Individuals are made aware of their rights under UK GDPR, including the right to withdraw consent and opt out of marketing at any time
  - We provide access to our Privacy Notice, which outlines data handling practices, retention, and sharing arrangements
  - All information is presented in a transparent and accessible way, ensuring individuals understand how their data will be used before it is collected

- If you obtained the data from a third party, what did they tell the individuals about reuse by third parties for other purposes and does this cover you?
  - Where personal data is obtained from a third party, we ensure that the provider has collected the data lawfully and transparently
  - We seek confirmation that individuals were informed their data may be shared with third parties for marketing or related purposes
  - We ensure that this information is sufficient to cover our intended use of the data before processing begins
  - We only use third-party data where there is a valid lawful basis (e.g. consent or soft opt-in, where applicable)
  - If adequate transparency has not been provided, we will not use the data for marketing purposes

- We provide our own privacy information to individuals at the earliest opportunity, ensuring they understand how their data is used by us
- Individuals are always given the option to opt out of communications and exercise their data protection rights
- All third-party data sharing and use is governed by our Data Sharing Policy and GDPR compliance framework

- How long ago did you collect the data? Are there any changes in technology or context since then that would affect expectations?
  - Personal data is typically collected at the point of interaction (e.g. enquiry, sign-up, or engagement) and is regularly reviewed to ensure it remains accurate and relevant
  - We do not retain or use data indefinitely; retention periods are defined in line with our Personal Data Retention Policy
  - Marketing data is periodically cleansed, and outdated or inactive contacts are removed to ensure continued relevance
  - We consider the context in which the data was originally collected, including the individual's expectations at that time
  - Where there have been changes in technology, communication methods, or regulatory expectations, we review and update our practices accordingly
  - If the original context no longer supports the intended use (e.g. outdated consent or long periods of inactivity), we will refresh consent or cease processing
  - This ensures that our use of personal data remains fair, up to date, and aligned with current expectations and GDPR requirements

- Is your intended purpose and method widely understood?
  - Yes — the purpose and method (email marketing using contact details) are widely understood and commonly used across industries
  - Individuals generally expect that, where they have engaged with a business or provided their details, they may receive relevant marketing communications
  - The use of basic contact data and limited segmentation to tailor communications is standard practice and aligns with industry norms
  - We ensure transparency by clearly explaining our processing at the point of data collection and within our Privacy Notice
  - Our approach is consistent with ICO guidance and PECR requirements, reinforcing that the processing is both familiar and expected

- Are you intending to do anything new or innovative?

- No. The processing involves standard B2B direct marketing practices that are well-established within the industry, and utilising industry-standard tools (Leadfeeder and Clay) to identify relevant professional business contacts. We are not using any new or intrusive technologies, nor are we engaging in large-scale automated profiling or the processing of special category data.

- Do you have any evidence about expectations – eg from market research, focus groups or other forms of consultation?
  - We rely on established industry practice and regulatory guidance (ICO and PECR), which indicate that individuals generally expect to receive marketing communications where they have engaged with an organisation
  - Our experience of client and prospect interactions shows that individuals anticipate relevant follow-up communications after enquiries, downloads, or event participation
  - Engagement metrics (e.g. open rates, click-throughs, and unsubscribe rates) are monitored to assess whether communications align with expectations
  - Low complaint and opt-out rates provide practical evidence that our marketing activity is not unexpected or intrusive
  - While formal market research or focus groups are not specifically undertaken for this purpose, our approach is informed by ongoing interaction data and recognised best practice guidelines

- Are there any other factors in the particular circumstances that mean they would or would not expect the processing?
  - The nature of the relationship (e.g. existing client or prior engagement) supports a reasonable expectation of receiving relevant communications
  - The context in which the data was collected (e.g. sign-ups, enquiries, or content downloads) makes follow-up marketing proportionate and expected
  - For contacts we obtain through third parties / applications such as LeadFeeder or Clay, we specifically identify job titles and functions which would hold relevant to the communications we are sending.
  - Clear privacy information and, where required, consent mechanisms ensure individuals are aware of how their data will be used
  - The inclusion of simple and accessible opt-out options reinforces user control and aligns with expectations
  - Our use of minimal, non-intrusive data and limited segmentation reduces the likelihood of the processing being perceived as unexpected or intrusive

- There are no factors in our processing that would override or conflict with these expectations, as all activity is conducted transparently and in line with UK GDPR and PECR requirements

**Likely impact**

- What are the possible impacts of the processing on people?
- Will individuals lose any control over the use of their personal data?
- What is the likelihood and severity of any potential impact?
- Are some people likely to object to the processing or find it intrusive?
- Would you be happy to explain the processing to individuals?
- Can you adopt any safeguards to minimise the impact?

- What are the possible impacts of the processing on people?
  - The impact on individuals is generally low, as the processing relates to standard email marketing using limited personal data
  - Individuals may receive marketing communications that they do not wish to engage with, which could cause minor inconvenience
  - There is a potential risk of perceived intrusion if communications are too frequent or not sufficiently relevant
  - However, this is mitigated through clear opt-out options and careful list management
  - There is a minimal risk to privacy, as we do not process sensitive data or carry out intrusive profiling
  - Strong security controls (aligned with ISO 27001) reduce the risk of unauthorised access or data breaches
  - Individuals retain full control over their data, including the right to object, unsubscribe, or request deletion
  - Overall, any potential impacts are limited, manageable, and mitigated through appropriate safeguards and compliance with UK GDPR and PECR

- Will individuals lose any control over the use of their personal data?
  - No — individuals do not lose control over their personal data as a result of this processing
  - Individuals retain full control through clear consent mechanisms (where applicable) and the ability to opt out at any time
  - Every marketing communication includes an easy and accessible unsubscribe option
  - Individuals can exercise their rights under UK GDPR, including access, rectification, erasure, and the right to object to processing
  - Preferences are respected and actioned promptly, ensuring ongoing control over how data is used
  - Processing is transparent, with clear privacy information provided at the point of data collection

- What is the likelihood and severity of any potential impact?

- The likelihood of negative impact is low, as the processing involves standard, well-controlled email marketing practices
- The severity of any potential impact is also low, typically limited to minor inconvenience (e.g. receiving unwanted emails)
- There is minimal risk of harm, as no sensitive data is processed and profiling is limited and non-intrusive
- Risks such as loss of control or privacy are mitigated through clear opt-out mechanisms and strong data protection practices
- Robust technical and organisational controls, aligned with ISO 27001, reduce the likelihood of security incidents
- Regular data review, consent management, and adherence to retention policies further minimise risk
- Overall, both the likelihood and severity of impact are low, and any residual risks are appropriately managed in line with UK GDPR requirements

- Are some people likely to object to the processing or find it intrusive?
  - Some individuals may perceive marketing emails as intrusive, particularly if they are not relevant or are received too frequently, however, this risk is expected and typical for email marketing activities.
  - We mitigate this by ensuring communications are targeted, proportionate, and aligned with the individual's interests or prior engagement
  - Clear opt-out (unsubscribe) options are provided in every communication, allowing individuals to stop messages easily
  - We respect preferences and promptly action unsubscribe or objection requests
  - We avoid excessive contact and regularly review marketing lists to maintain relevance
  - Overall, while a small number of individuals may object, the processing is designed to minimise intrusion and align with reasonable expectations under UK GDPR and PECR

- Would you be happy to explain the processing to individuals?
  - Yes

- Can you adopt any safeguards to minimise the impact?
  - Yes — a range of safeguards are in place to minimise any potential impact on individuals
  - We apply data minimisation, only using the minimum personal data necessary for email marketing
  - Clear consent mechanisms (where required) and transparent privacy information ensure individuals understand how their data is used
  - Every communication includes a simple and effective unsubscribe option, enabling individuals to opt out at any time

| |
|---|
| ○ We limit the frequency of communications and use light, non-intrusive segmentation to maintain relevance<br>○ Marketing lists are regularly reviewed and cleansed to remove outdated or inactive contacts<br>○ Strong technical and organisational security controls (aligned with ISO 27001) protect personal data from unauthorised access or loss<br>○ Defined data retention periods ensure personal data is not kept longer than necessary<br>○ Staff follow a Data Protection Code of Conduct, ensuring consistent and compliant handling of personal data<br>○ Processes are regularly reviewed and supported by independent GDPR compliance verification |

| | |
|---|---|
| Can you offer individuals an opt-out? | **Yes** / No |

## Making the decision

This is where you use your answers to Parts 1, 2 and 3 to decide whether or not you can apply the legitimate interests basis.

| | |
|---|---|
| Can you rely on legitimate interests for this processing? | **Yes** / No |
| Do you have any comments to justify your answer? (optional) | |
| LIA created by | Angel Broom (Marketing Lead) |
| LIA signed off by | Steve King (Technology Director) |
| Date | 27/08/2026 |

## What's next?

Keep a record of this LIA, and keep it under review.

Do a DPIA if necessary.

Include details of your purposes and lawful basis for processing in your privacy information, including an outline of your legitimate interests.