

LIA Demand Science US, LLC



This legitimate interest assessment (LIA) is for Demand Science US, LLC and all entities.

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?
- What benefit do you expect to get from the processing?
- Do any third parties benefit from the processing?
- Are there any wider public benefits to the processing?
- How important are the benefits that you have identified?
- What would the impact be if you couldn't go ahead with the processing?
- Are you complying with any specific data protection regulations that apply to your processing (e.g. profiling requirements, or e-privacy legislation)?
- Are you complying with other relevant laws?
- Are you complying with industry guidelines or codes of practice?
- Are there any other ethical issues with the processing?

Why do you want to process the data?

To collect unstructured, publicly available information to form complete and accurate business data records and make it available to provide our customers with access to a database of accurate business data records including BCI which enables them to promote their goods and services employing direct marketing to the right people (i.e., decision makers, influencers, champions) in other businesses, and to promote your business so it can be found when it is searched for by other businesses.

Such information could include identifiers, such as name, title, department, company name, company's officers, and certain company employees, business and/or cell phone numbers, office address, email addresses, social media data and similar information. We may combine the information we obtain from such sources with information we otherwise collect.

We do not collect or use financial account numbers, Social Security numbers, pharmaceutical prescriptions, medical records or any other sensitive information about a specific individual for online behavioral advertising.

Device Fingerprint. We use browser fingerprinting technology to enhance our understanding of how users interact with our website. Browser fingerprinting involves collecting and analyzing certain configuration details of your browser and operating system, such as screen resolution, installed plugins, fonts, and other non-identifying characteristics, to generate a unique identifier. Please note that while we use these configurations to create the identifier, we do not store or retain any of the underlying data used in its generation. The resulting identifier is solely used for tracking, identifying, and reporting on website visitors' interactions. This helps us improve our services, better understand visitor behaviour, and assess the effectiveness of our website and marketing efforts.

What benefit do you expect to get from the processing?

Improved Services: Enhancing the quality and efficiency of our services by analyzing user data to understand preferences and behaviours.

Marketing: Conducting targeted marketing campaigns to reach the right audience with relevant offers, which can increase engagement and sales.

Operational Efficiency: Streamlining internal processes and operations, leading to cost savings and better resource management.

Customer Relationship Management: Building and maintaining strong relationships with customers by providing personalized experiences and support.

This will allow our products and services to operate more effectively while ensuring that the processing does not infringe on individuals' rights and freedoms.

Do any third parties benefit from the processing?

Our B2B data is beneficial to our clients for marketing and offers them several benefits:

Enhanced Targeting: Companies can identify and understand their target audience more precisely, leading to more effective and relevant marketing campaigns.

Personalization: Data allows for the creation of personalized marketing messages and campaigns, improving engagement and conversion rates.

Optimized Campaigns: By analyzing past performance data, businesses can refine their strategies for better ROI and more efficient use of marketing budgets.

Data-Driven Decisions: Reliable data enables companies to make informed decisions based on measurable insights rather than assumptions, leading to more strategic and successful marketing efforts.

Competitive Advantage: Access to high-quality B2B data can give companies a competitive edge by allowing them to stay ahead of market trends and better meet customer needs.

Improved Customer Relationships: Understanding customer behaviours and preferences helps businesses build stronger businesses.

These benefits collectively contribute to more effective marketing strategies and better business outcomes.

Are there any wider public benefits to the processing?

When businesses perform well, the public can experience several wider benefits:

Successful businesses contribute to overall economic growth, leading to increased national income and improved living standards.

Thriving businesses create more job opportunities, reducing unemployment rates and providing financial stability for individuals and families.

Innovation and Development: Profitable businesses often invest in research and development, leading to technological advancements and innovative products that can improve quality of life.

Competition among successful businesses drives improvements in the quality and variety of products and services available to consumers.

Many businesses engage in corporate social responsibility (CSR) activities, supporting local communities through charitable donations, sponsorships, and volunteer programs.

Profitable businesses contribute significantly to government tax revenues, which can be used to fund public services such as healthcare, education, and infrastructure.

These benefits collectively enhance the overall well-being and prosperity of society.

How important are the benefits that you have identified?

The ability to process publicly available business Personally Identifiable Information (PII) is crucial to the success of a Demand Science, LLC for several reasons:

Accurate and detailed business PII allows us to provide their clients with highly targeted leads, increasing the effectiveness of marketing campaigns and improving client satisfaction.

Access to business PII enables the creation of personalized marketing strategies, which can lead to higher engagement and conversion rates for clients.

Data-driven insights from business PII help clients optimize their marketing efforts, leading to better resource allocation and higher returns on investment.

Providing high-quality, actionable business data gives data brokers a competitive edge in the market, attracting more clients and retaining existing ones.

By helping businesses thrive through effective marketing, data brokers contribute to overall economic growth, which benefits the broader economy and society.

These benefits are essential for Demand Science, LLC to deliver value to our clients, maintain a competitive position in the market, and drive business success.

What would the impact be if you couldn't go ahead with the processing?

If we were unable to process B2B Personally Identifiable Information (PII), we would face several significant challenges:

Reduced Targeting Accuracy: Without access to detailed business PII, the ability to provide precise and targeted leads to clients would be diminished, leading to less effective marketing campaigns.

Limited Personalization: The lack of business PII would hinder the creation of personalized marketing strategies, resulting in lower engagement and conversion rates.

Decreased Competitive Edge: Demand Science, LLC would struggle to maintain a competitive advantage without high-quality, actionable business data, potentially losing clients to competitors who can offer better insights.

Suboptimal Campaigns: Clients would have to rely on less accurate data, leading to inefficient resource allocation and lower returns on investment.

Economic Impact: The overall economic contribution of Demand Science LLC would be reduced, as our ability to help businesses thrive through effective marketing would be compromised.

These effects would significantly impact the value Demand Science, LLC to provide our clients and their overall business success.

Are you complying with any specific data protection regulations that apply to your processing (e.g. profiling requirements, or e-privacy legislation)?

Yes, we comply with all applicable, global data protection regulations that apply to our processing activities, including:

GDPR: We adhere to the General Data Protection Regulation (GDPR), which includes provisions on automated decision-making and profiling. This involves ensuring we have a lawful basis for processing, conducting Data Protection Impact Assessments (DPIAs), and providing transparency to individuals.

E-Privacy Legislation: We comply with e-privacy regulations, which govern electronic communications and marketing activities. This includes obtaining consent for marketing communications and ensuring the security and confidentiality of electronic communications.

Profiling Requirements: We follow the guidelines for profiling under the GDPR, which include conducting a balancing test to ensure that our legitimate interests do not override individuals' rights and freedoms and providing individuals with the option to object to profiling.

These measures help us ensure that our data processing activities are lawful, transparent, and respectful of individuals' privacy rights.

Are you complying with other relevant laws?

Yes, we comply with all GDPR and privacy laws in the EU, and the UK GDPR and relevant additional privacy laws in the UK such as the PECR. This includes:

General Data Protection Regulation (GDPR): We adhere to all principles and requirements, such as obtaining lawful consent, ensuring data minimization, and conducting Data Protection Impact Assessments (DPIAs) when necessary

E-Privacy Directive: We comply with regulations governing electronic communications, including obtaining consent for cookies and direct marketing activities

Accountability and Transparency: We maintain detailed records of our data processing activities and ensure transparency by informing individuals about how their data is used.

Data Subject Rights: We respect and facilitate the rights of data subjects, such as the right to access, rectify, and erase their personal.

Security Measures: We implement appropriate technical and organizational measures to protect personal data against unauthorized access, loss, or damage.

These measures ensure that our data processing activities are lawful, transparent, and respectful of individuals' privacy rights.

What about North America?

Additionally, we comply with all relevant data privacy laws and regulations in North America, including the applicable US state data privacy regulations such as the CCPA, and TCPA. We also comply with PIPEDA and the Canadian Radio-television Telecommunications Commission's (CRTC) Unsolicited Telecommunications Rules (UTR).

Are you complying with industry guidelines or codes of practice?

We follow the Information Commissioner's Office (ICO) guidelines on the use of customers' personal data, ensuring compliance with data protection laws.

These guidelines help us maintain high standards in our marketing activities and ensure we respect the rights and privacy of individuals.

There are several ethical issues we have considered when processing B2B data:

Privacy Concerns: Even though B2B data often involves business information, it can still include personal data about individuals within those businesses. Ensuring privacy and protecting this data is crucial.

Transparency: It is important to be transparent about how data is collected, used, and shared. Lack of transparency can lead to mistrust and damage relationships with clients

Consent: Obtaining explicit consent from individuals before collecting or using their data is essential to maintain trust and comply with privacy regulations

Data Security: Ensuring that data is securely stored and protected from breaches is a fundamental ethical responsibility

Fair Use: Data should be used fairly and without discrimination. This includes avoiding biases in data analysis and ensuring that all clients are treated equally

Accountability: Organizations must take responsibility for their data practices and be prepared to address any issues that arise from their data processing activities

Addressing these ethical issues helps build trust, maintain compliance with regulations, and foster long-term relationships with clients.

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?
- Is the processing proportionate to that purpose?
- Can you achieve the same purpose without the processing?
- 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?

Yes, we believe that the processing of the data would achieve our purpose.

Is the processing proportionate to that purpose?

Yes, we believe that the processing of the data would be proportionate to the purpose.

Can you achieve the same purpose without the processing?

No.

Can you achieve the same purpose by processing less data, or by processing the data in another more obvious or less intrusive way?

We minimize the data we hold to ensure:

Data Privacy: Protecting the privacy of individuals by only collecting and storing the necessary information.

Compliance: Adhering to data protection regulations such as GDPR, which require data minimization.

Security: Reducing the risk of data breaches by limiting the amount of data that needs to be protected.

Efficiency: Streamlining data management processes, making it easier to maintain and update records.

Trust: Building trust with clients and customers by demonstrating a commitment to responsible data handling.

By minimizing the data we hold, we can better protect privacy, comply with regulations, and maintain efficient and secure data management practices.

Part 3: Balancing test

You need to consider the impact on individuals' interests, 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? • Is it data which people are likely to consider particularly 'private'? • Are you processing children's data or data relating to other vulnerable people? • Is the data about people in their personal or professional capacity?
<u>Is it special category data or criminal offence data?</u> No. <u>Is it data which people are likely to consider particularly 'private'?</u> No, we may obtain personally identifiable information, including Business Profile Information, from publicly available sources, such as from public databases, web pages and social media platforms, or from third-party providers, vendors and integrators (collectively, "Partners") who gather data from a variety of sources including data co-ops or publicly-available sources that we use to develop professional profiles that we maintain in a Business Profile Information database. <u>Are you processing children's data or data relating to other vulnerable people?</u> We do not knowingly collect information from children or vulnerable people. In the event that we learn that we have collected personal data children or vulnerable people, we will delete that information as permitted by law.

Is the data about people in their personal or professional capacity?

Demand Science, LLC processes the following categories of **Business Contact Information (BCI)** that have been collected from publicly available or third-party sources:

- First Name & Surname
- Business Address
- Business Email Address
- Business Telephone Number
- Business Job Title
- Business Job Function
- Publicly Available Business Social Links

Demand Science, LLC does not knowingly process any sensitive personal data in the provision of solutions and services to its customers. **Additionally, we do not process any accounts, passwords, home addresses or other personal, non-business-related information.**

We may automatically collect information about your use of our Website, including, but not limited to, your IP host address, sites visited, ads seen, the date and time of the ad request, pages viewed, browser type, the referring URL, Internet Service Provider, search keywords, your computer's operating system and device fingerprint. The collection tools for this type of information may now or in the future include the following (collectively, "Tracking Tools"):

Reasonable expectations

- Do you have an existing relationship with the individual?
- What is 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?

Consent: If we direct marketing communications to an individual, in their individual capacity, we do so with their consent unless an exception applies. If they wish to withdraw their consent, they may unsubscribe through the email or contact us using the information in the Contact Us section of our Privacy Policy.

Legitimate Interest: We may process Personal Data for our legitimate interests or the legitimate interests of third parties, which include advertising or market and opinion research or promoting our customers' content to an individual in a professional capacity, as far as they have not objected to the use of their data; entering into a contract with a third party (which could include their employer) and performing our obligations under that contract; the examination and optimization of processes for

needs analysis; the further development of services and products as well as existing systems and processes; the disclosure of Personal Data within the framework of due diligence in the course of company sale negotiations; the enrichment of our data, e.g., by using or researching publicly accessible data; statistical evaluations or market analysis; benchmarking; the assertion of legal claims and defense in legal disputes which are not directly attributable to the contractual relationship; the restricted processing of data, if a deletion is not possible or only possible with disproportionately high effort due to the special type of storage; the prevention and investigation of fraudulent or criminal offences, if not exclusively for the fulfilment of legal requirements; and complying with our legal obligations in countries outside of the European Economic Area or the United Kingdom.

All EU citizens are sent a Fair Process Notification within 30 days of first processing, this is sent via email. Below is an example of one such notification.

Purpose and basis of the processing:

Klarity processes your business-specific personal data to provide our customers with access to our B2B database of accurate business data records, including Business Contact Information (BCI), which enables them to promote their goods and services employing direct marketing to the right people (i.e., decision makers, influencers, champions) in other businesses, and to promote your business, so it can be found when it is searched for by other businesses. You can learn more about how and why we process your data, and the appropriate lawful basis by viewing our privacy statement. (<https://fpn-klarity.com/privacy-policy/>).

Retention Period:

It is critical for our business to provide our customers with accurate data. We therefore retain data that may include your business personal information for as long we can determine it remains accurate. We will remove your data if we can confirm that it is no longer accurate, or you have requested us to stop processing your data.

What information do we process?

Klarity processes the following categories of data that have been collected from publicly available or third-party sources:

- *First Name & Surname*
- *Company Information*
- *Business Email Address*
- *Business Telephone Number*
- *Job Title*
- *Job Function*
- *Publicly Available Social Links*

Klarity does not process any sensitive personal data for the provision of products and services to its customers.

Your Rights:

You have rights over how your personal data is used. You can object to and/or restrict the processing of your personal data. You can ask us to update your data if it is inaccurate or request that it be erased. You may also request access to see what data we hold on you.

Any Questions?

If you have questions regarding this notice, or would like to unsubscribe from Klarity, please see our privacy statement or click unsubscribe. If you require further information or support, you can also contact your local supervisory authority.

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?	
We have a dedicated Privacy Compliance Team, who ensure that the Privacy Information Management System (PIMS) is kept up to date and any amendments are made in a timely fashion. Our Privacy Information Management System (PIMS) is an internal framework which helps us manage and protect Personally Identifiable Information (PII) in compliance with privacy regulations such as GDPR. Here are the key aspects of our PIMS: Framework and Standards, Policies and Procedures, Compliance, Risk Management, Continuous Improvement.	
Can you offer individuals an opt-out?	Yes

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
We collect and receive BCI from third-party sources, including partners. BCI is information pertaining to businesses and individuals that is readily available in the public domain, including but not limited to: business name, first and last name, business telephone number, job titles, work email addresses, and location in which a business is located and an individual works. We collect this information to provide our Products and Services to our customers. We ensure that any individual can perform their 'rights' under GDPR via several methods, we will not reject a request unless legal obliged to do so within the relevant laws.	
LIA completed by	Ashley Chambers Manager of Global Privacy & DPO
Date	23 rd Jan 2025