Lead Forensics Software Data Compliance Policy

The Lead Forensics Product

The Lead Forensics product is a market leading B2B sales and marketing enablement tool. It is SaaS (Software as a Service) and provides businesses with insight relating to their website visitors. Lead Forensics works on the basis of reverse business IP tracking. A small tracking code is placed on a business' website(s) which then enables them to identify the business IP addresses of their website visitors. Lead Forensics matches the identified business IP address to a wholly owned global database of businesses and business information.

The Lead Forensics software is almost entirely focused on leveraging business related information to effectively match a business IP address with wider business data to provide valuable business related visitor information to our customers. Lead Forensics does not identify any personal IP addresses, mobile devices or any other data than that associated with the business.

Business related data is not applicable under GDPR - which has the intention of protecting personal data. Therefore, the majority of the Lead Forensics solution and its features are not relevant to GDPR.

Contact Data

An additional feature of Lead Forensics aside from the main solution, is to provide customers with the contact information of key decision makers at the organisations that have pro-actively visited the company website. As this information contains details including first name, last name, email address and LinkedIN profile, this aspect of Lead Forensics constitutes the processing of personal data and therefore, is required to be compliant with GDPR.

Lead Forensics will only ever collect business IP addresses, which are then matched to a business profile, from there Lead Forensics offers customers the opportunity to purchase the contact details of relevant decision makers within the matched business. The data available will only relate to decision makers at the organisations that have pro-actively visited a customer's website, in this regard it is anticipated that this data will be leveraged by the Lead Forensics customer base under the lawful basis for processing of 'Legitimate Interests'. It is anticipated that Lead Forensics customers will select the most appropriate point of contact from the data provided by Lead Forensics to convey a highly relevant, targeted message either by email, telephone or by post to the business address and to the point of contact. Any correspondence will be based upon their likely interest in the organisation's product or service following their visit to the organisation's website.

Under GDPR, Lead Forensics will only ever process necessary personal data, which is limited to first name, last name, LinkedIN profile URL and email address. Lead Forensics will process further business related data such as business IP, business name, job function and business telephone numbers. No sensitive personal data will be collected or processed in any way.

Lead Forensics customers have the option of using Lead Forensics without leveraging contact data, in which case the Lead Forensics solution is unrelated to GDPR on the basis that it will only process business data. If a customer opts to use the contact data feature of Lead Forensics, it is deemed that this will be leveraged under the lawful basis of 'Legitimate Interests', however the customer will be responsible for ensuring the data used is processed within their business in a method that is

compliant with GDPR – each customer will be responsible for conducting their own due diligence checks and producing their own policies as applicable to their business.

Six Lawful Basis for Processing Personal Data

Under the **EU General Data Protection Regulation (GDPR)** there are six lawful basis for processing personal data. These are detailed as follows:

- **Consent**
  The individual has given clear consent for you to process their personal data for a specific purpose
- **Contract**
  The processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract
- **Legal Obligation**
  The processing is necessary for you to comply with the law (not including contractual obligations)
- **Vital Interests**
  The processing is necessary to protect someone's life
- **Public Task**
  The processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law
- **Legitimate Interests**
  The processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Source: ico.org.uk, February 2018.

The information relating to the six lawful basis for processing personal data is taken from the ICO website and the GDPR regulation documentation. Further information regarding the lawful basis for processing personal data can be found at ico.org.uk

Legitimate Interest Assessment (LIA)

Lead Forensics has carried out a Legitimate Interest Assessment (LIA) as advised by the ICO. Based upon that assessment it is deemed that the rights and freedoms of the data subjects would not be overridden in our processing of the personal data and that in no way would a data subject be caused harm by the Lead Forensics processing. Based upon our segmentation by organisation and by specific job function, coupled with our processing of personal data within the context of a business environment, it is deemed that any processing of data will be limited to business matters, and therefore any risk of personal compromise is extremely unlikely. It is also deemed that direct marketing and sales is necessary in the context of following up with website visitors in order to better serve visitors and to generate business sales.

Per the ICO guidance, Lead Forensics can confirm:

- We have checked that legitimate interests is the most appropriate basis
- We understand our responsibility to protect the individual's interests
- We have conducted a legitimate interests assessment (LIA) and kept a record of it, to ensure that we can justify our decision
- We have identified the relevant legitimate interests

- We have checked that the processing is necessary and there is no less intrusive way to achieve the same result
- We have done a balancing test, and are confident that the individual's interests do not override those legitimate interests
- We only use individuals' data in ways they would reasonably expect
- We are not using people's data in ways they would find intrusive or which could cause them harm
- We do not process the data of children
- We have considered safeguards to reduce the impact where possible
- We will always ensure there is an opt-out / ability to object
- Our LIA did not identify a significant privacy impact, and therefore we do not require a DPIA
- We keep our LIA under review every six months, and will repeat it if circumstances change
- We include information about our legitimate interests in our privacy notice

How we Procure Data

At Lead Forensics we procure data in a variety of ways, collected in line with the lawful basis of 'Legitimate Interests'. The following are ways in which we collect and process data:

Business Data

Although business data is not relevant under GDPR, Lead Forensics is committed to providing a transparent solution so that customers can effectively assess their own compliance. Lead Forensics collects business data via the following methods:

- Primary research – Lead Forensics has a UK based in-house team who gather data relating to business from publicly available information, using search engines and other online tools to research global businesses.
- Secondary research – Lead Forensics has a UK based in-house team who use existing publicly available sources of data such as Companies House and the WebCheck service to enhance the business data.
- Purchase – Lead Forensics purchases business information from a number of selected third party data vendors who are vetted to ensure the quality and validity of the business data provided.

Personal Data

Lead Forensics collection and processing of personal data is limited to:

- First name
- Last name
- Email address
- LinkedIN profile URL

Lead Forensics procures this personal data in the following ways:

- Primary research - Lead Forensics has a UK based in-house team who gather data relating to key decision makers at organisations from publicly available sources including the website of each business.
- Secondary research – Lead Forensics has a UK based in-house team who use existing publicly available sources to gather the information relating to key decision makers including the Directors' Register at Companies House, Dun & Bradstreet, Duedil and LinkedIN.
- Purchase – Lead Forensics purchases data from selected third party data vendors with key segmentation criteria to ensure that only decision makers from registered businesses are procured. All third party data vendors have been checked for GDPR compliance and to ensure the validity and accuracy of data.

Lead Forensics also uses automated scripts and algorithms to collect, process and validate both business data as well as the personal data detailed above. These automated processes are subject to the same compliance checks as all manual processes.

How we Ensure Data Validity and Currency

Lead Forensics has a UK based in-house data verification team who are responsible for ensuring the validity and currency of the data contained within the Lead Forensics solution. The team continually cleanse the data held within the Lead Forensics software, completing a full cleanse cycle of both business and personal data at least once every 12 months. Any records found to be out of date are placed into a deletion queue which is securely purged four times in a 12 month period.

The data verification team use both manual methods as well as automated scripts and algorithms via an extensive multi-staged process to ensure the utmost validity and currency of data. Lead Forensics takes data cleansing extremely seriously as this ensures a highly compliant solution as well as a high calibre solution for all of the Lead Forensics customers.

Data Storage and Retention

The data held within the Lead Forensics solution is processed and stored in the UK within a secure environment.

Lead Forensics has a continual cycle of cleansing and refreshing data, all data within the Lead Forensics solution is verified at least once in a 12 month cycle. Any invalid records are placed into a deletion queue, which is then securely purged four times in a 12 month period.

Request to Object

Any individual who has been identified as a website visitor by Lead Forensics has the right to object to receiving correspondence from a Lead Forensics customer by contacting them directly and requesting to object, you can find their specific processes for this by visiting their company website and reviewing their privacy policies.

Should you wish to withdraw from Lead Forensics processing your personal data for use by the Lead Forensics software, please make your request in writing:

By emailing:
data-compliance@leadforensics.com

Or by writing to:
Data Compliance, Lead Forensics, Building 3000, Lakeside, North Harbour, Portsmouth, PO6 3EN.

All requests will be processed within 30 days. Your details will be added to a suppression file to ensure that your details cannot be processed by the Lead Forensics software in future. Please note that this applies only to the processing of your personally identifiable data, not that of the business data which does not fall under the remit of GDPR.

Request for Deletion

It is important to understand the difference between a right to object and a request for deletion. If you request deletion, we will remove any data we hold about you from the Lead Forensics software. This will also mean that we will remove you from our suppression files. If you are removed from our suppression files, there is a risk that your data may be processed again in the future if your details are

re-added to our software by our data procurement team. If you do not wish for Lead Forensics to process your personal data in the future, we would recommend you request to object rather than a request for deletion, as this will ensure that your details are always suppressed from processing.

The option however is yours, and in either case we will process your request within 30 days.

Please make your request in writing by emailing:
data-compliance@leadforensics.com

Or by writing to:
Data Compliance, Lead Forensics, Building 3000, Lakeside, North Harbour, Portsmouth, PO6 3EN.

Request for Data Held

You may request that we send you all of the data we hold that relates to you. Please make your request in writing;

By emailing:
data-compliance@leadforensics.com

Or by writing to:
Data Compliance, Lead Forensics, Building 3000, Lakeside, North Harbour, Portsmouth, PO6 3EN.

We will process and respond to your request within 30 days, this service will be free of charge.

This policy was last reviewed and updated on the 7th February 2018. Policies are periodically reviewed to ensure compliance with the current compliance environment.

For questions relating to this policy, please contact data-compliance@leadforensics.com