

Data Processing Agreement

Lead Ignition Ltd: standard terms for processing client personal data (UK GDPR Article 28)

Maintained by	Version
Lead Ignition Ltd	1.1
Next review	Applies to
12 months after approval, or on material change	Every client of Lead Ignition Ltd for whom we process personal data
Classification	Approval
Client	Signed by Alex Moyies, Director, 12 October 2026

1. Parties and how this agreement applies

- 1.1
- This Data Processing Agreement (the **DPA**) is between Lead Ignition Ltd, a company registered in England and Wales with company number 15542026, whose registered office is at 71-75 Shelton Street, Covent Garden, London WC2H 9JQ (**Lead Ignition, we, us**), and the client named in the Key Details or in Annex 4 (the **Client, you**).
- 1.2
- This DPA forms part of, and is incorporated by reference into, our SaaS Terms and Conditions and every Key Details, order form or statement of work that refers to them (together, the **Main Agreement**). It applies automatically when you accept the Main Agreement. It may also be signed as a separate document, in which case it applies from the date the second of us signs it, or from the start of the Main Agreement if earlier.
- 1.3
- Annex 4 is a separate document, prepared by us and signed by both parties, that records any options or variations agreed for a particular client. Where no Annex 4 has been completed and signed, the standard terms of this DPA apply without variation.
- 1.4
- This DPA applies for as long as we process Client Personal Data, including after the Main Agreement ends until the data has been returned and deleted under clause 12.

2. Definitions

- 2.1
- In this DPA:
- (a)
- Data Protection Law** means the UK GDPR, the Data Protection Act 2018, the Privacy and Electronic Communications (EC Directive) Regulations 2003 (**PECR**) and any other law relating to personal data that applies to a party, each as amended or replaced from time to time;
- (b)
- UK GDPR** has the meaning given in section 3(10) of the Data Protection Act 2018;
- (c)
- controller, processor, data subject, personal data, personal data breach, processing and special category data** have the meanings given in Data Protection Law;
- (d)
- Client Personal Data** means personal data that we process on your behalf in providing the services under the Main Agreement, as described in Annex 1;
- (e)
- Sub-processor** means any third party we engage to process Client Personal Data;
- (f)
- Business Day** means a day other than a Saturday, Sunday or public holiday in England;
- (g)
- ICO** means the Information Commissioner's Office;

- (h) **Restricted Transfer** means a transfer of Client Personal Data (including remote access to it) from the UK to any other country;
- (i) **Trust Page** means the page at leadignition.co.uk/trust#sub-processors, or any replacement page we tell you about.

2.2 Words such as "including" do not limit the words before them. A reference to writing includes email.

3. Roles of the parties

- 3.1 You are the controller, and we are your processor, of all Client Personal Data. Annex 1 sets out the subject matter, duration, nature and purpose of the processing, the types of personal data and the categories of data subjects.
- 3.2 We are a separate controller only for business contact and billing data that we need to run our relationship with you, such as the names and work contact details of your staff who deal with us, and records of our own calls and meetings with you. We handle that data under our Privacy Notice, not this DPA.
- 3.3 You are responsible for:
 - (a) having a lawful basis for all processing of Client Personal Data, including any condition needed for special category data;
 - (b) giving data subjects the information required by Articles 13 and 14 of the UK GDPR, including telling them where calls are recorded or transcribed;
 - (c) obtaining any consent required under Data Protection Law, including under PECR for marketing messages you send using our services; and
 - (d) the accuracy of Client Personal Data and the lawfulness of your instructions.

Joint controllers

- 3.4 Where you share control of Client Personal Data with another organisation (a **Joint Controller**), for example a parent organisation or a partner you share the data with, you warrant that you have in place an arrangement with that Joint Controller that meets Article 26 of the UK GDPR.
- 3.5 We are not a party to that arrangement. We act only on your instructions and not on the instructions of the Joint Controller, unless you tell us in writing that the Joint Controller may instruct us on specified matters.
- 3.6 Your instructions may include giving the Joint Controller, or named individuals working for it, defined access to Client Personal Data. Any such access will be recorded in Annex 4 or in a written instruction from you, will be limited to the data, users and permissions you specify, and will be removed when you tell us. You are responsible for the Joint Controller's use of that access.

4. Processing on your instructions

- 4.1 We will process Client Personal Data only on your documented instructions, unless UK law requires otherwise. If UK law requires us to process Client Personal Data in another way, we will tell you before we do so, unless that law prevents us from telling you.
- 4.2 Your documented instructions are: the Main Agreement and this DPA; the way you configure and use the services (including the workflows, automations, integrations and user permissions you set up or ask us to set up); and any other reasonable written instructions you give us that are consistent with the Main Agreement. Instructions that change the scope of the services may be subject to a change fee under the Main Agreement.
- 4.3 We will tell you immediately if, in our opinion, an instruction breaks Data Protection Law. We may suspend acting on that instruction until you confirm or change it.

- 4.4 We will never use Client Personal Data for our own purposes, including for our own marketing, product development, training of AI models or analytics, and we will never sell it.
- 4.5 We will make sure that everyone we authorise to process Client Personal Data (including our directors and any contractors) is bound by a duty of confidentiality, is given access only where they need it to provide the services, and processes the data only on your instructions.

5. Security

- 5.1 We will implement and maintain appropriate technical and organisational measures to protect Client Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access, as required by Article 32 of the UK GDPR. Our current measures are set out in Annex 2.
- 5.2 We will review our measures at least once a year and when there is a material change to the services. We may update them, provided the overall level of protection is not reduced.
- 5.3 You are responsible for the security measures within your control, including managing your users and their permissions, using strong passwords and multi-factor authentication, and keeping your own devices and systems secure. We are not responsible for a compromise caused by the acts or omissions of your users or your systems, but this does not reduce our own obligations under this clause 5.

6. Sub-processors

- 6.1 You give us general written authorisation to engage Sub-processors. The Sub-processors in use on the date of this DPA are listed in Annex 3. The current list is published on the Trust Page.
- 6.2 We will give you at least 14 days' written notice before adding or replacing a Sub-processor, or, where our own supplier gives us less notice than that of a change to its sub-processors, as much notice as we receive. Notice may be given by email to your main contact and by updating the Trust Page.
- 6.3 You may object to a new or replacement Sub-processor on reasonable data protection grounds by telling us in writing (to dpo@leadignition.co.uk) within the notice period. We will discuss the objection with you in good faith and, where we reasonably can, offer an alternative. If we cannot resolve the objection, you may end the affected service, without penalty, by giving us written notice. We will refund any fees you have paid in advance for the part of the affected service after it ends.
- 6.4 We will have a written contract with each Sub-processor that imposes data protection obligations which provide at least the same level of protection as this DPA, to the extent they apply to the processing the Sub-processor carries out.
- 6.5 Our CRM platform provider (listed in Annex 3) uses its own sub-processors under its own terms. We pass on to you the notices we receive from it about changes to those sub-processors. Clause 6.3 applies to those changes as if they were changes to our own Sub-processors, with the notice period being the period we receive. Its list is referenced on the Trust Page rather than copied into this DPA.
- 6.6 We remain responsible to you for the performance of each Sub-processor's data protection obligations, subject to clause 13.
- 6.7 Integrations you choose to connect to your account (for example a booking, payments or event platform that you hold your own account with) are your own suppliers and not our Sub-processors, unless we contract with them for you. Annex 4 records any client-specific Sub-processors.

7. International transfers

- 7.1 We will not make a Restricted Transfer, or allow a Sub-processor to make one, unless the transfer is covered by one of the following:
 - (a) UK adequacy regulations, including the UK Extension to the EU-US Data Privacy Framework (the UK-US data bridge) where the recipient is certified under it;

- (b) the International Data Transfer Agreement (**IDTA**) or the International Data Transfer Addendum to the EU Standard Contractual Clauses (**UK Addendum**) issued by the ICO, together with any transfer risk assessment required by Data Protection Law; or
 - (c) another safeguard or exception permitted by Data Protection Law.
- 7.2 Annex 3 shows where each Sub-processor processes data and the safeguard relied on. You authorise the transfers described there.

8. Helping you meet your obligations

- 8.1 If we receive a request from an individual exercising their rights under Data Protection Law in relation to Client Personal Data, we will pass it to you within 2 Business Days. We will not respond to the individual ourselves, other than to acknowledge receipt and say we have passed the request on, unless you instruct us to.
- 8.2 Taking into account the nature of the processing and the information available to us, we will give you reasonable help to:
- (a) respond to requests from individuals, including by using the export, search and deletion features of the services;
 - (b) carry out data protection impact assessments and any prior consultation with the ICO; and
 - (c) respond to enquiries from the ICO or another regulator about the processing.
- 8.3 Help that goes beyond what the self-service features of the services allow, or that takes more than a reasonable amount of time, may be charged at our standard rates, which we will tell you before starting the work. We will not charge for help needed because of our own breach of this DPA.
- 8.4 If we receive a request from the ICO, a court or a law enforcement body for Client Personal Data, we will tell you promptly (unless the law prevents us) and will not disclose the data unless UK law requires us to.

9. Personal data breaches

- 9.1 We will tell you without undue delay, and in any event within 24 hours of becoming aware, of any personal data breach affecting Client Personal Data. This includes a breach reported to us by a Sub-processor. We will notify the breach contacts named in Annex 4 (or, if none are named, your main contact) by phone and email. We become aware of a personal data breach when we have a reasonable degree of certainty that a security incident has led to Client Personal Data being compromised. Where we suspect a breach that is likely to affect you but are still investigating, we will tell you of the suspicion within the same 24 hours.
- 9.2 Our notice will include, as far as the information is available at the time:
- (a) a description of what happened and when, and how we became aware of it;
 - (b) the categories and approximate number of data subjects and records concerned;
 - (c) the likely consequences of the breach;
 - (d) the steps we have taken or propose to take to contain it and reduce its effects; and
 - (e) the name and contact details of the person you can contact for more information.
- 9.3 Where we cannot provide all of this information at once, we will provide it in stages without further undue delay. We will keep you updated until the breach is contained, and will then give you a written summary of the cause and the steps taken to stop it happening again.
- 9.4 We will take reasonable steps to contain the breach and reduce its effects, and will help you meet your own obligations, including your 72-hour deadline to report to the ICO where required, any notice to a Joint Controller, and any communication with affected individuals.

- 9.5 We will not notify the ICO, a Joint Controller or affected individuals about a breach of Client Personal Data on your behalf without your agreement, unless the law requires us to.
- 9.6 Where a breach occurs at a Sub-processor, our ability to give you information depends on the Sub-processor notifying us. Our CRM platform provider (listed in Annex 3) has committed to notify us without undue delay after becoming aware of a breach affecting our data. Our 24-hour period runs from when we become aware under clause 9.1. For a breach at a Sub-processor, that is no later than when we receive its notice. We will pass on what we receive promptly.
- 9.7 Our notice of a breach is not an admission of fault or liability.

10. Special category data

- 10.1 You must not put special category data (such as health information) or criminal offence data into the services unless:
 - (a) you have confirmed to us in writing the condition under Article 9 of the UK GDPR (and, where relevant, Schedule 1 of the Data Protection Act 2018) on which you rely; and
 - (b) we have given our prior written approval, as required by clause 4.3(a) of our SaaS Terms and Conditions.
- 10.2 Our approval will say which systems the data may be stored in. Annex 4 records the approval. Special category data must be stored only in the systems named in Annex 4, and you must configure your forms, fields and workflows (or instruct us to configure them) so that it is not stored anywhere else.
- 10.3 If we become aware that special category data is being stored outside the systems named in Annex 4, we will tell you and may, on your instruction, remove it.
- 10.4 You must tell us in writing before you put personal data about children (anyone under 18) into the services, and Annex 4 will record it. Clauses 10.2 and 10.3 apply to it as if it were special category data. You remain responsible for having a lawful basis, for any parental consent the law requires, and for privacy information that children and their parents can understand. Where a form, page or app we build for you is likely to be accessed by children, we will help you meet the ICO's Age Appropriate Design Code and your duty under Article 25(1A) of the UK GDPR to take into account the children's higher protection matters, as part of your instructions.

11. Records and audits

- 11.1 We will keep a record of the processing we carry out for you as required by Article 30(2) of the UK GDPR, and will make available to you the information you reasonably need to show that we comply with this DPA.
- 11.2 Once a year, you (or a Joint Controller acting on your behalf) may ask us to complete a reasonable written questionnaire about our compliance with this DPA. We will answer it within a reasonable time.
- 11.3 We will also allow an on-site or remote audit, carried out by you or an independent auditor you appoint, if:
 - (a) the questionnaire does not reasonably answer your concerns;
 - (b) there has been a personal data breach affecting Client Personal Data; or
 - (c) the ICO or another regulator requires it.
- 11.4 Audits under clause 11.3:
 - (a) are at your cost;
 - (b) need at least 30 days' written notice, except after a breach or where a regulator requires it;
 - (c) will take place during business hours and will be planned so as not to disrupt our business unreasonably;
 - (d) must be carried out by people bound by confidentiality; and

- (e) will not happen more than once in any 12-month period, except after a breach or where a regulator requires it.

- 11.5 Audits do not extend to our Sub-processors' premises or systems. Where you need information about a Sub-processor, we will provide the reports and certifications that Sub-processor makes available to us, where we are allowed to share them.

12. Return and deletion at the end

- 12.1 You can export your data from the services at any time using the export features. On your request, or when the Main Agreement ends, we will provide a full export of Client Personal Data in a commonly used format (for example CSV for records, and the original file format for documents and recordings) within 10 Business Days.
- 12.2 We will keep Client Personal Data for 60 days after the Main Agreement ends, at no charge, so that you can complete your exit. Longer storage can be agreed in writing, and may be charged for. If you ask us in writing to delete Client Personal Data sooner, we will do so within 10 Business Days of your request, and confirm the deletion as described in clause 12.3.
- 12.3 At the end of that period we will give you at least 14 days' written warning, and then delete Client Personal Data from our systems and our Sub-processors' live systems. We will confirm the deletion to you in writing.
- 12.4 Backups held by our Sub-processors are deleted on their own backup cycle (for the CRM platform, backups age out after 7 days). We will not restore data from those backups other than to return it to you.
- 12.5 We may keep Client Personal Data after this period only where UK law requires us to, in which case clause 4.5 and clause 5 continue to apply to it for as long as we keep it.

13. Liability

- 13.1 Each party's liability under or in connection with this DPA is subject to the limits and exclusions of liability in the Main Agreement, unless Annex 4 sets a separate data protection liability cap, in which case that cap applies to the matters it covers instead.
- 13.2 Nothing in this DPA limits either party's liability where Data Protection Law, or any other law, does not allow it to be limited, or limits any rights data subjects have directly against either of us under Article 82 of the UK GDPR.

14. Term, changes and order of precedence

- 14.1 This DPA continues for as long as we process Client Personal Data. Clauses 9, 11, 12, 13 and this clause 14 continue to apply after the Main Agreement ends for as long as needed.
- 14.2 We may update this DPA where needed to reflect changes in Data Protection Law or guidance from the ICO, or to add new services. We will give you at least 30 days' written notice of any change. If a change reduces the protection given to Client Personal Data, you may end the affected services without penalty within that period if you do not agree. Annex 4 can only be changed by written agreement signed by both of us.
- 14.3 If there is any conflict on a matter relating to the processing of personal data, the following order of priority applies:
 - (a) Annex 4, where it expressly varies this DPA;
 - (b) this DPA;
 - (c) any Special Conditions in the Key Details;
 - (d) the Key Details; and
 - (e) the SaaS Terms and Conditions.
- 14.4 On all other matters the Main Agreement applies.

15. General

- 15.1 This DPA, and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with it, is governed by the law of England and Wales. The courts of England and Wales have exclusive jurisdiction.
- 15.2 If any part of this DPA is found to be invalid or unenforceable, the rest of it continues to apply.
- 15.3 This DPA may be signed electronically and in separate copies, which together form one agreement.
- 15.4 A person who is not a party to this DPA has no right under the Contracts (Rights of Third Parties) Act 1999 to enforce any of its terms.
- 15.5 Our contacts for this DPA: dpo@leadignition.co.uk for data protection matters, including instructions, individuals' requests, Sub-processor objections and audit requests; and security@leadignition.co.uk for personal data breaches and security incidents. Please report any suspected breach or security incident affecting the services to security@leadignition.co.uk and by phone on 020 7177 1702.

Annex 1: Details of the processing

All services

Item	Details
Controller	The Client
Processor	Lead Ignition Ltd
Duration	The term of the Main Agreement, plus the exit period in clause 12
Frequency	Continuous, for as long as the services are used
Retention	Set by the Client through its use of the services and its instructions. Deleted at the end as described in clause 12

Service A: the Lead Ignition CRM

Item	Details
Subject matter	Providing, configuring and supporting the Lead Ignition CRM (a white-labelled customer relationship management platform supplied by HighLevel Inc.)
Nature and purpose	Storing and organising contact records; managing enquiries, pipelines, appointments and calendars; sending and receiving email, SMS and WhatsApp messages; making, recording and transcribing calls where the Client enables it; forms, surveys and landing pages; automations and workflows; reporting; support, maintenance and troubleshooting by Lead Ignition
Data subjects	The Client's customers and prospective customers; their representatives; introducers, referrers and suppliers; website visitors who submit forms; the Client's own staff and users; children, only where recorded in Annex 4 (clause 10.4)

Personal data	Names and contact details; company and job details; enquiry, appointment and transaction details; communications and message content; notes, tasks and documents; call recordings and transcripts (where enabled); marketing preferences and consent records; form responses; technical data such as IP address and email engagement
Special category data	None, unless approved under clause 10 and recorded in Annex 4
Sub-processors	HighLevel Inc. and its sub-processors; Anthropic (Sparky, our in-CRM assistant); Cloudflare; Google LLC and Virtual Admin Assistance (where data is shared with us by email for support)

Service B: custom apps and portals

Item	Details
Subject matter	Building, hosting and supporting custom web applications and portals for the Client (for example field apps, fact-find apps and client portals)
Nature and purpose	Collecting, storing and displaying data entered by the Client's users or customers; producing documents; sending login and notification emails; syncing data with the Lead Ignition CRM or the Client's own systems where instructed; hosting, backups, support and maintenance
Data subjects	As for Service A, plus any other individuals whose data the app is designed to collect, as set out in the scope document or Annex 4
Personal data	As defined in the agreed scope for each app. Typically names, contact details, account and login details, form and job data, documents and photos
Special category data	Only where approved under clause 10 and recorded in Annex 4
Sub-processors	Supabase Inc.; Vercel Inc.; HighLevel Inc. (sends app login and notification emails through the client's CRM sub-account); Cloudflare; Anthropic (AI features, where enabled); Google LLC and Virtual Admin Assistance (where data is shared with us by email for support)

Our own meeting records

Lead Ignition's own notes, recordings and transcripts of its meetings with the Client are records of our own business, not Client Personal Data. We control them as set out in our Privacy Notice. The Client's customer records are not shown or discussed on recorded calls.

Annex 2: Technical and organisational measures

These are the measures we have in place on the date of this DPA. We review them at least annually.

Area	Measures
Governance	A small company run by its directors. Alex Moyies is the named data protection lead. Written data protection, information security and breach procedures. Sub-processor register reviewed every 6 months and whenever a provider notifies a change

Access control	Named accounts for every person; no shared logins. Multi-factor authentication on every business system that supports it. Password manager used for all business credentials. Access given only where needed for the work, reviewed annually and removed immediately when someone leaves
Client separation	Each client has its own CRM sub-account. Each client has its own admin users and controls its own user permissions. Platform supplier support access to client accounts is switched off by default
Encryption	Data encrypted in transit using TLS (TLS 1.2 or higher on the CRM platform). Data encrypted at rest using AES-256 on every hosting platform we use
Devices	Full-disk encryption required on devices used for business (FileVault on the company Mac, BitLocker or Windows device encryption on the company Windows laptop). Screen lock after no more than 5 minutes. Anti-malware required on both company laptops. Company-owned iPhone for work; personal phones used for work only under our signed Device and Acceptable Use Standard. Remote locate and lock or wipe available on company laptops and the company iPhone
Software development	Source code held in GitHub with dependency scanning. Changes tested in preview deployments before release. Row-level security enabled on app databases. Critical and high vulnerabilities remediated within 14 days of becoming aware
Artificial intelligence	AI features switched off by default on client CRM accounts. Client Personal Data is processed by AI only through our business accounts with Anthropic (Claude Team plan and API) under its Commercial Terms and DPA, never through personal or consumer AI accounts
Backups and recovery	CRM platform: daily backups managed by the platform, kept for 7 days; restore same working day where within our control. Custom apps: daily database backups kept for at least 7 days; target to restore within 2 business days with no more than 24 hours of data lost
Personnel	Directors and contractors bound by confidentiality. Contractors engaged under a non-disclosure agreement and given only the access they need
Incident response	Written breach procedure. Breaches notified to clients within 24 hours of becoming aware. Cyber incident response support available through our insurer
Suppliers	Sub-processors engaged under written data processing terms. Hosting in the UK where available for client apps

Annex 3: Sub-processors

The current list is published at [leadignition. co. uk/ trust#sub- processors](https://trust.leadignition.co.uk/trust#sub-processors).

Sub-processor	What it does	Where data is processed	Transfer safeguard
---------------	--------------	-------------------------	--------------------

HighLevel Inc. (the platform behind the Lead Ignition CRM)	Hosts client CRM data: contacts, messages, calls, recordings, transcripts and files	United States (Google Cloud and AWS). Platform support access to client accounts is switched off (see Annex 2)	UK-US data bridge (HighLevel is certified under the UK Extension to the EU-US Data Privacy Framework), with the UK IDTA or UK Addendum in HighLevel's DPA as a fallback, including for any support access from outside the UK and the US if it is ever switched on
Supabase Inc.	Databases for custom apps and portals	London, UK (eu-west-2) or Ireland (eu-west-1), as stated for each client project	UK adequacy (UK) or UK adequacy regulations for the EEA (Ireland); Supabase DPA
Vercel Inc.	Hosts custom apps and portals	London (lhr1) where stated for a client project; global edge network	Vercel DPA, with the UK IDTA and EU Standard Contractual Clauses
Google LLC (Google Workspace)	Email, documents, file storage and meetings	United States and Europe	UK-US data bridge (Google LLC is certified under the UK Extension), with SCCs and UK transfer terms in the Google Cloud DPA as a fallback
Anthropic	Claude Team plan and API: powers Sparky (our in-CRM assistant) and the AI features of our client portal, and is used by our staff for build, support, data imports and data cleaning	United States	UK Addendum to the EU SCCs in the Anthropic DPA, part of its Commercial Terms (no training on our data)
Cloudflare	DNS and security for Lead Ignition domains and apps	Global	Data Privacy Framework, or EU Standard Contractual Clauses with the UK Addendum, in the Cloudflare DPA
GitHub, Inc.	Stores the source code of the apps and portals we build; this can include configuration and occasional test or reference data relating to the Client	United States	UK-US data bridge (GitHub is certified under the UK Extension to the EU-US Data Privacy Framework), or the UK Addendum to the EU Standard Contractual Clauses in GitHub's DPA
Virtual Admin Assistance (VAA UK)	Virtual assistant support for Lead Ignition: managing our email inbox and calendar, so it may see Client Personal Data that you send us by email	United Kingdom	Not applicable (UK). Services agreement dated 12 March 2026, with a data processing addendum signed on 8 October 2026

Suppliers that a client contracts with directly (for example a ticketing or booking system) are the client's own processors, not ours, even where we build the integration that connects them to the client's CRM. They are recorded in that client's Annex 4.

HighLevel's own sub-processors (including Twilio, Mailgun, LeadConnector and OpenAI) are listed by HighLevel and referenced on our Trust Page. App login and notification emails from our custom apps are sent through the client's CRM sub-account, so they reach Mailgun as HighLevel's sub-processor, not ours. HighLevel Inc. (with LeadConnector LLC) is an active participant in the UK Extension to the EU-US Data Privacy Framework on the official Data Privacy Framework List (checked 10 October 2026, next certification due 15 September 2027). Google LLC and Cloudflare state the same in their privacy policies. Anthropic's DPA relies on the UK Addendum to the EU Standard Contractual Clauses. Pendo, which the CRM platform uses for product analytics, is on HighLevel's published sub-processor list. Contractors who may access client data are treated as Sub-processors and listed on

the Trust Page when engaged. At the date of this DPA, the only such contractor is Virtual Admin Assistance (VAA UK), listed above.

Annex 4: Client-specific options

Annex 4 is not part of this published document. Where a client needs options or variations (for example approval of special category or children's data under clauses 10.1 and 10.4, a joint controller, named breach contacts or a different liability cap), we prepare a separate Annex 4 for that client. It must name the client, refer to this DPA by version, and be signed by a director of Lead Ignition Ltd and by the client. It takes effect only when both have signed it.

No Annex 4 applies unless one has been signed in that way. Any other document, or any wording added to this DPA by anyone other than us, does not vary this DPA. Most clients need no Annex 4, and the standard terms apply to them in full.

For Lead Ignition Ltd

Alex Moyies

Signed electronically

Name: Alex Moyies, Director

Date: 12 October 2026

For the Client

Signed: _____

Name: _____

Position: _____

Date: _____