LFW

Legal

Data Processing Addendum

Last updated November 14, 2026

Version 1.0, effective November 14, 2026. All legal documents (lfw.com/legal/). Download PDF (lfw.com/legal/lfw-data-processing-addendum-v1.0.pdf).

This DPA forms part of the MSA (lfw.com/legal/msa/) between the Client and LFW.com LLC, doing business as LFW, when LFW processes personal data for Client. Client is the controller or business and LFW is its processor or service provider. If Client is itself a processor, it warrants that it may appoint LFW as a subprocessor and will pass on the controller's lawful instructions. LFW's own website, sales and business-account records are separately described in the Privacy Policy (lfw.com/privacy/).

1. Processing instructions and details

The subject matter is providing, securing, maintaining and supporting the services in the Order Form. Processing may include collection, recording, organization, storage, retrieval, use, transmission to approved providers, export and deletion. Processing lasts for the service term and the agreed return, deletion and backup-retention periods.

Data subjects may include Client's staff, families, members, participants, applicants, residents, suppliers and other authorized users. Data may include identity and contact details, account and permission records, applications, memberships, registrations, case and business records, communications, documents, payment references, activity and security logs, and any other fields Client lawfully configures. The Order Form must identify the actual categories and any sensitive data; a general list does not authorize every category. PHI requires a signed BAA and a configured HIPAA environment.

LFW will process only on Client's documented instructions, including the agreement, authorized product settings and written support requests, unless law requires otherwise. Where permitted, LFW will inform Client before legally required processing. LFW will promptly tell Client if an instruction appears to violate applicable data protection law and may pause that instruction while the parties resolve it. Client determines purposes, lawful bases, notices, consent, data accuracy, retention instructions and user permissions.

2. Purpose limits and confidentiality

LFW will not sell or share Client personal data for cross-context behavioral advertising, retain, use or disclose it outside the specified purposes or direct business relationship, or combine it with data from other clients or LFW's own activities except as applicable law permits a service provider. LFW will not use it to train models or for LFW's own advertising. LFW certifies that it understands and will comply with these restrictions and will notify Client if it can no longer comply. Client may take reasonable steps to verify compliance and stop and remedy unauthorized use.

People authorized to process data must have a duty of confidentiality and access only as needed for their duties. LFW remains responsible for its subprocessors' performance of delegated processing duties.

3. Security

LFW will maintain appropriate technical and organizational measures taking account of the nature, scope, context and risk of processing. The measures are described in the Information Security Policy (lfw.com/trust/information-security-policy/), Access Control Policy (lfw.com/trust/access-control-policy/), Incident Response Plan (lfw.com/trust/incident-response-plan/) and security page (lfw.com/security/). They include access restrictions, secure connections, credential controls, logging, backup and incident procedures appropriate to the service. Product controls depend on configuration; these links do not claim SOC 2 certification, disk encryption everywhere or a dedicated environment for every customer.

LFW will not materially reduce agreed security during a term. The Order Form must record additional measures required for sensitive data, including any HIPAA environment. No system can promise absolute security.

4. Incident notice

LFW will notify Client in writing without undue delay and within 24 hours of confirming a security incident affecting Client's data, matching the published Incident Response Plan. Where applicable law requires notice earlier, including notice without undue delay after awareness of a personal data breach, that earlier duty applies; confirmation is not a reason to defer a legally required notice. Notice goes to Client's contacts on file and will include the information then available about the event, affected data and people, likely effects, containment and remediation, and a contact for follow-up. LFW may provide details in stages without delaying the initial notice.

LFW will investigate, mitigate and reasonably assist Client with required notices and documentation. Client decides its regulatory and individual notices unless law requires LFW to notify directly. Notice is not an admission of fault. There is no additional promise of 24/7 support; statutory notice deadlines still apply.

5. Assistance and individual rights

Taking account of the processing and information available, LFW will reasonably assist Client with access, correction, portability, restriction, objection and deletion requests, security duties, impact assessments and consultation with regulators. LFW will forward requests about Client's data to Client and will not decide them independently unless law requires. Client must supply timely instructions and verify the person's authority. LFW will provide available product tools and relevant information; separately scoped assistance beyond included service must be quoted in advance, without limiting mandatory legal duties.

6. Subprocessors

Client authorizes the providers below only as applicable to its configured service. An optional integration is not proof that every customer's data is sent to it. A provider Client directly contracts and instructs may be Client's independent provider rather than LFW's subprocessor; the Order Form must record that role. LFW will impose written data protection duties at least as protective as those applicable to the delegated work.

- **Hetzner:** servers that run the hosted software, its databases and the local backup copy. Location: Ashburn, Virginia, United States.
- **Cloudflare:** DNS, proxy, firewall and edge functions (Workers); processes web request data, including IP addresses, and terminates encryption in transit. Cloudflare's network is global, so requests may pass through servers outside the United States on their way to LFW. Cloudflare R2 also holds encrypted operational backups that include Customer Data. R2 is a global service; no particular backup country or jurisdiction or US-only storage is promised. Any customer-specific residency requirement must be agreed in the Order Form and configured before the affected processing begins.
- **Amazon Web Services (SES):** all outbound email, including bounce notices; processes recipient addresses, names and message content. Region: us-east-2 (Ohio), United States.

- **Amazon Web Services (S3), Client-selected:** only where Client chooses its own S3 storage for records, in the region Client selects.
- **Google Workspace:** LFW's own email and calendar for support and booked calls; processes support correspondence and booking details.
- **Stripe:** payment processing through Client's own Stripe account, with LFW's technology fee where agreed. Stripe acts under Client's direct agreement with Stripe for those payments; card data goes directly to Stripe.

Optional providers, used only when Client enables them (none is configured by default):

- **AI providers:** Anthropic, OpenAI, Google (Gemini) or an OpenAI-compatible endpoint Client supplies, using Client's key or LFW's key as the Order Form states; processes the prompts and content Client sends to an enabled AI feature.
- **Twilio:** text messages, not enabled today; LFW will name it under the notice process below before enabling it for Client.
- **Client-directed integrations:** Microsoft 365 (Entra sign-in, SharePoint and OneDrive filing, Azure AI Translator in Client's own tenant), Google Search Console and Google Ads conversion upload, Smartcar vehicle data, Fastly cache purge, SFTP, SQL Server, and SAML or OIDC identity providers. These connect to accounts Client controls and act on Client's instructions; Client's agreement with each provider governs them.
- **Dedicated environments:** where an Order Form selects a dedicated environment in LFW's Azure or AWS account, the Order Form names the provider and region.

LFW keeps the current list on this page. Search, malware scanning and databases run on LFW's own servers and are not third-party providers.

LFW will give at least 30 days' written notice before adding or replacing a subprocessor that will process Client's data. Client may object on reasonable data-protection grounds within that period. The parties will seek an alternative; if none is reasonably available, Client may terminate the affected service before the change with a pro rata refund of unused prepaid fees. LFW will not send Client's data to the disputed new provider while the objection is unresolved. Mandatory law may require a different process.

7. Return and deletion

At Client's choice, LFW will return or delete personal data at the end of service, unless law requires retention. The hosted-software schedule provides export during service and a 30-day retrieval window after termination, followed by deletion of the instance and its data. Client may instruct earlier deletion. Backups expire under the applicable retention cycle, remain protected and are not used for another purpose; deletion instructions must be reapplied if a backup is restored. Legally required retained records remain restricted to that purpose. LFW will provide written confirmation of deletion on request.

Deletion procedure. When the 30-day retrieval window ends, LFW deletes the terminated customer's organization, its records, files and accounts from the live system and confirms the date in writing on request. Deletion is a deliberate operator step, logged in LFW's audit log, not left to automatic record-retention jobs.

Standard retention. Unless a written Order Form specifies a different lawful schedule, the standard policy is a 30-day retrieval window after service ends, deletion from active systems when that window ends, and expiry of ordinary Customer Data backup copies within a further 30 days, normally no later than 60 days after service ends. A lawful preservation obligation or legally required record may be retained separately, restricted to that purpose. Customer-specific retention and data-residency requirements must be documented in the Order Form and implemented before the affected processing begins.

Backup storage and expiry. Ordinary Customer Data backups use encrypted local storage and Cloudflare R2. They expire within 30 days of creation under the daily expiry policy; there is no long-term backup-history entitlement. This policy applies to the operational repositories that include Customer Data. Backups are protected and used to restore service; deletion instructions must be reapplied after restoration. Legally required business records retained in active systems remain restricted to that purpose and do not justify retaining ordinary backup copies beyond this cycle.

8. Evidence and audits

LFW will provide information reasonably needed to show compliance, normally through a written security questionnaire and available policy or control evidence under confidentiality duties. Client may submit reasonable follow-up questions. Questionnaires are the ordinary review method, not a waiver of a legally required audit, inspection or regulator's access. Where applicable law requires an audit by Client or its mandated independent auditor, LFW will allow and contribute to it under reasonable scope, notice, confidentiality and safeguards for other customers. No certification or external audit report is represented as existing.

9. Applicable privacy laws and transfers

Where applicable, this DPA implements processor duties under EU GDPR Article 28, UK GDPR, the California Consumer Privacy Act (CCPA), the Virginia Consumer Data Protection Act (CDPA) and other applicable US state privacy laws. Statutory terms apply only where the law applies; this DPA does not assert that every customer or LFW meets every law's thresholds. The parties will assist one another in complying with their respective duties.

Live Customer Data is hosted in Ashburn, Virginia. Local and Cloudflare R2 backup storage and retention are described in Sections 6 and 7. No specific R2 backup country or jurisdiction is promised. Web requests may pass through Cloudflare servers abroad on their way to LFW. US storage alone does not settle international-transfer requirements: access from another country and provider processing must also be assessed. A transfer from the EEA or UK to the US may itself be a restricted transfer. LFW will not make a restricted transfer without the required lawful safeguard.

EU transfers. Where EU GDPR applies to Customer Data transferred to LFW in the United States, the Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914 are incorporated by reference: Module Two where Client is a controller, Module Three where Client is a processor. In them: Clause 7 (docking) applies; Clause 9 uses option 2, general written authorization, with the notice and objection process in Section 6; the optional wording in Clause 11 is not used; the supervisory authority under Clause 13 is the one competent for Client; Clauses 17 and 18 choose the law and courts of Ireland. Annex I: Client is the data exporter, LFW the data importer, and the processing is described in Sections 2 and 3. Annex II is Section 5 of this DPA. Annex III is the provider list in Section 6.

UK and Swiss transfers. For UK GDPR, the International Data Transfer Addendum to the EU Standard Contractual Clauses issued by the UK Information Commissioner (version B1.0, in force 21 March 2022) is incorporated, with the details above as its tables; either party may end it as Section 19 of the Addendum allows. For the Swiss Federal Act on Data Protection, the same clauses apply with the Swiss Federal Data Protection and Information Commissioner as supervisory authority and references to the GDPR read as references to that Act.

Transfer assessment. LFW will give Client the information it reasonably needs for its own transfer assessment, will challenge any government request for Customer Data it may lawfully challenge, and will tell Client about any such request unless the law forbids it. As of the effective date, LFW has received no government request for Customer Data. LFW is not certified under the EU-U.S. Data Privacy Framework.

10. HIPAA and precedence

PHI is excluded unless the parties sign a BAA and LFW sets up the identified HIPAA environment. This DPA alone is not a BAA or an assurance that a default environment meets HIPAA. For processing duties this DPA controls conflicting MSA or Schedule terms; a signed BAA controls for PHI and mandatory transfer instruments control their subject. The MSA's government contract priority and public-records provisions apply, without reducing mandatory data-protection duties.