LetsDefend Infosec

Safeguarding Your Digital Journey

PRIVACY POLICY

Governance, Risk & Compliance | *IS Audits* | *VAPT* | *Cybersecurity Assessments*

Effective Date: 26/12/2024

Version: 1.0

www.letsdefend.in

Table of Contents

1. Introduction

LetsDefend Infosec ("LetsDefend Infosec," "the Company," "we," "us," or "our") is a cybersecurity firm providing Governance, Risk and Compliance (GRC) advisory, Information Systems (IS) audits, Vulnerability Assessment and Penetration Testing (VAPT), cybersecurity risk assessments, regulatory compliance support, and related security audit services. This Privacy Policy ("Policy") explains how we collect, use, disclose, store, transfer, and protect personal data in connection with our website, our services, and our business operations.

We recognize that the trust our clients, partners, job applicants, and website visitors place in us is central to our business as a security and compliance provider. We are committed to handling personal data lawfully, fairly, transparently, and with the same rigor we apply to protecting our clients' information assets.

This Policy applies to personal data we process as a data controller (in respect of our own website visitors, job applicants, and business contacts) and, where applicable, as a data processor or service provider (in respect of personal data we may encounter while delivering audit, VAPT, or assessment services on behalf of a client, which is governed additionally by the applicable service agreement, statement of work, and non-disclosure agreement).

2. Scope of This Policy

This Policy applies to:

- Visitors to our website at www.[yourdomain].com and any subdomains or web applications we operate (collectively, the "Site");
- Prospective, current, and former clients and their authorized representatives;
- Vendors, subcontractors, and business partners; and
- Any other individual whose personal data we process in the course of our business.

This Policy does not apply to information we process purely on behalf of a client as part of a security engagement (for example, system logs, network data, or personal data encountered incidentally during a VAPT engagement or IS audit). Such processing is governed by the relevant client contract, statement of work, non-disclosure agreement (NDA), and data processing agreement (DPA), and by applicable law, including §8 ("Confidentiality of Client and Engagement Data") below.

3. Definitions

- **"Personal Data" / "Personal Information"** means any information relating to an identified or identifiable natural person (a "Data Principal" under India's Digital Personal Data Protection Act, 2023 ("DPDP Act") or a "Data Subject" under the EU/UK General Data Protection Regulation ("GDPR")).
- **"Processing"** means any operation performed on personal data, including collection, recording, storage, use, disclosure, and erasure.
- **"Client Data"** means data, including personal data, provided by or accessed on behalf of a client in the course of delivering GRC, IS audit, VAPT, or assessment services.
- **"Services"** means our GRC solutions, IS audits, VAPT, cybersecurity assessments, compliance advisory, and related security audit services.

- **"DPDP Act"** means the Digital Personal Data Protection Act, 2023 of India, and its implementing rules.
- **"GDPR"** means Regulation (EU) 2016/679, as it applies in the European Economic Area, and/or the UK GDPR as retained under UK law, as applicable.

4. Categories of Personal Data We Collect

4.1 Website Visitors

When you visit our Site or interact with our online forms (for example, a contact form, quote request, newsletter sign-up, or resource download), we may collect:

- **Identity and contact data:** name, job title, company name, email address, phone number, business address;
- **Enquiry data:** the content of your message, service interests, and any information you voluntarily provide;
- **Technical data:** IP address, browser type and version, device identifiers, operating system, referring URL, and time zone setting;
- **Usage data:** pages visited, time spent on pages, click patterns, and other analytics collected through cookies and similar technologies (see §12).

4.2 Prospective and Existing Clients / Engagement-Related Data

In the course of scoping, contracting, and delivering our Services, we may collect:

- Business contact details of client representatives (name, designation, email, phone number);
- Commercial and contractual information, including billing and payment details;
- Information provided in connection with due diligence, onboarding, and Know-Your-Client (KYC) checks; and
- Client Data encountered during the performance of GRC advisory, IS audits, VAPT, or compliance assessments, which may incidentally include personal data present in client systems, logs, documents, or environments (see §8).

4.3 Information from Other Sources

We may also receive personal data from third parties, such as professional networking platforms, publicly available business directories, referral partners, and background-check or KYC service providers, in each case consistent with applicable law.

5. How We Collect Personal Data

We collect personal data:

- Directly from you, when you fill out a form, request a proposal, subscribe to updates, apply for a job, or otherwise communicate with us;
- Automatically, through cookies, web beacons, and similar technologies when you use our Site (see §12);
- From our clients, in connection with the scoping and delivery of engagements; and
- From publicly available sources or trusted third parties, such as professional networks or partner referrals.

6. Purposes and Legal Bases for Processing

We process personal data for the following purposes, relying on the legal bases indicated:

Purpose	Examples	Legal Basis (GDPR) / Grounds (DPDP Act)
Responding to enquiries	Replying to contact-form submissions and quote requests	Consent; steps prior to entering a contract
Contract performance	Proposing, contracting, and delivering GRC/IS audit/VAPT engagements	Performance of a contract; consent
Client and vendor management	Billing, onboarding, KYC, relationship management	Contract performance; legitimate interests; legal obligation
Marketing communications	Sending newsletters, service updates, and event invitations	Consent (opt-in/opt-out available at any time)
Site analytics and security	Understanding Site usage; detecting and preventing fraud or abuse	Legitimate interests; consent (for non-essential cookies)
Legal and regulatory compliance	Responding to lawful requests from regulators, courts, or law enforcement	Legal obligation; compliance with the DPDP Act, GDPR, and other applicable law

Where we rely on consent, you may withdraw consent at any time, without affecting the lawfulness of processing carried out before withdrawal, by contacting us using the details in §21.

7. How We Use Personal Data

We use personal data to:

- Provide, scope, and manage our Services, including proposals, statements of work, and engagement delivery;
- Communicate with you about your enquiries, engagements, invoices, and account matters;
- Improve and secure our Site, internal systems, and Services;

- Comply with legal, regulatory, contractual, and professional obligations (including retention obligations arising from audit and assurance standards); and
- Send marketing communications where you have consented, and allow you to opt out at any time.

We do not sell personal data, and we do not use personal data for automated decision-making that produces legal or similarly significant effects concerning you without human involvement.

8. Confidentiality of Client and Engagement Data

As a cybersecurity firm, we recognize that the data we may encounter while performing VAPT, IS audits, GRC advisory, and compliance assessments is highly sensitive - it can include personal data embedded in client systems, network configurations, credentials, logs, source code, and vulnerability findings. We apply the following principles to such Client Data:

- **Purpose limitation:** Client Data is accessed and used solely to perform the agreed scope of work and is not repurposed for any other business purpose without the client's written consent.
- **Contractual governance:** Every engagement is governed by a signed NDA and, where applicable, a data processing agreement that sets out roles, retention, sub-processing, and breach-notification obligations consistent with the DPDP Act and GDPR.
- **Need-to-know access:** Access to Client Data and assessment findings is restricted to engagement personnel on a least-privilege, need-to-know basis.
- **Secure handling:** Vulnerability findings, credentials, and sensitive artifacts are encrypted in transit and at rest, and are stored in access-controlled environments consistent with our internal information security management system.
- **Defined retention and secure disposal:** Engagement data and reports are retained only as long as necessary for delivery, quality assurance, and contractual/legal retention requirements, and are securely deleted or returned thereafter in accordance with the applicable contract.
- **No unauthorized disclosure:** Findings, vulnerabilities, and Client Data are never disclosed to third parties without the client's authorization, except where required by law.

If you believe your personal data has been processed by us in the course of a client engagement (for example, because your organization was the subject of an assessment we performed), any request regarding that data should generally be directed to the relevant client, who acts as the data controller for that processing; we will support our clients in responding to such requests as required by our contractual and legal obligations.

9. Data Sharing and Disclosure

We do not sell or rent personal data. We may share personal data with:

- Service providers and sub-processors who support our business operations (for example, cloud hosting, email delivery, analytics, payment processing, applicant-tracking, and IT support providers), under contractual confidentiality and data-protection obligations;
- Professional advisors, such as auditors, accountants, insurers, and legal counsel, where necessary for our legitimate business purposes;

- Regulators, law enforcement, courts, or other public authorities, where required or permitted by applicable law, or to establish, exercise, or defend legal claims;
- A successor entity in connection with a merger, acquisition, restructuring, or sale of assets, subject to appropriate confidentiality safeguards; and
- Any other party with your consent.

All third-party service providers who process personal data on our behalf are contractually bound to implement appropriate technical and organizational measures and to process personal data only on our documented instructions.

10. International Data Transfers

We are headquartered in India and may also serve clients in the European Economic Area (EEA), United Kingdom, and other jurisdictions. Where personal data is transferred outside the country in which it was originally collected including to India, to our service providers, or between our offices - we take steps designed to ensure an adequate level of protection, which may include:

- Reliance on adequacy decisions issued by the European Commission or the UK, where applicable;
- Standard Contractual Clauses (SCCs) approved by the European Commission, or the UK International Data Transfer Addendum, incorporated into our contracts with recipients outside the EEA/UK; and
- Other lawful transfer mechanisms recognized under the DPDP Act, GDPR, or other applicable data protection law.

You may contact us for further information on the safeguards we apply to a specific international transfer.

11. Data Security

Security is at the core of our business, and we apply commensurate rigor to our own systems and data. Our technical and organizational measures include:

- Encryption of personal data and sensitive engagement artifacts in transit and at rest;
- Role-based access controls, multi-factor authentication, and least-privilege access provisioning;
- Network segmentation, endpoint protection, and continuous security monitoring of our own environment;
- Regular internal and independent security testing of our systems, consistent with the standards we apply for our clients;
- Formal information security policies, staff security awareness training, and confidentiality obligations for all personnel and contractors; and
- A documented incident response plan, including procedures for detecting, containing, and reporting security incidents.

No method of transmission or storage is 100% secure. While we strive to protect personal data using commercially reasonable and industry-aligned safeguards, we cannot guarantee absolute security.

12. Data Retention

We retain personal data only for as long as necessary to fulfil the purposes described in this Policy, including to satisfy any legal, accounting, contractual, or reporting requirements. Retention periods vary depending on the category of data and typically include:

- **Website enquiry data:** retained for as long as needed to respond to your enquiry and for a reasonable period thereafter for record-keeping, unless you request earlier deletion;
- **Client and engagement records:** retained for the duration of the engagement plus any period required by contract, professional standards, or applicable law (which may extend to several years for audit and assurance records); and
- **Marketing data:** retained until you withdraw consent or unsubscribe.

When personal data is no longer required, we securely delete, anonymize, or archive it in accordance with our data retention and disposal procedures.

13. Cookies and Similar Tracking Technologies

Our Site uses cookies and similar technologies to operate essential functions, remember preferences, and understand how visitors use the Site. We use the following categories of cookies:

- **Strictly necessary cookies:** required for core Site functionality and security, and cannot be disabled;
- **Analytics/performance cookies:** help us understand visitor interactions to improve the Site, used only with your consent where required by law;
- **Functional cookies:** remember preferences to enhance your experience; and
- **Marketing cookies:** used, with your consent, to measure the effectiveness of our communications.

Where required by applicable law, we present a cookie consent banner allowing you to accept or reject non-essential cookies, and you can change your preferences at any time through the cookie settings on our Site or through your browser settings. Disabling certain cookies may affect Site functionality.

14. Your Rights

14.1 Rights of Data Principals under India's DPDP Act, 2023

If the DPDP Act applies to the processing of your personal data, you have the right to:

- Obtain a summary of the personal data we process about you and the processing activities undertaken (right to access information);
- Request correction, completion, and updating of your personal data (right to correction and updating);
- Request erasure of your personal data that is no longer necessary for the purpose for which it was processed, subject to legal retention requirements (right to erasure);
- Nominate another individual to exercise your rights on your behalf in the event of death or incapacity (right to nominate); and

- Have readily available means to register a grievance with us regarding the processing of your personal data (right to grievance redressal), as described in §18 below.

14.2 Rights of Data Subjects under the GDPR (EEA/UK Individuals)

If the GDPR applies to the processing of your personal data, you have the right to:

- Access the personal data we hold about you and obtain a copy;
- Rectify inaccurate or incomplete personal data;
- Erase your personal data in certain circumstances ("right to be forgotten");
- Restrict or object to processing, including processing for direct marketing purposes;
- Receive your personal data in a structured, commonly used, machine-readable format and transmit it to another controller (data portability);
- Withdraw consent at any time, without affecting the lawfulness of prior processing; and
- Lodge a complaint with your local supervisory authority, such as the UK Information Commissioner's Office (ICO) or the relevant EU data protection authority.

To exercise any of these rights, please contact us using the details in §21. We will respond within the timeframes required by applicable law and may need to verify your identity before actioning your request.

15. Automated Decision-Making and Profiling

We do not use personal data for automated decision-making, including profiling, that produces legal effects or similarly significantly affects individuals, without appropriate human oversight. Our Site analytics and marketing tools may use limited automated processing (for example, to segment communications), but such processing does not result in decisions with legal or similarly significant effect.

16. Children's Privacy

Our Site and Services are directed at businesses and professionals and are not intended for individuals under the age of 18. We do not knowingly collect personal data from children. If we become aware that we have inadvertently collected personal data from a child without appropriate consent, we will take steps to delete such data promptly.

17. Data Breach Notification

We maintain a documented incident response process for detecting, assessing, and responding to security incidents involving personal data. In the event of a personal data breach that is likely to result in a risk to the rights and interests of affected individuals, we will notify the affected individuals and/or the relevant supervisory authority (such as the India Data Protection Board or a relevant EU/UK supervisory authority) without undue delay and in accordance with applicable legal timeframes and requirements.

18. Grievance Redressal

We aim to acknowledge grievances promptly and resolve them within the timelines prescribed under the DPDP Act and, where applicable, the GDPR. If you are not satisfied with our response, you have the right to escalate your grievance to the India Data Protection Board (once constituted) or to the competent supervisory authority in your jurisdiction (for EEA/UK individuals).

19. Third-Party Websites and Links

Our Site may contain links to third-party websites, tools, or resources, including client portals, professional networking platforms, and industry publications. This Policy does not apply to those third-party sites, and we encourage you to review their privacy policies before providing any personal data.

20. Changes to This Privacy Policy

We may update this Policy from time to time to reflect changes in our practices, Services, or legal and regulatory requirements. Any changes will be posted on this page with a revised “Last Updated” date, and, where required by applicable law, we will provide additional notice or seek consent for material changes. We encourage you to review this Policy periodically.

21. Governing Law and Jurisdiction

This Policy is governed by the laws of India. For individuals located in the EEA or UK, nothing in this Policy limits any rights you may have under the GDPR or other applicable local law. Any disputes arising out of or in connection with this Policy shall be subject to the exclusive jurisdiction of the courts of Modasa, Gujarat, India, without prejudice to any statutory rights you may have to bring proceedings in your own jurisdiction.

22. Contact Us

If you have any questions, comments, or requests regarding this Privacy Policy or our data-processing practices, please contact us at:

LetsDefend Infosec

Address: 2nd Floor Ved Plaza Complex,

Meghraj Road, Modasa,

Gujarat-383315

Email: info@letsdefend.in

Phone: +91 7859957803

Website: www.letsdefend.in