Grivy - Public Privacy Policy

Effective Date: February 10, 2025

1. Introduction & Scope

This Privacy Policy describes how Grivy ("we", "us", or "our") collects, uses, protects, and discloses your personal information when you visit our website, use our services, or otherwise interact with us.

This policy applies to all personal data for which we act as the Data Controller (meaning we determine the purposes and means of processing).

2. Our Role in Data Processing

Our role in processing your data depends on our relationship with you.

- **As a Data Controller:** We act as a Data Controller when we collect personal information directly from you for our own purposes. This includes when you sign up for our newsletter, contact us for support, apply for a job, or are a representative of one of our clients or vendors.
- **As a Data Processor:** When we provide services to our business clients (e.g., running a marketing campaign on their behalf), our client is the Data Controller. We act as a Data Processor and only process personal information on their behalf and according to their instructions. In such cases, the client's privacy policy governs the processing of your data.

3. Personal Data We Collect

We collect different types of personal information depending on your interaction with us. This data is categorized as follows:

- **General Personal Information:**
    - **Identification Data:** Such as your name, job title, and company name.
    - **Contact Data:** Such as your email address, phone number, and physical address.
    - **Professional Data:** Such as your employment details, job history (for recruitment), or professional role.
    - **Technical Data:** Such as your IP address, browser type, device information, and cookies when you visit our website.
    - **Behavioral Data:** Such as information about how you interact with our website, services, or marketing emails (e.g., clicks, page views, opens).

    - **Communications Data:** Such as the content of your support tickets, emails, or other communications with us.
- **Specific (Sensitive) Personal Information:**
    - **Financial and Tax Data:** In limited circumstances, such as for processing payments from clients or managing our employees and contractors, we may collect financial data (e.g., bank account details, tax ID numbers).

4. Purpose and Legal Basis for Processing

We process your personal data for specific purposes and only when we have a valid legal basis to do so. The primary legal bases we rely on are **Consent**, **Contractual Necessity**, **Legal Obligation**, and **Legitimate Interest**.

Purpose of Processing	Examples of Activities	Legal Basis
Service Delivery	To provide our services and fulfill our contractual obligations to clients (e.g., Campaign Execution, Client Onboarding).	Contractual Necessity
Business Operations	To manage our business relationships with clients and vendors (e.g., Client Onboarding, Vendor Management).	Contractual Necessity / Legitimate Interest
Marketing & Growth	For lead generation, sending email marketing, and managing our CRM (e.g., Lead Generation, Email Marketing).	Consent (where required by law) or Legitimate Interest
Customer Support	To provide B2B and B2C customer support and manage inquiries (e.g., B2B Support, B2C Support).	Legitimate Interest (to provide a high-quality service)
HR & Recruitment	To manage our recruitment process and our employee relationships (e.g., Recruitment, Employee Administration).	Contractual Necessity / Legitimate Interest / Legal Obligation

Purpose of Processing	Examples of Activities	Legal Basis
Legal & Compliance	To meet our legal and regulatory obligations (e.g., financial record keeping, tax reporting).	Legal Obligation
Service Improvement	To analyze and improve our website, services, and internal processes.	Legitimate Interest

5. Data Disclosure and Transfer

We do not sell your personal information. We may share your data in the following circumstances:

- **Third-Party Service Providers:** We use trusted partners to help us operate our business. These providers are contractually bound to protect your data and only use it for the services we've requested. They include providers for:
    - Cloud Hosting & Productivity (e.g., **Google Workspace, Google Cloud Platform**)
    - CRM (e.g., **Salesforce**)
    - Finance and Accounting (e.g., **Xero**)
    - Customer Support (e.g., **Zendesk**)
    - Project Management (e.g., **Atlassian**)
    - HR Management (e.g., **Talenta**)
- **Legal Authorities:** If required by law, regulation, or a valid legal request, we may disclose your information to law enforcement or other public authorities.
- **Business Transfers:** In the event of a merger, acquisition, or sale of assets, your data may be transferred as part of that transaction.

Cross-Border Data Transfer Your personal information may be transferred to, processed, and stored in locations outside of your country of residence, where our service providers are located.

We will only conduct such international transfers in compliance with applicable data protection laws, such as the Indonesian PDP Law (UU 27/2022). We ensure your data is protected by relying on one of the following legal mechanisms: (a) Transferring to countries that have been deemed to have an "adequate" level of data protection by the relevant authorities; (b) Using adequate and binding safeguards, such as Standard Contractual Clauses (SCCs) or other approved data transfer agreements with our

third-party service providers; or (c) Obtaining your explicit consent for the specific transfer.

6. Your Rights as a Data Subject

Under applicable data protection laws, you have specific rights regarding your personal data. These include:

- **The Right to Access:** You can request a copy of the personal data we hold about you.
- **The Right to Rectification:** You can ask us to correct any inaccurate or incomplete data.
- **The Right to Erasure ("Right to be Forgotten"):** You can request that we delete your personal data, subject to certain exceptions (e.g., data we must keep for legal obligations).
- **The Right to Restrict Processing:** You can ask us to limit how we use your data in certain circumstances.
- **The Right to Data Portability:** You can request your data in a structured, machine-readable format to transfer to another service.
- **The Right to Object:** You can object to us processing your data, particularly for direct marketing purposes.
- **The Right to Withdraw Consent:** Where we rely on your consent to process data, you can withdraw that consent at any time.

How to Exercise Your Rights: To make a Data Subject Access Request (DSAR) or to exercise any other right, please contact us using the details in the "Contact Us" section below. We will respond to your request in accordance with applicable laws.

7. Profiling and Automated Decision-Making

We do not use your personal data for automated decision-making that produces legal or similarly significant effects on you.

We may use profiling for marketing purposes, such as segmenting our audience based on professional interests or service engagement to provide you with more relevant content and advertising. You have the **right to object** to this type of profiling at any time by contacting us or unsubscribing from our communications.

8. Data Security and Retention

Security: We are committed to protecting your data. We implement robust technical and organizational security measures to prevent unauthorized access, disclosure, alteration, or destruction of your information. These measures include:

- **Role-Based Access Control (RBAC)** to ensure only necessary personnel can access data.
- **Multi-Factor Authentication (MFA)** for critical systems.
- Data encryption in transit and at rest.
- We are actively working to align our security posture with international standards like **ISO 27001/27701**.

Retention: We retain your personal data only for as long as necessary to fulfill the purposes for which it was collected, or as required by our legal and regulatory obligations.

Our retention periods are defined by our Data Retention Policy and are based on:

- **Legal Requirements:** For example, financial, tax, and employee records are retained for up to **10 years** as required by law.
- **Contractual Needs:** Data related to client contracts is kept for the duration of the contract and a set period afterward.
- **Business Needs:** Marketing data or support tickets may be kept for **1-5 years** after our last interaction with you, after which it is securely deleted or anonymized.

9. Data Breach Notification

We have procedures in place to detect, investigate, and respond to personal data breaches. In the event of a breach, we will take immediate steps to contain and mitigate the harm.

In accordance with the Indonesian Personal Data Protection Law (UU 27/2022) and other applicable regulations, we will provide written notification to the relevant data protection authority and affected data subjects without undue delay, as required by law. This notification will describe the nature of the breach, the likely consequences, and the measures we are taking to address it.

10. Children's Privacy

Our services are not intended for or directed at individuals under the age of 13 (or the relevant age of digital consent in your jurisdiction). We do not knowingly collect personal information from children. If we become aware that we have inadvertently collected such information, we will take immediate steps to delete it.

11. Contact Us

If you have any questions about this Privacy Policy, our data practices, or wish to exercise your rights, please contact our Data Protection representative:

Email: privacy@grivy.com **Address:** Office 8 Tower, 18th Floor.Jend Sudirman Kav 52 Jakarta 12190

We may update this Privacy Policy from time to time. The "Effective Date" at the top of this policy will indicate the date of the latest revision.