DATA PROCESSING AGREEMENT (DPA) | Freelancea LLC
Effective Date: October 15, 2025
Last Updated: October 15, 2025

TABLE OF CONTENTS

1. INTRODUCTION AND DEFINITIONS

1.1 Purpose

This Data Processing Agreement ("DPA" or "Agreement") forms part of the Terms of Service between Freelancea, Inc. ("Freelancea," "we," "us," "our," "Data Processor," or "Processor") and you ("Customer," "Client," "Controller," or "you") and governs the processing of Personal Data by Freelancea on behalf of the Customer in connection with the provision of services through the Freelancea Platform.

This DPA is designed to ensure compliance with applicable Data Protection Laws, including but not limited to the General Data Protection Regulation (GDPR), UK GDPR, California Consumer Privacy Act (CCPA), California Privacy Rights Act (CPRA), and other international privacy regulations.

1.2 Definitions

For the purposes of this DPA, the following terms shall have the meanings set forth below:

"Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with a party, where "control" means ownership of at least 50% of the voting securities or equivalent interest.

"Applicable Data Protection Laws" or "Data Protection Laws" means all laws, regulations, and other legal requirements relating to privacy, data protection, and data security applicable to the processing of Personal Data under this DPA, including without limitation:

The General Data Protection Regulation (EU) 2016/679 ("GDPR")
The UK Data Protection Act 2018 and UK GDPR

The California Consumer Privacy Act (CCPA) as amended by the California Privacy Rights Act (CPRA)
The Virginia Consumer Data Protection Act (VCDPA)
The Colorado Privacy Act (CPA)
The Connecticut Data Privacy Act (CTDPA)
The Utah Consumer Privacy Act (UCPA)
Brazil's Lei Geral de Proteção de Dados (LGPD)
Canada's Personal Information Protection and Electronic Documents Act (PIPEDA)
Any other applicable national, federal, state, provincial, or local law relating to privacy or data protection

"Controller" means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data. For the purposes of this DPA, the Customer is the Controller.
"Customer Data" means all data, information, and content submitted, uploaded, transmitted, or otherwise provided by or on behalf of Customer or its users to the Services, including Personal Data.
"Data Breach" or "Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored, or otherwise processed.
"Data Protection Authority" or "Supervisory Authority" means an independent public authority established by a country or state to supervise compliance with Data Protection Laws.
"Data Subject" means an identified or identifiable natural person whose Personal Data is processed under this DPA. This may include:

Freelancers registered on the Platform
Clients posting jobs on the Platform
End users of Customer's services
Employees or contractors of Customer
Any other individual whose Personal Data is processed

"EEA" means the European Economic Area, consisting of the member states of the European Union plus Iceland, Liechtenstein, and Norway.
"Personal Data" means any information relating to an identified or identifiable natural person as defined by Applicable Data Protection Laws. This includes but is not limited to:

Name, email address, phone number
Postal address and billing information
IP address and device identifiers
Payment information and financial data
Professional information (skills, experience, education)
Profile information and photographs
Communication content and messages
Location data
Usage and behavioral data
Any other information that can directly or indirectly identify a person

"Processing" or "Process" means any operation or set of operations performed on Personal Data, whether or not by automated means, including:

Collection and recording
Organization and structuring
Storage and adaptation
Retrieval and consultation
Use and disclosure by transmission
Dissemination or otherwise making available
Alignment or combination
Restriction, erasure, or destruction

"Processor" means a natural or legal person, public authority, agency, or other body which processes Personal Data on behalf of the Controller. For the purposes of this DPA, Freelancea is the Processor.
"Security Incident" means any confirmed or suspected unauthorized or unlawful breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data.
"Services" means the Freelancea platform, website, mobile applications, API, and all related services provided by Freelancea to Customer as described in the Terms of Service.
"Standard Contractual Clauses" or "SCCs" means the standard contractual clauses for the transfer of Personal Data to third countries approved by the European Commission pursuant to GDPR Article 46(2)(c) and (d), as may be updated or replaced from time to time.
"Sub-Processor" means any third-party processor engaged by Freelancea to process Personal Data on behalf of Customer in connection with the Services.
"Supervisory Authority" means the relevant data protection authority with jurisdiction over the Customer or the processing activities in question.
"UK GDPR" means the GDPR as incorporated into United Kingdom law by the UK Data Protection Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019.

1.3 Interpretation

References to "including" or "includes" mean "including but not limited to"
Headings are for convenience only and do not affect interpretation
The singular includes the plural and vice versa
References to any law include amendments, replacements, or successor legislation
References to "writing" include electronic communications unless otherwise specified
Any conflict between this DPA and the Terms of Service shall be resolved in favor of this DPA with respect to data protection matters

1.4 Hierarchy of Documents

In the event of any conflict or inconsistency between the following documents, they shall be interpreted in the following order of precedence:

This Data Processing Agreement (DPA)

Standard Contractual Clauses (if applicable)
Terms of Service
Privacy Policy
Any other applicable policies or agreements

2. SCOPE AND APPLICATION

2.1 Scope of Processing

This DPA applies to all processing of Personal Data by Freelancea on behalf of Customer in connection with the provision of Services under the Terms of Service. The specific details of processing are set forth in Annex A (Details of Processing) attached hereto.

2.2 Duration

This DPA takes effect on the date Customer accepts the Terms of Service or begins using the Services (whichever is earlier) and remains in effect until the termination or expiration of the Services, subject to Section 13 (Term and Termination).

2.3 Who This DPA Applies To

This DPA applies to:

Business Customers: Organizations, companies, or entities that use Freelancea Services to engage freelancers or hire talent for business purposes, where the Customer determines the purposes and means of processing Personal Data.

Enterprise Clients: Large organizations with enterprise agreements who process substantial volumes of Personal Data through the Platform.

Agencies and Intermediaries: Marketing agencies, staffing firms, or other intermediaries who use Freelancea to provide services to their own clients.

Freelancers Acting as Controllers: Freelancers who engage other freelancers or process Personal Data of their own clients where they determine the purposes and means of processing.

2.4 Who This DPA Does Not Apply To

This DPA does not apply to:

Individual Freelancers (Personal Use): Individual freelancers using the Platform solely for their own freelance work, where Freelancea acts as Controller of their Personal Data under the Privacy Policy.

Clients Hiring for Personal Projects: Individuals hiring freelancers for personal, family, or household purposes where no business relationship exists.

Prospective Customers: Individuals or entities browsing the Platform without an active account or service agreement.

2.5 Geographic Scope

This DPA applies to the processing of Personal Data:

Regardless of where the Customer is located
Regardless of where the Data Subjects are located
In connection with the Services, regardless of where processing takes place
Subject to the requirements of Applicable Data Protection Laws in relevant jurisdictions

2.6 Incorporation by Reference

This DPA is incorporated by reference into and forms an integral part of the Terms of Service. By accepting the Terms of Service or using the Services, Customer agrees to be bound by this DPA.

2.7 Changes in Processing Activities

If Customer wishes to engage Freelancea for processing activities that differ materially from those described in Annex A, Customer must:

Provide written notice to Freelancea at legal@freelancea.net
Obtain written agreement from Freelancea before proceeding
Enter into an amended DPA or addendum if necessary

3. ROLES AND RESPONSIBILITIES

3.1 Customer as Data Controller

Customer acknowledges and agrees that it is the Data Controller with respect to Personal Data processed under this DPA. As Controller, Customer shall:

3.1.1 Lawful Basis for Processing

Determine the purposes and means of processing Personal Data
Ensure it has a lawful basis under Data Protection Laws for all processing
Obtain any necessary consents from Data Subjects
Provide required notices and information to Data Subjects
Comply with all Controller obligations under Data Protection Laws

3.1.2 Instructions to Processor

Provide clear, lawful, and documented instructions to Freelancea regarding the processing of Personal Data
Ensure instructions comply with Data Protection Laws
Not instruct Freelancea to process Personal Data in a manner that would violate Data Protection Laws
Update instructions as necessary to remain compliant

3.1.3 Data Quality and Accuracy

Ensure Personal Data provided to Freelancea is accurate, complete, and up-to-date
Not provide Personal Data to Freelancea unless lawfully obtained
Promptly notify Freelancea of any known errors or inaccuracies in Personal Data
Update or correct Personal Data as necessary

3.1.4 Data Subject Rights

Respond to Data Subject requests exercising their rights under Data Protection Laws
Notify Freelancea promptly of any Data Subject requests that require Freelancea's assistance
Not represent to Data Subjects that Freelancea is responsible for responding to their requests

3.1.5 Security Cooperation

Implement appropriate technical and organizational measures to protect Personal Data before transmitting to Freelancea
Promptly notify Freelancea of any security concerns or vulnerabilities
Cooperate with Freelancea in investigating and remediating security incidents
Not introduce malware, viruses, or malicious code into the Services

3.1.6 Compliance Obligations

Conduct Data Protection Impact Assessments (DPIAs) when required by Data Protection Laws
Consult with Supervisory Authorities when required
Maintain records of processing activities as required by Data Protection Laws
Ensure any third parties it authorizes to access the Services comply with Data Protection Laws

3.1.7 Use Restrictions

Use the Services only for lawful business purposes
Not use the Services to process Special Categories of Personal Data (as defined in GDPR Article 9) or Personal Data relating to criminal convictions without prior written agreement
Not process Personal Data of children under 18 without appropriate safeguards
Comply with all applicable laws regarding marketing communications and electronic communications

3.2 Freelancea as Data Processor

Freelancea acknowledges and agrees that it is the Data Processor with respect to Personal Data processed under this DPA. As Processor, Freelancea shall:

3.2.1 Processing Instructions

Process Personal Data only on documented instructions from Customer, including with regard to transfers of Personal Data outside the EEA or other applicable jurisdictions, unless required to do so by applicable law
Inform Customer if, in Freelancea's opinion, an instruction violates Data Protection Laws
Not process Personal Data for any purpose other than as instructed by Customer or as necessary to provide the Services

3.2.2 Confidentiality

Ensure that all persons authorized to process Personal Data are subject to appropriate confidentiality obligations (whether contractual or statutory)
Limit access to Personal Data to personnel who require access to perform services under the Terms of Service
Ensure personnel are trained on data protection principles and requirements
Maintain appropriate policies and procedures to protect Personal Data confidentiality

3.2.3 Security Measures

Implement and maintain appropriate technical and organizational measures to protect Personal Data as described in Section 6 (Security Measures)
Regularly test, assess, and evaluate the effectiveness of security measures
Update security measures as necessary to address new threats and vulnerabilities
Assist Customer in ensuring compliance with Customer's security obligations under Data Protection Laws

3.2.4 Sub-Processors

Engage Sub-Processors only in accordance with Section 7 (Sub-Processors)
Ensure Sub-Processors are bound by data protection obligations equivalent to those in this DPA
Remain fully liable to Customer for the performance of any Sub-Processor's obligations

3.2.5 Data Subject Rights

Assist Customer, taking into account the nature of processing, in responding to requests from Data Subjects to exercise their rights under Data Protection Laws as described in Section 5
Implement technical and organizational measures to facilitate Data Subject rights
Respond promptly to Customer's requests for assistance
Not respond directly to Data Subject requests unless authorized by Customer

3.2.6 Data Breach Notification

Notify Customer without undue delay upon becoming aware of a Personal Data Breach affecting Customer's Personal Data
Provide Customer with sufficient information to meet Customer's data breach notification obligations
Cooperate with Customer in investigating, mitigating, and remediating the breach
Implement measures to prevent future similar breaches

3.2.7 Compliance Assistance

Provide reasonable assistance to Customer in ensuring compliance with Customer's obligations under Data Protection Laws, including:

Data Protection Impact Assessments (DPIAs)
Prior consultations with Supervisory Authorities
Security risk assessments
Compliance audits and documentation

Charge reasonable fees for assistance that requires substantial effort beyond the scope of Services

3.2.8 Data Deletion and Return

Delete or return all Personal Data to Customer upon termination or expiration of Services, subject to Section 11 (Data Retention and Deletion)
Certify in writing that all Personal Data has been deleted or returned
Retain Personal Data only as required by applicable law

3.2.9 Documentation and Records

Maintain records of all categories of processing activities carried out on behalf of Customer as required by Data Protection Laws
Make such records available to Supervisory Authorities upon request
Provide Customer with information necessary to demonstrate compliance with this DPA
Cooperate with audits and inspections as described in Section 10

3.3 Freelancea as Independent Controller

Customer acknowledges that in certain circumstances, Freelancea acts as an independent Data Controller (not as Processor) for:

3.3.1 Platform Operations

User account creation and authentication
Platform security and fraud prevention
Service improvement and product development
Compliance with legal obligations
Communications about Services and updates
Aggregate analytics and reporting

3.3.2 Marketing Activities

Marketing communications to Customer's authorized users (with appropriate consent)
Market research and surveys
Event invitations and promotional activities

3.3.3 Legal and Compliance

Responding to legal requests and law enforcement
Protecting Freelancea's legal rights
Enforcing Terms of Service
Complying with regulatory requirements

For these purposes, Freelancea's Privacy Policy governs the processing, not this DPA. Customer acknowledges that Freelancea determines the purposes and means of such processing independently.

3.4 Joint Controller Situations

In limited circumstances, Customer and Freelancea may be considered Joint Controllers under Data Protection Laws. If this situation arises:

The parties will negotiate in good faith to determine their respective responsibilities
A joint controller agreement or addendum to this DPA may be required
Each party will be transparent about their respective roles to Data Subjects
Arrangements will be reflected in accordance with GDPR Article 26 or equivalent provisions

3.5 Restrictions on Customer Instructions
Freelancea is not required to comply with Customer instructions that:

Violate Data Protection Laws or other applicable laws
Are technically infeasible given the nature of the Services
Require Freelancea to violate its obligations to other customers
Would compromise the security or functionality of the Services
Require substantial modification to the Services not agreed upon
Are inconsistent with this DPA or the Terms of Service

If Freelancea believes an instruction falls into one of these categories, Freelancea will promptly inform Customer and the parties will discuss alternative approaches.

4. DATA PROCESSING PRINCIPLES
4.1 Principles of Data Processing
Both parties agree to comply with the following data processing principles established by Data Protection Laws:
4.1.1 Lawfulness, Fairness, and Transparency

Personal Data must be processed lawfully, fairly, and in a transparent manner
Customer must have a lawful basis for all processing (consent, contract, legitimate interests, legal obligation, vital interests, or public task)
Data Subjects must be provided clear information about processing activities
Processing must not be deceptive, unfair, or cause unjustified harm

4.1.2 Purpose Limitation

Personal Data must be collected for specified, explicit, and legitimate purposes
Personal Data must not be processed in a manner incompatible with those purposes
Further processing for archiving, research, or statistical purposes may be permitted under certain conditions
Customer must clearly define and document the purposes for processing

4.1.3 Data Minimization

Personal Data must be adequate, relevant, and limited to what is necessary for the processing purposes
Only Personal Data actually needed should be collected and processed
Unnecessary or excessive data collection is prohibited
Regular reviews should be conducted to ensure ongoing necessity

4.1.4 Accuracy

Personal Data must be accurate and, where necessary, kept up to date
Inaccurate Personal Data must be erased or rectified without delay
Reasonable steps must be taken to ensure accuracy
Data Subjects should have easy means to update their information

4.1.5 Storage Limitation

Personal Data must be kept in a form that permits identification of Data Subjects for no longer than necessary
Personal Data may be stored for longer periods only for archiving, research, or statistical purposes with appropriate safeguards
Retention periods should be defined and documented
Personal Data must be deleted or anonymized when no longer needed

4.1.6 Integrity and Confidentiality (Security)

Personal Data must be processed in a manner that ensures appropriate security
Protection against unauthorized or unlawful processing
Protection against accidental loss, destruction, or damage
Appropriate technical and organizational measures must be implemented
Security must be tested, assessed, and regularly evaluated

4.1.7 Accountability

Controllers must be able to demonstrate compliance with data protection principles
Appropriate documentation and records must be maintained
Data Protection Impact Assessments must be conducted when required
Policies, procedures, and training must be implemented
Regular audits and reviews should be conducted

4.2 Special Categories of Personal Data

4.2.1 Definition

Special Categories of Personal Data (also called "Sensitive Personal Data") include data revealing:

Racial or ethnic origin
Political opinions
Religious or philosophical beliefs
Trade union membership
Genetic data
Biometric data for identification purposes
Health data
Sex life or sexual orientation

4.2.2 Restrictions

Processing of Special Categories of Personal Data is generally prohibited unless specific conditions are met
Customer must not provide Special Categories of Personal Data to Freelancea without:

Prior written agreement from Freelancea
Explicit consent from Data Subjects (where required)
Another lawful basis under Data Protection Laws
Additional security and protection measures

If Customer provides Special Categories of Personal Data without authorization, Freelancea may immediately suspend or terminate Services

4.2.3 Criminal Conviction Data

Personal Data relating to criminal convictions and offenses may only be processed under the control of official authority or with appropriate legal authorization
Customer must not provide such data without prior written agreement

4.2.4 Children's Data

Special protections apply to Personal Data of children
Customer must obtain appropriate parental or guardian consent where required
Customer must implement age-appropriate safeguards and notices
Freelancea Services are not intended for users under 18

4.3 Processing for Specific Purposes
4.3.1 Service Provision
Freelancea will process Personal Data to:

Create and manage user accounts
Facilitate connections between freelancers and clients
Process payments and financial transactions
Provide customer support and communications
Enable messaging and collaboration features
Deliver notifications and updates
Maintain and improve the Services

4.3.2 Security and Fraud Prevention
Freelancea will process Personal Data to:

Detect and prevent fraud, scams, and abuse

Protect against security threats and vulnerabilities
Verify user identities and prevent unauthorized access
Monitor for suspicious activity
Investigate security incidents
Comply with security-related legal obligations

4.3.3 Legal Compliance
Freelancea will process Personal Data to:

Comply with legal obligations and regulatory requirements
Respond to law enforcement and government requests
Enforce Terms of Service and policies
Protect legal rights and interests
Comply with court orders and legal processes

4.3.4 Analytics and Improvement
Freelancea may process Personal Data to:

Analyze platform usage and performance
Generate aggregate statistics and insights
Improve and develop new features
Conduct research and testing
Optimize user experience

Note: Analytics processing must use pseudonymized or aggregated data whenever possible.
4.4 Automated Decision-Making and Profiling
4.4.1 Scope
The Services may involve automated decision-making or profiling, including:

Matching freelancers with relevant job opportunities
Risk assessment for fraud prevention
Personalized recommendations
Search ranking and filtering

4.4.2 Data Subject Rights
Data Subjects have the right to:

Be informed about automated decision-making
Obtain human intervention
Express their point of view
Contest the decision

4.4.3 Customer Obligations
If Customer uses Services involving automated decision-making with legal or similarly significant effects:

Customer must conduct a Data Protection Impact Assessment
Customer must implement appropriate safeguards
Customer must provide required notices to Data Subjects
Customer must not make solely automated decisions for Special Categories of Personal Data or children without explicit consent or substantial public interest basis

4.4.4 Freelancea Assistance
Freelancea will:

Provide information about automated decision-making logic
Assist Customer in implementing appropriate safeguards
Enable manual review and intervention when required
Document automated processing activities

5. DATA SUBJECT RIGHTS

5.1 Overview of Data Subject Rights

Under Data Protection Laws, Data Subjects have various rights regarding their Personal Data. Customer, as Controller, is primarily responsible for facilitating these rights. Freelancea will assist Customer as described below.

5.2 Right of Access (Right to Information)

5.2.1 Data Subject Rights
Data Subjects have the right to:

Confirm whether their Personal Data is being processed
Access their Personal Data
Receive information about processing activities
Obtain a copy of their Personal Data

5.2.2 Customer Responsibilities

Respond to Data Subject access requests within required timeframes (typically 30 days under GDPR)
Provide Personal Data in a concise, transparent, intelligible, and easily accessible form
Provide the first copy free of charge (reasonable fees may apply for additional copies)

5.2.3 Freelancea Assistance
Freelancea will:

Provide reasonable assistance in responding to access requests
Make available Personal Data within Freelancea's possession
Provide information about processing activities conducted by Freelancea
Respond to Customer requests within 10 business days or as otherwise agreed

5.2.4 Self-Service Tools
Customer may use the following self-service tools to facilitate access requests:

Account dashboard and profile settings
Data export functionality (where available)
API access for data retrieval
Reporting and analytics features

5.3 Right to Rectification (Right to Correction)
5.3.1 Data Subject Rights
Data Subjects have the right to:

Correct inaccurate Personal Data
Complete incomplete Personal Data
Update outdated information

5.3.2 Customer Responsibilities

Verify and correct inaccurate Personal Data
Respond to rectification requests promptly
Communicate corrections to recipients of the data where required

5.3.3 Freelancea Assistance
Freelancea will:

Provide tools for Customer to correct Personal Data
Correct inaccurate data upon Customer instruction
Implement corrected data across relevant systems
Notify Sub-Processors of corrections where necessary

5.3.4 Self-Service Correction
Many corrections can be made directly through:

Account settings and profile management
Dashboard edit functions
API updates
Bulk data import/update tools

5.4 Right to Erasure ("Right to be Forgotten")
5.4.1 Data Subject Rights
Data Subjects have the right to request deletion of their Personal Data when:

Personal Data is no longer necessary for the purposes collected
Consent is withdrawn (where processing was based on consent)

Personal Data was unlawfully processed
Legal obligation requires deletion
Data Subject objects to processing and there are no overriding legitimate grounds

5.4.2 Exceptions
Erasure may be refused when processing is necessary for:

Exercising freedom of expression and information
Compliance with legal obligations
Public health purposes
Archiving, research, or statistical purposes
Establishment, exercise, or defense of legal claims

5.4.3 Customer Responsibilities

Evaluate whether erasure exceptions apply
Balance Data Subject rights against other legal obligations
Respond to erasure requests within required timeframes
Document reasons for refusal if applicable

5.4.4 Freelancea Implementation
Upon receiving deletion instructions from Customer, Freelancea will:

Delete Personal Data from active systems within 30 days
Delete Personal Data from backup systems within 90 days
Confirm completion of deletion in writing
Retain minimal data only where legally required
Anonymize data that must be retained for legal or security purposes

5.4.5 Limitations on Deletion
Freelancea may retain certain Personal Data:

As required by applicable law (e.g., financial records, tax compliance)
To defend legal claims or comply with legal process
In backup systems for up to 90 days (not accessible for normal operations)
In anonymized or aggregated form that does not identify individuals

5.5 Right to Restriction of Processing
5.5.1 Data Subject Rights
Data Subjects have the right to restrict processing when:

Accuracy of Personal Data is contested (restriction during verification)
Processing is unlawful but Data Subject opposes erasure
Controller no longer needs data but Data Subject needs it for legal claims

Data Subject objects to processing (restriction pending verification)

5.5.2 Restricted Processing
When processing is restricted:

Personal Data may only be stored
Further processing requires Data Subject consent or is permitted only for:

Establishment, exercise, or defense of legal claims
Protection of rights of another person
Important public interest reasons

5.5.3 Customer Responsibilities

Evaluate restriction requests and determine appropriate action
Inform Data Subject before lifting restriction
Communicate restriction to data recipients where required

5.5.4 Freelancea Implementation
Freelancea will:

Mark Personal Data as "restricted" in relevant systems
Prevent unauthorized processing of restricted data
Alert personnel handling restricted data
Maintain restricted status until Customer provides further instructions
Implement technical measures to enforce restrictions

5.6 Right to Data Portability
5.6.1 Data Subject Rights
Data Subjects have the right to:

Receive Personal Data in a structured, commonly used, machine-readable format
Transmit data to another controller without hindrance
Request direct transmission to another controller (where technically feasible)

5.6.2 Scope
Data portability applies when:

Processing is based on consent or contract
Processing is carried out by automated means

5.6.3 Customer Responsibilities

Provide data in portable format (e.g., CSV, JSON, XML)
Respond to portability requests within required timeframes
Facilitate direct transmission when requested and feasible

5.6.4 Freelancea Support
Freelancea provides:

Data export functionality in common formats (CSV, JSON)
API access for programmatic data retrieval
Documentation of data structures and schemas
Reasonable assistance in facilitating portability
Support for bulk data exports

5.6.5 Export Formats
Available export formats include:

CSV (Comma-Separated Values)
JSON (JavaScript Object Notation)
XML (Extensible Markup Language)
PDF (for human-readable documents)

5.7 Right to Object
5.7.1 General Right to Object
Data Subjects have the right to object to processing based on:

Legitimate interests of Controller
Public interest or official authority
Profiling based on the above

Upon objection, Controller must cease processing unless:

Compelling legitimate grounds override Data Subject interests
Processing is necessary for legal claims

5.7.2 Right to Object to Direct Marketing
Data Subjects have an absolute right to object to:

Processing for direct marketing purposes
Profiling related to direct marketing

Upon objection, Controller must cease processing for those purposes.
5.7.3 Right to Object to Scientific/Historical Research
Data Subjects may object to processing for research or statistical purposes unless processing is necessary for public interest tasks.

5.7.4 Customer Responsibilities

Honor objections to direct marketing immediately
Evaluate other objections and balance interests
Cease processing if required
Document legitimate grounds if continuing processing

5.7.5 Freelancea Assistance

Freelancea will:

Cease processing upon Customer instruction
Implement suppression lists for marketing objections
Tag objection data appropriately in systems
Assist in evaluating technical feasibility of objections

5.8 Rights Related to Automated Decision-Making

5.8.1 Data Subject Rights

Data Subjects have the right not to be subject to solely automated decisions with legal or similarly significant effects, including profiling, unless:

Necessary for contract performance
Authorized by law with appropriate safeguards
Based on explicit consent

5.8.2 Required Safeguards

When automated decision-making is permitted:

Right to obtain human intervention
Right to express point of view
Right to contest the decision
Right to obtain explanation of decision

5.8.3 Customer Obligations

Conduct Data Protection Impact Assessment
Implement appropriate safeguards
Provide clear information to Data Subjects
Enable human review and intervention

5.8.4 Freelancea Support

Freelancea will:

Provide information about automated decision logic
Enable manual review capabilities where feasible

Document automated processing activities
Assist in implementing safeguards

5.9 Processing Data Subject Requests

5.9.1 Request Receipt

When Freelancea receives a Data Subject request:

Freelancea will promptly forward the request to Customer
Customer must respond to the Data Subject directly
Freelancea will not respond directly without Customer authorization
Freelancea will cooperate in verifying Data Subject identity

5.9.2 Verification

Both parties will:

Implement reasonable procedures to verify Data Subject identity
Request additional information if identity cannot be confirmed
Refuse manifestly unfounded or excessive requests
Balance security with Data Subject rights

5.9.3 Timelines

Customer must respond to Data Subject within applicable legal timeframes (typically 30 days under GDPR, 45 days under CCPA)
Customer may extend deadline by additional period with justification
Freelancea will respond to Customer assistance requests within 10 business days
Urgent requests (e.g., data breaches) will be prioritized

5.9.4 Fees

First request is generally free of charge
Reasonable fees may be charged for manifestly unfounded, excessive, or repetitive requests
Fees must be based on administrative costs
Fee structure must be transparent and communicated to Data Subject

5.9.5 Refusal

Requests may be refused when:

Manifestly unfounded or excessive
Identity cannot be verified
Disclosure would adversely affect rights of others
Legal obligations prevent compliance
Exceptions under Data Protection Laws apply

Customer must:

Document reasons for refusal
Inform Data Subject of
RetryHContinue

5.9.5 Refusal (continued)

Customer must:

Document reasons for refusal
Inform Data Subject of refusal reason and their right to complain to Supervisory Authority
Respond within required timeframes even if refusing the request
Consult legal counsel before refusing significant requests

5.9.6 Assistance Fee

Freelancea may charge reasonable fees for assistance with Data Subject requests that:

Require substantial custom development or modifications
Involve extensive manual review or data compilation
Are repetitive or manifestly excessive
Go beyond standard assistance obligations

Fees will be:

Communicated in advance
Based on actual costs incurred
Reasonable and proportionate
Subject to Customer approval before work begins

6. SECURITY MEASURES

6.1 Overview

Freelancea implements and maintains appropriate technical and organizational measures designed to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access. Security measures are designed considering the state of the art, implementation costs, nature of processing, and risks to Data Subjects.

6.2 Technical Security Measures

6.2.1 Access Controls

Authentication: Multi-factor authentication for administrative access
Authorization: Role-based access control (RBAC) limiting access based on job function
Least Privilege: Personnel granted minimum access necessary to perform duties
Access Logging: All access to Personal Data systems logged and monitored
Access Reviews: Quarterly reviews of access rights and permissions
Account Termination: Immediate revocation of access upon employment termination

6.2.2 Encryption

Data in Transit: TLS 1.2 or higher for all data transmissions
Data at Rest: AES-256 encryption for stored Personal Data
Database Encryption: Encryption of database files and backups
Key Management: Secure key storage using hardware security modules (HSMs)
Certificate Management: Regular rotation of SSL/TLS certificates

6.2.3 Network Security

Firewalls: Next-generation firewalls protecting all network perimeters
Intrusion Detection/Prevention: IDS/IPS systems monitoring for threats
Network Segmentation: Isolation of production, development, and testing environments
VPN Access: Required for remote administrative access
DDoS Protection: Distributed denial-of-service mitigation systems
Regular Scans: Weekly vulnerability scans of all external-facing systems

6.2.4 Application Security

Secure Development: OWASP Top 10 security practices integrated into development
Code Reviews: Security-focused code reviews before deployment
Input Validation: All user input validated and sanitized
Output Encoding: Prevention of cross-site scripting (XSS) attacks
CSRF Protection: Anti-CSRF tokens for all state-changing operations
SQL Injection Prevention: Parameterized queries and prepared statements
Security Headers: Implementation of security headers (CSP, HSTS, X-Frame-Options)

6.2.5 Data Protection

Data Masking: Masking of sensitive data in non-production environments
Tokenization: Tokenization of payment card information
Pseudonymization: Pseudonymization techniques where appropriate
Data Minimization: Technical controls limiting data collection
Automated Deletion: Scheduled deletion of data per retention policies
Backup Encryption: All backups encrypted with separate keys

6.2.6 Monitoring and Logging

SIEM System: Security Information and Event Management for centralized logging
Real-Time Alerts: Automated alerts for suspicious activities
Log Retention: Security logs retained for minimum 12 months
Audit Trails: Comprehensive audit trails for all Personal Data access and modifications
Log Protection: Logs stored securely and protected from tampering

Regular Review: Weekly review of security logs and alerts

6.2.7 Vulnerability Management

Patch Management: Security patches applied within 30 days of release (critical patches within 7 days)
Vulnerability Scanning: Weekly automated vulnerability scans
Penetration Testing: Annual third-party penetration testing
Bug Bounty Program: Responsible disclosure program for security researchers
Security Advisories: Monitoring of security advisories and threat intelligence
Remediation Tracking: Documented remediation plans for identified vulnerabilities

6.2.8 Endpoint Security

Antivirus/Anti-malware: Enterprise-grade protection on all endpoints
Device Encryption: Full disk encryption required on all devices
Mobile Device Management: MDM for mobile devices accessing company resources
Remote Wipe: Capability to remotely wipe lost or stolen devices
Patch Management: Automated patching for operating systems and applications
Application Whitelisting: Approved application lists for production systems

6.3 Organizational Security Measures

6.3.1 Security Governance

Information Security Policy: Comprehensive written security policies
Security Committee: Regular meetings of security leadership
Security Roadmap: Annual security improvement planning
Compliance Program: Ongoing compliance with security standards (ISO 27001, SOC 2)
Third-Party Assessments: Regular independent security assessments
Executive Oversight: Board-level oversight of security program

6.3.2 Personnel Security

Background Checks: Pre-employment background screening
Confidentiality Agreements: All personnel sign confidentiality agreements
Security Training: Mandatory annual security awareness training
Phishing Tests: Quarterly simulated phishing exercises
Specialized Training: Role-specific security training for technical staff
Clean Desk Policy: Enforcement of clean desk and clear screen policies
Exit Procedures: Comprehensive offboarding including access revocation

6.3.3 Physical Security

Data Center Security: Tier III or higher certified data centers
Access Control: Biometric or badge access to facilities

Video Surveillance: 24/7 video monitoring of sensitive areas
Visitor Management: Visitor logs and escort requirements
Equipment Disposal: Secure destruction of hardware containing data
Environmental Controls: Fire suppression, climate control, backup power

6.3.4 Vendor Management

Security Assessments: Security reviews of all vendors processing Personal Data
Contractual Obligations: Data protection terms in vendor contracts
Ongoing Monitoring: Regular reviews of vendor security practices
Sub-Processor Approval: Customer notification and approval process
Vendor Audits: Periodic audits of critical vendors
Vendor Termination: Secure data return/deletion upon vendor termination

6.3.5 Business Continuity and Disaster Recovery

Business Continuity Plan: Documented plans for service continuity
Disaster Recovery Plan: Procedures for recovery from major incidents
Backup Systems: Regular backups with geographically distributed storage
Backup Testing: Quarterly restoration testing
Redundancy: Redundant systems and infrastructure
RTO/RPO Targets: Recovery Time Objective <4 hours, Recovery Point Objective <1 hour
Annual Testing: Full disaster recovery exercise annually

6.3.6 Incident Response

Incident Response Plan: Documented procedures for security incidents
Incident Response Team: Designated team with defined roles
24/7 Monitoring: Round-the-clock security monitoring
Escalation Procedures: Clear escalation paths for incidents
Communication Plans: Templates for internal and external communications
Post-Incident Review: After-action reviews for all significant incidents
Continuous Improvement: Updates to procedures based on lessons learned

6.4 Data Center and Infrastructure Security

6.4.1 Data Center Certifications

Freelancea uses data centers with the following certifications:

ISO 27001 (Information Security Management)
SOC 2 Type II (Security, Availability, Confidentiality)
PCI DSS (Payment Card Industry Data Security Standard) where applicable
SSAE 18 attestations
Local compliance certifications as required

6.4.2 Infrastructure Providers

Primary infrastructure providers include:

Amazon Web Services (AWS): Primary cloud infrastructure provider
Google Cloud Platform (GCP): Secondary cloud infrastructure
Compliance documentation available upon request

6.4.3 Geographic Locations

Data centers are located in:

United States (primary)
European Union (for EU customers)
United Kingdom (for UK customers)
Other regions as needed to serve customers locally

6.4.4 Redundancy and Availability

Multi-zone deployment for high availability
Automatic failover capabilities
Load balancing across multiple servers
99.9% uptime SLA for core services

6.5 Security Testing and Validation

6.5.1 Penetration Testing

Frequency: Annual comprehensive penetration testing by independent third party
Scope: Web applications, APIs, infrastructure, social engineering
Methodology: OWASP Testing Guide, PTES (Penetration Testing Execution Standard)
Remediation: High/critical findings remediated within 30 days
Verification: Re-testing to confirm remediation effectiveness
Reporting: Summary reports available to enterprise customers upon request

6.5.2 Vulnerability Assessments

Automated Scanning: Weekly vulnerability scans of all systems
Manual Reviews: Quarterly manual security reviews of critical systems
Dependency Scanning: Automated scanning of third-party libraries and dependencies
Container Scanning: Security scanning of Docker containers and images
Infrastructure as Code: Security analysis of infrastructure configurations

6.5.3 Security Certifications

Freelancea maintains the following security certifications:

ISO 27001:2013 - Information Security Management System

SOC 2 Type II - Security, Availability, Confidentiality
PCI DSS Level 1 (for payment processing)
Annual recertification and audits

Certification reports available to enterprise customers under NDA.

6.6 Customer Security Responsibilities

6.6.1 Account Security

Customer is responsible for:

Maintaining confidentiality of account credentials
Implementing strong password policies for users
Enabling two-factor authentication where available
Promptly reporting suspected security incidents
Regularly reviewing account activity and access logs
Revoking access for terminated users

6.6.2 Data Security

Customer must:

Not introduce malware, viruses, or malicious code into Services
Implement appropriate security for data before transmission
Encrypt sensitive data when uploading to Services
Classify data appropriately and handle according to classification
Comply with own security policies and procedures

6.6.3 Access Management

Customer should:

Grant access on least-privilege basis
Regularly review and certify user access
Implement segregation of duties where appropriate
Monitor user activity for anomalies
Document access policies and procedures

6.7 Security Incident Notification

See Section 8 (Data Breaches and Incident Response) for detailed incident notification procedures.

6.8 Updates to Security Measures

6.8.1 Continuous Improvement

Freelancea continuously reviews and updates security measures to:

Address new and emerging threats
Implement new security technologies
Comply with evolving regulatory requirements
Incorporate industry best practices

Respond to audit findings and recommendations

6.8.2 Material Changes
Freelancea will:

Not materially decrease the overall security of Services
Notify Customer of material security changes that may adversely affect Customer
Provide reasonable notice before implementing changes requiring Customer action
Maintain security measures at least as protective as those described herein

6.8.3 Customer Notification
Notification of security changes will be provided through:

Email to designated Customer contacts
Platform announcements and notifications
Updates to this DPA or Security Documentation
Security bulletins and advisories

7. SUB-PROCESSORS
7.1 Authorization to Use Sub-Processors
7.1.1 General Authorization
Customer provides general authorization for Freelancea to engage Sub-Processors to process Personal Data on Customer's behalf, subject to the conditions set forth in this Section 7.
7.1.2 Sub-Processor Definition
A "Sub-Processor" is any third-party entity engaged by Freelancea to process Personal Data on behalf of Customer in connection with the Services.
7.2 Sub-Processor Obligations
7.2.1 Contractual Requirements
Freelancea shall:

Enter into written agreements with all Sub-Processors
Impose data protection obligations on Sub-Processors equivalent to those in this DPA
Ensure Sub-Processors are bound by confidentiality obligations
Require Sub-Processors to implement appropriate technical and organizational security measures
Ensure Sub-Processor contracts permit audits and inspections
Include provisions for data return or deletion upon termination

7.2.2 Liability
Freelancea remains fully liable to Customer for:

Performance of Sub-Processor obligations under this DPA
Acts and omissions of Sub-Processors
Any breach by Sub-Processor of data protection obligations

7.3 Current Sub-Processors

7.3.1 Sub-Processor List

Freelancea maintains a current list of Sub-Processors at:
The list includes:

Sub-Processor name and location
Description of processing activities
Data categories processed
Geographic location of processing

7.3.2 Major Sub-Processor Categories

Infrastructure Providers:

Amazon Web Services (AWS) - Cloud hosting and infrastructure

Location: United States, EU, UK
Purpose: Data storage, compute, networking

Google Cloud Platform (GCP) - Secondary cloud infrastructure

Location: United States, EU
Purpose: Backup, disaster recovery

Payment Processors:

Stripe, Inc. - Payment processing

Location: United States
Purpose: Credit card and ACH payment processing

PayPal Holdings, Inc. - Payment processing

Location: United States
Purpose: PayPal payments and withdrawals

Communication Services:

SendGrid (Twilio) - Email delivery

Location: United States
Purpose: Transactional and marketing emails

Twilio - SMS and communication services

Location: United States
Purpose: SMS notifications and two-factor authentication

Analytics and Monitoring:

Google Analytics - Website analytics

Location: United States
Purpose: Platform usage analytics

Mixpanel - Product analytics

Location: United States
Purpose: User behavior analysis

Customer Support:

Zendesk - Customer support platform

Location: United States
Purpose: Support ticket management

Intercom - Customer messaging

Location: United States
Purpose: Live chat and customer communications

Security Services:

Cloudflare - CDN and DDoS protection

Location: Global
Purpose: Content delivery and security

Auth0 (Okta) - Identity and access management

Location: United States
Purpose: Authentication services

7.4 New Sub-Processors

7.4.1 Notification Procedure

Before engaging a new Sub-Processor, Freelancea will:

Send email notification to Customer's designated contact (if provided)
Provide at least 30 days' notice before the new Sub-Processor processes Personal Data
Include Sub-Processor name, location, and processing purpose in notification

7.4.2 Customer Objection Rights

Customer may object to a new Sub-Processor by:

Notifying Freelancea in writing within 30 days of notification
Providing reasonable grounds for objection related to data protection compliance
Sending objection to support@freelancea.net

7.4.3 Resolution of Objections

If Customer objects to a new Sub-Processor:

Freelancea will use reasonable efforts to make available a change in Services or recommend a commercially reasonable alternative
If no alternative is available, Customer may terminate the affected Services
Termination will not relieve Customer of fees for services rendered before termination
If Customer does not object within 30 days, Customer is deemed to have accepted the new Sub-Processor

7.4.4 Emergency Sub-Processors

In emergency situations requiring immediate Sub-Processor engagement to:

Prevent service interruption
Address critical security issues
Comply with legal obligations
Respond to force majeure events

Freelancea may engage Sub-Processors with shortened notice period, followed by standard notification procedures as soon as practicable.

7.5 Sub-Processor Changes

7.5.1 Replacement Sub-Processors

When replacing an existing Sub-Processor:

Standard 30-day notification applies
Customer objection rights apply
Previous Sub-Processor must securely delete or return Personal Data
New Sub-Processor must meet equivalent security and compliance requirements

7.5.2 Sub-Processor Monitoring

Freelancea will:

Regularly assess Sub-Processor security and compliance
Conduct annual reviews of Sub-Processor performance
Monitor Sub-Processor security incidents and breaches
Require Sub-Processors to maintain appropriate certifications
Remove Sub-Processors that fail to meet requirements

7.6 Sub-Processor Audits

7.6.1 Freelancea Audits of Sub-Processors

Freelancea will:

Conduct regular audits of critical Sub-Processors
Review Sub-Processor security certifications (ISO 27001, SOC 2)
Investigate Sub-Processor security incidents
Verify Sub-Processor compliance with contractual obligations
Document audit findings and remediation actions

7.6.2 Customer Access to Sub-Processor Information

Customer may request:

Current Sub-Processor list and details
Sub-Processor security certifications and audit reports (subject to confidentiality)
Information about Sub-Processor security incidents affecting Customer data
Verification of Sub-Processor compliance with this DPA

7.6.3 Confidentiality

Sub-Processor audit reports and security documentation are confidential and may require:

Execution of non-disclosure agreements
Restrictions on use and disclosure
Direct receipt from Sub-Processor (rather than through Freelancea)

7.7 Affiliate Sub-Processors

7.7.1 Freelancea Affiliates

Freelancea may engage Freelancea Affiliate entities as Sub-Processors for:

Global service delivery
Regional customer support
Localized services
Administrative functions

7.7.2 Intra-Group Transfers

Transfers to Freelancea Affiliates:

Are subject to the same protections as third-party Sub-Processors
Comply with international data transfer requirements
Are covered by intra-group data transfer agreements
Are listed in the Sub-Processor inventory

8. INTERNATIONAL DATA TRANSFERS

8.1 Transfer Mechanisms

8.1.1 Overview

Freelancea may transfer Personal Data internationally, including from the EEA, UK, or Switzerland to countries that do not provide an adequate level of data protection as determined by the European Commission or relevant authorities.

8.1.2 Legal Basis for Transfers

International transfers of Personal Data are conducted based on:

Standard Contractual Clauses (SCCs): EU Commission-approved SCCs incorporated by reference
Adequacy Decisions: Transfers to countries with adequacy decisions
Binding Corporate Rules: For intra-group transfers
Certifications: Such as EU-U.S. Data Privacy Framework (if applicable)
Explicit Consent: Where Customer obtains Data Subject consent for specific transfers
Contractual Necessity: Where transfer is necessary to perform contract with Data Subject

8.2 Standard Contractual Clauses

8.2.1 Incorporation

The Standard Contractual Clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 ("EU SCCs"), as approved by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, are incorporated into this DPA by reference and form part of this Agreement.

8.2.2 Module Selection

The following modules of the EU SCCs apply:

Module Two: Controller to Processor transfers

Module Three: Processor to Sub-Processor transfers (where applicable)

8.2.3 SCC Terms
For purposes of the EU SCCs:

Clause 7 (Docking Clause): Optional docking clause does not apply unless otherwise agreed
Clause 9 (Use of Sub-Processors): General authorization applies as per Section 7 of this DPA
Clause 11 (Redress): Data Subjects have third-party beneficiary rights
Clause 17 (Governing Law): Law of Ireland (EU Member State where Data Exporter is established, or Ireland if not in EU)
Clause 18 (Choice of forum and jurisdiction): Courts of Ireland
Annex I: Details set forth in Annex B to this DPA
Annex II: Security measures set forth in Section 6 of this DPA
Annex III: Sub-Processor list set forth in Section 7 of this DPA

8.2.4 UK Addendum
For transfers subject to UK GDPR, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses ("UK Addendum"), issued by the UK Information Commissioner's Office, is incorporated by reference.
8.2.5 Swiss Addendum
For transfers subject to the Swiss Federal Act on Data Protection, the Swiss-specific requirements and adaptations to the SCCs are incorporated.
8.3 Transfer Impact Assessment
8.3.1 Assessment Obligation
Freelancea has conducted a Transfer Impact Assessment (TIA) to evaluate:

Laws and practices in destination countries
Risks to Personal Data from government access
Supplementary measures needed beyond SCCs
Overall adequacy of protection

8.3.2 Supplementary Measures
Based on the TIA, Freelancea implements supplementary technical and organizational measures:
Technical Measures:

End-to-end encryption for data in transit
Encryption of data at rest with customer-managed keys (where available)
Pseudonymization of data where feasible
Data minimization in international transfers
Secure access controls limiting access by jurisdiction

Organizational Measures:

Contractual prohibition on unlawful government access

Transparency reporting on government requests
Legal challenge procedures for overbroad requests
Staff training on data protection across jurisdictions
Incident notification for government access requests

Legal Measures:

Legal agreements with Sub-Processors in third countries
Commitment to challenge disproportionate access requests
Notification to Customer of government access requests (where legally permitted)

8.3.3 Monitoring and Review
Freelancea will:

Monitor legal developments in destination countries
Reassess transfer mechanisms if legal landscape changes
Implement additional safeguards as necessary
Suspend transfers if adequate protection cannot be ensured
Notify Customer of material changes affecting transfer adequacy

8.4 Specific Transfer Scenarios
8.4.1 EEA to United States
Transfers from EEA to United States are based on:

Standard Contractual Clauses
Supplementary measures as described in Section 8.3.2
EU-U.S. Data Privacy Framework certification (if and when Freelancea obtains certification)

8.4.2 UK to Third Countries
Transfers from UK are based on:

UK Addendum to Standard Contractual Clauses
UK adequacy regulations
Supplementary measures

8.4.3 Switzerland to Third Countries
Transfers from Switzerland are based on:

Swiss-adapted Standard Contractual Clauses
Swiss Federal Data Protection and Information Commissioner (FDPIC) guidance
Supplementary measures

8.4.4 Brazil to Other Countries
Transfers from Brazil under LGPD are based on:

Standard Contractual Clauses
ANPD (Brazilian Data Protection Authority) guidelines
Adequate level of data protection in destination country

8.4.5 Other Jurisdictions
For other jurisdictions with data localization or transfer restrictions:

Compliance with local data protection laws
Appropriate transfer mechanisms as required
Legal opinions as necessary
Customer notification of applicable restrictions

8.5 Data Localization Options
8.5.1 Regional Data Storage
For customers with data localization requirements, Freelancea offers:

EU Data Residency: Data stored exclusively in EU data centers
UK Data Residency: Data stored exclusively in UK data centers
Other Regional Options: Available upon request for enterprise customers

8.5.2 Limitations
Even with regional data storage:

Support and administrative access may occur from other locations
Backup and disaster recovery may involve other regions
Sub-Processors may process data in various locations
Aggregated and anonymized data may be processed globally

8.5.3 Requesting Data Residency
To request data residency options:

Contact sales@freelancea.net or your account manager
Specify required data localization jurisdiction
Review available options and pricing
Execute necessary amendments to Terms of Service

8.6 Government Access Requests
8.6.1 Legal Process
If Freelancea receives a legal demand for disclosure of Personal Data from government or law enforcement:

Freelancea will attempt to redirect the request to Customer
Freelancea will challenge overbroad or unlawful requests where feasible
Freelancea will notify Customer unless legally prohibited

Freelancea will disclose only the minimum data required by law

8.6.2 Transparency
Freelancea publishes transparency reports detailing:

Number and types of government requests received
Number of accounts/users affected
Number of requests challenged or rejected
Geographic source of requests

8.6.3 Customer Notification
Unless prohibited by law, Freelancea will:

Notify Customer of government access requests within 72 hours
Provide details of the legal basis for the request
Allow Customer opportunity to challenge the request
Consult with Customer on response where feasible

9. DATA BREACHES AND INCIDENT RESPONSE

9.1 Data Breach Definition

A "Personal Data Breach" or "Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored, or otherwise processed.
Examples include:

Unauthorized access to Personal Data systems
Ransomware or malware affecting Personal Data
Loss or theft of devices containing Personal Data
Accidental disclosure to unauthorized parties
Insider threats or malicious employee actions
Third-party breaches affecting Personal Data
Human error resulting in data exposure

9.2 Freelancea Obligations

9.2.1 Breach Detection and Assessment
Freelancea will:

Maintain security monitoring and detection systems
Investigate suspected security incidents promptly
Assess whether an incident constitutes a Personal Data Breach
Determine the scope, severity, and impact of the breach
Document all findings and actions taken

9.2.2 Customer Notification
Timing:

Freelancea will notify Customer without undue delay
Notification will be provided within 72 hours of Freelancea becoming aware of the breach
If full information is not available within 72 hours, Freelancea will provide initial notification followed by updates

Method:

Email to Customer's designated security contact
Phone call for high-severity breaches
Through Customer's account dashboard or portal
Via emergency contact procedures if standard methods fail

Content:
Notification will include, to the extent known:

Nature of the Personal Data Breach
Categories and approximate number of Data Subjects affected
Categories and approximate number of Personal Data records affected
Likely consequences of the breach
Measures taken or proposed to address the breach
Measures taken or proposed to mitigate potential adverse effects
Name and contact details of Freelancea's data protection officer or other contact point
Recommendations for Customer action

9.2.3 Cooperation and Assistance
Freelancea will:

Cooperate with Customer in investigating the breach
Provide reasonable assistance in Customer's breach response
Assist Customer in meeting regulatory notification obligations
Provide necessary information for Customer to notify Supervisory Authorities
Provide necessary information for Customer to notify affected Data Subjects
Participate in meetings or calls to discuss the breach and response
Provide written confirmation and documentation as reasonably requested

9.3 Customer Obligations
9.3.1 Regulatory Notification
Customer, as Controller, is responsible for:

Determining whether to notify Supervisory Authorities
Notifying Supervisory Authorities within required timeframes (typically 72 hours under GDPR)

Providing required information to Supervisory Authorities
Documenting reasons if not notifying authorities

9.3.2 Data Subject Notification
Customer is responsible for:

Determining whether to notify affected Data Subjects
Notifying Data Subjects without undue delay when required
Providing Data Subjects with required information
Recommending steps Data Subjects should take

9.3.3 Documentation
Customer should:

Document all breach-related decisions and actions
Maintain records of breach notifications
Keep evidence of compliance with notification obligations
Be prepared to demonstrate compliance to Supervisory Authorities

9.4 Incident Response Process
9.4.1 Detection and Identification (Phase 1)

Security monitoring systems detect anomaly
Security Operations Center (SOC) investigates alert
Incident Response Team evaluates whether incident affects Personal Data
Severity classification assigned (Critical, High, Medium, Low)
Incident tracking number created

9.4.2 Containment and Mitigation (Phase 2)

Immediate steps taken to contain the breach
Affected systems isolated if necessary
Unauthorized access blocked
Vulnerabilities patched or remediated
Additional monitoring implemented
Evidence preserved for investigation

9.4.3 Investigation and Assessment (Phase 3)

Forensic investigation conducted
Scope and impact determined
Root cause identified
Affected Personal Data catalogued
Number of Data Subjects estimated

Potential harm assessed

9.4.4 Notification (Phase 4)

Customer notified per Section 9.2.2
Assistance provided for regulatory and Data Subject notifications
Updates provided as investigation progresses
Final incident report prepared

9.4.5 Recovery and Remediation (Phase 5)

Affected systems restored to normal operation
Additional security controls implemented
Monitoring enhanced
Affected data secured or remediated
Business operations normalized

9.4.6 Post-Incident Review (Phase 6)

Lessons learned analysis conducted
Incident response procedures reviewed and updated
Security improvements identified and implemented
Staff training updated
Final report provided to Customer

9.5 Breach Severity Classification
Critical Severity:

Large-scale breach affecting >10,000 Data Subjects
Breach of Special Categories of Personal Data
Breach likely to result in high risk to Data Subject rights
Ransomware with data exfiltration
Insider threat with malicious intent
Notification: Immediate (within 24 hours)

High Severity:

Breach affecting 1,000-10,000 Data Subjects
Unauthorized access to sensitive Personal Data
Breach likely to result in significant risk
Data exfiltration by external party
Notification: Within 48 hours

Medium Severity:

Breach affecting 100-1,000 Data Subjects
Limited unauthorized access
Moderate risk to Data Subjects
Accidental disclosure to unauthorized party
Notification: Within 72 hours

Low Severity:

Breach affecting <100 Data Subjects
Minimal unauthorized access
Low risk to Data Subjects
Quickly contained with minimal exposure
Notification: Within 72 hours

9.6 Customer Breach Reporting
9.6.1 Customer-Caused Breaches
If Customer becomes aware of a breach caused by:

Customer's misuse of Services
Compromised Customer credentials
Customer employee or contractor actions
Third parties authorized by Customer

Customer must:

Notify Freelancea promptly at support@freelancea.net
Provide details of the incident
Cooperate in investigation and remediation
Take immediate steps to prevent further unauthorized access

9.6.2 Joint Investigation
For breaches involving both parties:

Parties will cooperate in joint investigation
Responsibility and liability will be determined based on facts
Each party responsible for own regulatory notifications
Coordinated response where appropriate

9.7 Breach Documentation
9.7.1 Freelancea Records
Freelancea will maintain records of all Personal Data Breaches, including:

Facts relating to the breach

Effects of the breach
Remedial action taken
Documentation sufficient to demonstrate compliance

9.7.2 Customer Access
Customer may request:

Copies of breach documentation
Incident response reports
Forensic investigation findings (subject to confidentiality)
Evidence of remediation

9.7.3 Retention
Breach records will be retained for:

Minimum 5 years after breach resolution
Longer if required by applicable law
Duration of any9.7.3 Retention (continued)
Breach records will be retained for:
- Minimum 5 years after breach resolution
- Longer if required by applicable law
- Duration of any litigation or regulatory investigation
- As necessary to demonstrate compliance

9.8 Third-Party Breaches
9.8.1 Sub-Processor Breaches
If a Sub-Processor experiences a breach affecting Customer Personal Data:
- Sub-Processor must notify Freelancea per contractual obligations
- Freelancea will notify Customer as described in Section 9.2.2
- Freelancea will coordinate response with Sub-Processor
- Freelancea remains liable for Sub-Processor breaches

9.8.2 Upstream Breaches
If Customer experiences a breach affecting data stored in Freelancea Services:
- Customer must notify Freelancea promptly
- Freelancea will assist in investigation and remediation
- Freelancea will implement additional security measures if needed
- Customer remains responsible for regulatory notifications

10. AUDITS AND COMPLIANCE
10.1 Audit Rights
10.1.1 Customer Audit Rights
Customer has the right to audit Freelancea's compliance with this DPA through:

- Review of compliance documentation and certifications
- Information security audits
- On-site inspections (subject to restrictions below)
- Third-party audit reports
- Questionnaires and assessments

10.1.2 Frequency and Scope
Standard Audits:
- Customer may request audit information once per calendar year at no charge
- Additional audits may be subject to reasonable fees
- Audits must be reasonably scoped to data protection compliance
- Audits must not unreasonably interfere with Freelancea's business operations

Triggered Audits:
- Additional audits permitted following a Personal Data Breach
- Audits may be required by Supervisory Authority
- Emergency audits for critical compliance concerns

10.2 Compliance Documentation
10.2.1 Available Documentation
Freelancea will make available upon request:

Security Certifications:
- ISO 27001 Certificate
- SOC 2 Type II Report (under NDA)
- PCI DSS Attestation of Compliance (if applicable)
- Other relevant security certifications

Policies and Procedures:
- Information Security Policy (summary)
- Data Breach Response Plan (summary)
- Business Continuity Plan (summary)
- Vendor Management Procedures (summary)

Processing Documentation:
- Details of processing activities (Annex A)
- Sub-Processor list and details
- International data transfer documentation
- Data retention schedules

Compliance Evidence:
- Completed questionnaires (e.g., SIG, CAIQ)
- Vendor security assessments
- Penetration test summaries (under NDA)

- Vulnerability scan results (summary)

10.2.2 Documentation Format
Documentation may be provided as:
- Digital copies via secure file transfer
- Access to secure online portal
- Copies of third-party audit reports
- Written responses to questionnaires
- Virtual or in-person presentations

10.2.3 Confidentiality
Audit documentation is confidential and:
- May require execution of Non-Disclosure Agreement
- Must not be shared with third parties without Freelancea consent
- Must be used only for evaluating Freelancea's compliance
- May contain redactions to protect other customers or security details

10.3 Third-Party Audit Reports
10.3.1 SOC 2 Type II
Freelancea undergoes annual SOC 2 Type II audits covering:
- Security
- Availability
- Confidentiality
- Processing Integrity (where applicable)
- Privacy (where applicable)

Availability:
- Reports available to enterprise customers under NDA
- Summary available to other customers upon request
- Reports updated annually
- Bridge letters provided if needed between audit periods

10.3.2 ISO 27001
Freelancea maintains ISO 27001:2013 certification:
- Annual surveillance audits
- Full recertification every three years
- Certificate available upon request
- Statement of Applicability available under NDA

10.3.3 Other Certifications
Additional certifications maintained as applicable:
- PCI DSS for payment processing
- Industry-specific certifications as needed
- Regional compliance certifications

10.4 On-Site Audits

10.4.1 Requesting On-Site Audit

Customer may request on-site audit by:

- Providing 60 days' written notice to office@freelancea.net
- Specifying audit scope and objectives
- Identifying audit personnel and qualifications
- Proposing audit dates and duration
- Signing Freelancea's standard audit agreement

10.4.2 Freelancea Approval

Freelancea may reasonably:

- Approve, modify, or decline audit requests
- Limit audit frequency (typically one on-site audit per year)
- Restrict audit scope to data protection matters
- Require confidentiality agreements
- Charge reasonable fees for audit accommodation
- Propose alternative audit approaches

10.4.3 Audit Conduct

During on-site audits:

- Auditors must comply with Freelancea's security and facility policies
- Auditors may not access other customers' data
- Auditors may not disrupt business operations
- Auditors must protect confidential information observed
- Freelancea personnel will accompany auditors
- Auditors may not install software or access production systems

10.4.4 Audit Reports

Following audit:

- Auditors provide findings report to Customer
- Customer shares relevant findings with Freelancea
- Freelancea responds to findings within 30 days
- Parties collaborate on remediation plan for legitimate issues
- Follow-up audits may verify remediation

10.5 Supervisory Authority Audits

10.5.1 Cooperation Obligation

Freelancea will:

- Cooperate with Supervisory Authority audits and investigations
- Provide requested information and documentation
- Make personnel available for interviews
- Allow on-site inspections as required by law
- Implement corrective actions as directed

10.5.2 Customer Notification
Freelancea will notify Customer:
- Upon receipt of Supervisory Authority audit or investigation notice
- Of the scope and nature of the inquiry
- Of any findings or enforcement actions
- Of required corrective actions
- As legally permitted (some investigations may be confidential)

10.6 Audit Fees
10.6.1 Standard Audit Information
Provided at no charge:
- Annual provision of standard compliance documentation
- Responses to reasonable compliance questionnaires
- Certificate and attestation copies
- Sub-Processor list access
- Basic compliance inquiries

10.6.2 Chargeable Audit Services
Reasonable fees may apply for:
- On-site audits (travel, personnel time, facility costs)
- Custom audit reports or documentation
- Extensive questionnaire completion requiring significant effort
- Multiple audits per year beyond standard allowance
- Expedited audit requests
- Audits requiring substantial custom work

Fee Schedule:
- On-site audit accommodation: $5,000 per day plus expenses
- Custom documentation: $200 per hour
- Extensive questionnaires (>100 questions): $150 per hour
- Emergency/expedited requests: 1.5x standard rates

10.6.3 Enterprise Customer Terms
Enterprise customers with dedicated account management may receive:
- Increased audit allowances
- Reduced or waived audit fees
- Dedicated compliance support
- Customized compliance reporting
- As negotiated in enterprise agreement

10.7 Continuous Compliance Monitoring
10.7.1 Internal Audits
Freelancea conducts:

- Quarterly internal security audits
- Annual compliance assessments
- Continuous security monitoring
- Regular policy and procedure reviews
- Staff compliance training and testing

10.7.2 External Assessments
Regular external assessments include:
- Annual penetration testing
- Quarterly vulnerability scanning
- Third-party security reviews
- Certification audit cycles
- Vendor risk assessments

10.7.3 Compliance Dashboard
Enterprise customers may access compliance dashboard featuring:
- Current certification status
- Recent audit summaries
- Security metrics and KPIs
- Sub-Processor updates
- Incident notifications
- Compliance calendar

10.8 Remediation and Corrective Actions
10.8.1 Finding Classification
Audit findings classified as:
- Critical: Immediate risk requiring urgent remediation
- High: Significant risk requiring prompt remediation
- Medium: Moderate risk requiring planned remediation
- Low: Minor improvement opportunity

10.8.2 Remediation Timelines
Standard remediation timeframes:
- Critical findings: 7 days
- High findings: 30 days
- Medium findings: 90 days
- Low findings: 180 days

10.8.3 Remediation Tracking
For each finding:
- Assign owner and due date
- Develop remediation plan
- Track progress and status
- Verify completion

- Document resolution
- Update controls and procedures

10.8.4 Customer Communication

Freelancea will:
- Notify Customer of material audit findings
- Provide remediation plans
- Update Customer on remediation progress
- Confirm completion of remediation
- Implement preventive measures

11. DATA RETENTION AND DELETION

11.1 Data Retention Principles

11.1.1 General Principles

Personal Data will be retained only:
- As long as necessary for the purposes collected
- As required by applicable law
- As necessary to fulfill contractual obligations
- As necessary to establish, exercise, or defend legal claims
- In accordance with documented retention schedules

11.1.2 Retention Schedule

Freelancea maintains documented retention schedules specifying:
- Data categories and types
- Retention periods for each category
- Legal or business justification
- Deletion procedures
- Exceptions and extensions

11.2 Retention Periods by Data Category

11.2.1 Account and Profile Data

Active Accounts:
- Retained for duration of account activity
- Updated as modified by users
- Available for user access and management

Inactive Accounts:
- Accounts inactive for 3+ years: notification sent
- Accounts inactive for 4 years: subject to deletion
- Grace period provided before deletion
- Enterprise accounts may have different terms

Closed Accounts:

- Profile data: deleted within 90 days
- Historical transaction data: retained per Section 11.2.3
- Anonymized analytics: may be retained indefinitely

11.2.2 Communication Data
Messages and Communications:
- Retained while accounts are active
- Deleted within 90 days of account closure
- Platform messages: 7 years for legal/dispute purposes
- Support communications: 7 years
- Marketing communications: Until consent withdrawn + 30 days

11.2.3 Financial and Transaction Data
Payment Information:
- Payment card data: tokenized, not stored by Freelancea
- Payment history: 7 years (tax and legal compliance)
- Transaction records: 7 years
- Invoices and receipts: 7 years
- Tax documentation: As required by tax law (typically 7-10 years)

11.2.4 Technical and Usage Data
Log Data:
- Security logs: 12 months minimum
- Access logs: 12 months
- System logs: 6 months
- Application logs: 6 months

Usage Data:
- Raw usage data: 24 months
- Aggregated analytics: Indefinitely (anonymized)
- Session data: 90 days
- Cookie data: Per cookie policy (typically 12-24 months)

11.2.5 Verification and Compliance Data
Identity Verification:
- KYC/AML documentation: 7 years after account closure
- Identity verification records: 7 years
- Background check results: 7 years

Compliance Records:
- Data Subject request records: 7 years
- Consent records: 7 years after withdrawal
- Privacy notices and acknowledgments: 7 years
- Audit records: 7 years

11.2.6 Dispute and Legal Data

Legal Matters:
- Data related to disputes: Until resolution + 7 years
- Litigation hold data: Until hold lifted + applicable retention period
- Subpoenas and legal requests: 7 years
- Fraud investigation records: 7 years

11.3 Data Deletion Procedures

11.3.1 Deletion Methods

Freelancea employs the following deletion methods:

Logical Deletion:
- Data marked as deleted in database
- Not accessible through normal operations
- Physically deleted within specified timeframes
- Used for immediate user-facing deletion

Physical Deletion:
- Data permanently removed from production systems
- Overwriting of storage media
- Crypto-shredding for encrypted data
- Verification of successful deletion

Backup Deletion:
- Data removed from backup systems
- May take up to 90 days as backups age out
- Not accessible for restoration
- Documented backup rotation procedures

11.3.2 Deletion Timelines

User-Initiated Deletion:
- Immediate logical deletion
- Physical deletion from production: within 30 days
- Deletion from backups: within 90 days
- Confirmation provided to user

Account Closure:
- Account data: deleted within 90 days
- Financial records: retained per Section 11.2.3
- Legal hold data: retained until hold lifted

Contractual Deletion:
- Upon termination: deleted within 180 days

- Unless Customer requests earlier deletion
- Subject to legal retention requirements
- Certification of deletion provided upon request

11.3.3 Exceptions to Deletion
Personal Data may be retained beyond standard periods when:

Legal Obligations:
- Required by applicable law or regulation
- Subject to legal hold or litigation
- Necessary for tax or financial compliance
- Required for regulatory investigations

Legitimate Interests:
- Necessary to establish, exercise, or defend legal claims
- Required to protect rights of Freelancea or others
- Necessary to prevent fraud or security threats
- Required for audit and compliance purposes

Technical Limitations:
- Contained in backups until natural rotation (max 90 days)
- Aggregated in analytics without identifiers
- Anonymized and no longer Personal Data
- Pseudonymized for research purposes

11.4 Customer Data Deletion Requests
11.4.1 Requesting Deletion
Customer may request deletion by:
- Submitting request to support@freelancea.net
- Specifying data categories and scope
- Providing verification of authority
- Acknowledging impact on Services

11.4.2 Deletion Process
Upon receiving deletion request:

Day 1-5: Request Review
- Verify Customer authority
- Confirm scope of deletion
- Identify affected data
- Assess legal retention requirements
- Confirm irreversibility with Customer

Day 6-30: Deletion Implementation

- Delete data from production systems
- Remove data from active databases
- Purge cached data
- Update indexes and search systems

Day 31-90: Backup Purge
- Data removed as backups rotate
- Verification of backup purge
- No data accessible for restoration

Day 91: Certification
- Provide written certification of deletion
- Confirm exceptions (if any)
- Document retention justifications

11.4.3 Partial Deletion
Customer may request deletion of specific data categories:
- Specify categories to be deleted
- Retain other data as necessary
- May impact Services functionality
- Requires detailed documentation

11.5 Data Anonymization
11.5.1 Anonymization Standards
When anonymization is used:
- Data must be irreversibly de-identified
- Re-identification must not be reasonably possible
- Pseudonymization alone is not sufficient
- Aggregation thresholds applied (typically k-anonymity ≥ 5)
- Indirect identifiers removed or generalized

11.5.2 Anonymized Data Uses
Anonymized data may be retained indefinitely for:
- Platform improvement and optimization
- Aggregate analytics and reporting
- Research and development
- Benchmarking and industry insights
- Training machine learning models

11.5.3 Verification
Anonymization procedures:
- Documented and validated
- Regularly reviewed and updated
- Tested for re-identification risk

- Audited for effectiveness

11.6 Data Return

11.6.1 Return Upon Termination

Upon termination or expiration of Services:
- Customer may request return of Personal Data
- Request must be made within 30 days of termination
- Data provided in portable format
- Returned via secure transfer method

11.6.2 Return Format

Data returned in:
- CSV (Comma-Separated Values)
- JSON (JavaScript Object Notation)
- XML (Extensible Markup Language)
- Database dump (for enterprise customers)
- Other formats as mutually agreed

11.6.3 Return Process

Timeline:
- Request received: Day 0
- Data compilation: Days 1-14
- Quality assurance: Days 15-21
- Secure transfer: Days 22-30
- Confirmation and verification: Days 31-45

Delivery Method:
- Encrypted file transfer (SFTP, secure cloud storage)
- Physical media (encrypted USB/hard drive) for large datasets
- API access for programmatic retrieval
- Direct database connection (enterprise)

11.6.4 Post-Return Deletion

After data return:
- Freelancea will delete data per Section 11.3
- Unless Customer requests retention for specific purpose
- Legal retention requirements still apply
- Deletion certification provided

12. LIABILITY AND INDEMNIFICATION

12.1 Liability Allocation

12.1.1 General Liability Principles

- Each party liable for its own breach of obligations under this DPA

- Liability determined based on applicable Data Protection Laws
- Liability may be joint and several for certain violations
- Independent causes of action under GDPR and other laws

12.1.2 Freelancea Liability

Freelancea is liable for:
- Failure to implement appropriate security measures
- Unauthorized processing contrary to Customer instructions
- Engaging unauthorized Sub-Processors
- Data breaches caused by Freelancea negligence
- Violation of Data Protection Laws in Freelancea's control
- Acts and omissions of Sub-Processors

12.1.3 Customer Liability

Customer is liable for:
- Providing unlawful processing instructions
- Failing to obtain necessary consents or legal basis
- Providing inaccurate or misleading information
- Failing to respond to Data Subject requests appropriately
- Violations of Data Protection Laws as Controller
- Compromised Customer credentials or account security
- Misuse of Services by Customer personnel

12.2 Limitations of Liability

12.2.1 Incorporation by Reference

The limitations of liability set forth in the Terms of Service apply to this DPA, except:
- Where prohibited by applicable Data Protection Laws
- For liability under GDPR Article 82 or equivalent provisions
- For willful misconduct or gross negligence
- For breaches of confidentiality obligations
- As otherwise required by law

12.2.2 GDPR Liability Framework

Under GDPR Article 82:
- Data Subjects may receive compensation for material or non-material damage
- Controllers and Processors may be held liable
- Processor liable only if failed to comply with obligations or acted outside lawful instructions
- Processor exempt from liability if proves no responsibility for damage
- Where multiple parties involved, each party liable for entire damage
- Parties may claim back from other parties their share of responsibility

12.2.3 California and US State Laws

Under CCPA/CPRA and similar laws:
- Statutory damages may apply for certain violations

- Private right of action for data breaches
- Service provider liability for non-compliant processing
- Civil penalties imposed by regulatory authorities

12.2.4 Other Jurisdictions
Liability under other Data Protection Laws as applicable:
- UK GDPR: Similar to EU GDPR framework
- LGPD (Brazil): Compensation for material and moral damages
- PIPEDA (Canada): Federal Court jurisdiction for violations
- Other laws: As specified by jurisdiction

12.3 Indemnification
12.3.1 Customer Indemnification of Freelancea
Customer will indemnify, defend, and hold harmless Freelancea from:
- Claims arising from Customer's violation of Data Protection Laws
- Claims arising from unlawful Customer instructions
- Claims arising from Customer's failure to obtain necessary consents
- Claims arising from inaccurate information provided by Customer
- Claims by Customer's Data Subjects based on Customer's actions
- Third-party claims arising from Customer's misuse of Services
- Regulatory fines/penalties resulting from Customer's violations

Exclusions: Does not apply to extent caused by Freelancea's breach.

12.3.2 Freelancea Indemnification of Customer
Freelancea will indemnify, defend, and hold harmless Customer from:
- Claims arising from Freelancea's violation of Data Protection Laws
- Claims arising from Freelancea's breach of security obligations
- Claims arising from unauthorized Sub-Processor engagement
- Claims by Data Subjects based solely on Freelancea's actions as Processor
- Third-party claims arising from Freelancea's negligence or willful misconduct

Exclusions: Does not apply to extent caused by Customer's breach or instructions.

12.3.3 Indemnification Procedures
Party seeking indemnification must:
- Promptly notify indemnifying party of claim
- Provide reasonable cooperation in defense
- Allow indemnifying party to control defense
- Not admit liability or settle without consent

Indemnifying party must:
- Assume defense with qualified counsel
- Keep indemnified party informed

- Obtain consent before settlement affecting indemnified party
- Pay judgments, settlements, and reasonable defense costs

12.4 Insurance

12.4.1 Freelancea Insurance

Freelancea maintains:

- Cyber Liability Insurance: $5,000,000 per occurrence
- Professional Liability Insurance (E&O): $5,000,000 per occurrence
- General Commercial Liability: $2,000,000 per occurrence
- Coverage for data breach response costs
- Coverage for regulatory defense and fines (where insurable)

12.4.2 Certificate of Insurance

Upon request:

- Freelancea will provide Certificate of Insurance
- Available to enterprise customers
- Updated annually or upon policy renewal
- Subject to confidentiality obligations

12.5 Regulatory Fines and Penalties

12.5.1 GDPR Fines

Under GDPR:

- Administrative fines up to €20 million or 4% of global annual turnover
- Supervisory Authorities have discretion in imposing fines
- Factors considered: nature, gravity, duration, intent, mitigation, cooperation
- Both Controllers and Processors may be fined

12.5.2 Responsibility Allocation

- Each party responsible for fines resulting from its own violations
- Joint violations: responsibility allocated based on contribution to violation
- Customer not responsible for fines arising solely from Freelancea violations
- Freelancea not responsible for fines arising solely from Customer violations as Controller

12.5.3 Cooperation on Regulatory Matters

Both parties will:

- Cooperate in responding to regulatory inquiries
- Share relevant information and documentation
- Participate in regulatory proceedings as needed
- Implement corrective actions to resolve violations
- Avoid actions that increase regulatory risk

12.6 Mitigation of Damages

12.6.1 Duty to Mitigate

Both parties have duty to:

- Take reasonable steps to mitigate damages
- Minimize harm to Data Subjects
- Prevent escalation of incidents
- Cooperate in damage mitigation efforts
- Implement corrective measures promptly

12.6.2 Failure to Mitigate

Failure to mitigate may:
- Reduce or eliminate recovery of damages
- Affect liability allocation
- Impact indemnification obligations
- Be considered in regulatory proceedings

13. TERM AND TERMINATION

13.1 Term

13.1.1 Effective Date

This DPA takes effect on the earlier of:
- Date Customer accepts Terms of Service
- Date Customer begins using Services
- Date specified in enterprise agreement

13.1.2 Duration

This DPA remains in effect until:
- Termination or expiration of Services
- Termination by either party as provided herein
- Superseded by amended DPA

13.2 Termination Rights

13.2.1 Termination for Convenience

Termination of underlying services:
- Customer may terminate Services per Terms of Service
- This DPA terminates upon termination of Services
- Data processing obligations continue through wind-down period

13.2.2 Termination for Breach

Material breach:
- Either party may terminate for material breach
- Written notice specifying breach required
- 30-day cure period (unless breach not curable)
- Immediate termination for uncured material breach

Examples of material breach:
- Repeated or systemic violations of Data Protection Laws

- Failure to implement required security measures
- Unauthorized disclosure of Personal Data
- Refusal to cooperate with audits or investigations
- Material misrepresentation regarding compliance

13.2.3 Termination for Sub-Processor Objection
Customer may terminate if:
- Customer objects to new Sub-Processor
- Freelancea cannot provide reasonable alternative
- Termination right specified in Section 7.4.3

13.2.4 Termination for Legal Requirement
Either party may terminate if:
- Continuing DPA would violate applicable law
- Court order requires termination
- Regulatory authority mandates termination
- Performance becomes impossible due to legal changes

13.3 Effects of Termination
13.3.1 Data Processing
Upon termination:
- Freelancea will cease processing Personal Data
- Except as necessary to complete data return or deletion
- Except as required by applicable law
- Customer instructions regarding data return/deletion control

13.3.2 Data Return or Deletion
Customer must elect (within 30 days of termination):

Option 1 - Data Return:
- Freelancea returns all Personal Data
- Format and method per Section 11.6
- Completed within 45 days
- Followed by deletion of remaining data

Option 2 - Data Deletion:
- Freelancea deletes all Personal Data
- Per procedures in Section 11.3
- Completed within 180 days
- Certification of deletion provided

Default: If Customer does not elect, deletion applies.

13.3.3 Survival of Obligations

The following provisions survive termination:
- Confidentiality obligations (indefinitely)
- Liability and indemnification (per statute of limitations)
- Data deletion/return obligations (until completed)
- Audit rights (for 12 months post-termination)
- Warranty disclaimers and limitations (indefinitely)
- Governing law and dispute resolution (indefinitely)
- Any obligations accrued before termination

13.4 Suspension

13.4.1 Freelancea Suspension Rights

Freelancea may suspend Services if:
- Customer materially breaches DPA
- Customer uses Services for unlawful purposes
- Customer's account compromised and suspension necessary for security
- Required by court order or law enforcement
- Necessary to prevent harm to other customers or Freelancea
- Customer fails to pay fees (per Terms of Service)

13.4.2 Suspension Procedures

Before suspension (except emergencies):
- Notice to Customer specifying reason
- Opportunity to cure (typically 5-10 business days)
- Consultation to resolve issues

During suspension:
- Data processing limited to storage and security
- Customer access may be restricted
- Data not deleted during suspension period
- Fees may continue to accrue

Reinstatement:
- Upon cure of issue causing suspension
- Verification of compliance
- May require additional security measures

13.5 Data Protection After Termination

13.5.1 Legal Retention

Even after termination, Personal Data may be retained:
- As required by applicable law (e.g., 7 years for financial records)
- To defend legal claims or comply with legal process
- In backup systems for up to 90 days
- In anonymized form for legitimate purposes

13.5.2 Continued Protection
Retained Personal Data remains subject to:
- Appropriate security measures
- Confidentiality obligations
- Access restrictions
- This DPA's requirements (for retained data only)

13.5.3 Final Deletion
After legal retention periods:
- All remaining Personal Data deleted
- Per standard deletion procedures
- Final certification provided if requested

14. AMENDMENTS AND UPDATES

14.1 Amendment Process

14.1.1 Freelancea-Initiated Amendments

Freelancea may amend this DPA to:
- Comply with changes in Data Protection Laws
- Reflect changes in Services or processing activities
- Incorporate new security measures or technologies
- Address regulatory guidance or enforcement actions
- Correct errors or clarify ambiguities
- Improve data protection practices

14.1.2 Notice of Amendments

Material amendments:
- Email notification to Customer's registered email address
- At least 30 days' advance notice
- Effective date specified in notice
- Summary of material changes provided

Non-material amendments:
- May be effective immediately
- No specific email notification required
- Customer responsible for reviewing periodic updates

14.1.3 Customer Acceptance

Continued use of Services after effective date constitutes acceptance of amendments.

If Customer objects to material amendment:
- Customer must notify Freelancea within 30 days
- Customer may terminate Services without penalty
- Termination must occur before amendment effective date

- Previous DPA version governs through termination

14.2 Customer-Requested Amendments

14.2.1 Request Process

Customer may request amendments by:
- Submitting written request to legal@freelancea.net
- Describing proposed changes and justification
- Explaining legal or business requirement
- Proposing implementation timeline

14.2.2 Freelancea Review

Freelancea will:
- Review request in good faith
- Respond within 30 days
- Consider operational and legal feasibility
- Propose alternatives if request cannot be accommodated

14.2.3 Custom Amendments

For enterprise customers:
- Custom DPA amendments may be negotiated
- Subject to mutual agreement and documentation
- May require additional fees
- Executed via formal amendment or addendum
- Contact enterprise sales team

14.3 Regulatory Changes

14.3.1 Changes in Law

If Data Protection Laws change materially:
- Freelancea will assess impact on DPA
- Update DPA as necessary for compliance
- Notify Customer of required changes
- Implement necessary technical/organizational measures
- Absorb reasonable costs of compliance

14.3.2 New Jurisdictions

When Customer expands to new jurisdictions:
- Customer must notify Freelancea
- Parties assess applicability of local Data Protection Laws
- DPA amendments may be required
- Additional terms or addenda may be necessary
- Services may require configuration changes

14.4 Version Control

14.4.1 DPA Versioning

- Each DPA version assigned unique version number
- Previous versions archived and accessible
- Effective dates clearly documented

Current Version: 2.0 (January 15, 2025)
Previous Versions:
- Version 1.0 (March 1, 2023)

14.4.2 Applicable Version
- Latest version applies to all active customers
- Unless enterprise agreement specifies otherwise
- Transitional periods provided for material changes
- Previous versions available for reference

14.5 Standard Contractual Clauses Updates
14.5.1 SCC Changes
If Standard Contractual Clauses are updated by regulatory authorities:
- Freelancea will adopt updated SCCs
- DPA updated to incorporate new SCCs
- Customer notification provided
- Transition period as required by regulations
- No Customer action required unless specified

14.5.2 Alternative Transfer Mechanisms
If new data transfer mechanisms become available:
- Freelancea may adopt alternative mechanisms
- Where they provide equivalent or better protection
- Customer notification provided
- DPA updated accordingly

15. GOVERNING LAW AND DISPUTE RESOLUTION
15.1 Governing Law
15.1.1 General Provisions
This DPA is governed by:
- Laws of Ireland (for EU customers)
- Laws of United Kingdom (for UK customers)
- Laws of State of Delaware, USA (for US customers)
- Laws of applicable jurisdiction (for other customers)

Without regard to conflicts of law principles.

15.1.2 Data Protection Laws
Notwithstanding governing law:

- Applicable Data Protection Laws control data protection matters
- GDPR applies to processing of EEA Data Subjects' data
- UK GDPR applies to processing of UK Data Subjects' data
- CCPA/CPRA applies to California residents' data
- Other Data Protection Laws apply as relevant

15.1.3 Standard Contractual Clauses
For Standard Contractual Clauses:
- Clause 17 (Governing Law): Ireland or EU Member State where Customer established
- Clause 18 (Jurisdiction): Courts of Ireland or relevant EU Member State
- UK Addendum: Governed by laws of England and Wales

15.2 Dispute Resolution
15.2.1 Informal Resolution
Before formal proceedings:
- Parties will attempt to resolve disputes amicably
- Senior representatives will meet and negotiate in good faith
- 30-day informal resolution period
- Escalation to executive leadership if needed

Contact for disputes:
- Freelancea: legal@freelancea.net
- Attention: General Counsel

15.2.2 Mediation
If informal resolution fails:
- Either party may propose mediation
- Mediator selected by mutual agreement or per JAMS/AAA rules
- Mediation location: Dublin, Ireland (EU) or San Francisco, California (US)
- Costs split equally between parties
- Mediation confidential and non-binding

15.2.3 Litigation
Venue and Jurisdiction:

For EU Customers:
- Courts of Ireland or Customer's EU Member State
- As specified in Standard Contractual Clauses

For UK Customers:
- Courts of England and Wales
- As specified in UK Addendum to SCCs

For US Customers:

- State and federal courts in San Francisco County, California
- Each party consents to personal jurisdiction

For Other Customers:
- Courts of Ireland or Customer's jurisdiction
- As mutually agreed or per applicable law

15.2.4 Arbitration
By mutual agreement:
- Disputes may be submitted to binding arbitration
- JAMS International Arbitration Rules or ICC Rules
- One arbitrator unless15.2.4 Arbitration (continued)
By mutual agreement:
- Disputes may be submitted to binding arbitration
- JAMS International Arbitration Rules or ICC Rules
- One arbitrator unless parties agree to three
- Arbitration location: Dublin, Ireland (EU) or San Francisco, California (US)
- Arbitration conducted in English
- Award final and binding, enforceable in any court
- Each party bears own costs unless arbitrator orders otherwise

15.3 Exceptions to Dispute Resolution
15.3.1 Equitable Relief
Either party may seek:
- Injunctive or equitable relief in court
- Without prior mediation or arbitration
- For breaches threatening irreparable harm
- For intellectual property infringement
- For confidentiality violations
- For data security emergencies

15.3.2 Regulatory Proceedings
Nothing prevents:
- Data Subject complaints to Supervisory Authorities
- Supervisory Authority investigations or enforcement
- Compliance with regulatory orders or requirements
- Cooperation with government investigations

15.3.3 Small Claims
Claims within small claims court jurisdiction:
- May be brought in small claims court
- Without mediation or arbitration
- Subject to small claims court rules and procedures

15.4 Data Subject Rights

15.4.1 Third-Party Beneficiary Rights

Data Subjects are third-party beneficiaries with right to:

- Enforce provisions of this DPA protecting their rights
- Bring claims directly against Freelancea under Standard Contractual Clauses
- Seek remedies under applicable Data Protection Laws
- Lodge complaints with Supervisory Authorities

15.4.2 Data Subject Litigation

Data Subjects may bring claims:

- In courts of their habitual residence (under GDPR)
- In courts where Controller or Processor is established
- Under applicable Data Protection Laws
- Without affecting Freelancea-Customer dispute resolution

15.5 Class Action Waiver

15.5.1 Individual Claims Only

TO THE EXTENT PERMITTED BY LAW:

- Each party may bring claims only in individual capacity
- Not as plaintiff or class member in class or representative action
- Arbitrator may not consolidate multiple parties' claims
- Arbitrator may not preside over representative or class proceeding

15.5.2 Exceptions

Class action waiver does not apply to:

- Data Subject rights under Data Protection Laws
- Regulatory or government enforcement actions
- Claims where class action waiver is prohibited by law
- Collective actions expressly permitted by applicable law

15.6 Limitation Periods

15.6.1 Statute of Limitations

Claims must be brought within:

- Limitation period specified by applicable Data Protection Laws
- For GDPR claims: As specified by EU Member State law (typically 3-6 years)
- For contractual claims: Per governing law (typically 4-6 years)
- For tort claims: Per governing law (typically 2-4 years)

15.6.2 Discovery Rule

Limitation period begins when:

- Claim accrues (facts known or reasonably discoverable)
- Not necessarily when damage occurs
- As determined by applicable law

15.7 Severability

If any provision held invalid or unenforceable:
- Remaining provisions remain in full effect
- Invalid provision modified to achieve intended effect
- Or severed if modification not possible
- DPA interpreted to give maximum effect to valid provisions

16. CONTACT INFORMATION

16.1 Freelancea Contact Information

16.1.1 General Inquiries

Data Protection Questions:
- Email: support@freelancea.net
- Response time: 5 business days

Legal and Compliance:
- Email: legal@freelancea.net
- Response time: 10 business days

16.1.2 Data Protection Officer

Freelancea Data Protection Officer:
- Email: office@freelancea.net
- Address: Freelancea, Inc.
  1910 Thomes Ave
Cheyenne, WY 82001
  United States

16.1.3 Security and Incident Response

Security Incidents:
- Email: office@freelancea.net
- Response time: Immediate for critical incidents

Data Breach Notifications:
- Email: office@freelancea.net
- Available: 24/7 for confirmed breaches

16.1.4 Data Subject Rights

Data Subject Requests:
- Email: office@freelancea.net
- Mail: Freelancea, Inc.

16.1.5 Sub-Processors and Audits
Sub-Processor Information:
- Email: office@freelancea.net
- Updates: Automatic notification if subscribed

Audit Requests:
- Email: office@freelancea.net
- Notice required: 60 days for on-site audits
- Documentation requests: 10 business day response

16.1.6 Enterprise Support
Enterprise Customer Support:
- Dedicated account manager (for enterprise customers)
- Email: enterprise@freelancea.net
- Phone: Available to enterprise customers
- Priority support and expedited response

16.2 Customer Responsibilities
16.2.1 Maintaining Contact Information
Customer must:
- Provide accurate contact information
- Designate primary contact for DPA matters
- Update contact information promptly when changed
- Ensure contacts authorized to receive confidential information
- Monitor designated email addresses regularly

16.2.2 Designated Contacts
Customer should designate:

Primary DPA Contact:
- Name and title
- Email address
- Phone number
- Authority to make data protection decisions

Security Contact:
- For incident notifications
- Available 24/7 or with escalation procedures
- Email and phone

Data Subject Rights Contact:
- For forwarding Data Subject requests
- Response time commitments

Legal/Compliance Contact:
- For legal and regulatory matters
- Authority to negotiate amendments

16.2.3 Updating Contact Information
Customer may update contacts:
- Through account settings at https://www.freelancea.net
- By email to support@freelancea.net
- Through dedicated account manager (enterprise customers)
- Takes effect within 5 business days of notification

16.3 Supervisory Authorities
16.3.1 Relevant Supervisory Authorities
EU/EEA Data Subjects:
- Lead Supervisory Authority: Data Protection Commission (Ireland)
  Website: https://www.dataprotection.ie
  Email: info@dataprotection.ie
  Address: 21 Fitzwilliam Square South, Dublin 2, D02 RD28, Ireland
  Phone: +353 (0)761 104 800

UK Data Subjects:
- Information Commissioner's Office (ICO)
  Website: https://ico.org.uk
  Email: casework@ico.org.uk
  Address: Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF, United Kingdom
  Phone: +44 (0)303 123 1113

California Residents:
- California Privacy Protection Agency
  Website: https://cppa.ca.gov
  Email: info@cppa.ca.gov
  Address: 2101 Arena Boulevard, Sacramento, CA 95834, United States

Other US States:
- State Attorney General offices with consumer protection authority
- Contact information varies by state

16.3.2 Right to Lodge Complaint
Data Subjects have the right to:
- Lodge complaint with relevant Supervisory Authority
- Particularly in their habitual residence, place of work, or place of alleged infringement
- Without prejudice to other administrative or judicial remedies
- Free of charge

16.4 Additional Resources

16.4.1 Freelancea Resources

Documentation and Policies:
- Privacy Policy: https://www.freelancea.net/privacy-policy.html
- Cookie Policy: https://www.freelancea.net/cookie-policy.html
- Terms of Service: https://www.freelancea.net/terms-and-conditions.html

Support and Help:
- support@freelancea.net
- Live Chat: Available through platform (business hours)

16.4.2 Industry Resources

Standards Organizations:
- ISO (International Organization for Standardization): https://www.iso.org
- NIST (National Institute of Standards and Technology): https://www.nist.gov
- Cloud Security Alliance: https://cloudsecurityalliance.org

Professional Associations:
- International Association of Privacy Professionals (IAPP): https://iapp.org
- European Data Protection Board: https://edpb.europa.eu

Regulatory Guidance:
- European Commission (GDPR): https://ec.europa.eu/info/law/law-topic/data-protection
- ICO Guidance: https://ico.org.uk/for-organisations/guide-to-data-protection/
- NIST Cybersecurity Framework: https://www.nist.gov/cyberframework

17. SIGNATURES AND ACCEPTANCE

17.1 Agreement Formation

17.1.1 Electronic Acceptance

This DPA is entered into when:
- Customer accepts Terms of Service (which incorporate this DPA)
- Customer clicks "I Agree" or similar button
- Customer begins using Services after DPA becomes available
- Customer executes enterprise agreement incorporating this DPA

17.1.2 No Physical Signature Required

Physical signatures are not required:
- Electronic acceptance is legally binding
- Equivalent to written signature under applicable law
- E-SIGN Act and similar laws apply
- Electronic records maintained as proof of acceptance

17.1.3 Enterprise Agreements

For enterprise customers requiring executed agreements:
- Custom signature pages may be provided
- Executed via DocuSign or similar platform
- Physical copies available upon request
- Execution process coordinated by enterprise sales team

17.2 Authority and Authorization
17.2.1 Customer Representations
By accepting this DPA, Customer represents and warrants:
- Customer has authority to enter into this Agreement
- Customer has obtained necessary approvals
- Signatory is authorized to bind Customer
- Customer will comply with all obligations under this DPA
- Information provided to Freelancea is accurate and complete

17.2.2 Freelancea Representations
Freelancea represents and warrants:
- Freelancea has authority to enter into this Agreement
- Freelancea will comply with obligations under this DPA
- Services will be provided substantially as described
- Freelancea has necessary technical and organizational capabilities

17.3 Entire Agreement
17.3.1 Complete Agreement
This DPA, together with:
- Terms of Service
- Privacy Policy
- Standard Contractual Clauses (where applicable)
- Any executed enterprise agreement

Constitutes the entire agreement regarding data processing and supersedes all prior or contemporaneous agreements, representations, or understandings.

17.3.2 Integration
This DPA integrates and supersedes:
- Prior data processing agreements
- Prior privacy commitments
- Oral representations regarding data protection
- Email commitments not incorporated into written agreement

Exception: Written enterprise agreements or amendments executed after this DPA.

17.3.3 No Reliance
Customer acknowledges:

- Has not relied on representations outside this DPA
- Has had opportunity to review and negotiate terms
- Has consulted legal counsel as deemed appropriate
- Accepts terms voluntarily and with full understanding

17.4 Modifications and Waivers

17.4.1 Written Modifications

Modifications to this DPA must be:
- In writing (electronic acceptable)
- Per amendment process in Section 14
- Or via executed amendment/addendum for enterprise customers
- Signed or accepted by both parties (for bilateral amendments)

17.4.2 No Oral Modifications

Oral modifications are not binding:
- Email alone may not constitute modification (unless from authorized representative)
- Phone conversations do not modify DPA
- Written confirmation required for enforceability

17.4.3 Waivers

No waiver of any provision:
- Is effective unless in writing
- Constitutes waiver of any other provision
- Constitutes continuing waiver
- Prevents enforcement of that provision in the future

17.5 Counterparts

This DPA may be executed in counterparts:
- Each counterpart constitutes an original
- All counterparts together constitute one agreement
- Electronic signatures are acceptable
- Faxed or scanned signatures are binding

17.6 Language

17.6.1 Controlling Language

The English language version of this DPA is the binding and controlling version:
- Translations provided for convenience only
- In case of conflict, English version controls

17.6.2 Available Languages

This DPA is available in:
- English (controlling version)
- Spanish
- French

- German
- Portuguese
- Italian
- Japanese
- Chinese (Simplified)
- Korean

17.7 Effectiveness

17.7.1 Effective Date

This DPA version is effective: January 15, 2025

Applies to:
- New customers from effective date forward
- Existing customers: 30 days after publication or continued use of Services
- Enterprise customers: As specified in enterprise agreement or 30 days after notice

17.7.2 Prior Versions

For customers who accepted prior versions:
- Prior version governs until this version becomes effective
- Transition period provided for material changes
- Previous versions archived and available
- No retroactive application unless required by law

17.8 Notices and Communication

17.8.1 Notice Requirements

Notices under this DPA must be:
- In writing (email acceptable for routine matters)
- Sent to designated contacts per Section 16
- In English (translations may accompany)
- Clearly marked "DPA Notice" or "Data Protection Notice"

17.8.2 Deemed Receipt

Notices deemed received:
- Email: 24 hours after sending (if no bounce-back)
- Physical mail: 5 business days after postmark (domestic), 10 days (international)
- Courier: Upon delivery confirmation
- Platform notification: When posted to account

17.8.3 Address Changes

Party changing contact information must:
- Notify other party within 10 business days
- Update information per Section 16.2.3
- Ensure no interruption in communications

ANNEXES

ANNEX A: DETAILS OF PROCESSING

A.1 Subject Matter and Nature of Processing
Subject Matter:
- Provision of freelance marketplace and collaboration platform
- Facilitation of connections between clients and freelancers
- Project management and communication tools
- Payment processing and financial transactions
- Platform administration and support

Nature of Processing:
- Collection, storage, and organization of Personal Data
- Automated matching and recommendation algorithms
- Communication facilitation (messaging, video calls)
- Payment processing and fund transfers
- Analytics and reporting
- Security monitoring and fraud prevention

A.2 Purpose of Processing
The Personal Data is processed for the following purposes:
- Creating and managing user accounts
- Facilitating job postings and applications
- Enabling communication between users
- Processing payments and financial transactions
- Providing customer support
- Ensuring platform security and preventing fraud
- Improving Services and developing new features
- Complying with legal and regulatory obligations
- Enforcing Terms of Service
- Sending notifications and updates
- Generating analytics and insights

A.3 Duration of Processing
Processing Duration:
- Active Accounts: Duration of account activity
- Closed Accounts: Up to 90 days for most data (longer for financial/legal records)
- Specific retention periods: As detailed in Section 11.2
- Backups: Up to 90 days beyond deletion from production systems
- Legal requirements: As required by applicable law (typically 7 years for financial records)

A.4 Categories of Data Subjects
Personal Data relates to the following categories of Data Subjects:

Freelancers:
- Registered freelancers offering services on the Platform
- Independent contractors and consultants
- Agencies representing multiple freelancers

Clients:
- Businesses and organizations hiring freelancers
- Individual clients posting projects
- Agency representatives
- Enterprise account administrators

End Users:
- Employees of Customer accessing the Platform
- Contractors engaged through Customer's account
- Third parties invited by Customer to collaborate

Website Visitors:
- Prospective users browsing the Platform
- Job seekers reviewing opportunities
- Researchers and analysts

Support Contacts:
- Customer support personnel
- Technical support contacts
- Billing and financial contacts

A.5 Categories of Personal Data
The following categories of Personal Data are processed:

Identity Information:
- Full name
- Username/handle
- Date of birth
- Government-issued ID information (for verification)
- Photographs and profile pictures
- Social media profiles and links

Contact Information:
- Email address
- Phone number

- Physical address
- Time zone
- Preferred contact methods

Professional Information:
- Work history and experience
- Education and certifications
- Skills and expertise
- Portfolio samples and work examples
- Professional references
- Rates and pricing information
- Availability and calendar information

Financial Information:
- Payment card information (tokenized)
- Bank account details
- Payment history and invoices
- Billing address
- Tax identification numbers (when required)
- Transaction records

Account and Usage Information:
- Account credentials (hashed passwords)
- Login history
- IP addresses and device identifiers
- Browser type and version
- Operating system
- Cookies and tracking technologies
- Feature usage and engagement metrics
- Search queries and filters
- Preferences and settings

Communication Data:
- Messages between users
- Email correspondence
- Support tickets and communications
- Video call metadata
- File attachments and shared documents
- Comments and reviews

Behavioral Data:
- Platform navigation patterns
- Click-through data
- Job application history

- Hiring decisions and outcomes
- Ratings and reviews (given and received)
- Project milestones and deliverables

Technical Data:
- Device information
- Network information
- Location data (approximate)
- Session data
- Error logs and diagnostics

Compliance and Verification Data:
- Identity verification documents
- Background check results (where permitted)
- Compliance questionnaire responses
- Regulatory filings

A.6 Special Categories of Personal Data
Processing of Special Categories of Personal Data is generally prohibited unless:
- Customer obtains prior written authorization from Freelancea
- Appropriate legal basis exists under applicable Data Protection Laws
- Enhanced security measures are implemented
- Explicit consent obtained from Data Subjects (where required)

Prohibited Special Categories (without authorization):
- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data for unique identification
- Health data
- Data concerning sex life or sexual orientation
- Criminal conviction data

Note: Some professional information (e.g., disability accommodations, diversity information) may be considered Special Category data in certain jurisdictions and requires appropriate handling.

A.7 Technical and Organizational Measures
See Section 6 (Security Measures) for comprehensive details. Summary includes:

Technical Measures:
- Encryption (TLS 1.2+ in transit, AES-256 at rest)
- Access controls (MFA, RBAC, least privilege)

- Network security (firewalls, IDS/IPS, segmentation)
- Application security (OWASP compliance, secure coding)
- Monitoring and logging (SIEM, audit trails)
- Backup and recovery systems

Organizational Measures:
- Security governance and policies
- Personnel training and background checks
- Incident response procedures
- Vendor management program
- Business continuity planning
- Regular audits and assessments
- ISO 27001 and SOC 2 Type II compliance

ANNEX B: STANDARD CONTRACTUAL CLAUSES

B.1 Module Two: Controller to Processor
The parties agree that the Standard Contractual Clauses set out in the Annex to the European Commission's Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 ("EU SCCs") are incorporated into and form part of this DPA.

Module Two (Controller to Processor) applies where:
- Customer is the data exporter (Controller)
- Freelancea is the data importer (Processor)
- Transfer is from EEA to third countries without adequacy decision

B.2 SCC Specifications

Clause 7 – Docking Clause
The optional docking clause does not apply unless otherwise agreed in writing.

Clause 9 – Use of Sub-Processors
The data importer (Freelancea) has the data exporter's (Customer's) general authorization for the engagement of Sub-Processors from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes concerning the addition or replacement of Sub-Processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the Sub-Processor(s).

Clause 11 – Redress
Data Subjects are third-party beneficiaries and may enforce this DPA and the SCCs against both the data exporter and data importer.

Clause 13 – Supervision
Option 1 applies: The supervisory authority of the data exporter is the Data Protection Commission of Ireland for EU customers, or the supervisory authority in the EU Member State where the data exporter is established.

Clause 17 – Governing Law
The Clauses shall be governed by the law of Ireland, or the law of the EU Member State in which the data exporter is established (if in the EU).

Clause 18 – Choice of Forum and Jurisdiction
The courts of Ireland shall have jurisdiction over disputes arising from the Clauses, or the courts in the EU Member State where the data exporter is established.

B.3 Annexes to SCCs

Annex I.A – List of Parties

Data Exporter:
- Name: Customer (as identified in Terms of Service or enterprise agreement)
- Address: As provided in Customer account information
- Contact: As provided in Section 16
- Role: Controller
- Activities: As described in Customer's business and use of Services

Data Importer:
- Name: Freelancea, Inc.
- Address: 123 Market Street, Suite 500, San Francisco, CA 94103, United States
- Contact: dpo@freelancea.net
- Role: Processor
- Activities: Provision of freelance marketplace platform and related services

Annex I.B – Description of Transfer

Categories of Data Subjects: As specified in Annex A.4
Categories of Personal Data: As specified in Annex A.5
Special Categories of Data: None (unless specifically authorized per Annex A.6)
Frequency: Continuous during term of Services
Nature of Processing: As specified in Annex A.1
Purpose: As specified in Annex A.2
Duration: As specified in Annex A.3

Annex I.C – Competent Supervisory Authority
- Data Protection Commission (Ireland) for EU customers
- Or the supervisory authority in the EU Member State where data exporter is established

Annex II – Technical and Organizational Measures
As described in Section 6 (Security Measures) of this DPA.

B.4 UK International Data Transfer Addendum
For transfers subject to UK GDPR, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (Version B1.0) issued by the Information Commissioner's Office is incorporated by reference with the following specifications:

Table 1: Parties
- As specified in Annex I.A above

Table 2: Selected SCCs, Modules and Selected Clauses
- Addendum EU SCCs: As specified in Section B.1 above
- Date of EU SCCs: 4 June 2021
- EU SCCs version: As applicable on effective date of this DPA

Table 3: Appendix Information
- As specified in Annexes I.A, I.B, I.C, II, and III above

Table 4: Ending this Addendum
- Ending situations as provided in UK Addendum

B.5 Swiss Data Transfer Agreement
For transfers subject to the Swiss Federal Act on Data Protection (FADP), the EU SCCs apply with the following modifications:

- References to "Regulation (EU) 2016/679" are to be understood as references to the Swiss FADP
- References to "EU," "Union," and "Member State" include Switzerland
- The supervisory authority is the Swiss Federal Data Protection and Information Commissioner (FDPIC)
- Data subjects are entitled to enforce rights in Switzerland under Swiss law

B.6 Alternative Transfer Mechanisms
If and when alternative transfer mechanisms become available that provide equivalent or greater protection (e.g., adequacy decisions, approved certification mechanisms, approved codes of conduct):
- Freelancea may rely on such mechanisms
- With notice to Customer
- SCCs remain in effect as fallback mechanism
- No degradation of protection provided to Data Subjects

ANNEX C: SUB-PROCESSOR LIST
Current as of January 15, 2025

C.1 Infrastructure and Hosting

Amazon Web Services (AWS)
- Entity: Amazon Web Services, Inc.
- Location: United States, European Union, United Kingdom, and other regions
- Processing Activity: Cloud infrastructure, data storage, compute services, database hosting
- Data Categories: All Customer Data
- Security: ISO 27001, SOC 2 Type II, PCI DSS
- Website: https://aws.amazon.com

Google Cloud Platform (GCP)
- Entity: Google LLC
- Location: United States, European Union
- Processing Activity: Secondary cloud infrastructure, backup services, disaster recovery
- Data Categories: Backup data, certain analytics data
- Security: ISO 27001, SOC 2 Type II
- Website: https://cloud.google.com

C.2 Payment Processing

Stripe, Inc.
- Entity: Stripe, Inc.
- Location: United States
- Processing Activity: Payment processing, credit card transactions, ACH transfers
- Data Categories: Payment information, transaction data, billing information
- Security: PCI DSS Level 1
- Website: https://stripe.com

PayPal Holdings, Inc.
- Entity: PayPal Holdings, Inc.
- Location: United States
- Processing Activity: PayPal payments, withdrawals, money transfers
- Data Categories: Payment information, transaction data, PayPal account information
- Security: PCI DSS Level 1
- Website: https://paypal.com

C.3 Communication Services

SendGrid (Twilio)
- Entity: Twilio Inc.
- Location: United States

- Processing Activity: Transactional email delivery, email API services
- Data Categories: Email addresses, message content, delivery metrics
- Security: SOC 2 Type II
- Website: https://sendgrid.com

Twilio
- Entity: Twilio Inc.
- Location: United States
- Processing Activity: SMS notifications, two-factor authentication, voice services
- Data Categories: Phone numbers, message content, authentication codes
- Security: SOC 2 Type II, ISO 27001
- Website: https://twilio.com

C.4 Analytics and Monitoring

Google Analytics
- Entity: Google LLC
- Location: United States
- Processing Activity: Website analytics, user behavior tracking
- Data Categories: Usage data, IP addresses (anonymized), device information
- Security: ISO 27001
- Website: https://analytics.google.com
- Note: IP anonymization enabled

Mixpanel
- Entity: Mixpanel, Inc.
- Location: United States
- Processing Activity: Product analytics, user engagement tracking
- Data Categories: Usage data, behavioral data, feature engagement
- Security: SOC 2 Type II, GDPR compliant
- Website: https://mixpanel.com

C.5 Customer Support

Zendesk
- Entity: Zendesk, Inc.
- Location: United States
- Processing Activity: Customer support ticketing, helpdesk management
- Data Categories: Support inquiries, contact information, communication history
- Security: SOC 2 Type II, ISO 27001
- Website: https://zendesk.com

Intercom
- Entity: Intercom, Inc.

- Location: United States
- Processing Activity: Live chat, customer messaging, in-app communications
- Data Categories: Chat messages, contact information, user profiles
- Security: SOC 2 Type II, ISO 27001
- Website: https://intercom.com

C.6 Security Services

Cloudflare
- Entity: Cloudflare, Inc.
- Location: Global (data centers worldwide)
- Processing Activity: Content delivery network (CDN), DDoS protection, web security
- Data Categories: IP addresses, HTTP request data, security logs
- Security: SOC 2 Type II, ISO 27001
- Website: https://cloudflare.com

Auth0 (Okta)
- Entity: Okta, Inc.
- Location: United States
- Processing Activity: Identity and access management, authentication services
- Data Categories: Authentication credentials, login history, user profiles
- Security: SOC 2 Type II, ISO 27001, ISO 27018
- Website: https://auth0.com

C.7 Data Processing and Analysis

Snowflake
- Entity: Snowflake Inc.
- Location: United States, European Union (depending on configuration)
- Processing Activity: Data warehousing, analytics processing
- Data Categories: Aggregated usage data, analytics data (pseudonymized where possible)
- Security: SOC 2 Type II, ISO 27001, PCI DSS
- Website: https://snowflake.com

C.8 Monitoring and Error Tracking

Sentry
- Entity: Functional Software, Inc. dba Sentry
- Location: United States
- Processing Activity: Error tracking, application performance monitoring
- Data Categories: Error logs, stack traces, technical diagnostic data
- Security: SOC 2 Type II
- Website: https://sentry.io

C.9 Video Communication

Zoom Video Communications
- Entity: Zoom Video Communications, Inc.
- Location: United States
- Processing Activity: Video conferencing, screen sharing
- Data Categories: Video/audio data, participant information, meeting metadata
- Security: SOC 2 Type II, ISO 27001, FedRAMP
- Website: https://zoom.us

C.10 Document Management

DocuSign
- Entity: DocuSign, Inc.
- Location: United States
- Processing Activity: Electronic signature, document management
- Data Categories: Contract documents, signature data, participant information
- Security: SOC 2 Type II, ISO 27001
- Website: https://docusign.com

DOCUMENT HISTORY

Version 2.0 (January 15, 2025) - Current Version
- Complete restructuring and expansion of DPA
- Enhanced security measures and detailed technical controls
- Expanded Sub-Processor provisions with notification procedures
- Comprehensive international data transfer provisions including Transfer Impact Assessments
- Detailed breach notification and incident response procedures
- Enhanced audit rights and compliance documentation
- Comprehensive data retention schedules
- Updated for compliance with GDPR, UK GDPR, CPRA, and emerging regulations
- Incorporated updated Standard Contractual Clauses (2021)
- Added UK and Swiss addenda for international transfers

Version 1.0 (March 1, 2023)
- Initial Data Processing Agreement
- Basic security measures
- Standard Sub-Processor authorization
- General data retention provisions
- Original Standard Contractual Clauses
- Basic breach notification procedures

ACKNOWLEDGMENT AND ACCEPTANCE

By using the Freelancea Services or accepting the Terms of Service, you acknowledge that you have read, understood, and agree to be bound by this Data Processing Agreement.

For questions about this DPA, contact:
Data Protection Officer
Freelancea, Inc.
Email: support@freelancea.net

Last Updated: January 15, 2025
Effective Date: January 15, 2025
Version: 2.0

END OF DATA PROCESSING AGREEMENT

_____ _____

Client Name Company Representative

Date: _____ Date: _____