Data Processing Agreement
(pursuant to Article 28 GDPR)

between

the recipient of the above offer
hereinafter referred to as the "Controller"

and

Flowtify GmbH
Holzmarkt 59-65
50676 Cologne, Germany

hereinafter referred to as the "Processor"

Preamble

The Controller intends to engage the Processor for the services specified in § 3 of this Data Processing Agreement. As part of the contract performance, personal data will be processed. In particular, Article 28 of the GDPR imposes specific requirements for such data processing. To comply with these requirements, the parties enter into the following agreement, which is not separately remunerated unless expressly agreed otherwise.

§ 1 Definitions

(1) Processor, as per Article 4(8) GDPR, is a natural or legal person, authority, agency, or other body that processes personal data on behalf of the Controller.
(2) Personal data, in accordance with Article 4(1) GDPR, refers to any information relating to an identified or identifiable natural person (hereinafter referred to as the "data subject"). An identifiable natural person is one who can be identified, directly or indirectly, particularly by reference to an identifier such as a name, an identification number, location data, an online identifier, or one or more specific factors that express the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
(3) Processing, in accordance with Article 4(2) GDPR, encompasses any operation or set of operations that is performed on personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment, or combination, restriction, erasure, or destruction.
(4) Supervisory authority, according to Article 4(21) GDPR, refers to an independent public authority established by a Member State pursuant to Article 51 GDPR.

§ 2 Designation of the Competent Data Protection Supervisory Authority

(1) The competent supervisory authority for the Controller is the State Commissioner for Data Protection in the federal state of the Controller.
(2) The competent supervisory authority for the Processor is the State Commissioner for Data Protection of North Rhine-Westphalia.
(3) The Controller and the Processor will cooperate with the supervisory authority in fulfilling their duties upon request.

§ 3 Subject of the Contract

(1) The Processor provides the services specified in the preceding Flowtify contract ("Master Contract") for the Controller. The Processor processes personal data exclusively on behalf and according to the instructions of the Controller. The scope and purpose of data processing by the Processor are outlined in the Master Contract. The Controller is responsible for assessing the legality of data processing.
(2) To specify the mutual data protection rights and obligations, the parties enter into this contract. The provisions of this contract take precedence over those of the Master Contract when in doubt.
(3) The provisions of this contract apply to all activities related to the Master Contract in which the Processor and its employees or individuals appointed by the Processor come into contact with personal data originating from the Controller or collected for the Controller.
(4) The duration of this contract is determined by the duration of the Master Contract, unless additional obligations or termination rights beyond this are specified in the following provisions.

§ 4 Right of Instruction

(1) The Processor may only collect, process, or use data within the scope of the Master Contract and in accordance with the Controller's instructions. This particularly applies to the transmission of personal data to a third country or international organization. If the Processor is obliged by the law of the European Union or the Member States to further process the data, it informs the Controller of these legal requirements before processing.
(2) The Controller's instructions are initially defined by this contract and can be changed, supplemented, or replaced by the Controller in writing or in text form (individual instruction) after that. The Controller is entitled to issue appropriate instructions at any time, including instructions for the correction, deletion, and blocking of data.
(3) All instructions issued are to be documented by both the Controller and the Processor. Instructions that go beyond the services agreed in the Master Contract are treated as requests for a change in services.
(4) If the Processor believes that an instruction from the Controller violates data protection regulations, it informs the Controller. The Processor is entitled to suspend the execution of the relevant instruction until it is confirmed or modified by the Controller. The Processor may refuse to execute an obviously unlawful instruction.

§ 5 Type of Processed Data, Data Subjects

(1) In the course of performing the Master Contract, the Processor accesses the personal data specified in Appendix 1.
(2) The data subjects affected by the data processing are also outlined in Appendix 1.

§ 6 Processor's Security Measures

(1) The Processor is obliged to comply with the legal data protection regulations and not disclose or grant access to information obtained from the Controller to third parties. Documents and data are to be secured against unauthorized access, taking into account the state of the art.
(2) In its area of responsibility, the Processor will organize the internal organization to meet the specific requirements of data protection. The Processor takes all necessary technical and organizational measures for the appropriate protection of the Controller's data according to Article 32 of the GDPR, especially the measures listed in Appendix 2. The Processor reserves the right to change the security measures taken, ensuring that the contractually agreed level of protection is not diminished.
(3) The data protection contact person is reachable at privacy@flowtify.de.
(4) Individuals employed in data processing by the Processor are prohibited from collecting, processing, or using personal data without authorization. The Processor ensures that all individuals entrusted with the processing and fulfillment of this contract (hereinafter referred to as "employees") commit to confidentiality or are subject to appropriate legal confidentiality obligations. The confidentiality obligations continue to apply even after the contract's termination.

§ 7 Information Obligations of the Processor

(1) In the event of disruptions, suspicion of data protection violations, breaches of contractual obligations by the Processor, suspicion of security-related incidents, or other irregularities in the processing of personal data by the Processor, by individuals employed by the Processor in the context of the contract, or by third parties, the Processor shall promptly inform the Controller in writing or in text form. The same applies to inspections of the Processor by the data protection supervisory authority.
(2) The Processor shall promptly take the necessary measures to secure the data and mitigate any adverse consequences for the data subjects. The Controller shall be informed of these actions and further instructions shall be sought.
(3) Furthermore, the Processor is obligated to provide the Controller with information at any time, to the extent that the data of the Controller is affected by a breach as described in paragraph 1.

§ 8 Controller's Inspection Rights

(1) The Controller may verify the technical and organizational measures of the Processor. To do so, the Controller may conduct the inspection personally, or through an expert third party, provided that the third party is not in a competitive relationship with the Processor, and after prior coordination during normal business hours. The Controller shall conduct inspections only to the extent necessary and without disproportionately disrupting the Processor's operations.
(2) Upon written request by the Controller, the Processor shall provide all information and evidence required for the execution of an inspection of the technical and organizational measures of the Processor within a reasonable timeframe.
(3) The Controller shall document the results of the inspection and inform the Processor. In case of errors or irregularities identified by the Controller, especially in the review of the results of the services, the Controller shall promptly inform the Processor. If the inspection reveals facts that require changes to the established procedure to prevent their recurrence, the Controller shall promptly inform the Processor of the necessary procedural changes.

§ 9 Use of Subcontractors

(1) The contractually agreed services or the sub-services described below are carried out with the involvement of the subcontractors listed in Appendix 3. In the context of its contractual obligations, the Processor is authorized to establish further subcontractor relationships with subcontractors ("subcontractor relationship"). The Processor shall inform the Controller of any changes related to the engagement or replacement of subcontractors. The Controller may object to such changes. The Processor selects subcontractors carefully based on their suitability, reliability, and processing location (primarily in the European Economic Area (EEA)). If the Processor establishes further subcontractor relationships, it is obliged to transfer its data protection obligations from this contract to the subcontractor. Exceptionally, data transfers to third countries outside the EEA are in compliance with the provisions of Article 44 et seq. GDPR.
(2) A subcontractor relationship, as defined in these provisions, does not exist when the Processor commissions third parties with services considered purely ancillary. These include, for example, postal, transport, and shipping services, cleaning services, telecommunications services without a specific connection to services provided by the Processor to the Controller, and security services. Maintenance and testing services are subject to approval for subcontractor relationships, to the extent that these are provided for IT systems used in connection with the services provided to the Controller.

§ 10 Inquiries and Rights of Data Subjects

(1) The Processor shall assist the Controller, to the extent possible, with suitable technical and organizational measures in fulfilling the Controller's obligations under Articles 12–22 and 32 to 36 GDPR.
(2) If a data subject asserts their rights, such as the right to information, correction, or deletion concerning their data directly to the Processor, the Processor shall not respond independently but shall promptly refer the data subject to the Controller and await the Controller's instructions.

§ 11 Liability pursuant to Article 82 GDPR

(1) In the internal relationship with the Processor, the Controller is generally responsible for compensating data subjects for damages they incur as a result of data processing or usage that is impermissible or incorrect under data protection laws.
(2) The parties shall each be exempt from liability if one party can prove that it is in no way responsible for the circumstances that resulted in damage to a data subject.

§ 12 Extraordinary Termination Right

The Controller may terminate the Master Contract in whole or in part without notice if the Processor fails to fulfill its obligations under this contract, intentionally or with gross negligence violates provisions of the GDPR, or cannot or will not comply with the Controller's instructions. In the case of simple - that is, neither intentional nor grossly negligent - violations, the Controller shall set a reasonable deadline for the Processor to rectify the violation.

§ 13 Termination of the Master Contract

(1) After the termination of the Master Contract or at any time upon the Controller's request, the Processor shall return all documents, data, and data carriers provided to it, or, upon the Controller's request, delete them, provided there is no obligation under Union law or the law of the Federal Republic of Germany to store personal data. This includes any data backups maintained by the Processor. The Processor must document the proper deletion of any remaining data.
(2) The Controller has the right to control the complete and contract-compliant return or deletion of data at the Processor in an appropriate manner.
(3) Beyond the end of the Master Contract, the Processor is obliged to treat confidentially any data that has become known to it in connection with the Master Contract. This agreement remains valid beyond the end of the Master Contract for as long as the Processor possesses personal data that was transmitted to it by the Controller or collected on behalf of the Controller.

§ 14 Final Provisions

(1) The parties agree that the right of retention by the Processor, as defined in § 273 of the German Civil Code (BGB), is excluded concerning the data to be processed and the associated data carriers.
(2) Amendments and supplements to this contract must be made in writing. This also applies to a waiver of this formal requirement. Individual contractual agreements take precedence over this. (3) Should any provision of this contract be or become invalid or unenforceable, this shall not affect the validity of the remaining provisions.
(4) This agreement is subject to German law. The exclusive place of jurisdiction is Düsseldorf.

Annex 1 to the Data Processing Agreement

Description of Data/Data Categories, Purpose of Data Processing, and Data Subjects

The subject matter and duration of the contract, as well as the scope and nature of data collection, processing, or utilization, are derived from the main contract. Specifically, the following data are an integral part of the data processing:

Type of data	Purpose of data processing	Affected
Employee user data • First name • Last name • E-mail address	• Access management (login, permissions, etc.)	• Employees of the client • External persons named by the client
Data that users may collect during use: • Employee / user data • signatures • Text entries • Photos • Photo descriptions • Number queries • Yes / No queries • Date / Time queries • Single / Multiple Choice queries • QR or barcode queries • If applicable, uploaded documents with personal content	Use of the flowtify application for paperless self-documentation, self-monitoring and other documentation purposes of one-time or recurring activities in order to structure, organize or optimize operational processes.	• Client • Employees of the client • External persons named by the client. • External persons whose data has been transferred to the contractor by the client, an employee of the client or an external person named by the client.
Master data of the client • Company name • Contact person • Company address • E-mail address • Phone number	Correspondence with the client,	• Contact person • Person in charge of the client

Annex 2 to the Data Processing Agreement

Technical and Organizational Measures of the Processor pursuant to Article 32 of the GDPR

No servers are operated in the office premises of Flowtify GmbH.

Confidentiality

Access Control

- The company building is completely enclosed.
- The company building has a manual locking system.
- The entrance door has a doorknob on the outside.
- Each employee is provided with a key to the company building.
- The allocation of keys is documented and regularly reviewed.
- Visitors are always accompanied by at least one employee of Flowtify GmbH.
- Service providers are carefully selected.

Access Control

- The allocation and management of user rights for individual systems is exclusively carried out by system administrators.
- All work devices that process personal data are personalized for the respective employee, password-protected, and use the current operating system.
- Employees are instructed to lock their workstations when leaving.
- Employees are instructed to keep their workstations clean and to keep documents with personal data inaccessible to third parties (clean desk policy).
- The use of a secure password follows certain rules, such as including at least one uppercase letter, one lowercase letter, a special character, and a number, and having a minimum length of 12 characters.
- In all systems, where available, the security measure of "2-factor authentication" is standardly activated for each user.

Access Control

- Defined user groups.
- Each user is assigned a unique login.
- Separation of system files from different applications.
- Separation of user files from different users.
- Use of a file shredder.
- Minimal number of administrators.

Separation Control

- Separation of development, testing, and production environments.
- Physical separation (systems/databases/data storage).
- Multitenancy capability of relevant applications.
- Control through an authorization concept.

Pseudonymization

- Pseudonymization is applied wherever possible.
- Separation of reference data.
- Personal data is anonymized or pseudonymized to the greatest extent possible when shared or after the legal retention period has expired.

Integrity

Transfer Control

- Secure data transport (SSL).
- Data carrier encryption.
- Automated email encryption whenever possible.

Entry Control

- Logging of data input, modification, and deletion.
- Traceability of input, modification, and deletion of data through individual user names.
- Clear responsibilities for deletions.

Availability and Resilience

Availability Control

- Regular updates of the software used.
- Backup and recovery concept.
- Regular tests for data recovery.

Procedures for Regular Review, Assessment, and Evaluation

Data Protection Measures

- Commitment of employees to data confidentiality.
- Documentation of an overview of processing activities.
- The effectiveness of technical protective measures is reviewed annually.
- Internal data protection officer: Parshin Mortazi, Flowtify GmbH, privacy@flowtify.de
- Regular sensitization of employees to data confidentiality.

Incident Response Management

- Reporting process for data breaches to data protection authorities is in place.
- Reporting process for data breaches to data subjects is in place.

Data Protection-Friendly Defaults

- No more personal data is collected than necessary for the respective purpose.

Order Control

- Prior review of security measures taken by the processor.
- Selection of the processor with due diligence, particularly regarding data protection and security.
- Conclusion of the necessary data processing agreement or EU standard contractual clauses.
- Obligation for the processor to appoint a data protection officer when the obligation to appoint one is in place.
- Arrangement for the use of further subcontractors.
- Regular review of the processor and its level of protection.

Attachment 3 to the GDPR

Commissioned Subcontractors:

Currently, the following subcontractors have been commissioned by the contractor:

Microsoft Ireland Operations, Ltd., One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521

- Hosting
- Location Hosting: Frankfurt am Main (Germany)
- https://www.microsoft.com/de-de/cloud/compliance
- https://www.microsoft.com/en-us/licensing/product-licensing/products

Salesforce.com Germany GmbH, Erika-Mann-Str. 63, 80636 Munich, Germany

- Customer Management & Customer Service
- Location Hosting: Frankfurt am Main (Germany)
- https://status.salesforce.com/search/flowtify
- https://compliance.salesforce.com/en
- https://www.salesforce.com/content/dam/web/en_us/www/documents/legal/Agreements/data-processing-addendum.pdf

The technical and organizational measures of the subcontractors are listed on the following pages.

Technical and Organizational Measures for Microsoft Ireland Operations, Ltd.

Organization of IT Security

Responsibility for Security

- Microsoft has appointed one or more security officers responsible for coordinating and monitoring security rules and procedures.

Functions and Responsibilities Regarding Security

- Microsoft employees who have access to customer data are required to maintain confidentiality.

Risk Management Program

- Microsoft conducted a risk assessment before processing customer data or initiating online services.
- Microsoft archives security records as part of retention obligations after they are no longer in effect.

Asset Management

Asset Inventory

- Microsoft maintains an inventory of all media on which customer data is stored. Access to such media is restricted to Microsoft employees who are authorized in writing.

Asset Handling

- Microsoft classifies customer data to facilitate identification and appropriate access restrictions to customer data.
- Microsoft establishes restrictions on printing customer data and has procedures for disposing of printed materials containing customer data.
- Microsoft employees must obtain permission from Microsoft before storing customer data on portable devices, remotely accessing customer data, or processing customer data outside Microsoft's facilities.

Personnel Security

Security Training

- Microsoft informs its employees about relevant security procedures and their respective roles. Microsoft uses only anonymous data in training.

Physical and Environmental Security

Physical Access to Facilities

- Microsoft restricts access to facilities where information systems processing customer data are located to identified authorized individuals.

Physical Access to Components

- Microsoft keeps records of incoming and outgoing media containing customer data, including the type of media, the authorized sender/recipient, date and time, the number of media, and the types of customer data contained.

Protection Against Interruptions

- Microsoft uses a variety of industry-standard systems to prevent data loss due to power outages or line disruptions.

Disposal of Components

- Microsoft uses industry-standard processes to erase customer data when no longer needed.

Communication and Operations Management

Operating Policy

- Microsoft maintains security records that describe security measures and the corresponding procedures and responsibilities of employees who have access to customer data.

Data Recovery Procedures

- Microsoft continuously creates multiple copies of customer data, from which customer data can be recovered, at least once a week (unless no customer data has been updated during that period).
- Microsoft stores copies of customer data and data recovery procedures at a location different from the primary computer devices processing customer data.
- Microsoft has specific procedures governing access to copies of customer data.
- Microsoft reviews data recovery procedures at least once every six months, except for Azure Government Services procedures, which are reviewed every twelve months.
- Microsoft logs data recovery actions, recording information about the responsible person, the description of the recovered data, and, if necessary, details about data manually entered during data recovery.

Malware

- Microsoft performs anti-malware controls to prevent malicious software from gaining unauthorized access to customer data, including malicious software from public networks.

Data Across Borders

- Microsoft encrypts customer data transmitted over public networks or enables the customer to encrypt such data.
- Microsoft restricts access to customer data on media leaving Microsoft's facilities.

Event Logging

- Microsoft logs access and use of information systems containing customer data by recording the access ID, time, granted or denied permission, and corresponding activity or allows the customer to log.

Access Control

Access Policy

- Microsoft maintains a record of the security permissions of individuals who have access to customer data.

Access Authorization

- Microsoft maintains and updates records of employees authorized to access Microsoft systems containing customer data.
- Microsoft deactivates login credentials that have not been used for a specified period, which must not exceed six months.
- Microsoft designates employees authorized to grant, modify, or revoke authorized access to data and resources.
- If multiple people have access to systems containing customer data, Microsoft ensures that these individuals have separate IDs/login credentials.

Least Privilege

- Technical support staff is only allowed access to customer data when necessary.
- Microsoft restricts access to customer data to those individuals who need such access to perform their job duties.

Integrity and Confidentiality

- Microsoft instructs employees to disable administrative sessions when they leave facilities under Microsoft's control or when computers are left unattended.
- Microsoft assigns unique and confidential IDs to employees with access to customer data.

Authentication

- Microsoft uses industry-standard procedures to identify and authenticate users attempting to access information systems.
- When authentication methods rely on passwords, Microsoft requires that passwords be regularly renewed.
- When authentication methods rely on passwords, Microsoft requires passwords to be a minimum of eight characters.
- Microsoft ensures that deactivated or expired identifiers are not assigned to anyone else.
- Microsoft monitors repeated attempts to gain access to information systems with invalid passwords or allows

the customer to do so.

- Microsoft maintains industry-standard procedures for deactivating passwords that have been manipulated or accidentally disclosed.
- Microsoft uses industry-standard procedures to protect passwords, including procedures to maintain the confidentiality and integrity of passwords during allocation, distribution, and storage.

Network Design

- Microsoft conducts controls to prevent individuals from receiving access rights that have not been assigned to them in order to access customer data that they should not access.

Handling of Information Security Incidents

Incident Response Process

- Microsoft maintains records of security breaches, including a description of the breach, the duration, the consequences of the breach, the name of the person who reported the incident, the person to whom the incident was reported, and the procedure for data recovery.
- For each security breach that qualifies as a security incident (as described in the "Security Incident Reporting" section above), Microsoft notifies (as described in the "Security Incident Reporting" section above) the customer immediately and in any case within 72 hours.
- Microsoft investigates disclosures of customer data, including questions about what data was disclosed, to whom and when, or allows the customer to do so.

Service Monitoring

- Microsoft's security personnel review logs at least every six months to recommend any necessary remedies.

Business Continuity Management

- Microsoft maintains emergency and alternative plans for the facilities where Microsoft information systems processing customer data are located.
- Microsoft's redundant storage and data recovery procedures are designed to attempt to reconstruct customer data in its original or most recently replicated state before the time of loss or destruction.

Technical and Organizational Measures by Salesforce.com Germany GmbH

Architecture and Data Separation

The Covered Services are operated in a multi-tenant architecture designed to separate and restrict access to customer data based on business requirements. The architecture provides effective logical data separation for different customers using customer-specific "Organization IDs" and allows the use of role-based access rights for users. Additional data separation is ensured by providing separate environments for different functions, especially for testing and production.

Processing Control

Salesforce has implemented procedures to ensure that customer data is processed only in accordance with the entire chain of processing activities by Salesforce and its subprocessors only in accordance with customer instructions. In particular, Salesforce and its affiliated companies have entered into written agreements with their subprocessors that include obligations for the protection of privacy, data protection, and data security and provide a level of protection that is appropriate for their processing activities. Compliance with these obligations, as well as the technical and organizational data security measures by Salesforce and its subprocessors, are subject to regular audits.

Third-Party Functionalities

Certain functionalities of the Covered Services use features provided by third parties. The Account Intelligence feature in Sales Cloud - Account News, Lightning News, Account Logos, and Account Autofill work by sending standard fields from the customer's Account object to Salesforce's Einstein platform, currently hosted by AWS, where this data is matched with content such as news articles provided through Sales Cloud. Customers can disable the Account Intelligence features.

If customers use messaging to send or receive mobile messages, such as SMS messages, the content of these messages and related information about these messages are received by

(a) aggregators - companies that act as intermediaries in transmitting mobile messages or providing mobile phone numbers, and

(b) carriers - companies that provide wireless message services to subscribers over wireless or wireline telecommunications networks. Such aggregators and carriers have access to message content and related information, store it, and transmit it and related information to provide these features. For over-the-top messaging services, such as Facebook Messenger and WhatsApp, the content of messages sent or received through such a service and related information about such messages are received by entities that enable such over-the-top messaging services.

Audits and Certifications

The following security and data protection audits and certifications apply to one or more of the Covered Services. More information can be found here.

In addition, the Covered Services undergo security assessments by internal personnel and third parties at least once a year, including assessments of infrastructure and application security vulnerabilities.

Salesforce uses infrastructure provided by Amazon Web Services, Inc. ("AWS") to host or process customer data transmitted to certain Covered Services and features. Information on security and data protection audits and certifications received by AWS, including ISO 27001 certification and SOC reports, is available on the AWS Security website and the AWS Compliance website.

Salesforce uses the infrastructure provided by Heroku to host or process customer data transmitted to certain Covered Services and features. Information about security and data protection audits and certifications received by Heroku, including ISO 27001 certification and SOC reports, is available in the Heroku security, privacy, and architecture documentation.

Security Controls

The Covered Services include a variety of configurable security controls that allow customers to tailor the security of the Covered Services for their own use. More information about these controls can be found in the Salesforce Security Guide. Information about multi-factor authentication and single sign-on for access to the Covered Services can be found in the respective notices and license information (NLI).

Certain Covered Services and Features use AWS to host or process customer data; more information on the security provided by AWS is available on the AWS Security website, including an overview of AWS security processes.

Security Policies and Procedures

The Covered Services are operated in accordance with the following policies and procedures to enhance security:

- Customer passwords are stored with a one-way salted hash.
- User access logs are maintained, which include the date, time, user ID, executed URL or entity ID, operation performed (created, updated, deleted), and source IP address. Note that the source IP address may not be available if NAT (Network Address Translation) or PAT (Port Address Translation) is used by the customer or their ISP.
- In case of suspicion of unauthorized access, Salesforce may provide customers with log entries for use in forensic analysis, if available. This service is provided to customers on a time and material basis.
- Logs of physical access to the data center, system infrastructure, and applications are retained for a minimum of 90 days. Logs are stored in a secure area to prevent tampering.
- Passwords are not logged.
- Certain administrative changes to the Covered Services (e.g., password changes and the addition of custom fields) are tracked in an area known as "Setup Audit Trail" and are viewable by a customer's system administrator. Customers can download and locally store this data.
- Salesforce personnel do not set a defined password for a user. Passwords are reset to a random value (which must be changed upon first use) and are automatically emailed to the requesting user.

Intrusion Detection

Salesforce or an authorized third party monitors the Covered Services for unauthorized intrusion using network-based and/or host-based intrusion detection mechanisms. Salesforce may analyze data collected by users' web browsers for security purposes, including detecting compromised browsers to prevent fraudulent authentications and ensure the proper functioning of the Covered Services.

Security Logs

All systems used in the provision of the Covered Services, including firewalls, routers, network switches, and operating systems, log information to their respective system logging device or a central syslog server (for network systems) to allow security reviews and analysis.

Incident Management

Salesforce maintains policies and procedures for security incident management. Salesforce notifies affected customers promptly of any unauthorized disclosure of their respective customer data by Salesforce or its agents to the extent permitted by law.

Salesforce publishes system status information on the Salesforce Trust website. Salesforce typically notifies customers of significant system incidents by email and, for incidents lasting more than an hour, may invite affected customers to a conference call about the incident and Salesforce's response.

User Authentication

Access to Covered Services, except for Experience Cloud (formerly Community Cloud) guest users, requires authentication through one of the supported mechanisms as described in the Salesforce Security Guide, including user ID/password, SAML-based federation, OpenID Connect, OAuth, social login, or delegated authentication, as determined and controlled by the customer. Upon successful authentication, a random session ID is generated and stored in the user's browser to maintain and track session status.

Physical Security

The production data centers used for the provision of the Covered Services have access control systems that allow access to secure areas only for authorized personnel. These facilities are designed to withstand adverse weather conditions and other reasonably foreseeable natural conditions, use redundant electrical and telecommunications systems, employ environmental systems to monitor temperature, humidity, and other ambient conditions, and include strategically placed heat, smoke, and fire detection and suppression systems. The facilities are secured 24/7 by security personnel, indoor and outdoor surveillance cameras, two-factor access control, and escorted access. In case of a power outage, uninterruptible power supplies and continuous power solutions are used to ensure power supply while systems are transferred to on-site backup generators.

Failover and Backup

All network components, network accelerators, load balancers, web servers, and application servers are configured in a redundant configuration. All customer data transmitted to the Covered Services is stored on a primary database server with multiple active clusters for high availability. Customer data is stored on highly redundant carrier-class disk storage and multiple data paths to ensure reliability and performance. All customer data transmitted to the Covered Services, up to the last confirmed transaction, is automatically and nearly real-time replicated to the secondary site and secured in localized data stores. Backups are integrity-checked and stored in the same data centers as their instance.

Disaster Recovery

The production data centers are designed to minimize the risk of single points of failure and provide a resilient environment to support service continuity and performance. The Covered Services use secondary facilities that are geographically distinct from the primary data centers, along with the required hardware, software, and internet connectivity in case Salesforce's production facilities in the primary data centers are no longer available. Salesforce has disaster recovery plans and tests them at least once a year.

The objectives of the disaster recovery plans for the Covered Services are currently as follows: (a) recovery of the Covered Service (recovery time objective) within 12 hours after Salesforce declares a disaster, and (b) a maximum loss of customer data (recovery point objective) of 4 hours. These objectives do not include a disaster or multiple disasters that compromise both data centers simultaneously and exclude development and test bed environments, such as the Sandbox service.

Viruses

The Covered Services do not scan for viruses that may be contained in attachments or other customer data uploaded to the Covered Services. However, uploaded attachments are not executed within the Covered Services and therefore cannot harm or jeopardize the Covered Services by containing a virus.

Data Encryption

The Covered Services use industry-standard encryption products to protect customer data and communication during transmissions between the customer's network and the Covered Services, including Transport Layer Encryption (TLS) using at least 2048-bit RSA server certificates and symmetric 128-bit encryption keys. Furthermore, all data, including customer data, is transmitted over encrypted connections using AES-256 encryption between data centers for replication purposes.

Return of Customer Data

Within 30 days of contract termination, customers can request the return of their respective customer data they have transmitted to the Covered Services (provided that this data has not been deleted by the customer or if the customer has not removed the managed package in which the customer data was stored). Salesforce provides such customer data in downloadable files in comma-separated value (.csv) format and attachments in their native format. The aforementioned return of customer data for managed packages may not be available if the packages were removed prior to contract termination.

Deletion of Customer Data

Unless otherwise stated below, customer data transmitted to the Covered Services is retained in an inactive state within the Covered Services for 120 days after termination of all subscriptions associated with an environment; thereafter, it is securely overwritten or deleted from production within 90 days and from backups within 180 days. Physical media on which customer data is stored during the term of the contract are not removed from the data centers used by Salesforce to host customer data unless the media have reached the end of their useful life or are deprovisioned; in such cases, the media are sanitized before removal. This process is subject to applicable legal requirements.

Without limiting the ability of customers to request the return of their customer data transmitted to the Covered Services, Salesforce reserves the right to reduce the number of days it retains this data after contract termination. Salesforce will update this Salesforce documentation on security, privacy, and architecture in the event of such a change.

Day 0, subscription is terminated	Day 0 - 30	Day 30 - 120	Day 121 - 211	Day 121 - 301
	Data available for return to the customer	Data inactive and no longer available	Data deleted or overwritten from production	Data from backups deleted or overwritten

Sensitive Data

Important: Customers must use either "Platform Encryption" for supported field types and file attachments or the "Classic Encryption" feature for custom fields and manage the lifecycle of their encryption keys when they transmit data from cardholders, authentication data, credit or debit card numbers, or any security codes or passwords to the Covered Services. Customers must not otherwise transmit such data to the Covered Services. For other categories of sensitive data, customers should also consider the use of "Platform Encryption" or "Classic Encryption."

For Intelligent Form Reader, if a customer uses a part of this Covered Service in connection with a decision process with legal or similarly significant consequences, the customer must ensure that the final decision is made by a human.

Clarification: The above limitations do not apply to financial data provided to Salesforce for the purpose of verifying the financial qualifications of its customers and collecting payments; the processing of such data is subject to Salesforce's website privacy policies.

Analytics

Salesforce may track and analyze the use of the Covered Services for security purposes and to assist Salesforce in improving both the Covered Services and the user experience when using the Covered Services. For example, this information may be used to understand and analyze trends or track which of our features are most frequently used to improve product functionality.

Salesforce may share anonymous usage data with Salesforce service providers to support tracking, analysis, and improvement. Furthermore, Salesforce may share such anonymous usage data on an aggregated basis as part of normal business operations; for example, we may make information publicly available to demonstrate trends in the general use of our services.

Interaction with Other Services

The Covered Services can interact or be integrated with other services provided by Salesforce or third parties. When third-party systems connect to the Covered Services, these external systems provide metadata to the Covered Services to maintain the intended integration functionality, such as an external system providing a third-party data record ID, file name, folder name, or similar label used to identify a record being sent to the Covered Services. Salesforce may capture and store such metadata to ensure product functionality and to assist in troubleshooting, support, and security purposes. Salesforce provides reasonable protection for such metadata and treats it in accordance with our privacy policy. Documentation on security, privacy, and architecture for services provided by Salesforce can be found in the Trust and Compliance documentation.