Pardot Security, Privacy and Architecture

Published: September 11, 2020

Salesforce's Corporate Trust Commitment

Salesforce is committed to achieving and maintaining the trust of our customers. Integral to this mission is providing a robust security and privacy program that carefully considers data protection matters across our suite of services, including protection of Customer Data as defined in Salesforce's Master Subscription Agreement.

Services Covered

This documentation describes the architecture of, privacy-related certifications received for, and the administrative, technical, and physical controls applicable to, the services branded as Pardot (the "Pardot Services"). Customers may choose to use related products and features branded as Pardot Einstein; these features run across two infrastructures, the infrastructure described by this Documentation, and the infrastructure described by the Einstein Platform Documentation, as further described in the Einstein Platform Documentation.

Architecture and Data Segregation

The Pardot Services are operated in a multitenant architecture that is designed to segregate and restrict Customer Data access based on business needs. The architecture provides an effective logical data separation for different customers via a customer-specific unique identifier and allows the use of customer and user role based access privileges. Additional data segregation is ensured by providing separate environments for different functions, especially for testing and production. The specific infrastructure used to host Customer Data is described in the "Infrastructure and Sub-processors" documentation available here.

Control of Processing

Salesforce has implemented procedures designed to ensure that Customer Data is processed only as instructed by the customer, throughout the entire chain of processing activities by Salesforce and its sub-processors. In particular, Salesforce and its affiliates have entered into written agreements with their sub-processors containing privacy, data protection and data security obligations that provide a level of protection appropriate to their processing activities. Compliance with such obligations as well as the technical and organizational data security measures implemented by Salesforce and its sub-processors are subject to regular audits. The "Infrastructure and Sub-processors" documentation describes the sub-processors and certain other entities material to Salesforce's provision of the Pardot Services.

Third-Party Functionality

Certain features of the Pardot Services use functionality provided by third parties. Certain advanced email features in Pardot, such as advanced analytics reporting on email viewing and the ability to perform email rendering tests on different devices and email clients, are powered by a third-party partner. Analytics, email templates and other data associated with these features may be accessed or stored by the third-party partner.

Audits and Certifications

The following privacy-related certifications are applicable to the Pardot Services:

- **Binding Corporate Rules (BCR) for Processors:** Customer Data submitted to the Pardot Services is within the scope of the Salesforce BCR for Processors. The most current version of the Salesforce

BCR for Processors is available on Salesforce's website, currently located at https://www.salesforce.com/company/privacy/.

- **EU-U.S. and Swiss-U.S. Privacy Shield certification**: Customer Data submitted to the Pardot Services is within the scope of a Salesforce's annual certification to the EU-U.S. Privacy Shield Framework and Swiss-U.S. Privacy Shield Framework as administered by the U.S. Department of Commerce. The current certification is available at https://www.privacyshield.gov/list by searching under "Salesforce."
- **TRUSTe certification**: Salesforce's Website Privacy Statement and privacy practices related to the Pardot Services are assessed by TRUSTe annually, for compliance with TRUSTe's Certification and Verification Assessment Criteria. For more information on the status of Salesforce's certification/verification status, click here.
- **APEC Privacy Recognition for Processors (PRP)**: Customer Data submitted to the Pardot Services is within the scope of Salesforce's PRP certification under the APEC Privacy Framework. The current certification is published in the PRP Compliance Directory here.
- **System and Organization Controls (SOC) report**: Salesforce's information security control environment applicable to Pardot undergoes an independent evaluation in the form of a Service Organization Control (SOC) 2 report. Salesforce's most recent SOC 2 report for Pardot is available upon request from your organization's Salesforce account executive.
- **ISO 27001/27017/27018 certification**: Salesforce operates an information security management system (ISMS) for the PardotServices in accordance with the ISO 27001 international standard. Pardot is also aligned to ISO 27017 and ISO 27018. Salesforce has achieved ISO 27001/27017/27018 certification for its ISMS from an independent third party. The scope of Salesforce's ISO 27001/27017/27018 certification applicable to the Pardot Services is available here.

Additionally, the Pardot Services undergo security assessments by internal personnel and third parties, which include infrastructure vulnerability assessments and application security assessments, on at least an annual basis.

Security Controls

The Pardot Services include a variety of configurable security controls that allow customers to tailor the security of the Pardot Services for their own use. These controls include:

- **Login IP Allowlisting:** Enables customers to define the range of IP addresses from which their users will access the application, preventing unauthorized access from outside a customer's organization.
- **Role-based Access Controls (RBAC)**: Enables customers to configure permissions and privileges for individual users and groups of users based on their roles within the organization and their use of the Pardot Services, e.g., Email Export Allowlist - Enables customers to define which users are able to receive exported material via email from the Pardot Services.
- **Customer Configurable Security**: Customers have the option to enable CAPTCHAs after multiple failed logins by users, and to define additional security settings such as account lockout and session timeouts.
- **Single Sign-On:** Customers that also use the Salesforce Services (as defined in the Trust and Compliance Documentation) and that have enabled the Salesforce Connector may take advantage of single-sign on features offered by Pardot and Salesforce. This allows login to the Pardot Services via a Salesforce Services login, and takes advantage of the additional identity federation options provided by Salesforce.
- **Email Login Verification:** Customers are required to use Email Login Verification in the event that

Two-Factor Authentication, Single Sign-On, or IP Location Allowlisting security features are not enabled. Email Login Verification is a process by which a login from a new device or IP address requires users to receive an email with an authorization link that must be clicked to allow login and set a cookie on the device browser, facilitating subsequent logins to succeed with username and password authentication only.

- **Two-Factor Authentication:** Customers may opt to enable two-factor authentication, a process by which Pardot users are prompted to provide a verification code from a two-factor authentication app for every user login.

Security Policies and Procedures

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

- User passwords are stored using a salted hash format and are not transmitted unhashed.
- User access log entries may be maintained, containing date, time and source IP address. Note that source IP address might not be available if NAT (Network Address Translation) or PAT (Port Address Translation) is used by a Customer or its ISP.
- If there is suspicion of inappropriate access to the Pardot Services, Salesforce may provide customers log entry records to assist in forensic analysis. This service will be provided to customers on a time and materials basis.
- Audit and security logs will be kept for one year.
- Logs will be kept in a secure area to prevent tampering.
- Passwords are not logged.
- Salesforce personnel will not set a defined password for a user. Users are provided unique links via email. Upon clicking such links, a user must create a password in accordance with password length and complexity requirements.

Intrusion Detection

Salesforce, or an authorized independent third party, will monitor the Pardot Services for unauthorized intrusions using network-based intrusion detection mechanisms. Salesforce may analyze data collected by users' web browsers (e.g., device type, screen resolution, time zone, operating system version, browser type and version, system fonts, installed browser plug-ins, enabled MIME types, etc.) for security purposes, including to detect compromised browsers, to prevent fraudulent authentications, and to ensure that the Pardot Services function properly.

Security Logs

All Salesforce systems used in the provision of the Pardot Services, including firewalls, routers, network switches and operating systems, log information to their respective system log facility or a centralized log server (for network systems) in order to enable security reviews and analysis.

Incident Management

Salesforce maintains security incident management policies and procedures for the Pardot Services. Salesforce notifies impacted customers without undue delay of any unauthorized disclosure of their respective Customer Data by Salesforce or its agents of which Salesforce becomes aware to the extent permitted by law.

User Authentication

Access to the Pardot Services requires identity verification, which are encrypted via TLS while in transmission. Following a successful authentication, a random session ID is generated and stored in the user’s browser to preserve and track session state.

Physical Security

Production data centers used to provide the Pardot Services have access control systems. These systems permit only authorized personnel to have access to secure areas. These facilities are designed to withstand adverse weather and other reasonably predictable natural conditions, are secured by around-the-clock guards, two-factor access screening, and escort-controlled access, and are also supported by on-site back-up generators in the event of a power failure.

Reliability and Backup

All networking components, SSL accelerators, load balancers, Web servers and application servers are configured in a redundant configuration. All Customer Data submitted to the Pardot Services is stored on a primary database server with multiple secondary servers for redundancy. All Customer Data submitted to the Pardot Services is stored on enterprise-class disk storage using RAID disks and multiple data paths to ensure reliability and performance. All Customer Data submitted to the Pardot Services is automatically replicated on a near real-time basis at the database layer and is backed up in an encrypted form on a regular basis and stored in an off-site backup location for 90 days, after which it is securely overwritten or deleted from the Pardot Services. Any backups are verified for integrity.

Disaster Recovery

Salesforce has disaster recovery plans in place and evaluates them at least once per year. The Pardot Services utilize disaster recovery facilities that are geographically remote from their primary data centers, along with required hardware, software, and Internet connectivity, in the event Salesforce production facilities at the primary data centers were to be rendered unavailable. The Pardot Services’ disaster recovery plans currently have the following target recovery objectives: (a) restoration of the Pardot Service within three business days after Salesforce’s declaration of a disaster; and (b) maximum Customer Data loss of one business day; excluding, however, a disaster or multiple disasters causing the compromise of both data centers at the same time, and excluding development and test bed environments.

Malicious Software

The Pardot Services do not scan for malicious software that could be included in attachments or other Customer Data uploaded into the Pardot Services by a customer. Uploaded attachments, however, are not executed in the Pardot Services and therefore will not damage or compromise the Pardot Services by virtue of containing malicious software.

Data Encryption

The Pardot Services use industry-accepted encryption products to protect Customer Data and communications during transmissions between a customer's network and the Pardot Services, using TLS 1.2+ leveraging at least 2048-bit RSA keys and cipher suites requiring at least 128-bit symmetric encryption keys. The Pardot Services disallow deprecated cipher suites and TLS versions below TLS 1.2.

Return of Customer Data

Within 30 days post contract termination, customers may request return of their respective Customer Data submitted to the Pardot Services. Salesforce shall provide such Customer Data via a downloadable file in comma separated value (.csv) format and attachments in their native format.

Deletion of Customer Data

After termination of the Pardot Services, Customer Data submitted to the Pardot Services is retained in inactive status within the Pardot Services for 90 days. After the 90 day period, Customer Data is securely overwritten or deleted. In accordance with the Reliability and Backup section above, Customer Data submitted to the Pardot Services (including Customer Data retained in inactive status) will be encrypted and stored on an off-site backup location for 90 days, after which it is securely overwritten or deleted from the Pardot Services. This process is subject to applicable legal requirements.

Without limiting the ability for customers to request return of their Customer Data submitted to the Pardot Services, Salesforce reserves the right to reduce the number of days it retains such data after contract termination. Salesforce will update this Pardot Security, Privacy, and Architecture Documentation in the event of such a change.

Sensitive Data

Important: The following types of sensitive personal data may not be submitted to the Pardot Services: birthdates, government- issued identification numbers; and financial information (such as credit or debit card numbers, any related security codes or passwords, and bank account numbers).

Additionally, for the Pardot Services, the following types of sensitive personal data may not be submitted: personal health information, where Customer is a health care provider, health care clearinghouse, health plan, or an entity performing functions on behalf of such entities, except in limited circumstances where, subject to restrictions, Salesforce has expressly permitted such submission contractually.

If Customer does submit personal health information or other sensitive or regulated data to the Pardot Services, then Customer is responsible for ensuring that its use of the Pardot Services to process that information complies with all applicable laws and regulations.

For clarity, the foregoing restrictions do not apply to financial information provided to Salesforce for the purposes of checking the financial qualifications of, and collecting payments from, its customers, the processing of which is governed by the Salesforce Website Privacy Statement.

Analytics

Salesforce may track and analyze the usage of the Pardot Services for the purposes of security and helping Salesforce improve both the Pardot Services and the user experience in using the Pardot Services. For example, we may use this information to understand and analyze trends or track which of our features are used most often to improve product functionality.

Salesforce may share anonymous usage data with Salesforce's service providers for the purpose of helping Salesforce in such tracking, analysis and improvements. Additionally, Salesforce may share such anonymous usage data on an aggregate basis in the normal course of operating our business; for example, we may share information publicly to show trends about the general use of our services.

Interoperation with Other Services

The Pardot Services may interoperate or integrate with other services provided by Salesforce or third parties. Security, Privacy and Architecture documentation for services provided by Salesforce is available in the Trust and Compliance Documentation. Salesforce also provides a variety of platforms and features that allow Salesforce users to learn about Salesforce products, participate in communities, connect third-party applications, and participate in pilots, testing and assessments, which are outside the scope of this documentation. Salesforce may communicate with users that participate in such platforms and features in a manner consistent with our Privacy Statement. Additionally, Salesforce may contact users to provide transactional information about the Pardot Services; for instance, through the Adoption Manager program or through system-generated messages, such as Chatter notifications. Salesforce offers customers and users the ability to deactivate or opt out of receiving such messages.