ta Privacy and Security Are		ODP	Content / Commerce Clouds, Personalization	Experimentation / Full Stack
Physical Access Controls	The prevention, where Processor reasonably can, of unauthorised persons from gaining access to Software Services Processing Personal Data (physical access control).	**Data processing:** Optimizely hosts its Software Services within US or EU (pending) based data centre providers, which is the choice of Data Exporter. Additionally, Optimizely maintains contractual relationships with vendors in order to provide the Software Services. Optimizely relies on contractual agreements, privacy policies, and vendor compliance programs in order to assure the protection of data processed or stored by these vendors. Further Optimizely may require for support purposes only, to allow processing to occur with Optimizely Affiliates, some of whom are located outside of the EU/EEA, specifically the US and the Philippines. **Physical and environmental security:** By formal/technical access procedures, the access to the involved data processing centres is regulated. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two- factor authentication a minimum of two times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.	**Data processing:** Optimizely hosts its Software Services within EU, US, UK, Norway, Canada, Singapore/Hong Kong or Australia based data centre providers, which is the choice of Data Exporter. Additionally, Optimizely maintains contractual relationships with vendors in order to provide the Software Services. Optimizely relies on contractual agreements, privacy policies, and vendor compliance programs in order to assure the protection of data processed or stored by these vendors. Further Optimizely may require for support purposes only, to allow processing to occur with Optimizely Affiliates, some of whom are located outside of the EU/EEA, specifically the UK (pending), US, Vietnam and Australia. **Physical and environmental security:** Optimizely hosts its product infrastructure with multi-tenant, data centre providers. The data centre providers' physical and environmental security controls are audited for ISO 27001 compliance, among other certifications.	**Data processing:** Optimizely hosts its Software Services within US data centre providers. Additionally, Optimizely maintains contractual relationships with vendors in order to provide the Software Services. Optimizely relies on contractual agreements, privacy policies, and vendor compliance programs in order to assure the protection of data processed or stored by these vendors. Further Optimizely may require for support purposes only, to allow processing to occur with Optimizely Affiliates, some of whom are located outside of the EU/EEA, specifically the US. **Physical and environmental Security** Optimizely uses industry-leading cloud platforms (currently Google Compute Cloud and Amazon Web Services) to host its production systems for the Optimizely Service. Access to these data centers is limited to authorized personnel only, as verified by biometric identity verification measures. Physical security measures for these data centers include: on-premises security guards, closed circuit video monitoring, and additional intrusion protection measures. We rely on their third party attestations of their physical security. Within our headquarters, we employ a number of industry-standard physical security controls.
Logical Access Controls	The prevention, where Processor reasonably can, of Software Services Processing Personal Data from being used without authorisation (logical access control).	**Product access:** Optimizely takes the following measures to ensure secure access: - Secured access connections and technologies for the authentication control are implemented to regulate the access to the Data Processor's systems and internal support-tools. - Techniques for encryption are used to secure user authentications. The Data Processor follows a formal process to permit the access to the Data Processor's resources or to deny such access. Unique login names, strong passwords and periodic examinations of the access lists exist to guarantee the appropriate use of user accounts. All groups which have access to the Data Processor's services are controlled by a regular examination. All named measures are described in a formalised concept of authorisation.	**Limitations of Privilege & Authorization Requirements** **Product access:** A subset of Optimizely's employees have access to the products and to customer data via controlled interfaces. The intent of providing access to a subset of employees is to provide effective customer support, to troubleshoot potential problems, and to detect and respond to security incidents. All access requests are logged. Employees are granted access by role. **Background checks:** All new Optimizely employees undergo a 3rd party background check prior to being extended an employment offer, as local laws allow. All employees are required to conduct themselves in a manner consistent with company guidelines, non- disclosure requirements, and ethical standards.	**Data Access:** To your visitor and account data stored on the Optimizely Service is restricted within Optimizely to employees and contractors who have a need to know this information to perform their job function, for example, to provide customer support, to maintain infrastructure, or for product enhancements (for instance, to understand how an engineering change affects a group of customers). Optimizely currently requires the use of single sign-on, strong passwords and/or 2-factor authentication for all employees to access production servers for the Optimizely Service. **Single Sign-On:** Optimizely lets you implement Single Sign-On (SSO) through SAML 2.0, an open standard data format for exchanging authentication and authorization information. This allows your team to log in to Optimizely using their existing corporate credentials. SSO is an account-level feature that will apply across all projects and experiments. Single Sign-On is available on select packages only, so please consult your order form for eligibility. **Session Management:** Each time a user signs into the Optimizely Service, the system assigns them a new, unique session identifier, currently consisting of 64 bytes of random data designed for protection against brute forcing. Other controls include: - Session Timeout. All sessions are designed to have a hard timeout (currently set to 7 days). Single Sign-On sessions are configured with an inactivity timeout as well (currently, 4 hours). There is an optional setting to terminate any sessions after 15 minutes of inactivity. - Sign Out. When signing out of the Optimizely Service, the system is designed to delete the session cookie from the client and to invalidate the session identifier on Optimizely servers.
Data Access Controls	Ensuring, where Processor reasonably can, that persons entitled to use Software Services Processing Personal Data gain access only to such Personal Data as they are entitled to accessing in accordance with their access rights and Controller's instructions, and that, in the course of Processing or use and after storage, Personal Data cannot be read, copied, modified or deleted without authorisation (data access control).	**Authorization:** The granting of access rights is based on the job responsibilities of the user and on a need-to-know basis and has to be authorised and granted by the corresponding supervisor of the person who makes an application for it. The authorisations are made by workflow tools. The access to productive systems is only granted to users who are periodically trained and authorised for the corresponding action. The access to productive systems is also immediately withdrawn in case of a termination of the contract of employment or in case of an assignment of a different task.	**Authentication:** Optimizely implemented functions allowing Customers to implement their own password policy. Customers who interact with the products via the user interface must authenticate before accessing non-public customer data. **Authorization:** Customer data is stored in multi-tenant storage systems accessible to Customers via only application user interfaces and application programming interfaces. Customers are not allowed direct access to the underlying application infrastructure. The authorization model in each of Optimizely's products is designed to ensure that only the appropriately assigned individuals can access relevant features, views, and customization options. Authorization to data sets is performed through validating the user's permissions against the attributes associated with each data set. **Application Programming Interface (API) access:** Public product APIs may be accessed using an API key or through Oauth authorization. **Preventing Unauthorised Product Use:** Optimizely implements industry standard access controls and detection capabilities for the internal networks that support its products. **Access controls:** Network access control mechanisms are designed to prevent network traffic using unauthorised protocols from reaching the product infrastructure. The technical measures implemented differ between data centre providers and include Virtual Private Cloud (VPC) implementations and security group assignment, along with traditional enterprise firewall and Virtual Local Area Network (VLAN) assignment.	Authentication: Optimizely requires authentication for access to all application pages on the Optimizely Service, except for those intended to be public. Secure Communication of Credentials. Optimizely currently uses TLS-encrypted POST requests to transmit authentication credentials to the Optimizely Service. Password Management: We have processes designed to enforce minimum password requirements for the Optimizely Service. We currently enforce the following requirements and security standards for end user passwords on the Optimizely Service: - Passwords must be a minimum of 8 characters in length and include a mix of uppercase and lowercase letters as well as numbers and symbols - Multiple logins with the wrong username or password will result in a locked account, which will be disabled for a period of time to help prevent a brute-force login, but not long enough to prevent legitimate users from being unable to use the application - Email-based password reset links are sent only to a user's pre-registered email address with a temporary link - Optimizely rate limits multiple login attempts from the same email address - Optimizely prevents reuse of recently-used passwords Password Hashing: End user account passwords stored on the Optimizely Service are hashed with a random salt using industry-standard techniques. We currently use HMAC-SHA256 and run through 86000 rounds of PBKDF2. 2-Step Verification: 2-Step Verification increases the security of your Optimizely Service account by adding a second level of authentication when signing in. Instead of relying only on a password, 2-Step Verification will also require you to enter a temporary code that you access from your mobile phone. 2-Step Verification is intended to help you: - Protect your website and mobile application when your Optimizely password is stolen; - Add an additional layer of security against password phishing attacks; and - Adhere to guidelines set by your enterprise security policy.

Data Transfer Controls	Ensuring, where Processor reasonably can, that Personal Data cannot be read, copied, modified or deleted without authorisation during electronic transmission, transport or storage on storage media, and that the target entities for any transfer of Personal Data by means of data transmission facilities can be established and verified (data transfer control).	**Authenication:** The remote access to data on Data Processor's production machines depends on a connection to the company's network which is regulated via a double authentication. **In-transit:** The transmission of Personal Data to and from the Data Processor's network is completed with the help of commonly accepted security and encryption technologies. **Network Security:** The data processing systems are protected against the risk of intrusion with the help of suitable software and hardware whose effectiveness and updating is checked periodically. The routers are appropriately configured to secure the Data Processor's internal network from unauthorised external connections and to secure that computer connections and data flow do not breach the logical access adjustment control of the Data Processor systems. Amendments on the hardware-based network components or on their configurations need the acceptance of the designated person in charge and are subject to a change management process. **Firewall Security:** Data Processor has a firewall configuration regulation which defines acceptable ports. Only used ports and services are open. The access for the amendment of the firewall configuration is restricted to an internal team of security experts. Such team regularly examines critical firewall regulations.	In-transit: Optimizely makes HTTPS encryption (also referred to as SSL or TLS) available on every one of its login interfaces and as included in specific orders on every customer site hosted on the Optimizely products. Optimizely's HTTPS implementation uses industry standard algorithms and certificates. At-rest: Optimizely stores user passwords following policies that follow at least industry standard practices for security. Intrusion detection and prevention: Optimizely implemented a Web Application Firewall (WAF) solution to protect all hosted sites as well as Optimizely Service access. The WAF is designed to identify and prevent attacks against publicly available network services. Penetration testing: Optimizely maintains relationships with industry recognized penetration testing service providers for four annual penetration tests. The intent of the penetration tests is to identify and resolve foreseeable attack vectors and potential abuse scenarios.	Optimizely monitors and updates its communication technologies periodically with the goal of providing network security. **SSL/TLS:** By default all communications from your end users and your visitors with the Optimizely Service are encrypted using industry-standard communication encryption technology. Optimizely currently uses Transport Layer Security (TLS), with regular updates to ciphersuites and configurations. **Network Security:** Optimizely regularly updates network architecture schema and maintains an understanding of the data flows between its systems. Firewall rules and access restrictions are reviewed for appropriateness on a regular basis. **Infrastructure Security:** Optimizely uses an Intrusion Detection System (IDS), a Security Incident Event Management (SIEM) system and other security monitoring tools on the production servers hosting the Optimizely Service. Notifications from these tools are sent to the Optimizely Security Team so that they can take appropriate action.
Entry Controls	Ensuring the establishment of an audit trail to document whether and by whom Personal Data have been entered into, modified in, or removed from Personal Data Processing systems (entry control).	**Security Incident Response:** The security policy contains a precise description of the steps to be taken when a security incident relating to Personal Data is detected, as well as of the persons in charge of dealing with the incident, in order to return to the normal situation as quickly as possible. The procedure for reporting and managing security incidents includes a record of each incident, the time at which it occurred, the person reporting it, to whom it was reported and the effects thereof. The circumstances of any incident are to be analysed in order to elaborate preventive measures or make adaptations so as to avoid a repetition of this type of incident.	**Detection:** Optimizely designed its infrastructure to log extensive information about the system behaviour, traffic received, system authentication, and other application requests. Internal systems aggregated log data and alert appropriate employees of malicious, unintended, or anomalous activities. Optimizely personnel, including security, operations, and support personnel, are responsive to known incidents. **Response and tracking:** Optimizely maintains a record of known security incidents that includes description, dates and times of relevant activities, and incident disposition through its Security Incident Management process. Suspected and confirmed security incidents are investigated by the Optimizely Security Incident Response Team (SIRT); and appropriate resolution steps are identified and documented. For any confirmed incidents, Optimizely will take appropriate steps to minimize product and Customer damage or unauthorised disclosure. **Communication:** If Optimizely becomes aware of unlawful access to Customer data stored within its products, Optimizely will: 1) notify the affected Customers of the incident; 2) provide a description of the steps Optimizely is taking to resolve the incident; and 3) provide status updates to the Customer contact, as Optimizely deems necessary. Notification(s) of incidents, if any, will be delivered to one or more of the Customer's contacts in a form Optimizely selects, which may include via email or telephone.	**Access Logs:** Logs are kept at all account levels for the following key changes that end users make to experiments: - Account: Sign-in / Sign-out - Experiments: Archiving, Creating, Deleting, Start/Pause and Updating - Update Project Settings Detailed logs are available in the "Change History" tab from your account home page. This Change History provides details on changes in your Optimizely snippet code, so you can have an audit trail of these code changes on your experiments and can quickly isolate any accidental edits.
Control of Instructions	Ensuring that where Processor is Processing Personal Data that they are done solely in accordance with the Customer's instructions (control of instructions).	**Data input control:** Effective input control is applied to ensure that Personal Data cannot be read, copied, modified or re- modified without authorization in the course of Processing or use and after storage. All access requests are logged and their compliance is monitored. Because detection data are also personal data, any operation performed on these data is submitted to adequate security measures. **Job Controls:** The functions and obligations of every individual with access to the Personal Data are clearly defined, updated and documented. Measures are adopted to make staff familiar and periodically trained with respect to the specific rules applicable to their functions and the consequences of any breach of these rules.	The Optimizely Marketing Product provides a solution for Customers to conduct their marketing and sales activities. Customers control the data types collected by and stored within their portals. Optimizely never sells personal data to any third party. **Terminating Customers:** Core Customer Data in active (i.e., primary) databases is purged upon a customer's written request, or for our Software Services listed at https://www.Optimizely.com/about/privacy/trust-center/, 30 days after a Customer terminates all agreements for such Software Services with Optimizely. Marketing information stored in backups, replicas, and snapshots is not automatically purged, but instead ages out of the system as part of the data lifecycle. Optimizely reserves the right to alter data purging period in order to address technical, compliance, or statutory requirements. "Core Customer Data" includes (i) the name, email address, phone number, online user name(s), telephone number, and similar information voluntarily submitted by visitors to Customer's landing pages on the Software Service, and (ii) data related to Customer's visitors' social media activities to the extent such activities can be tied to an identifiable individual; and excludes (i) analytics data, (ii) Customer Data, (iii) aggregated anonymous data, (iv) logs, archived data or back-up data files, (v) other data that is not reasonably practicable for us to delete and (v) other data that is or becomes generally known to the public without breach of any obligation owed to Customer.	**Job Controls:** Optimizely has implemented several employee job controls to help protect the information stored on the Optimizely Service: - All Optimizely employees are required to sign confidentiality agreements prior to accessing our production systems. - All Optimizely employees are required to receive security and privacy training at time of hire, as well as quarterly security and/or privacy awareness training. - Employee access to production systems that contain your data is logged and audited - Optimizely employees are subject to disciplinary action, including but not limited to termination, if they are found to have abused their access to customer data - Starting on May 18, 2017, new Optimizely employees are subject to background check prior to employment, where permitted by law

Availability Controls	Ensuring, where Processor reasonably can, that Personal Data are protected against accidental destruction or loss (availability control).	**Disaster Recovery:** Personal data is protected from accidental destruction or loss through effective retrieval systems, disaster recovery and business continuity planning. The procedures laid down for making backup copies and for recovering data ensure that they can be reconstructed in the state they were at the time they were last backed up.	**Infrastructure availability:** The data centre providers use commercially reasonable efforts to ensure a minimum of 99.9% uptime. The providers maintain a minimum of N+1 redundancy to power, network, and HVAC services. **Fault tolerance:** Backup and replication strategies are designed to ensure redundancy and fail-over protections during a significant processing failure. Customer data is backed up to multiple durable data stores and replicated across multiple data centers and availability zones. **Online replicas and backups:** All databases are backed up and maintained using at least industry standard methods. An optional higher level of service allows production databases to replicate data between no less than 1 primary and 1 secondary database. Optimizely's Software Services are designed to ensure redundancy and enable failover when the customer purchases this level of service. The server instances that support the products are also architected with a goal to prevent single points of failure. This design assists Optimizely operations in maintaining and updating the product applications and backend while limiting downtime.	**Disaster Recovery** The infrastructure for the Optimizely Service is designed to minimize service interruption due to hardware failure, natural disaster, or other catastrophes. Features include: - State of the art cloud providers: We use Google App Engine and Amazon Web Services, which are trusted by thousands of businesses to store and serve their data and services. - Data replication: To help ensure availability in the event of a disaster, we replicate data across multiple data centers. - Backups: We perform daily, weekly, and monthly backups of data stored on the Optimizely Service, which are tested regularly. - Continuity plan: We have an office located in Amsterdam to assist in business continuity should regional issues at our global headquarters in San Francisco, California disrupt our ability to provide the services or support to you. **Incident Response** Optimizely has an Incident Response Plan designed to promptly and systematically respond to security and availability incidents that may arise. The incident response plan is tested and refined on a regular basis.
Separations Controls	Ensuring, where Processor reasonably can, that Personal Data collected for different purposes can be processed separately, based on Customer's instructions (separation control), use of, where applicable and reasonably practicably possible, industry standard encryption and/or pseudonymization.	**Data Segregation:** Each data Processing is made on database systems which are separated by a system of logical and physical access controls in the network. **User Roles:** The Personal Data Processing is only made for the purpose as further specified in the Agreement.	**Product Improvement:** Optimizely's collection of personal data from its Customers is to provide and improve our Software Services and shall be done in an aggregate and anonymous manner. Optimizely does not use that data for other purposes that would require separate processing.	**Segregation Controls** **Data Segregation.** The code snippet for the Optimizely Service (the javascript client for the web experimentation product) is designed to be unique to your account. Optimizely's systems for the Optimizely Service are designed to logically separate your data from that of other customers. Optimizely's application logic is designed to enforce this segmentation by permitting each end user access only to accounts that the user has been granted access to. **User Roles.** The Optimizely Service is designed for use cases ranging from single account holders to large teams. User roles specify different levels of permissions that you can use to manage the users on your Optimizely Service account. You can invite users to your account without giving all team members the same levels of permissions. These user permission levels are especially useful when there are multiple people working on the same project or experiment.
Organizational Controls	Security Policy and Counsellor, Supervision, Inspection and Maintenance	The Data Processor has drawn up a written policy in relation to data security, giving a precise description of the security strategies and protection features selected for data security. The Security Policy takes into account the real risks the Personal Data are exposed to. It includes a description of how to manage security incidents, a description of the awareness-raising process for the policy within the organization and a description of the various responsibilities and organizational rules. It also specifies the measures foreseen for keeping the security system up-to-date after installation. The security policy has been approved by the relevant persons in charge and has been adequately disseminated within the organisation. A reassessment of the technical and organisational measures is performed on a regular basis in order to assure that the initial goals and the measures taken remain up-to- date so that improvements can be made if necessary. In case of reorganisation or modification of infrastructure, security controls are updated. The security policy will be adapted where necessary as a result of modifications or reassessment. The Data Processor has appointed a security counsellor, who is in charge of the implementation of the security policy. The security counsellor possesses the necessary competences, is adequately trained and will not be able to discharge any function or take up any responsibility that is incompatible with that of a security counsellor. **Centralized Documentation:** The Data Processor has completed centralised documentation relating to security, which is complete and formalized, proportional to security needs, up-to-date at any time and accompanied by a directory at the disposal of properly authorized persons whenever necessary.		**Product Security Overview** Optimizely's software security practices are measured using industry-standard security models (currently, the Building Security In Maturity Model (BSIMM)). The Optimizely software development lifecycle (SDLC) for the Optimizely Service includes many activities intended to foster security: - Defining security requirements - Design (threat modeling and analysis, security design review) - Development controls (static analysis, manual peer code review) - Testing (dynamic analysis, Bug Bounty Program, 3rd party security vulnerability assessments) -- We currently use unit, integration, and end-to-end tests, where applicable, to catch regressions -Deployment controls (such as change management and canary release process). Optimizely designs, reviews and tests the software for the Optimizely Service using applicable OWASP standards. **Code Assessments** The software we develop for the Optimizely Service is continually monitored and tested using processed designed to proactively identify and remediate vulnerabilities. We regularly conduct: - Automated source code analysis designed to find common defects - Peer review of all code prior to being pushed to production - Manual source code analysis on security-sensitive areas of code - Third-party application security assessments and penetration tests performed annually **Bug Bounty Program** Optimizely currently offers a bug bounty program to encourage reporting of security issues with our product. Bugs can be reported via the program, or via email at security@optimizely.com.