Data Privacy and Security Areas		Optimizely Measures
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 various Software Services offerings within EU, US, UK, Norway, Canada, Singapore/Hong Kong or Australia based data centre providers, which is the choice of Data Exporter. Not all products are availilable in all locations. 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.
Logical Access Controls	The prevention, where Processor reasonably can, of Software Services Processing Personal Data from being used without authorisation (logical access control).	**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 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).	**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, in some cases, 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.
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).	**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 uses at-rest encryption whereever technically possible using industry standard mechanisms. **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. **Penetration testing:** Optimizely maintains relationships with industry recognized penetration testing service providers for annual penetration tests and ongoing monitoring. The intent of the penetration tests is to identify and resolve foreseeable attack vectors and potential abuse scenarios.
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).	**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.
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).	The Optimizely Marketing Automation 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 (unless otherwise contractually specified). 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.
Availability Controls	Ensuring, where Processor reasonably can, that Personal Data are protected against accidental destruction or loss (availability control).	**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.
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.	**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.
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. Such documentation should at least contain the following elements: the identity of the security counsellor, the security policy, the implementation of security measures, an inventory of the personal data being processed, their localisation and the operations performed on them, a nominative list of the bodies or appointees having access to the data; the system and network configuration, technical documentation about the security controls that were introduced, a schedule of planned operations, the detection policy, security control test plans, incident reports, audit reports, if any. **Organizational Security:** The Data Processor has made available sufficient and adequate organizational, technical and financial resources to organize security. Information classification procedures have been elaborated. Whenever necessary, an inventory can be drawn up and all Personal Data being processed can be localized, irrespective of the type of data carrier. Guidelines on Personal Data protection have been elaborated and disseminated within the organisation in order to ensure that all employees participating in the Processing of Personal Data are sufficiently informed about their duties and responsibilities during Processing operations.