



Zayo Customer Privacy Statement

At Zayo, we know how important privacy is to our customers. So we've created this privacy statement to explain our approach to the collection, use, and disclosure of customer information. This privacy statement aligns with the transparency requirements of the EU General Data Protection Regulation (GDPR), effective 25 May 2018.

Definitions

Data subjects – people whose information is processed.

Personal data – any information that relates to an identified or identifiable living individual. This includes, for example, information such as name, address, telephone number, email address, and identification number.

Processing – any set of actions which is performed on personal data such as collecting, recording, organizing, structuring, storing, altering, retrieving, using, disclosing, or destroying.

Controller – the entity that determines the processes and means of processing.

Processor – the entity that processes personal data on behalf of the controller.

Context

Zayo provides direct communications infrastructure services to customers globally. As part of providing those services, Zayo may act as a controller or a processor, or neither. This privacy statement explains our position with respect to the different services Zayo provides.

For Data Services and Network Infrastructure [including Dark Fibre, Wave, SONET, Ethernet]:

Zayo provides infrastructure and bandwidth services that permit customers to transport data in accordance with customer contractual requirements. The Customer is responsible for ensuring the data transmitted through these services is appropriately protected and compliant with current privacy legislation. Although customer information is moving through Company infrastructure, Zayo is NOT acting in the role of a processor of customer data. Zayo does not possess any direct or administrative access to any customer content that is transmitted through our communication infrastructure. This separation is maintained through both technological and security controls implemented on our service architecture.

For Cloud Services [Object Based Storage Services]:

Zayo provides and operates cloud based capabilities and infrastructure that permit storage and lifecycle management activities for customer content. Through these services, Zayo is acting in the role of a processor on behalf of the Customer [the controller]. Zayo has prepared a Data Processor Addendum [DPA] in accordance with GDPR Article 28. Please make a request through your designated Zayo contact to initiate the process for executing a DPA.

Zayo as a Controller:

Zayo collects personal data from customers in order to administer customer accounts and comply with customer contracts.

1. Categories of Personal Data Collected

Contact Information – Zayo collects customers’ name, business address, telephone number, job title, email address, portal access credentials.

Zayo generally collects this information directly from data subjects. In cases where contact information is provided by the Customer in accordance with contractual requirements, the Customer is responsible for ensuring that any personal data submitted to Zayo has been obtained in accordance with relevant data protection requirements. Where applicable, Customer warrants that it has obtained any required consent from the data subject prior to providing personal data to Zayo.

Identity Information – Zayo collects government issued identity information [e.g., drivers license, passport], palm or fingerprint biometric identifiers, and CCTV video image.

Zayo collects this information directly from the data subject at each designated Zayo facility.

Network Traffic Data – Zayo collects data that is captured through system logging and data flow management systems including, but not limited to, source and destination Internet Protocol [IP] addresses and domain name, date and time indicators, and other network layer protocol header information as collected based on service capabilities.

2. Purposes and Legal Bases for Processing Personal Data

Zayo processes contact information as necessary for the performance of a contract between Zayo and the Customer. Contact information is needed for ongoing contract administration, to provide customer notices and service announcements, to assist with service incident resolution, to install and maintain services on customer premises and to address billing and payment inquiries.

Zayo processes identity information as necessary for the performance of a contract between Zayo and the Customer. Customer contracts require that physical security controls be implemented to prevent unauthorized access to colocation facilities and customer equipment. Identity information is collected to authenticate individuals based on customer approvals.

Zayo processes network traffic data consistent with its legitimate interests in ensuring the integrity of services and to support security incident and event management.

3. Categories of Recipients of Personal Data

Zayo shares personal data with several categories of recipients.

Contact information may be used/accessed by Zayo employees including client services, sales, network/service operations staff and both Zayo and 3rd party operations personnel.

Identity information may be used/accessed by Zayo facility operation employees and 3rd party facility and security services providers at designated facilities.

Network traffic data may be used/accessed by designated Zayo network administrators/platform managers and Zayo Security Operations Centre [SOC] staff.

4. Data Transfers

Zayo endeavours to limit data transfers wherever possible. Where data transfers are necessary, Zayo ensures that recipients of this data have appropriate safeguards in place. With respect to the personal data categories described above, Zayo executes necessary data transfers on the following legal bases:

Contact information is managed within Salesforce on infrastructure located in the United States. This data transfer is necessary for the performance of a contract between Zayo and the Customer.

Identity information does not require data transfer. All data is maintained locally within the jurisdiction where it is collected and used.

Network traffic data is transferred to Zayo operations within Canada in accordance with the European Commission's adequacy decision.

5. Data Retention

Zayo retains contact information for as long as the Customer maintains an active account and for 7 years after account termination in order to comply with legal and financial reporting obligations. In other cases, when information is no longer required in support of a defined purpose, it will be deleted.

Zayo retains identity information for the duration of valid access to designated facilities. CCTV images are kept up to 30 days after which they are deleted.

Zayo retains network traffic data for 90 days after which it is archived for 1 year before being deleted.

6. Data Subject Rights

You have the right to:

- Request further details on the processing of your personal data;
- Request a copy of the personal data that you have provided to us;
- Correct or remove any inaccurate personal data we hold; and
- Object to any processing based on legitimate interests grounds, unless our reasons for undertaking that processing outweigh any prejudice to your data protection rights; and

To update, correct, or remove personal data or to object to the processing of your information, please contact us at sales@zayo.com. Where contact information has been provided by your employer [our Customer], please direct your request to your employer for corrective action. Due to the nature of personal data use, Zayo reserves the right to verify any corrections with customer contract authorities prior to making any changes.

For all other inquiries, please contact us, in writing, at privacy.office@zayo.com. In your request, please clearly articulate the nature of the concern/request as specifically as possible. Prior to release of any information, we may be required to ask for additional information from you in order to verify your identity before disclosure.

If you consider that privacy requests have not been addressed adequately by Zayo or the processing of Personal Data infringes the GDPR, you have the right to lodge a complaint with the office of the Data Protection Commissioner or Supervisory Authority in the country where you reside.

7. Organization Details and Contact Information

Head Office:

Zayo Group LLC
1805 29th Street, Suite 2050,
Boulder Colorado, USA, 80301

European Offices:

Harmsworth House, 13-15 Bouverie Street , London, EC4Y 8DP
19-21 rue Poissonnière, Paris 75002, France.

Privacy Office :

Director, Global Privacy
privacy.office@zayo.com

Statement updated: May 25, 2018