Zoom Answer Call Data Protection Policy (GDPR)

Table of Contents

Introduction

Zoom Answer Call Ltd is committed to conducting its business in accordance with all applicable Data Protection laws and regulations.

This policy sets forth the expected behaviours of Zoom Answer Call's Employees and Third Parties in relation to the collection, use, retention, transfer, disclosure and destruction of any Personal Data belonging to the Data Subject, defined as a person interacted with as part of the providing the Service or the management of the Service provided for the Customer, as described in the Customer Contract.

Personal Data is any information which relates to an identified or Identifiable Natural Person. Personal Data is subject to certain legal safeguards and other regulations which impose restrictions on how organisations may process Personal Data.

An organisation that handles Personal Data and makes decisions about its use is known as a Data Controller. Any person (other than an employee of the data controller) who processes the data on behalf of the Data Controller is a Data Processor.

Zoom Answer Call, acting as a Data Controller for its own data, and acting as a Data Processor for its Customers, is responsible for ensuring compliance with the Data Protection requirements outlined in this policy. Non-compliance may expose Zoom Answer Call to complaints, regulatory action, fines and/or reputational damage.

Zoom Answer Call's leadership is fully committed to ensuring continued and effective implementation of this policy, and expects all Zoom Answer Call Employees and Third Parties to share in this commitment. Any breach of this policy will be taken seriously and may result in disciplinary action or business sanction.

This policy has been approved by Zoom Answer Call's Data Protection Officer, Ken Tracy.

Scope

This policy applies to all Processing of Personal Data in digital form, including electronic mail, telephone calls and data collected during those calls, documents created for word processing software, or where it is held in manual files, that are structured in a way that allows ready access to information about individuals.

Policy

Governance

Data Protection Officer

Zoom Answer Call has established a Data Protection Officer (Ken Tracy) whose duties include:

- Informing and advising Zoom Answer Call and its Employees who carry out Processing pursuant to Data Protection regulations, national law or Union based Data Protection provisions
- Ensuring the alignment of this policy with Data Protection regulations, national law or Union based Data Protection provisions

- Acting as a point of contact for and cooperating with Data Protection Authorities
- The establishment and operation of a system providing prompt and appropriate responses to Data Subject requests
- Informing senior managers, officers, and directors of Zoom Answer Call of any potential corporate, civil and criminal penalties which may be levied against Zoom Answer Call and/or its Employees for violation of applicable Data Protection laws
- Ensuring establishment of procedures and standard contractual provisions for obtaining compliance with this Policy by any Third Party who:
    - provides Personal Data to a Zoom Answer Call Entity
    - receives Personal Data from a Zoom Answer Call Entity
    - has access to Personal Data collected or processed by a Zoom Answer Call Entity

Data Protection by Design

To ensure that all Data Protection requirements are identified and addressed when designing new systems or processes and/or when reviewing or expanding existing systems or processes, each of them must go through an approval process before continuing.

Zoom Answer Call must ensure that a Data Protection Impact Assessment (DPIA) is conducted for all new and/or revised systems or processes for which it has responsibility. The subsequent findings of the DPIA must then be submitted to the DPO for review and approval.

Compliance Monitoring

To confirm that an adequate level of compliance that is being achieved by Zoom Answer Call in relation to this policy, the Data Protection Officer will carry out an annual Data Protection compliance audit. Each audit will, as a minimum, assess:

- Compliance with Policy in relation to the protection of Personal Data, including:
    - The assignment of responsibilities
    - Raising awareness
    - Training of Employees
- The effectiveness of Data Protection related operational practices, including:
    - Data Subject rights
    - Personal Data transfers
    - Personal Data incident management
    - Personal Data complaints handling
- The level of understanding of Data Protection policies and Privacy Notices
- The accuracy of Personal Data being stored
- The conformity of Data Processor activities

- The adequacy of procedures for redressing poor compliance and Personal Data Breaches

The Data Protection Officer, in cooperation with management, will devise a plan with a schedule for correcting any identified deficiencies within a defined and reasonable time frame.

Data Protection Principles

Zoom Answer Call has adopted the following principles to govern its collection, use, retention, transfer, disclosure and destruction of Personal Data:

Where Zoom Answer Call is acting as the Data Controller:

Principle 1: Lawfulness, Fairness and Transparency

Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. This means, Zoom Answer Call must tell the Data Subject what Processing will occur (transparency), the Processing must match the description given to the Data Subject (fairness), and it must be for one of the purposes specified in the applicable Data Protection regulation (lawfulness).

Principle 2: Purpose Limitation

Personal Data shall be collected for specified, explicit and legitimate purposes and not further Processed in a manner that is incompatible with those purposes. This means Zoom Answer Call must specify exactly what the Personal Data collected will be used for and limit the Processing of that Personal Data to only what is necessary to meet the specified purpose.

Principle 3: Data Minimisation

Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are Processed. This means Zoom Answer Call must not store any Personal Data beyond what is strictly required.

Principle 4: Accuracy

Personal Data shall be accurate and, kept up to date. This means Zoom Answer Call must have in place processes for identifying and addressing out-of-date, incorrect and redundant Personal Data.

Principle 5: Storage Limitation

Personal Data shall be kept in a form that permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data is Processed. This means Zoom Answer Call must, wherever possible, store Personal Data in a way that limits or prevents identification of the Data Subject.

Principle 6: Integrity & Confidentiality

Personal Data shall be Processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful Processing, and against accidental loss, destruction or damage. Zoom Answer Call must use appropriate technical and organisational measures to ensure the integrity and confidentiality of Personal Data is maintained at all times.

Principle 7: Accountability

The Data Controller shall be responsible for and be able to demonstrate compliance. This means Zoom Answer Call must demonstrate that the six Data Protection Principles (outlined above) are met for all Personal Data for which it is responsible.

Where Zoom Answer Call is acting as the Data Processor:

Principle 1: The status and obligations of Zoom Answer Call and the Customer

Zoom Answer Call acts as a provider of outsourced contact centre and related services to the Customer. All Personal Data collected or Processed by Zoom Answer Call or its Sub-Processors shall be owned by the Customer for whom Zoom Answer Call is providing the Service.

The Data Subject is client of the Customer, or a person wishing to interact with the Customer, or a person whom the Customer has permission to interact with. The Customer is the Data Controller and assumes the responsibilities of Data Controller as defined in the GDPR.

Zoom Answer Call will only process personal data in order to provide the Services and according to the specific, agreed, written instruction of the Customer. The Customers' instructions for the processing of personal data should be in accordance with data protection laws and regulations.

Zoom Answer Call will not be liable for any personal data protection-related claim brought by an individual data subject arising from an act or omission of Zoom Answer Call, to the extent that the act or omission resulted directly from Customers' instructions. The Customer indemnifies Zoom Answer Call for all claims, demands, losses, liabilities, fines and costs resulting from its adherence to such instructions in relation to the processing of personal data.

Zoom Answer Call will act in good faith that any Customer interaction it is requested to perform by the Client will already be covered by a lawful basis, unless stipulated in the schedule of amendments. Zoom Answer Call is able to advise or confirm and record consent as specified by the Customer as Data Controller.

Zoom Answer Call will notify the Customer immediately if it believes that an instruction for the processing of Personal Data will or may infringes data protection laws and regulations. If Zoom Answer Call identifies a valid legal requirement for it to process personal data other than in accordance with Client's instructions, it will when possible inform the Customer of the legal requirement prior to processing.

Principle 2: Purpose Limitation

Zoom Answer Call will act as a Data Processor for the Customer to provide the Service, it may use Sub-Processors to fulfil the Service and will expect all Sub-Processors to adhere to this agreement.

The categories of Personal Data processed by Zoom Answer Call and its Sub-Processors can include phone numbers, addresses, email addresses, or any other Personal Data as necessary to perform the Service.

Principle 3: Storage Limitation, Deletion, Data Minimisation

The Service will be provided for as long as the Customer Contract is considered binding. Upon termination of the Service, Personal Data is to be destroyed or returned to the Customer at the Customers request. Please note, some data may take some time to destroy, for example held in strongly encrypted backup systems. In this case the data will be destroyed as the backup lifecycle removes old backups.

Principle 4: Integrity & Confidentiality

Personal Data shall be Processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful Processing, and against `accidental loss, destruction or damage. Zoom Answer Call must use appropriate technical and organisational measures to ensure the integrity and confidentiality of Personal Data is maintained at all times.

Data Collection: When Zoom Answer Call is acting as a Data Controller

Data Sources

Personal Data should be collected only from the Data Subject unless one of the following apply:

- The nature of the business purpose necessitates collection of the Personal Data from other persons or bodies
- The collection must be carried out under emergency circumstances in order to protect the vital interests of the Data Subject or to prevent serious loss or injury to another person

If Personal Data is collected from someone other than the Data Subject, the Data Subject must be informed of the collection unless one of the following apply:

- The Data Subject has received the required information by other means
- The information must remain confidential due to a professional secrecy obligation
- A national law expressly provides for the collection, Processing or transfer of the Personal Data

Where it has been determined that notification to a Data Subject is required, notification should occur promptly, but in no case later than:

- One calendar month from the first collection or recording of the Personal Data
- At the time of first communication if used for communication with the Data Subject
- At the time of disclosure if disclosed to another recipient

Data Subject Consent

Zoom Answer Call will obtain Personal Data only by lawful and fair means and, where appropriate with the knowledge and Consent of the individual concerned. Where a need exists to request and receive the Consent of an individual prior to the collection, use or disclosure of their Personal Data, Zoom Answer Call is committed to seeking such Consent.

Data Subject Notification

Zoom Answer Call will, when required by applicable law, contract, or where it considers that it is reasonably appropriate to do so, provide Data Subjects with information as to the purpose of the Processing of their Personal Data.

When the Data Subject is asked to give Consent to the Processing of Personal Data and when any Personal Data is collected from the Data Subject, all appropriate disclosures will be made, in a manner that draws attention to them, unless one of the following apply:

- The Data Subject already has the information
- A legal exemption applies to the requirements for disclosure and/or Consent.

The disclosures may be given orally, electronically or in writing. If given orally, the person making the disclosures should use a suitable script or form approved in advance by the Office of Data Protection. The associated receipt or form should be retained, along with a record of the facts, date, content, and method of disclosure.

Data Collection: When Zoom Answer Call is acting as a Data Controller

Data Subject Notification

Where it has been determined that notification to the Customer is required, notification should occur promptly. Zoom Answer Call must only act on the documented instructions of the Data Controller in these circumstances.

External Privacy Notice

The Zoom Answer Call website will include an online 'Privacy Notice' and an online 'Cookie Notice' fulfilling the requirements of applicable law.

Data Use

Data Processing (As a Data Controller)

Zoom Answer Call uses the Personal Data of its Contacts for the following broad purposes:

- The general running and business administration of Zoom Answer Call
- To provide services to Zoom Answer Call customers
- The ongoing administration and management of customer services

The use of a Contact's information should always be considered from their perspective and whether the use will be within their expectations or if they are likely to object. For example, it would clearly be within a Contact's expectations that their details will be used by Zoom Answer Call to respond to a Contact request for information about the products and services on offer. However, it will not be within their reasonable expectations that Zoom Answer Call would then provide their details to Third Parties for marketing purposes.

Zoom Answer Call will Process Personal Data in accordance with all applicable laws and applicable contractual obligations. More specifically, Zoom Answer Call will not Process Personal Data unless at least one of the following requirements are met:

- The Data Subject has given Consent to the Processing of their Personal Data for one or more specific purposes

- Processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract
- Processing is necessary for compliance with a legal obligation to which the Data Controller is subject
- Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller
- Processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a Third Party (except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject, in particular where the Data Subject is a child)

There are some circumstances in which Personal Data may be further processed for purposes that go beyond the original purpose for which the Personal Data was collected. When making a determination as to the compatibility of the new reason for Processing, guidance and approval must be obtained from the Data Protection officer before any such Processing may commence.

In any circumstance where Consent has not been gained for the specific Processing in question, Zoom Answer Call will address the following additional conditions to determine the fairness and transparency of any Processing beyond the original purpose for which the Personal Data was collected:

- Any link between the purpose for which the Personal Data was collected and the reasons for intended further Processing
- The context in which the Personal Data has been collected, in particular regarding the relationship between Data Subject and the Data Controller
- The nature of the Personal Data, in particular whether Special Categories of Data are being Processed, or whether Personal Data related to criminal convictions and offences are being Processed
- The possible consequences of the intended further Processing for the Data Subject
- The existence of appropriate safeguards pertaining to further Processing, which may include Encryption, Anonymisation or Pseudonymisation

Special Categories of Data

When acting as a Data Controller, Zoom Answer Call will only Process Special Categories of Data (also known as sensitive data) where the Data Subject expressly consents to such Processing or where one of the following conditions apply:

- The Processing relates to Personal Data which has already been made public by the Data Subject
- The Processing is necessary for the establishment, exercise or defence of legal claims
- The Processing is specifically authorised or required by law

- The Processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving consent
- Further conditions, including limitations, based upon national law related to the Processing of genetic data, biometric data or data concerning health

In any situation where Special Categories of Data are to be Processed, prior approval must be obtained from the Data Protection Officer and the basis for the Processing clearly recorded with the Personal Data in question. Where Special Categories of Data are being Processed, Zoom Answer Call will adopt additional protection measures.

Children's Data

Children are unable to Consent to the Processing of Personal Data for information society services. When acting as a Data Controller, consent must be sought from the person who holds parental responsibility over the child.

Data Quality (As a Data Controller)

Zoom Answer Call will adopt all necessary measures to ensure that the Personal Data it collects and Processes is complete and accurate in the first instance, and is updated to reflect the current situation of the Data Subject. The measures adopted by Zoom Answer Call to ensure data quality include:

- Correcting Personal Data known to be incorrect, inaccurate, incomplete, ambiguous, misleading or outdated, even if the Data Subject does not request rectification.
- Keeping Personal Data only for the period necessary to satisfy the permitted uses or applicable statutory retention period.
- The removal of Personal Data if in violation of any of the Data Protection principles or if the Personal Data is no longer required.
- Restriction, rather than deletion of Personal Data, insofar as:
    - a law prohibits erasure
    - erasure would impair legitimate interests of the Data Subject
    - the Data Subject disputes that their Personal Data is correct and it cannot be clearly ascertained whether their information is correct or incorrect

Digital Marketing

As a general rule Zoom Answer Call will not send promotional or direct marketing material to a Zoom Answer Call Contact through digital channels such as mobile phones, email and the Internet, without first obtaining their Consent. Where Personal Data Processing is approved for digital marketing purposes, the Data Subject must be informed at the point of first contact that they have the right to object, at any stage, to having their data Processed for such purposes. If the Data Subject puts forward an objection, digital marketing related Processing of their Personal Data must cease immediately and their details should be kept on a suppression list with a record of their opt-out decision, rather than being completely deleted. It should be noted that where digital marketing is carried out in a 'business to business' context, there is no legal requirement to obtain an indication of Consent to carry out digital marketing to individuals provided that they are given the opportunity to opt-out.

Data Retention

To ensure fair Processing, Personal Data will not be retained by Zoom Answer Call for longer than necessary in relation to the purposes for which it was originally collected, or for which it was further Processed.

In line with personal data minimisation regulatory guidance, the Supplier will retain Client personal data according to the standard schedule:

- Live or accessible Personal data held on databases, scripting tool(s) and customer relationship management (CRM) tools – maximum retention period of 24 to 36 months
- Call and screen recordings – maximum retention period of 30 days

At the end of the retention period accessible data will be deleted. Any requirement to vary these retention periods should be provided by Client and detailed in the Schedule of Amendments to this Agreement in the Customer Contract.

Some offline data may be retained for a longer time period, for example in encrypted backups. Any such data will be removed during the natural lifecycle of the backup processes.

At or prior to the maximum retention period, Zoom Answer Call may anonymise data points from this data so that it ceases to be personal identifiable information, but is available to the Supplier as non-personal aggregated data. Anonymisation will be performed under best practice as recommended by http://ukanon.net/ in association with GDPR recommendations from the ICO and GDPR Article 29 working party.

Data Backups

Zoom Answer Call creates multiple backup copies of data, including personal data. This data is required for business continuity and audit purposes. It would be technically impractical and/or prohibitively expensive to segment this data by Client. When historic backup data is retained it is stored in a highly secure manner. Access is restricted to a small number of senior management personnel via highly secure encrypted systems.

Upon restoration of any backups any personal data flagged within the period for removal or amendment will be re-removed or updated as needed.

Data Protection

Zoom Answer Call will adopt physical, technical, and organisational measures to ensure the security of Personal Data. This includes the prevention of loss or damage, unauthorised alteration, access or Processing, and other risks to which it may be exposed by virtue of human action or the physical or natural environment.

The minimum set of security measures to be adopted by Zoom Answer Call is provided in the Zoom Answer Call 'Information Security Policy'.

Data Subject Requests

When acting as a Data Controller, Zoom Answer Call will establish a system to enable and facilitate the exercise of Data Subject rights related to:

- Information access
- Objection to Processing
- Objection to automated decision-making and profiling
- Restriction of Processing
- Data portability
- Data rectification
- Data erasure

If an individual makes a request relating to any of the rights listed above, Zoom Answer Call will consider each such request in accordance with all applicable Data Protection laws and regulations. No administration fee will be charged for considering and/or complying with such a request unless the request is deemed to be unnecessary or excessive in nature.

Data Subjects are entitled to obtain the following information about their own Personal Data:

- The purposes of the collection, Processing, use and storage of their Personal Data
- The source(s) of the Personal Data, if it was not obtained from the Data Subject
- The categories of Personal Data stored for the Data Subject
- The recipients or categories of recipients to whom the Personal Data has been or may be transmitted, along with the location of those recipients
- The envisaged period of storage for the Personal Data or the rationale for determining the storage period
- The use of any automated decision-making, including Profiling
- The right of the Data subject to:
    - object to Processing of their Personal Data
    - lodge a complaint with the Data Protection Authority
    - request rectification or erasure of their Personal Data
    - request restriction of Processing of their Personal Data

When acting as a Data Controller, a response to each request will be provided within 30 days of the receipt of the written request from the Data Subject. Appropriate verification must confirm that the requestor is the Data Subject or their authorised legal representative.

Data Subjects shall have the right to require Zoom Answer Call to correct or supplement erroneous, misleading, outdated, or incomplete Personal Data.

If Zoom Answer Call cannot respond fully to the request within 30 days, the following information will be provided to the Data Subject within the specified time:

- An acknowledgement of receipt of the request
- Any information located to date
- Details of any requested information or modifications that will not be provided to the Data Subject, the reason(s) for the refusal, and any procedures available for appealing the decision.
- An estimated date by which any remaining responses will be provided
- An estimate of any costs to be paid by the Data Subject (e.g. where the request is excessive in nature)
- The name and contact information of the Zoom Answer Call individual who the Data Subject should contact for follow up

It should be noted that situations may arise where providing the information requested by a Data Subject would disclose Personal Data about another individual. In such cases, information must be redacted or withheld as may be necessary or appropriate to protect that person's rights.

When acting as a Data Processor to the Customer, any requests will be passed to the Customer as per written instructions.

Law Enforcement requests & Disclosures

In certain circumstances, it is permitted that Personal Data be shared without the knowledge or Consent of a Data Subject. This is the case where the disclosure of the Personal Data is necessary for any of the following purposes:

- The prevention or detection of crime
- The apprehension or prosecution of offenders
- The assessment or collection of a tax or duty
- By the order of a court or by any rule of law

If Zoom Answer Call Processes Personal Data for one of these purposes, then it may apply an exception to the Processing rules outlined in this policy but only to the extent that not doing so would be likely to prejudice the case in question. If Zoom Answer Call receives a request from a court or any regulatory or law enforcement authority for information relating to a Zoom Answer Call Contact, the Data Protection Officer must immediately notify the Office of Data Protection who will provide comprehensive guidance and assistance.

Data Protection Training

All Zoom Answer Call Employees that have access to Personal Data will have their responsibilities under this policy outlined to them as part of their staff induction training. In addition, Zoom Answer Call will provide regular Data Protection training and procedural guidance for their staff.

The training and procedural guidance set forth will consist of, at a minimum, the following elements:

- The Data Protection Principles set forth in this Policy
- Each Employee's duty to use and permit the use of Personal Data only by authorised persons and for authorised purposes
- The need for, and proper use of, the forms and procedures adopted to implement this policy.
- The correct use of passwords, security tokens and other access mechanisms
- The importance of limiting access to Personal Data, such as by using password protected screen savers and logging out when systems are not being attended by an authorised person.
- Securely storing manual files, print outs and electronic storage media
- The need to obtain appropriate authorisation and utilise appropriate safeguards for all transfers of Personal Data outside of the internal network and physical office premises
- Proper disposal of Personal Data by using secure shredding facilities
- Any special risks associated with particular departmental activities or duties

Data Transfer

When acting as a Data Controller, Zoom Answer Call may only transfer Personal Data where one of the transfer scenarios list below applies:

- The Data Subject has given Consent to the proposed transfer
- The transfer is necessary for the performance of a contract with the Data Subject
- The transfer is necessary for the implementation of pre-contractual measures taken in response to the Data Subject's request
- The transfer is necessary for the conclusion or performance of a contract concluded with a Third Party in the interest of the Data Subject
- The transfer is legally required on important public interest grounds
- The transfer is necessary for the establishment, exercise or defence of legal claims
- The transfer is necessary in order to protect the vital interests of the Data Subject

Zoom Answer Call will only transfer Personal Data to, or allow access by, Third Parties when it is assured that the information will be Processed legitimately and protected appropriately by the recipient. Where Third Party Processing takes place, Zoom Answer Call will first identify if, under applicable law, the Third Party is considered a Data Controller or a Data Processor of the Personal Data being transferred.

Where the Third Party is deemed to be a Data Controller, Zoom Answer Call will enter into an appropriate agreement with the Controller to clarify each party's responsibilities in respect to the Personal Data transferred. This agreement forms the Service as described in the Customer Contract.

Where the Third Party is deemed to be a Data Processor, Zoom Answer Call will enter into an adequate Processing agreement with the Data Processor. The agreement must require the Data Processor to protect the Personal Data from further disclosure and to only Process Personal Data in compliance with Zoom Answer Call instructions. In addition, the agreement will require the Data Processor to implement appropriate technical and organisational measures to protect the Personal Data as well as procedures for providing notification of Personal Data Breaches. When Zoom Answer Call is outsourcing services to a Third Party (including Cloud Computing services), they will identify whether the Third Party will Process Personal Data on its behalf and whether the outsourcing will entail any Third Country transfers of Personal Data. In either case, it will make sure to include adequate provisions in the outsourcing agreement for such Processing and Third Country transfers. Zoom Answer Call shall conduct regular audits of Processing of Personal Data performed by Third Parties, especially in respect of technical and organisational measures they have in place.

The Zoom Answer Call website will list all subcontractors that have, directly or indirectly, any access to Customer-related Data.

- At least 30 days before Zoom Answer Call authorises and permits any new subcontractor to access Customer-related Data, Zoom Answer Call will update the applicable website
- If the Customer does not approve of a new subcontractor, they can object to this proposed subcontractor anytime during the 30 days
- After this 30-day period, the Customer is considered to have accepted the appointment of a new subcontractor

Policy Maintenance

The Data Protection Officer is responsible for the maintenance and accuracy of this policy. The current version of the document will be available on the Zoom Answer Call website.

Notice of significant revisions shall be provided to Zoom Answer Call Employees, Customers and Sub-Processors.