AudienceProject

Privacy & Security guidelines for employees

Introduction

AudienceProject requires every person within the organisation to adhere to these guidelines as well as all underlying applicable policies, standards, procedures or training material (“Policies”).

When you are hired, and if applicable thereafter, you will be requested to acknowledge that you are aware of, understand and agree to comply with these guidelines and our Policies. These guidelines will be deemed to apply to you as a condition of your employment.

It is the responsibility of every employee to read, understand and comply with AudienceProject Privacy and Security guidelines and underlying Policies and to seek guidance when appropriate.

You acknowledge that failure to comply with these guidelines and underlying Policies may lead to disciplinary action up to and including termination of employment.

I. Laptop & Mobile Device Policy

Upon employment by AudienceProject (the "company"), employees will be provided with the professional equipment necessary, at AudienceProject's sole discretion, to perform their work duties. Professional equipment will be provided by the company to the employees in accordance with the company's Equipment Policy and with the appropriate security settings and parameters.

Unless otherwise agreed in writing between the employee and AudienceProject, all processional equipment provided by the company to the employees will remain the property of the company.

Employees are responsible for the safety of their professional equipment. All employees must use their professional equipment in compliance with this policy.

1. Key rules

a. Key rules during employee onboarding process

- Access to all software and applications required to manage the employment relationship (e.g. Absence.IO, Corpay, Pleo, etc) and perform work duties (e.g. VPN, Slack, AudienceReport, Atalassian, etc) will be granted by the company during the employee onboarding process. Employees shall install software and applications downloaded exclusively from JAMF in compliance with company's instructions and under the supervision of their manager. Employees must not download other software and applications without prior written approval from their manager. Employees acknowledge that the use of unlicensed software and applications is illegal and puts the company at significant legal risk.

- Access to the company's IT systems and records from non-office locations must always be done through Virtual Private Network ("VPN"). Employees must ensure to have a VPN function installed on their professional equipment during the onboarding process. For any further questions or information, employees may use the following Slack channel (#ops-requests).

- Laptops and other mobile devices must be protected by a password, which can be completed by a fingerprint or a pin code. As part of the onboarding process, the employee's manager, in collaboration with the company's IT department, must ensure to set up the appropriate password, fingerprint, or pin code in order to protect information held on a laptop or a mobile device.

- Mail, file and password services accessed on laptops and other mobile devices must be protected by two-factor authentication. As part of the employee onboarding process, the employee's manager, in collaboration with the company's IT department, must ensure to set up the appropriate two-factor authentication application on the laptop or mobile device.

- By default, all computer screen displays, including laptops, must be locked with the password protected screen saver after 10 minutes of inactivity.

b. Key rules during employment relationship

- Employees are prohibited from changing security settings and parameters or amending configuration files on any laptop or mobile device provided to them by AudienceProject. This includes disabling passwords, pin codes and any installed security programs such as anti-virus applications.

- Employees must save all work-related documents to the locally installed company cloud-drives. Employees must not store files in local document folders.

- Unless otherwise specified in company's Equipment Policy, employees must not access, download, or use company's data, including personal data, and/or work-related documents on their personal equipment (e.g. employee's personal laptop, mobile phone, USB stick or external

hard disk) and more generally on any equipment other than the professional equipment provided specifically for this purpose by company.

- Employees must never send company's data, including personal data, or work-related documents to their private email address(es), phone number(s) or other other communication service(s) that is not provided by the company.

c. Key rules during travels and remote work

- Employees must not leave their professional equipment (e.g. laptop, mobile phone) unattended in public places (e.g. airports, train stations, hotels, restaurants, etc), even for a very short period of time.

- When working in public places (e.g. airports, train stations, hotels, restaurants, etc), care should be taken to prevent others from being able to view potentially confidential information. The use of privacy filters is highly recommended for these circumstances as these reduce the viewing angle of the screen and prevent casual observers from being able to see confidential information on the screen.

- When working in public places, employees must not access or use company's confidential information (such as information related to a customer, an employee or a partner), if there is a possibility that the information could be viewed or otherwise accessed by unauthorized individuals.

- When travelling, employees must not use public WIFI networks for accessing AudienceProject's IT systems and interfaces containing customers' or partners' confidential information and/or data (including personal data), such as secure enclaves. If needed, employees must apply for an international 3LikeHome subscription which will allow the employee to utilize its mobile-subscription for data-roaming. Alternatively, employees may use their private phone data via the personal hotspot function and get reimbursed in accordance with the company's Equipment Policy.

- When travelling, employees must always remember to connect through VPN connections to ensure encrypted communications.

- When travelling by air, employees must always carry their professional equipment in a cabin baggage and never check it in the hold.

- Outside of working hours, employees must store professional equipment (e.g. laptop, mobile phone) in a secure and locked place such as a locked room or cabinet located in their private place of stay (i.e., in their private home or hotel room, and excluding, for example, train station lockers, gym lockers, shared hotel lockers, etc).

d. Key rules during employee offboarding process

- Upon leaving employment or changing to a new role where the professional equipment is no longer required, employees must return the equipment to their manager. The employee's manager shall ensure that the equipment is returned to the company prior to the termination of the employment relationship.

- Employees must never access, use, and/or store company data, including personal data, or company's confidential information after the termination of their employment contract. The employee's manager shall ensure, in collaboration with the company's IT department, that the employee will no longer have access to the company's IT systems and records after the termination of the employment contract.

2. Reporting the loss or theft of your professional equipment

Any loss or theft of the professional equipment provided by the company (e.g. laptop, mobile phone, etc.) must be immediately reported to:

- Your manager. The manager must then forward the information to AudienceProject Security Incident Response Team ("SIRT"). The SIRT will take any appropriate security measure based on the circumstances and in accordance with company's Data Breach and Information Security Incident policy, including suspending/deleting access to accounts, initiating a remote wipe and/or a password rotation.

AND

- The police. Employees must obtain and keep a crime incident / reference number and communicate that number to his/her manager. The manager must then forward the information to the SIRT.

**SIRT core team: CEO, CPTO, Head of Architecture, Legal Counsel and DPO.*

II. Internet, email & social media usage policy

This policy sets out the obligations and expectations of employees of AudienceProject, including contractors and temporary employees, who use the company's IT facilities for internet and email purposes. IT facilities are provided to assist with day-to-day work. It is important that they are used responsibly, are not abused, and that individuals understand the legal and ethical obligations that apply to them, as well as professional expectations.

All resources provided by the company, including laptops, email and software are provided for legitimate use. Employees acknowledge that if there are occasions where it is deemed necessary to examine data beyond normal company activity, such as in the case of a security incident or a data breach, the company maintains the right to examine any systems and inspect and review all data recorded in those systems (for example login details). This will be undertaken by authorised employees only and in accordance with applicable regulations.

AudienceProject encourages employees to avoid saving private information or correspondence, such as health-related information, in their professional equipment. In the event that the employees decide to save their private information in their professional equipment, employees must ensure that private emails and/or correspondence are clearly labelled and identified as private (for example "EMPLOYEE FULL NAME PRIVATE") in the subject section of the emails and/or correspondence. In the same way, employees must ensure that private documents are saved in a specific folder clearly labelled and identified as private.

1. Use of Internet

Use of the Internet by employees is encouraged where such use is consistent with employees' work duties and complies with the following rules:

- Employees must not participate in any online activities that are likely to bring the company into disrepute, create or transmit material that might be defamatory or incur liability on the part of the company, or adversely impact on the image of the company.

- Employees must not use the internet for illegal or criminal activities, such as, but not limited to, software and music piracy, terrorism, or fraud. Employees must not visit or download any content or material from an illegal website or application.

- Employees must not visit or download any material from a website or an app infringing a third-party intellectual property rights. In particular, employees must not download commercial software or any copyrighted materials belonging to third parties, unless such downloads are covered or permitted under a commercial agreement or other such licence.

- Employees must not knowingly introduce any form of computer virus into the company's computer network.

- Employees' use of the internet for personal reasons (e.g. online banking, shopping, information surfing) must be limited, reasonable and not distract them from work.

2. Use of email

Upon employment, the company will provide the employee with a business email address. For the duration of the employment relationship, the employee's business email address must be used primarily for business purposes, or other purposes compatible with the employee's work duties, such as the management of the employment relationship. Reasonable personal use of the business email is permitted as long as it does not detrimentally affect the employee's work duties and, more generally, the company's business activity. Employees are responsible for all actions relating to their business email account.

- Employees must ensure that no other person has access to their business email account.

- All outgoing email is filtered to detect and prevent a virus infection being sent from the company's equipment. AudienceProject subscribes to a third-party checking service so that all incoming email is filtered for the protection of the company from email virus infection and unsolicited junk mail (e.g. spam). For security purposes, the company reserves the right to introduce company-wide content checking if this is deemed appropriate and in compliance with applicable regulations.

- Caution should be used when opening any attachments or emails from unknown senders. Any concerns about external emails, including files containing attachments, must be discussed with employees' managers. If the employee suspects a scam or a phishing attempt, the employee must report it in compliance with the company's Phishing Awareness training material.

- Employees must not use their personal email address for business purposes. In particular, for compliance reasons, employees must not use their personal email address to send, share or store work-related data, including personal data, and confidential information.

Employees acknowledge that emails may be disclosed as part of legal proceedings (e.g. tribunals), and as part of disciplinary proceedings, in compliance with applicable regulations.

3. Use of social media

Online social media platforms are an important part of modern-day communication. They allow for the exchange of ideas, opinions, and information about both personal and work-related issues. Whilst all employees of AudienceProject are welcome to participate in social media it is important that they do so responsibly.

When using social media platforms, employees must comply with the following rules:

- Employees must not post illegal, offensive, and inappropriate pictures or comments, or anything that might cause embarrassment to the company, its employees, partners, clients etc or damage the company's business activity or reputation. Employees will be held accountable for any comments in which the company is identified or identifiable, for any breaches of copyright or any defamatory postings.

- Employees must avoid identifying themselves as working for the company unless they are representing it in some capacity and have been authorised by the company, or unless the social media platform concerned is used for legitimate professional purposes (e.g. LinkedIn).

III. Access to IT systems & records

1. General rules

As a principle and to minimise the risk of data exposure, the company follows the principles of least privilege through a team-based-access-control model when provisioning system access. Employees are authorised to access company's data, IT systems and records solely to the extent necessary for their job function, role and responsibilities.

Company will not grant employees access, and employees must not seek to obtain the same, to company's data, IT systems and/or records unless it is strictly necessary to enable the employees to perform their work duties.

Upon employment, and as part of the employee onboarding process, the company will provide the employee with all necessary access and login details.

Passwords must comply with the following requirements: 10 characters minimum and not be the same as the 15 previous passwords.

A password rotation will be initiated by the company every 365 days.

Users will be locked out after 5 failed login attempts and disable automatically if suspicious device activity is detected.

Upon termination of the employment, and as part of the employee offboarding process, the employee's access and login details will be permanently removed/deleted.

Further information is available in the Access Controls section of AudienceProject Security Overview.

2. Specific rules regarding access to production environment

The services offered by the company include integrations with partners. Partners may require the company to implement supplementary security and organisational rules. In addition to the above-mentioned general rules, employees must comply with all applicable specific rules or policies.

A production environment is a real-time setting where the latest versions of software, products, or updates are pushed into live, usable operation for the intended end users.

Regarding access to a production environment, before an employee is granted access to a production environment, access must be approved by the tech team lead and the head of architecture. The employee is required to complete internal training for such access, including training on the relevant team's systems and reading the relevant training documentation.

Access rights to production environments will be monitored at least semi-annually by the company's IT department.

IV. Data protection overview

The purpose of these guidelines is to provide employees with an overview of the main principles and legal requirements relating to privacy and data protection.

Processing data is part of AudienceProject core business activities. Therefore, company's compliance with applicable privacy and data protection regulations such as the GDPR or the ePrivacy Directive is crucial and must be a priority for every employee across the company.

Nevertheless, privacy and data protection regulations are complex and may vary from country to country. All employees are expected to refrain from engaging in activities which may contravene the requirements of privacy and data protection regulations. Failing to adhere to the applicable privacy and data protection regulations carries criminal and personal liability for the employee and AudienceProject. When in doubt as to whether or not something contravenes privacy and data protection regulations, employees should seek clarification from the legal department and/or AudienceProject Data Protection Officer prior to proceeding.

1. Personal data

According to article 4 (1) of the GDPR, personal data means "*any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*".

Examples of personal data include:

- name and surname,
- a home address,
- an email address,
- an ID card number,
- an Internet Protocol (IP) address,
- a cookie ID,
- browsing history,
- bank accounts,
- tax reports,
- biometric data (like fingerprint),
- a social security number,
- passport number,
- photographs of individuals etc.

2. Personal data collected and processed to deliver advertising campaign measurement services

The services offered by AudienceProject include personal data collected via AudienceProject online data collection devices (such as pixels) and personal data collected via AudienceProject panels.

Data collected via AudienceProject online data collection devices (such as pixels) include the following:

- IP addresses and approximate general locations derived from such IP addresses,
- Date/time stamps,
- Device type,
- Browser type,
- Operating systems,
- Referring pages,
- Device identification ID and/or advertising ID,
- Local storage objects and event/clickstream data,
- TC string.

In this case, AudienceProject collects data on behalf of its clients and in accordance with its clients instructions. AudienceProject acts as a data processor. This means that AudienceProject must collect and process the data as agreed with the client in the data processing agreement. AudienceProject data processing agreement is currently available at: https://privacy.audienceproject.com/en-GB/for-clients/data-processing-agreement.

Data collected via AudienceProject panels include the following categories of data:

- Age,
- Gender,
- Income,
- Education,
- Household size,
- Number of children in the household,
- Employment.

In this case, AudienceProject collects data for its own business purposes. AudienceProject acts as an independent data controller. This means that it is AudienceProject's responsibility to comply with applicable privacy and data protection regulations, including the GDPR.

3. Sensitive data

Some types of personal data, usually called sensitive data, belong to special categories which deserve more protection. According to article 9 of the GDPR, sensitive data include data that reveals information about:

- an individual's health,
- an individual's sex life or sexual orientation,
- an individual's racial or ethnic origin,
- an individual's political opinions, religious or philosophical beliefs,
- an individual's biometric and genetic data,
- trade union membership,
- commission or alleged commission of any offence.

The processing of an individual's sensitive data is prohibited, except under specific circumstances that justify its processing (such as explicit consent).

As a principle, AudienceProject does not allow the collection and processing of sensitive personal data. As an exception, AudienceProject may accept to collect and process sensitive personal data on behalf and according to the instruction of a customer, if the project concerned is approved by the management and the legal departments and provided that legally required contractual and security measures are implemented.

For any further information, please read article 9 of the GDPR.

4. Data processing

According to article 4 (2) of the GDPR, the processing of an individual's personal data includes any type of activity (processing operation) performed whether or not by automated means on or with the individual's personal data.

Examples of processing operations include collecting, recording, organising, using, modifying, storing, disclosing an individual's personal data.

5. GDPR Key principles

In accordance with the European Data Protection Board ("EDPB") guidelines, when processing an individual's personal data, an organisation must comply with the following 6 key principles of the GDPR.

o Lawfulness, Fairness and Transparency

Any processing of personal data must be lawful, fair and transparent.

According to article 6 of the GDPR, to be lawful data processing must be based on one of the following legal basis:

- consent,
- performance of a contract,
- legitimate interests,
- compliance with a legal obligation,
- data subject's vital interests (this legal basis is not relevant for AudienceProject),
- public interest (this legal basis is not relevant for AudienceProject).

If the processing is based on consent, the organisation must ensure that this consent is freely given, informed, specific and unambiguous. In other words, there must be no doubt that individuals are aware of what they agree to, for what purposes the processing is being done, and that this consent was actively given before the processing started. Furthermore, individuals should be able to freely withdraw their consent.

o Purpose limitation

An organisation can only collect personal data for specified, explicit and legitimate purposes. The processing of an individual's data must be strictly limited to the purpose(s) initially established, and therefore not processed for subsequent or other purpose(s) that are incompatible with the initial purposes. This notably means that it is not possible to collect data if there is not already a specific use case for it - i.e., no collection of data "just in case."

o Data minimisation

An organisation can only collect personal data that is strictly necessary and proportionate in light of the purpose envisaged. This notably means that if the service's functionalities would not be impacted in the absence of such data (including in cases where another solution, that does not use personal data, can be implemented to reach the same levels of service), the concerned data should not be collected - i.e., less is better.

o Accuracy

The personal data of individuals that your organisation processes must be accurate and kept up to date. Inaccurate personal data must be rectified or erased.

o Storage limitation

The storage of individuals' personal data must be limited in time, in light of the purpose for which this data was collected and processed. As such, individuals' personal data must be deleted or anonymised once this data is no longer necessary. In practice, this means that an organisation should have an internal policy in place regarding data retention periods per different purpose, as well as a procedure for deleting data.

o Security

The processing of individuals' data must be done in a secure way. In this sense, robust data protection safeguards, such as appropriate cybersecurity measures, must be put in place to ensure that

individuals' data is adequately protected. These measures must prevent accidental, unauthorised, or unlawful disclosure, loss, destruction or damage of individuals' personal data.

For any further information, please read AudienceProject Security Overview.

6. Data subjects' rights

In accordance with articles 12 to 22 of the GDPR, data subjects have the following rights:

The right to be informed (article 13): data subjects have the right to be provided with clear, transparent, and easily understandable information about why and how the data controller uses their personal data, and their rights. This is the purpose of AudienceProject Privacy Policies.

The right to file a complaint with a supervisory authority (article 13): data subjects have the right to contact the data protection authority of their country in order to file a complaint against the data controller's data protection and privacy practices.

The right of access (article 15): data subjects have the right to access any personal data the data controller holds about them (subject to certain restrictions). In exceptional circumstances the data controller may charge a reasonable fee for providing such access but only where permitted by law (e.g. where the requests are manifestly unfounded or excessive).

The right to rectification (article 16): data subjects have the right to have their personal data rectified if the concerned data is incorrect or outdated and/or completed if it is incomplete.

The right to erasure (also called the "right to be forgotten") (article 17): in some cases, data subjects have the right to have their personal data erased or deleted. However, it is not an absolute right, as the data controller may have legal or legitimate grounds for retaining the concerned personal data.

The right to withdraw consent at any time for personal data processing based on consent (article 17): data subjects must be able to withdraw consent to the data controller processing of their personal data when such processing is based on consent. For example, regarding the data AudienceProject processes through a pixel, end-users must be able to withdraw consent at any time. Another example, regarding the data AudienceProject processes through its surveys, panellists must be able to withdraw consent at any time.

The right to object to processing based on legitimate interests (article 17): data subjects must be able to object at any time to the data controller processing of their personal data when such processing is based on the data controller legitimate interests.

The right to restriction (article 18): this means that the processing of the concerned personal data is restricted, so that the data controller can store it, but not use nor process it further. It applies in limited circumstances set out in the GDPR.

The right of data portability (article 20): the data subject has the right to move, copy or transfer personal data from our database to another. This only applies to personal data that the data subject has provided, where processing is based on a contract or data subject's consent, and the processing is carried out by automated means.

The right to object to direct marketing (article 21): data subjects must be able to unsubscribe or opt out of marketing communication at any time. The easiest way to do this is usually by clicking on the "unsubscribe" link in any email or communication the data controller may send to the data subject or to follow any other opt-out instructions communicated by the data controller.

7. Exercise of data subjects' rights

AudienceProject enables data subjects to exercise their rights through the following means:

- **Via AudienceProject privacy policies**

AudienceProject provides data subjects with the required information ("right to be informed") through its Privacy Policies.

- **Via email**

If data subjects wish to exercise their rights, for example make a data deletion request, they can contact us at privacy@audienceproject.com. Data subjects' requests are currently processed by the legal and the tech departments through AudienceProject's Technical Support Requests system.

- **Via AudienceProject website**

Data subjects can exercise their rights directly via AudienceProject "Opt-out and my data" webpage.

V. Report a security incident or personal data breach

AudienceProject utilises various information systems and holds a large amount of data and information, which may include personal data or confidential information. Care should be taken to protect these information assets from incidents, either accidentally or deliberately, that could compromise their security.

In the event of a data breach or an information security incident, it is crucial that appropriate actions are taken to minimise associated risks. The purpose of this policy is to set out the procedure that should be followed to ensure a consistent and effective approach is in place for managing data breach and information security incidents across AudienceProject.

This policy applies to all AudienceProject employees, contractors and third parties aware of or involved in a security incident or a personal data breach related to AudienceProject business activity. All employees, contractors or third party agents who access, use or manage AudienceProject's information are responsible for reporting data breach and information security incidents in compliance with this policy.

Failure to adhere to this policy will be addressed by necessary disciplinary actions in accordance with AudienceProject's employee's policies and third party contractual clauses relating to non-conformance with the Information Security Policy and related policies.

1. Security Incident or personal data breach

An incident in the context of this policy is an event which has caused or has the potential to cause damage to AudienceProject's information assets or reputation.

Examples of incidents include:

- Accidental loss or theft of confidential information or personal data or equipment on which such data is stored (e.g. loss of paper records, laptop, mobile phone),
- Unauthorised use, access to or modification of confidential information or information systems (e.g. sharing of login, deliberately or accidentally, leading to unauthorised use, access to or modification of confidential information or information systems),
- Unauthorised disclosure of confidential information or personal data (e.g. email sent to an incorrect recipient),
- Compromised user account (e.g accidental disclosure of user login details through phishing),
- Failed or successful attempts to gain unauthorised access to AudienceProject data and IT systems,
- Equipment failure,
- Malware infection,
- Disruption to or denial of IT services.

2. Reporting a security incident or personal data breach

If you become aware of a security incident or a personal data breach that might have affected AudienceProject information, data, operations, business processes, network, or facilities, you must immediately report the incident/personal data breach via email to the SIRT at: sirt@audienceproject.com.

When you report an incident/personal data breach, please make sure to provide the following information in your email. If some or all of the information is not yet available, you must still immediately send as much information as possible and thereafter complete your report as soon as the missing information become available:

- the date of the incident/personal data breach,
- indication of the information of personal data types involved,
- the approximate number of data subjects or information records affected,

- indicate the areas affected by the incident (confidentiality, Integrity, availability),
- description of actions already taken (if any),
- any additional relevant information about the incident/data breach.

The SIRT will then process the report in compliance with AudienceProject Data breach and Information Security Incident policy.

VI. Report a phising attempt

1. Phising attempt

Phishing is an attempt to steal personal information or break in online accounts using deceptive emails, messages, ads, or sites that look similar to sites you already use.

Phishing messages or content may:

- ask for your personal or financial information,
- ask you to click links or download software,
- impersonate a reputable organisation, like your bank, a social media site you use, or your workplace,
- impersonate someone you know, like a family member, friend, or coworker.

2. Report a phising attempt

If you receive a phishing email or message, you must immediately report it through AudienceProject build-in reporting system as described in AudienceProject Phishing Awareness training material.

If you have already clicked on a phishing link, please notify immediately the SIRT via email at: sirt@audienceproject.com.

Please make sure to read, understand and comply with AudienceProject Phishing Awareness training material.

Last updated: March 2024