# Data Protection Policy

Powered by AudienceProject

Version 1.37

# Introduction

Data protection and security takes many forms. It is important to understand that data protection and security not 'just' is a technical challenge being handled by the tech-department. The very best firewalls and drive encryption technologies are rendered useless if we leave our laptops open and exposed to public access. The same goes if we save files carelessly without upholding strict discipline about what should be saved and who should have access. That's why this document is for everyone. Not just the data-scientists or developers. Security and privacy concerns every person in the company from the receptionist to the CEO.

The document covers our physical security measures like the office security policies, laptop and mobile device policies. It also covers Audience Projects internal internet- and email policies. You will also find guideline to data protection which covers data subjects, personal data definitions, guidelines and rules for processing data and handling SARS requests. Finally the document handles our data security breach policies as well.

Detailed guidance for configuring security on our networks and infrastructure are not included in this document. If you are a developer or data scientist? Please request access the the CIS Amazon Web Services Foundations document that provides prescriptive guidance for configuring security options for a subset of Amazon Web Services with an emphasis on foundational, testable, and architecture agnostic settings.

But before you dive into our policies and guidelines I would like to share a few thoughts from Kostas - one of our (many) brilliant data scientists about the nature of privacy in our industry. It will serve as an important reminder to always follow the mantra of *privacy by design* in every aspect of our business.

# Foreword

*I have a subtle point about privacy. I have noticed that at no point does the analytics or ad tech industry need to know who you really are. Ad tech does not need to know what your real name is, what your parents real names are, your actual street address or any other piece of information that identifies you as you to another human being. It is a little bit hard to explain, but I will try.*

*Ad tech is powered by algorithms and these algorithms operate in an abstract space where your true identity is not important. Most ad tech knows you by a random number that was assigned to you. All your interests are also represented by random numbers. The place you live yet another. Ad tech algorithms only care about the relationships between these numbers, not what the numbers actually represent in the real world.*

*Here is how it works: You get assigned a random number, e.g. 123, to represent you. Then, ad tech will attempt to link your number, 123, with the numbers of boxes that represent products or services that you might be interested in. For example, a box A could be people who need a vacation and box B could be people who could be tempted to buy a new BMW. Ideally, if you really need a vacation and someone really wants to sell you that vacation, then a connection between 123 and A should be made. From ad tech's perspective, the number 123 is linked to the box A. The algorithm does not need to use labels like "Alice Anderson" or "Bob Biermann", because the numbers 1 and 2 will get the job done just fine -- from a mathematical point of view.*

*At some point your true identity becomes interesting, long after ad tech has left the scene. At some point, somebody (e.g. a human being or a robot) might need to print your real name and street address on a card box box, put the product you ordered inside and ship it via DHL. Up until that exact point, your name, street address or any other personally identifiable information is utterly unimportant to anybody. Nobody cares and no advertisement algorithm needs to know. I think this is an important point.*

*Ad-tech algorithms, if not ad tech itself, can have a massive and positive impact on areas of life that you probably care about. For example, algorithms can help you with your health, personal finance, insurances, education, whether you should buy Bitcoin or Either today, or whether you should attend job interview A instead of job interview B today, or your kids attend school X or Y. In these areas, relatively unaltered algorithms from ad tech can help.*

*It is important to keep in mind, that again no algorithm needs to know your name in order to work. Not even if that algorithm is looking through your medical record and correlating your stats with the stats of million of other patient records.*

*Of course it is true that your real identity can be learned from seemingly anonymised data. It might even be fairly trivial to do so, using good old detective skills. Differential privacy has some*

*fairly hard results in that area. However, the main point is that someone has to make a conscious decision to look into the data on a mission to find you and possibly design a new algorithm for that purpose.*

*Now I get to my main point. Yes, ad tech CAN know who you are with some detective work. However, ad tech does not NEED to know who you are in order to work. This is so important because it means that we can potentially harness the power of algorithms in areas of life that matter — without compromising the privacy of anybody.*

*It is not going to be easy to obtain the granular and self-controlled privacy that is needed, but it is worthwhile. And that is why I joined ad tech in the first place, because the computer science problems are interesting and important — and well, interesting and important things tend to pay well.*

# Laptop & Mobile Device Policy

## Introduction

Laptops, tablets and smartphones are versatile, portable and highly desirable devices. As a result, this type of device is at greater risk of theft, both for the device itself and as has been noted more recently, for any data that may be held on it. This document is intended to ensure that a person allocated a laptop, tablet or other mobile device understands the associated risk and assumes the appropriate level of responsibility for AudienceProject's property.

## Scope

The scope of this policy covers all employees (full time, temporary or contract staff) who use laptops, tablets and smartphones provided by AudienceProject.

## Security Risk

Laptops, tablets and mobile phones are vulnerable to loss and theft due to their portability and small size. Thieves may target these devices both on AudienceProject's premises and also whilst in transit. Although the majority of thefts will be carried out in order to resell the device for a quick profit, a significant number of laptops or other mobile devices are stolen for the (sensitive) data they may hold. Such information, if revealed, may cause embarrassment, have a negative impact on the reputation of the Company and may result in financial, commercial or competitive loss to AudienceProject.

## User Responsibility

## General rules

- ❏ Laptops, tablets and other mobile devices **must** be protected by a password, fingerprint or pin code.
- ❏ Mail, file and password services accessed on Laptops, tablets and other mobile devices **must** be protected by two-factor authorisation.
- ❏ Access to our network from non-office locations **must** always be done through VPN.
- ❏ Hard Drives on laptops **must** be encrypted.

- ❏ Find your phone (Android) or Find my iPhone (IOS) must be enabled on all mobile devices.
- ❏ Laptop or other mobile device users **must** take shared responsibility for the security of their equipment.
- ❏ Any laptop or other mobile device(s) issued to staff remains the property of AudienceProject.
- ❏ Upon leaving employment or changing to a new role where the laptop or other mobile device is no longer required, the member of staff **must** return the laptop or mobile device to their manager or the AudienceProject Help Desk. The member of staff's line manager will ensure that the equipment is returned to the AudienceProject Help Desk.
- ❏ Before installing software onto mobile devices, staff members should contact the AudienceProject Help Desk for authorisation. Where possible, installations should be carried out by AudienceProject technical staff. When installing applications on mobile devices only official stores should be used e.g. App Store, Google Play.
- ❏ Use of unlicensed software is illegal and puts AudienceProject at significant legal risk.
- ❏ Users are specifically prohibited from changing security settings or amending configuration files on any laptop or mobile device issued to them. This includes disabling passwords, pin codes and any installed security programs (e.g. Anti-Virus applications).
- ❏ In the event that a laptop or other mobile device is stolen, the user must notify the police and / or any other appropriate authority. It is the user's responsibility to obtain a crime reference number and to inform both their manager and the AudienceProject Help Desk as soon as possible after the event to ensure a remote wipe and password rotation can be initiated.
- ❏ Loss of data or information caused by disregarding the recommendations made in this document shall be the sole responsibility of the user of the laptop or mobile device.

## Physical Security

Apart from the financial cost associated with replacing a stolen laptop or mobile device there are associated hidden costs. These include loss of productivity, data replacement, increased insurance premiums and so on. All AudienceProject laptop or mobile device users are therefore encouraged to take the following physical security measures to prevent the theft of laptops, other mobile devices and sensitive information.

- ❏ Laptops, tablets and mobile devices **must not** be left in full view in a vehicle even for a short period of time. Laptops, tablets and mobile devices must be locked in the boot.

- ❏ Laptops, tablets and mobile devices **must not** be left in a vehicle overnight, even in a locked boot.
- ❏ When leaving a laptop, tablet or mobile device unattended for an extended period of time, the laptop, tablet or mobile device **must** be locked in a drawer, a cupboard, or if possible, secured with a cable lock. It **must not** be left out at any site or at any other location or office over-night.
- ❏ Laptops, tablets or mobile devices **must never** be left unattended in public places even for a very short period of time.
- ❏ When travelling by air, laptops, tablets and mobile devices **must** always be carried in the cabin and never checked into the hold.

## Access control and Data protection

- ❏ All AudienceProject users **must** use a password or pin code in order to protect information held on a laptop or mobile device.
- ❏ All computer screen displays, including laptops, **must** be locked with the password protected screen saver when left unattended.
- ❏ Mail-, file- and password-services accessed on Laptops, tablets and other mobile devices **must** be protected by two-factor authorisation.
- ❏ When working in public places such as restaurants, hotel lobbies, on trains or aircraft, care should be taken to prevent others from being able to view potentially sensitive information. The use of Privacy Filters is recommended for these circumstances as these reduce the viewing angle of the screen and prevent casual observers from being able to see sensitive information on the screen. Loss of sensitive data or information could materially damage AudienceProject.
- ❏ When not connected to the network, Users should save all work related documents to the locally installed company cloud-drives. **Do not store files in local document folders!**
- ❏ Any changes made to files (or data) normally stored on the company's cloud-drives whilst not connected to the company network will automatically be synchronized with company network next time the device is connected to the Internet . This will reduce the risk of losing information following a physical failure of the device. Version control is automatically applied to any such documents.
- ❏ When travelling, do not use free WIFI networks for connecting your devices to the internet. Use only approved vendors and if needed, apply for a international 3LikeHome subscription which will allow you to utilize your mobile-subscription for data-roaming.

- ❏ When travelling, always connect through VPN connections to ensure communication is encrypted.

## Reporting the loss or theft of a Mobile Device

Any loss or theft of an AudienceProject supplied mobile device (laptop, tablet, mobile phone, external hard disk etc.) **must** be reported to the police and a crime incident / reference number obtained. This should be done immediately after the loss or theft has been discovered. Once the crime reference number has been obtained, the loss or theft **must** be reported to the AudienceProject Help Desk.If a mobile phone is lost or stolen, the sim card **must** be blocked immediately also outside working hours. AudienceProject will block the number and arrange for a replacement handset to be issued. This should be done before contacting the police or the AudienceProject Help Desk and will minimise potential costs associated with misuse.

## Do's and Don'ts

- ❏ **Do** create and use a password or pin code to prevent unauthorised access to the laptop, tablet or other mobile device. Use fingerprint scanners when available.
- ❏ **Do** turn your laptop, tablet or mobile device off and put it in an appropriate carrying case when travelling.
- ❏ **Do** keep all drinks and any other liquids away from your laptop, tablet or mobile device. Any spillage on the device can result in data loss and expensive repairs.
- ❏ **Do** avoid turning off your laptop when the hard disk light is on. This can result in data corruption and / or data loss.
- ❏ **Do** make sure that you always work with documents or data files in your AudienceProject Cloud Drive.
- ❏ **Do** report a loss or theft as soon as possible after the event.
- ❏ **Do** use a Privacy Filter if working in a public place (e.g. on a train, airplane or in a hotel lobby).
- ❏ **Don't** subject the laptop, tablet or mobile device to extreme temperature changes (ie don't use or store near radiators or fan heaters). Mobile devices are designed to work within a defined temperature range so exposing them to extreme temperatures (highs or lows) may cause the device to malfunction or behave unpredictably.
- ❏ **Don't** leave the laptop or other mobile device unattended. If you need to leave your desk, put the laptop, tablet or mobile device in a lockable drawer or take it with you. Lock your

office door. If you are travelling and cannot keep the laptop, tablet or mobile device with you when it is not in use, then where possible, place the laptop, tablet or mobile device in the Hotel safe, or at the very least lock it in your room.

- ❏ **Don't** use your laptop, tablet or mobile device for accessing sensitive AudienceProject related information in public places if there is a possibility that the information could be viewed by unauthorised individuals and hence lead to information theft.

## Violations and Penalties

Violation of this policy may result in disciplinary action.

# Email & internet usage policy and guideline

## Introduction

This policy sets out the obligations and expectations on employees of AudienceProject, including affiliates, contractors and temporary staff, 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.

## Authorisation

No person is allowed to use company IT facilities who has not previously been authorised to do so. Unauthorised access to IT facilities is prohibited and may result in either disciplinary action or criminal prosecution.

## Legislation

All users shall comply with the relevant legislation.

Any information which the company holds is potentially disclosable to a requester under one of these pieces of legislation. This includes emails too. Users need to be sure that they are not breaching any data protection when they write and send emails. This could include but is not limited to:

- ❏ Passing on personal information about an individual or third party without their consent.
- ❏ Keeping personal information longer than necessary.
- ❏ Sending personal information to a country outside the EU. Email should where possible be avoided when transmitting personal data about a third party. Any email containing personal information about an individual may be liable to disclosure to that individual under the Data Protection Act. This includes comment and opinion, as well as factual information. Therefore this should be borne in mind when writing emails, and when keeping them. Emails which do not contain personal information, but which contain other information, some of which might also be liable to disclosure.

## Responsibilities

All Users are expected to act in a manner that will not cause damage to IT facilities or disrupt IT services. Any accidental damage or disruption must be reported as soon as possible after the incident has occurred. Users are responsible for any IT activity which is initiated under their username.

Use of the company Internet

- ❏ Use of the Internet by employees is encouraged where such use is consistent with their work or with the goals and objectives of AudienceProject. Reasonable personal use is permissible subject to the following:
- ❏ Users 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.
- ❏ Users must not visit, view or download any material from an internet site which contains illegal or inappropriate material. This includes, but is not limited to, poronography (including child pornography), obscene matter, race hate material,violence condoning messages, criminal skills, terrorism, cults, gambling and illegal drugs.
- ❏ Users must not knowingly introduce any form of computer virus into the company's computer network.
- ❏ Personal use of the internet must not cause an increase for significant resource demand, e.g. storage, capacity, speed or degrade system performance.
- ❏ Users must not "hack into" unauthorised areas.
- ❏ Users 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.
- ❏ Users must not use the internet for personal financial gain.
- ❏ Users must not use the Internet for illegal or criminal activities, such as, but not limited to, software and music piracy, terrorism, fraud, or the sale of illegal drugs.
- ❏ Users must not use the internet to send offensive or harassing material to other users.

- Use of the internet for personal reasons (e.g. online banking, shopping, information surfing) must be limited, reasonable and not distract from work.
- Use of social networking sites such as, but not limited to, Facebook, LinkedIn, Youtube, Twitter, Bebo, Flickr, MySpace etc is allowable so long as it is reasonable, proportionate and does not interfere with work. Access other than for legitimate business, academic or study purposes, should be confined to breaks, lunch or other non-work or study periods, unless there is a specific work or study related need. In using social networking sites users should be mindful of the following:

    - Users should not post offensive and inappropriate pictures or comments, or anything that might cause embarrassment to the company, its employees, partners, clients etc. Users 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 in particular should avoid identifying themselves as working for the company unless they are representing it in some capacity. Where identification with the company is given (whether it be an employee or student), personal blogs or other personal posts should contain disclaimers making it clear that the opinions expressed are solely those of the author and do not represent the company's views.
    - Employees in particular should not give recommendations, endorsements or references for individuals, companies, partner organisations or products if they are identifying themselves with the company in any capacity.

Staff may face disciplinary action or other sanctions (see below) if they breach this policy and/or bring embarrassment on the company or bring it into disrepute. This applies whether use is made of the company's IT or their own.

## Use of Email

Emails sent or received on the email system form part of the official records of AudienceProject; they are not private property.

The company does not recognise any right of employees to impose restrictions on disclosure of emails within the company. Emails may be disclosed as part of legal proceedings (e.g. tribunals),

and as part of disciplinary proceedings. Users are responsible for all actions relating to their email account/account username and should therefore make every effort to ensure no other person has access to their account. Personal use of email is permitted so long as it does not detrimentally affect the wider responsibilities and duties of employees and students and subject to the following:

- ❏ Personal use of email must not disrupt the company's wider IT systems (e.g. the deliberate importation of any form of computer virus) or cause an increase for significant resource demand, e.g. storage, capacity, speed or degrade system performance.
- ❏ Personal use of email must not harm the company's reputation, bring it into disrepute, incur liability on the part of the company, or adversely impact on its image. • Seeking to gain access to restricted areas of the network or other "hacking activities" is strictly forbidden
- ❏ Email must not be used for the creation, retention or distribution of disruptive or offensive messages, images, materials or software that include offensive or abusive comments about ethnicity or nationality, gender, disabilities, age, sexual orientation, appearance, religious beliefs and practices, political beliefs or social background. Employees or students who receive emails with this content from other employees or students of the company should report the matter to their manager.
- ❏ Users must not send email messages that might reasonably be considered by recipients to be bullying, harassing, abusive, malicious, discriminatory, defamatory, and libellous or contain illegal or offensive material, or foul language.
- ❏ Users must not upload, download, use, retain, distribute, or disseminate any images, text, materials, or software which might reasonably be considered indecent, obscene, pornographic, or illegal.
- ❏ Users must not engage in any activity that is likely to

    - ❏ Corrupt or destroy other users' data or disrupt the work of other users or staff effort or company resources, or engage in activities that serve to deny service to other users
    - ❏ Be outside of the scope of normal work-related duties or studies – for example, unauthorised selling/advertising of goods and services

- ❏ Affect or have the potential to affect the performance of damage or overload AudienceProject's system, network, and/or external communications in any way
- ❏ Be a breach of copyright or license provision with respect to both programs and data, including intellectual property rights

- ❏ Use of the company's email system for personal emails is permitted but must be reasonable and limited and must not interfere with work. Non-work or study-related email should be saved in a separate folder from work or study-related email.
- ❏ Staff who receive improper email from individuals inside or outside the company, should discuss the matter in the first with their manager.

## Good practice

The company has good practice guidelines for dealing with email and post when staff are out of the office for longer than three days. When activating the "out of office" facility messages should name an alternative member of staff for correspondents to contact if necessary. This will ensure that any important requests are picked up and dealt with within required timescales.

During periods of absence when highly important emails are anticipated, the employee (or manager) should make arrangements for notification and access by another appropriate member of staff.

Where sensitive and confidential information needs to be sent via email for practical reasons, please be aware that email is essentially a non-confidential means of communication. Emails can easily be forwarded or archived without the original sender's knowledge. They may be read by persons other than those they are intended for.

Sensitive and confidential data should therefore not be sent by e-mail. If a client need to provide the employee with sensible data AudienceProject should provide the client with a secure upload location. Please contact AudienceProject Helpdesk for instructions on how to create secure file requests.

Users must exercise due care when writing emails to avoid being rude or unnecessarily terse. Emails sent from the AudienceProject may be interpreted by others as official statements. Users are responsible for ensuring that their content and tone is appropriate. Emails often need to be as formal and businesslike as other forms of written correspondence.

Users should delete all personal emails and attachments when they have been read and should also delete all unsolicited junk mail. In the process of archiving emails, users should ensure inappropriate material is not archived.

All outgoing mail is filtered to detect and prevent a virus infection being sent from the AudienceProject's equipment. The company reserves the right to introduce company-wide content checking if this is deemed appropriate.

Caution should be used when opening any attachments or emails from unknown senders. Users must best endeavour to ensure that any file downloaded from the internet is done so from a reliable source. It is a disciplinary offence to disable the virus checker. Any concerns about external emails, including files containing attachments, should be discussed with the Help Desk.

## Legitimate access to prohibited material

There may be circumstances where Users feels that the nature of their work or studies means that they are required to access or use material prohibited under this policy. If so, this should be discussed with their manager in advance. The company is legally responsible for the content and nature of all materials stored on/accessed from its network and therefore Users must understand that the company will never sanction the committal of acts that are illegal, including the viewing of child pornography.

## Monitoring

All resources of the AudienceProject, including computers, email and software are provided for legitimate use. If there are occasions where it is deemed necessary to examine data beyond that of the normal business activity of the AudienceProject then, at any time and without prior notice, the company maintains the right to examine any systems and inspect and review all data recorded in those systems. This will be undertaken by authorised staff. Any information stored on a computer, whether the information is contained on a hard drive, computer disk or in any other manner may

be subject to scrutiny by the AudienceProject. This examination helps ensure compliance with internal policies and the law. It supports the performance of internal investigations and assists in the management of information systems.

AudienceProject subscribes to a 3rd party checking service so that all incoming email is filtered for the protection of the AudienceProject from email virus infection and unsolicited junk mail (e.g. spam).

AudienceProject performs extensive logging of all user driven actions on our internal applications, software and network.

## Social Media Guidelines

Online social media sites such as Facebook, LinkedIn, Myspace, Twitter etc, 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. Nothing that they say or infer should embarrass the company, damage its interests or reflect negatively on it.

Employees must be mindful of how they represent themselves on social media sites as the lines between public and private, personal and professional expression are easily blurred. Accurate information is important, both about oneself and the company. Employees will be held accountable for anything they say which directly or by inference is relevant to the company.

The following guidelines are designed to help employees to use social media sites in ways that are within both the letter and spirit of the law and which do not embarrass the company. They supplement the guidance contained in the main Email and Internet Usage policy.

### Use of Social Networking Sites

An employee social media profile and comments are unlikely to be of interest to the company where no direct or indirect reference is made to it. However, it may concern the company if the nature of a communication is controversial, provocative and defamatory and the identity of the individual and their association with the AudienceProject can be deduced. Comments that

undermine the professional credibility and integrity of employees will be of concern to the AudienceProject.

When discussing issues directly or indirectly connected with the AudienceProject, it is important to be accurate and to correct factual errors and misleading comments as soon as they become known.

Employees must not disclose confidential or sensitive information about AudienceProject. They alone are responsible for respecting copyright, data protection and financial disclosure laws. They are also responsible for understanding and agreeing a site's terms of reference.

Under no circumstances should sites be used to verbally abuse, ridicule, humiliate or make insinuations against employees, clients and other individuals. Employees should be mindful of the tone they employ in all their communications and postings. Privacy and individual feelings should be respected at all times. Do not allow inferences to be drawn that might identify an individual or organisation and which might cause embarrassment or damage to them. Defamation can lead to claims against employees and the company.

If an individual is approached by a social media contact about content on their site relating to the AudienceProject, they should bring this to the attention of their line manager before they respond.

## Improper use

The AudienceProject has no wish to stifle responsible discussion about itself. However, instances where the AudienceProject is brought into disrepute may constitute misconduct or gross misconduct and if so will be investigated under the Disciplinary Procedure.

# The Guide to Data Protection

Research data containing 'personal data' will be subject to the data protection law. The law places obligations on you as a researcher. Details of particular circumstances can make a major difference, so conclusions reached in an individual case may well differ from those suggested here.

This guide does not constitute, and should not be construed as, legal advice.

## Introduction

The data protection laws regulates the use of information that relates to an identifiable living individual, as well as information which, when combined with other data accessible to the researchers, would permit the individual's identification (personal data). It places obligations on those who are responsible for determining the purposes for which the personal data is processed (data controllers), and gives rights to those who are the subject of that data (data subjects). Processing of personal data for research purposes falls under the general provisions of the law, but some specific research-related exemptions are provided.

We assume that you are an employee who works for, or with AudienceProject, and you are concerned about the application of the data protection legislation to the collection, storage, use transfer and disposal of your research data, including requests for access to that data by data subjects (subject access requests) and third parties.

Remember, this guide is a simply guidance aiming to help you have a better-informed discussion with your clients, or to consider steps you might take in advance.

## Data subjects

A data subject is simply an individual who is the subject of personal data. Thus, from the time of their birth to the time of their death, a person will be a 'data subject' where another party is collecting personal data about them. Whether a person is capable of exercising their rights as a data subject is another issue.

For example, in the UK the DPA 1998 has no minimum age requirement. Children can thus exercise their DP rights provided they are capable of understanding the nature of those rights. How you handle DP issues in relation to children involved in research projects requires sensitivity to the point at which a child is mature enough to make their own decisions, and must respect those, including where a child revokes a consent made on their behalf earlier by a parent or guardian.

Equally elderly and vulnerable data subjects may (or may not) wish a third party to exercise their rights for them – it is up to the third party to provide evidence of their right to do so. Deceased persons are not data subjects, as personal data refers to living individuals. However, commitments made to data subjects, e.g. that their identity will not be disclosed, may remain enforceable by their estate after they have died.

From a related FoI perspective, the exemption for personal data in the Freedom of Information Act ceases on death of the data subject (in Scotland there is a 100 year FoI exemption for a deceased person's medical records), but disclosure of, or access to, the deceased person's personal data will require consideration of third party personal data, e.g. that of relatives, and of any duty of confidence between researcher and deceased.

You may also need to consider whether personal data that was accessible to you by virtue of consent of the data subject will remain accessible after their death, if their personal representatives refuse access, or there is no personal representative to give permission: e.g. medical records.

## The rights of data subjects

Data subjects have a variety of rights with regard personal data about them held by data controllers. Failure to respect these rights can result in civil or criminal actions against the data controller. Most data subject rights are linked to, and/or depend for their usefulness upon, the availability of an effective right of subject access. Subject access means that a data subject is entitled to be told by a data controller whether personal data about them is being processed by, or on behalf of, that data controller, and to be given access to a copy of that data.

The rights include the ability to:

- ❏ Make subject access requests
- ❏ Prevent processing likely to cause damage or distress
- ❏ Prevent processing for direct marketing purposes
- ❏ Take action for compensation if they suffer damage caused by breach of the Act
- ❏ Take action to rectify, block, erase or destroy inaccurate data
- ❏ Request the Information Commissioner to assess whether the Act has been breached

In principle, these rights apply to personal data collected for research purposes. However, research data can be exempted from certain of these rights.

### Requests to delete personal data used in research

A  data subject may write to you and require that you not process, or cease processing, their personal data because it is causing, or is likely to cause unwarranted and substantial damage or distress, to them or to another person. In such circumstances, you must give notice within 21 days of receipt that you will comply with the notice or provide reasons why you believe the request to be unjustified and whether you intend to refuse to comply or comply only in part with the request. The data subject may challenge any refusal in court.

## Personal data

'Personal data' means information that relates to an identifiable living individual, as well as information which, when combined with other data accessible to the researchers, would permit the individual's identification.

This includes any expression of opinion about the individual and any indication of the intentions of the data controller, or any other person, in respect of the individual. While for many types of research it will be obvious when you are processing personal data.

Further issues may arise in specialised areas of research, for example if you are researching in large data sets concerning human subjects. 'Big data' research suggests that in certain

circumstances processing of data which appears on its face to be anonymous may allow researchers (and third parties with access to resulting research datasets) to identify individuals through data 'triangulation' and reconciliation of multiple sources. When developing such research (e.g. text and data mining projects), it is advisable to consider the risk of de-anonymisation, the impact that this might have on individuals, and how possible negative impacts might be prevented or ameliorated.

## Sensitive personal data

There exist a distinction between 'personal data' and 'sensitive personal data'. Processing of 'sensitive personal data' is subject to more stringent rules and generally requires more careful consideration. Sensitive personal data is defined as personal data relating to the data subject's:

- ❏ Racial or ethnic origin
- ❏ Political opinions
- ❏ Religious beliefs or other beliefs of a similar nature
- ❏ Membership of a trade union
- ❏ Physical or mental health or condition
- ❏ Sexual life
- ❏ Commission or alleged commission of any offence
- ❏ Involvement in criminal proceedings for any offence or alleged offence committed by them, including outcomes such as judgement and sentencing.

AudienceProject does not allow the collection and use of sensitive personal data on AudienceReport, UserReport and AudienceData unless it is part of an pre-approval legal research project undertaking in collaboration with universities or other research institutions. Such projects must always be pre-approved by management.

If you intend to process sensitive personal data in the course of your research, or there is a possibility that sensitive personal data may be processed, this will impact upon the conditions you will need to satisfy to carry out that processing lawfully, the justifications you may need to provide

to your research ethics committee (REC), and the uses to which the research data and research outputs can be put.

It should be noted that the Act does not consider the context of the data processed. For example, if you are interviewing research participants in government about the role of trade unions in ensuring fairness for people with disabilities, if a participant has a disability or is a trade union member, and this is recorded, then the Act applies, eg "Mr X, Deputy Chair of the Print Workers Union's Disability Rights Committee", or "Ms Y, Minister for Trade who has [particular disability].

It does not matter that the interviewees occupy public positions/roles because of disability or union membership. Nor does it matter that the focus of the interviews is an official process. The default position is that the data is 'sensitive personal data': the Act and secondary legislation then provide conditions under which it is permitted to process that data.

## Anonymous data

Data which cannot be linked to an identifiable living individual is not personal data and thus in principle falls outside the DP regime. However, until data is anonymised, it will be considered ‘personal data’.

Additionally, certain types of research (eg data mining and matching) may result in anonymous data becoming linked or re-linked to an identifiable data subject. Risks relating to the possibility of de-anonymisation should thus be considered where appropriate.

### The difference between anonymous and pseudonymous data

The issue of anonymisation is a complex one. Technically, data is only anonymised when an individual can no longer be identified from it. Thus a dataset that has been ‘link-coded’, with names and other key identifiers removed, but which is linked to a separate file held by, or accessible to, the researcher which enables individual research subjects to be identified (including, potentially, consent forms) is not anonymised – such a dataset would usually be considered to be ‘pseudonymised’. Both raw datasets containing names and other key identifiers, and pseudonymised datasets capable of linkage to identifying data held by the data controller, will be subject to the regulation regarding personal data.

A key principle of data protection is ‘data minimisation’, ie if data is not collected, the risk of its future misuse is automatically reduced. In a system context, you might consider for example, whether satisfactory outcomes can be achieved without collection of personal data or with only minimal collection of personal data: e.g. your work  may not require a data subject’s date of birth, just their age range, or just the first part of their postcode rather than their full address.

There may be good reasons why a dataset containing personal data is not fully anonymised e.g. where researchers wish to undertake long term studies with the same research subjects, or where anonymity would prevent other researchers from testing the validity of the data.

Additionally, fully anonymising data may be difficult to achieve with certain types of dataset, for example if the research context is such that even without obvious identifiers like a name or address, an individual may still be identifiable to researchers from the data processed, or in combination with other data that they hold; or identifiable to third parties from the data processed and information or knowledge already available to the public.
In such cases, you must ensure that the data is processed in accordance with the law.

## How to effectively anonymize research data

It is useful to think about the issue of anonymisation in terms of both the original raw dataset, and in aggregated reports  drawing upon information from the original dataset.
In datasets held by you, data will be effectively anonymised if all data that would allow you to identify an individual data subject has been destroyed: if you can identify them the data is personal data.

In report outputs that we publish, data will be effectively anonymised if, on the balance of probabilities, individuals cannot be identified by third parties cross-referencing the ‘anonymised’ data with information or knowledge already available to the public. The data disclosed will not be personal data.

## Data provided by a third party

If you are supplied with personal data by a third party, it is not unusual to find that they are unclear on your respective positions under the law. In such circumstances you may be asked to sign a 'data processing agreement', which states that the third party is the data controller and you are a 'data processor'.

In fact, unless you are processing the personal data on behalf of that third party, you cannot legally be a 'data processor' – if you are determining the purpose for which the data is processed, i.e. research which is not commissioned by the third party, then you are a data controller as well.

If you and the third party are processing the data for different purposes, you are 'data controllers in common', and you are both responsible for your respective processing. You cannot contract out this responsibility under the law.

It is in the best interests of AudienceProject  that the relationship between you and the original data controller is accurately characterised and an appropriate agreement agreed between the parties. Failure to do so may leave both you and the supplier of data misinformed about your respective liabilities in the event of a breach of the law, and lead to inadequate analysis and audit.

Any such agreements should automatically be referred to your DPO. You should not sign any DP agreement yourself; it should be signed by the properly authorised person in AudienceProject.

Regardless of the documentation, in such circumstances you should assume that, in the event of a breach both parties maybe deemed to be data controllers. As such, it is sensible to operate on the assumption that AP will be liable if there is a breach of the law, and organise your project so as to be able to demonstrate that you have acted as a responsible data controller.

# Processing data

Processing is defined as 'obtaining, recording or holding the data or carrying out any operation or set of operations on the data'.

In practice, if you collect, record, organise, store, adapt/alter, retrieve, consult and use, disclose by transmission/dissemination, align/combine, block, erase or destroy personal data, you are processing it.

The breadth of the definition means that the full lifecycle of personal data used for research purposes, from its collection, through to either its destruction or anonymisation, is considered 'processing' for the purposes of the law, whether on paper or in electronic form.

## Processing personal data

You must process personal data in accordance with the law. The eight 'data protection principles' are the basic rules which provide a framework for compliance, they are:

1. Personal data shall be processed fairly and lawfully
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed
4. Personal data shall be accurate and, where necessary, kept up to date
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes
6. Personal data shall be processed in accordance with the rights of data subjects under this Act
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data
8. Personal data shall not be transferred to a country or territory outside the EU unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

## Fair and lawful processing

For you to process personal data fairly and lawfully, issues such as how the data is collected (ie where data subjects deceived or misled as to the purpose of the processing), and the information you will provide to data subjects (eg who is the data controller, the purpose for which it is to be processed, any information especially relevant to the particular processing and third parties to whom the data may be supplied) must be considered.

Additionally, the guidelines sets out six conditions for processing of personal data: you must meet at least one of these before the processing can be considered fair and lawful. Two of those conditions are usually appropriate for researchers:

- ❏ The data subject has given their consent to the processing
- ❏ The processing is necessary for the purposes of legitimate interests pursued by the data controller or by third parties to whom the data are disclosed, unless it would prejudice the rights and freedoms or legitimate interests of the data subject.

For most research projects involving personal data, consent would be the normal condition under which empirical research is conducted, but if the nature of your research makes it impracticable or otherwise undesirable to attempt to seek/obtain such consent, you could consider establishing a reasoned case that the processing is necessary for the purpose of a legitimate interest, and would not unfairly damage the interests of the data subjects. This would provide an alternative condition for the conduct of research.

The ICO suggests that where a condition specifies that processing must be necessary for the purpose stated; you should be able to show that it would not be possible to achieve your purpose(s) with a reasonable degree of ease without the processing of personal data. Where you could achieve, with a reasonable degree of ease, a purpose using data from which the personal identifiers have been removed, that would be the more appropriate course of action.

## Telling data subjects the reasons for collecting their data

When collecting data from research subjects it will normally be expected for you to tell people who you are, the name of the company that will hold the data, what you are going to do with their information and who it will be shared with.

However, you may wish to tell them more than this, eg information about their rights of access to their personal data, or your arrangements for keeping their data secure. If you think the person would be surprised by a potential use of their personal data by you, you should make a point of explaining it.

Providing such information will normally be expected as part of the process of obtaining 'informed consent' for ethical purposes: it will also ensure that information is collected and used fairly for data protection purposes.

It is good practice to try to put yourself in the position of the people you're collecting information about, eg information notices should be written taking into account the likely language skills and reading levels of the average member of the research subject cohort, and should not resort to legal or academic jargon.

Simply telling most research subjects that "your data will be processed in conformity with the law of XYZ" is pointless. Unless they are data protection experts, research subjects will often have little idea what this means either in terms of their rights or of your obligations. That is inadequate for both ethical and legal purposes.

It is important that prospective participants understand the information being conveyed to them in order to obtain their consent. Materials you produce for the purpose of informing research participants should be appropriately drawn up for those who have poor, or non-existent, levels of literacy, or for whom English is not their native language.

Based on your assessment of the characteristics of their research participants, you should provide an assessment of whether particular difficulties or risks may arise in the provision of appropriate information about the research, and if so, how you intend to convey your information to facilitate

understanding, eg written documentation might be supplemented with audio and/or visual aids, language barriers might be addressed by the use of an intermediary who has the necessary language skills to ensure effective communication etc.

### Requirements for consent

As we've already noted, consent is not the only DP condition under which personal data can be processed, so if you can satisfy another condition applicable to research, this is not a barrier to your research. However, prior informed consent is seen as a key component of most human subject research.

## Obligation to check that third party data was obtained in an appropriate manner

This will depend on issues such as: where and when the data was collected, what information was provided to data subjects, the expectations of data subjects about how their data would be used, the potential impact of reuse on data subjects' rights and freedoms, the importance of the data to the research and the importance of the research to the public interest.
Whether you can use the data will depend not just upon the position at law, but also upon your ethical viewpoint. For example, if you receive recent data from an overseas institution where you know that written consent was not obtained and/or the collector was in a position of authority relative to the participants at the time, regardless of the DP position, it is unlikely that AudienceProject would consider the data collection to be ethical.

Where you reuse data collected by a third party for research purposes you still have obligations to data subjects including the primary obligation to process their data 'fairly'.

If you know the data was not obtained fairly, then by definition you are not in conformity with the DP Principles. It would be reasonable to expect you to have engaged in at least some investigation of the circumstances in which the personal data was obtained.

Where you are using historical personal data collected at a time prior to DP legislation and/or when ethical standards for collection of research data were different, you should still decide prior

to processing whether research use of the data is fair, whether data subjects could reasonably be informed of the reuse of their data, and what risks the proposed reuse poses for data subjects. It is good practice to keep a record of your decisions and the reasons for them.

Where you are receiving personal data as part of a research consortium, it will be expected that you have ensured that your partners will be collecting the data in conformity with both relevant DP law and ethical practice.

## Recording online conversations and actions

If you're lurking in an internet chat room, do you have to let all the participants know you're recording their conversations? Disappointingly for those seeking a definitive answer, both legally and ethically the answer is 'it depends on the context'. The internet is increasingly a site for research, and studies of and on the internet cut across all academic disciplines. Indeed, the term 'internet research' covers a wide range of technologies, devices, capacities, uses, and social spaces.

Examples of internet research with DP implications include:

- Collecting data or information, eg through online interviews, surveys, archiving, or automated means of data scraping
- Studying how people use and access the internet, eg through collecting and observing activities or participating on social network sites, listservs, web sites, blogs, games, virtual worlds, or other online environments or contexts
- Using visual and textual analysis, semiotic analysis, content analysis, or other methods of analysis to study the web and/or internet-facilitated images, writings, and media forms.

The temptation with much internet data is to argue 'But the data is already public…', this overlooks both the legal requirement that personal data must be processed not just 'lawfully' but also 'fairly', and the ethical principle that, as far as possible, researchers should avoid causing harm to their research subjects.

You must consider the specifics of your project, including its risks to data subjects and its social benefits, in addition to considering the practicality of communicating information about your research to the subjects of that research for DP purposes.

# Processing sensitive personal data

We have already noted that there is  a distinction between 'personal data' and 'sensitive personal data'. You may process 'sensitive personal data' if you meet one of the conditions for processing personal data and one of 10 additional conditions.

Four of these additional conditions are likely to apply to researchers:

- ❏ The data subject has given their explicit consent to the processing of the personal data
- ❏ The personal data has been made public as a result of steps deliberately taken by the data subject
- ❏ Use of the data is necessary for medical research undertaken by a health professional, or a person owing an equivalent duty of confidentiality
- ❏ Use of the data is in the substantial public interest, necessary for research purposes and neither supports measures or decisions with respect to any particular individual, nor is likely to cause substantial damage or substantial distress to any person.

The first condition appears to be the normal basis on which non-medical research involving the processing of sensitive personal data proceeds. There is no requirement that 'explicit consent' need be in written or recorded form (although written or recorded consent will provide the best evidence that consent was actually given explicitly).
It may not always be practicable or possible to obtain explicit consent for the processing of sensitive personal data (for example, a large-scale study of case files held in court archives) in which case the recourse to the fourth condition may be appropriate. If you can demonstrate that your methodology and use of the data meets its requirements, then you may process the sensitive personal data.

# Special rules for processing personal data as research data

There are certain exemptions for the use of personal data for 'research purposes,' including statistical or historical purposes. If you can show that your processing for research purposes is not to be used to support measures or decisions targeted at particular individuals, and will not cause substantial distress or damage to a data subject, you can:

- ❏ Process personal data for purposes other than for which they were originally obtained (permitting the secondary analysis of datasets, for example) - exemption from Principle 2
- ❏ Effectively hold personal data indefinitely (permitting long-term archiving of research data, for example) – exemption from Principle 5.

Additionally, where the research results (in articles, research reports, dissertations etc.), or any resulting statistics, are effectively anonymised, you can claim an exemption from the data subject's right of access to their personal data held in your research dataset – partial exemption from Principle 6.

As a result, if your research meets the requirements of an exemption, your processing and archiving of research data is made simpler. However, there is no blanket exemption from the Data Protection Principles for research purposes. Thus, for example:

- You should inform data subjects of any new data processing purposes, the identity of the data controller, and any disclosures that may be made – Principle 1
- Data subjects must be able to meaningfully exercise their right to object to your data processing because it would cause/has caused them significant damage or distress – Principle 6
- You must ensure appropriate security of the data, including higher levels of security for sensitive data, as appropriate – Principle 7.

To take advantage of the exemptions, you should be able to:

- Identify the condition for processing you intend to use
- Show, as appropriate, that you have made an objective assessment that your new processing is both necessary for your research and proportionate to your purpose
- Demonstrate your research meets the exemption criteria.

Where you are processing archived data which has been fully anonymized (eg by destruction of link codes, or removal of identifying factors) this will not fall within the scope of DP.

## Informing data subjects when reusing data sets

Where you wish to carry out research on an existing dataset containing personal data, notification of data subjects may be avoided if:

- ❑ The data was obtained directly from the data subject, but your new processing purpose was not known at the time, and you can make a plausible case that it is now 'not practicable' to provide the relevant information;
- ❑ You have obtained the data from a third party; and
- ❑ Provision of information to data subjects would involve disproportionate effort; and
- ❑ The data subject has made no prior demand in writing for information about the processing; OR if they have made a demand in writing, you do not have sufficient information about them to determine whether you are processing personal data about them, and you notify them in writing that you cannot provide the required information because of your inability to make that determination, with reasons for that inability;and
- ❑ You record the reasons for believing that 'disproportionate effort' applies.

Assessing practicality and disproportionate effort should include factors such as cost, time and ease of provision of information weighed against benefit/risk to the individual. Where data is obtained from elsewhere, particularly if the data is not recent, then it may be impossible, or at least disproportionately difficult, to inform the data subjects.

# Security of research data

Research data may be collected in many ways, eg paper questionnaires, tape or digital recordings of interviews and focus groups, online surveys; and stored in a range of formats eg handwritten notes, analogue and digital recordings, computer files. Each mechanism for collecting and storing data poses particular issues with regard to security against unauthorised access and use, prevention of accidental loss or damage, and eventual disposal.
As data controller you are responsible for ensuring that personal data is held appropriately, taking into account the nature of the data, e.g. if it is sensitive personal data, it may justify requiring greater protective measures, eg access controls, encryption and audited disposal.

As a researcher, it is your role to ensure that everyone is adequately informed about the nature of your research data, the scale of data to be collected, how you intend to protect data gathered during field work, whether and when data will be pseudonymised or anonymised, how long it needs to be retained etc.

- Identify the means and mechanisms you will employ for collecting, processing and storing your research data
- Demonstrate your understanding of the particular legal and ethical risks pertaining to those means and mechanisms, e.g. use of internet based tools
- Provide details of measures taken to secure research data e.g. physical security of equipment and notes (at work, at home and in the field), and digital security mechanisms, such as system, program and file passwording and use of encryption.

Failure to address security issues appropriately, particularly where data is unlawfully disclosed, may result in breaches of AudienceProject's ethics rules, as well as your workplace being audited or fined.

# Appropriate technical and organisational measures

What are considered to be ‘appropriate technical and organisational measures’ will vary depending upon the personal data processed and as the ‘state of the art’ in technical security measures and data management protocols changes over time. As such, the answer to this question is not fixed.

For example: as the cost of encryption falls, its availability in recording and storage devices becomes standard, and its use becomes simpler, there will be an expectation not just that it is used for particularly risky or sensitive personal data, but that it is used ubiquitously to protect all personal data. If encryption of even basic personal data becomes the norm, a researcher’s failure to use it will increasingly be seen as bad data management practice, even if the risk that inadvertent disclosure presents to data subjects is relatively low.

# Storing data in the cloud

Cloud computing is a term that encompasses a wide range of use cases and implementation models. In essence, a computing ‘cloud’ is a large shared pool of computing resources including data storage.
It is assumed here that the question refers to cloud storage solutions run in large data centres accessed by customers over the public internet (often called ‘the public cloud'). Advantages of public cloud storage are low cost, rapid scalability, and easy accessibility.
Questions that should be asked about personal data storage in the cloud from a data protection perspective are:

- ❏ What is the nature of the personal data to be stored in the cloud?
- ❏ What measures are there to prevent loss of, or damage to, the data?
- ❏ Is the data secured against unauthorised access and are all accesses audited?
- ❏ Is the data encrypted at the end-user’s location or at the cloud service provider?
- ❏ Can data be processed in specific geographic locations?
- ❏ Can the data be easily extracted from the cloud service?

- ❏ Can the data be verifiably deleted from the cloud service?
- ❏ Does the cloud service conform to recognised data management/security standards, e.g. ISO 27001 or 27002?
- ❏ Whose law applies to the cloud service provider?
- ❏ Whose law applies to the contract between you and the cloud service provider?

If you cannot answer questions like these you should think very carefully about whether the cloud service you are seeking to use can meet your requirement to utilise appropriate technical and organisational measures to protect the personal data you are processing.

## Web surveys

Web surveys are an important tool of conducting empirical research online. If used with appropriate attention to the type of personal data being collected and with a clear understanding on your part of the possible risks, their use should be unobjectionable.

A key thing to remember is that potential data protection breaches are often not caused by the technology employed, but are down to researchers not fully understanding the risks of the technologies they are using, or engaging in research practices which compromise the security of those services.

The following examples demonstrate how data protection law breaches might occur:
A researcher posts a link to a web-based questionnaire on an e-mail list, asking for responses. Her website contains a web page providing a detailed outline of the research and describing how the data collected will be used.

- ❏ The link in the e-mail goes directly to the questionnaire, inadvertently bypassing the web page of information, meaning respondents never see it. At the start of the questionnaire, where consent to use their personal data is requested, respondents have not been given adequate information to provide informed consent

- ❏ The link in the e-mail goes to the start of the questionnaire, which contains a further link to the web page of information. However, that link is at the bottom of the questionnaire web page and respondents may not scroll down far enough to see it.

Another researcher collects sensitive personal data from respondents using a web-based questionnaire. He states that responses will be confidential and held securely.

- A respondent's computer caches the questionnaire pages, including responses, leaving them accessible to other users of that computer

- The link between respondents' computers and the computer hosting the questionnaire is unencrypted, and communications between them can be intercepted

- The web survey software does not compartmentalise questionnaires. Any researcher in the researcher's department, including research students, can view both questionnaire and responses

# Collaboration

## Sharing data outside of the EU

As a rule of thumb AP are not allowed to transfer personal data that we hold outside the EU unless the country or territory to which the data is to be sent ensures an ‘adequate level of personal data protection’ for data subjects.

All European Economic Area countries (the EU Member States, plus Iceland, Liechtenstein and Norway) are assumed to have an adequate level of protection. There are thus no legal restrictions on your transfer of personal data to other EEA countries, provided you have informed research subjects that their personal data may be shared with these partners.

However, always seek advice on an appropriate formal data sharing/data controller agreements before any commitments are made.

## Sharing data outside of the EEA

The European Union only considers a few countries outside the EEA to have ‘adequate protection’. These are Andorra, Argentina, Australia, Switzerland, Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, and Uruguay.

Where you intend to share data containing personal data with partners outside the EEA, this may be possible, provided you have informed research subjects that their personal data may be shared with these institutions, if:

- The country to which the data will be sent has been accepted as ensuring an 'adequate level of protection' by the EU Commission; or
- Your department has undertaken an adequacy assessment to determine whether there is adequate protection for the rights of individuals, in all the circumstances of the transfer; or
- The data subjects have given their informed consent to the transfer; or

- The transfer is made on contractual terms of a kind approved by management as ensuring adequate safeguards for the rights and freedoms of data subjects.

Determining which of the possibilities apply to your research will require an expert assessment, and thus potential transfers of personal data outside the EEA should always be referred to your superior well in advance of any transfers taking place.

## Collecting personal data from research subjects outside of the EU

Personal data that is processed in the EU by a data controller, regardless of where it is collected and the nationality of the data subjects, will fall under EU regulations, and foreign data subjects are entitled to exercise the same rights over their personal data as EU citizens.
For processing to be fair you should provide the research subjects with information about your project in a form that is comprehensible to them, this may involve translating the information into other languages.

If you are collecting personal data in other countries, you should also be aware of any national legislation that applies to your processing, including the international transfer of that data to the EU e.g. if you were collecting data from research subjects in Hong Kong, it will have its own data protection laws.

It is good practice to make clear in the information you provide to overseas research subjects that their data will be transferred to, and processed in, the EU, and to ensure that you have their consent, ideally in writing or some other permanent form, to such a transfer. International data is usually subject to heightened scrutiny by RECs due to a broader range of ethical risks, including possible data protection complications.

# Archiving data

## Anonymising personal data before archiving

Long term storage usually requires that a data is anonymised before it is archived for long periods. It can be difficult to honour SAR requests on archived data due to the inherent inert state of archived data.

In each case it should be evaluated if there will be any ill effects on the potential revisiting or reuse of the results and research? And if there is special arrangements with the Client regarding retention of data for auditing purposes.

## Disposing of data which does not require archiving

If you have personal data which is not required to be formally archived, it should be anonymised or destroyed when it is no longer required for the purpose for which it was collected. The proper disposal of data is vital for compliance with data protection rules, and for maintaining guarantees of confidentiality and anonymity for research participants.

As a basic standard, when no longer required:

- ❏ Data held in paper form should be disposed of by shredding. Most institutions will have appropriate shredding systems in place for disposal of confidential data
- ❏ Data held in digital form should, wherever possible, be destroyed by multiple over-writing. Simply using the 'delete' function on a computer (even if you empty the 'recycling bin'), or even doing a simple disk reformat, will not usually erase data permanently
- ❏ Data held in non-rewritable digital media, such as CD-Roms, DVDs and Blu-ray Discs, should be disposed of by destruction of the physical media (eg by shredding).

Disposal of higher risk data, such as 'sensitive personal data', may require greater security measures, including third party audit of equipment and media to ensure data is effectively deleted.

Care should be taken to examine and erase research data from all digital equipment, including voice recorders, laptops, cameras, etc. This is particularly important where equipment is to be disposed of to third parties (eg by donation or resale). AudienceProject will routinely remove and securely dispose of internal storage media, such as computer hard disks, prior to disposal of equipment.

# Subject access requests (SARs)

A subject access request (SAR) is a written request by or on behalf of a data subject for information about whether data is held by a data controller about them, what the data is, why it is being processed, and to whom it has been or may be given.

Members of the public may confuse FoI requests and data protection SARs, but if it is clear that the data subject is asking for their personal data than a request should be treated as a SAR. A SAR does have to be in writing, but does not have to be hard copy, e.g. an e-mail may suffice.

There are circumstances where it is legitimate for a third party to make a SAR on behalf of a data subject.

## What to do if you think you have received a SAR

Contact AudienceProject's data privacy officer.

## What to do if your data is subject to a SAR

We are required to confirm whether or not it holds personal data about the data subject, and to supply the information, or a refusal notice, within 40 calendar days from receipt of the request. Because of the time limit, all requests must be forwarded to our DPO immediately. The DPO will work with you to determine:

- ❏ Whether you are in fact holding personal data relating to the requester
- ❏ Whether you are required to provide the data, or if there is a relevant exemption
- ❏ If personal data is to be provided, whether that data can be released 'as is', or whether some of it needs to be redacted, explained, or placed in a particular format.

## Providing data to the data subject

While a requester is entitled to see their own personal data: this is not a right to see copies of documents that contain their personal data, although providing original documents may be the easiest way for you to provide the relevant information, unless significant redaction is required. Personal data has to be supplied in permanent form, unless the data subject agrees otherwise. If the data subject asks for the information in a particular form, and you can reasonably easily supply it to your DP practitioner in that form, you should do so, as this will help your department meet its duty to be helpful to requesters.

You should remember that some digital data formats can contain information that is not visible but can still be extracted. In order to ensure that your institution does not supply information inadvertently that it should not, it will be helpful for you to advise our DPO on the formats you have used, and any technical issues you are aware of relevant to those formats.
Your department must provide information to a data subject in 'intelligible form', ie the information you provide to your DPO should be comprehensible to the average person, and this may require you to provide an explanation of project abbreviations or data held in coded form.

## SAR exemptions

There are limited grounds for not providing a requester with their personal data. The two primary grounds that would apply to research data are:

- ❏ The personal data is exempt as research data from subject access
- ❏ It would involve disclosing information about another individual.

Whatever your reasons for not wishing to provide data, we strongly recommend that our DPO take over correspondence with the requester.

## Information that may identify other individuals

AudienceProject does not have to comply with a SAR if this means disclosing information about another individual who can be identified from that information, unless:

- ❏ The other individual has consented to the disclosure; or
- ❏ It is reasonable in the context to disclose without their consent.

This decision will involve balancing the data subject's right of access against the other individual's rights in respect of their own personal data. It is strongly advised that this determination should be left to the DPO.

## Redaction

Redaction term refers to the practice of removing some information from a document while leaving other information intact.

It is typically used to remove exempt information, eg in the case of a SAR, the personal data of a third party. Because redactions must be done carefully, it is strongly advised that they should be left to the DPO.

## Someone other than the data subject requesting access

There are circumstances where a third party can make a SAR on behalf of a data subject e.g. where a third party can provide you with evidence of that authority. However, under normal circumstances, you should not make the personal data available to third parties outside those you have already identified to research subjects as having access to the personal data. If you are relying on consent as your condition for processing, you should, unless it is impractical to do so, seek data subject's further consent for the additional parties' access.

The law however, permits third parties who are legally authorised to do so, to demand access to the personal data you hold, for specific purposes, e.g. police officers in possession of a court order requiring disclosure.

# Data security breach policy

## Introduction

AudienceProject utilises various information systems and holds a large amount of data / information which may include personal or confidential information (about people), and also non-personal information which could be sensitive or commercial, for instance financial data.

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 vital that appropriate actions are taken to minimise associated risks.

## Purpose

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.

## Scope

This policy applies to all AudienceProject staff, contractors and third party agents handling AudienceProject information assets.

## Responsibilities

All users of AudienceProject's information assets are required to familiarise themselves with and comply with this policy.

All individuals who access, use or manage AudienceProject's information are responsible for reporting data breach and information security incidents immediately to their manager and the AudienceProject Helpdesk.

## Compliance

AudienceProject has an obligation to comply with relevant statutory, legal and contractual requirements. The Data Breach and Information Security Incident Policy is part of the Information Security suite of policies, designed to ensure data breach and information security incidents are reported promptly and managed properly to mitigate any risks to the confidentiality, integrity and availability of University information and information systems.

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

## Definition of an incident

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 are:

- ❏ Accidental loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of paper record, laptop, iPad or USB stick)

- ❏ Unauthorised use, access to or modification of data or information systems (e.g. sharing of user login details (deliberately or accidentally) to gain unauthorised access or make unauthorised changes to data or information systems)

- ❏ Unauthorised disclosure of sensitive or confidential information (e.g. email sent to an incorrect recipient or document posted to an incorrect address or addressee), or personal information posted onto the website without consent

- ❏ Compromised user account (e.g. accidental disclosure of user login details through phishing)
- ❏ Failed or successful attempts to gain unauthorised access to University information or information systems
- ❏ Equipment failure
- ❏ Malware infection
- ❏ Disruption to or denial of IT services

## Reporting an incident

Data breach and information security incidents should be reported immediately to management as well as the AudienceProject Helpdesk, as the primary point of contact. The report should include full and accurate details of the incident, including who is reporting the incident, what type of incident it is, if the data relates to people, and how many people are involved. Helpdesk will keep a log of this information.

## Investigation and Risk Assessment

Depending on the type of incident, management will instigate the relevant incident management team or inform the relevant individual to investigate the incident. An investigation will be started within 24 hours of the incident being discovered, where possible.

The investigation will establish the nature of the incident, the type of data involved, and where personal data is involved, who the subjects are and how many personal records were breached.

The investigation will consider the extent of a system compromise or the sensitivity of the data involved, and a risk assessment will be performed as to what might be the consequences of the incident, for instance whether harm could come to individuals or whether data access or IT services could become disrupted or unavailable.

## Containment and Recovery

The incident management team or relevant individuals will determine the appropriate course of action and the required resources needed to limit the impact of the incident. This might require isolating a compromised section of the network, alerting relevant staff or shutting down critical equipment.

Appropriate steps will be taken to recover system or data losses and resume normal business operation. This might entail attempting to recover any lost equipment, using backup mechanisms to restore compromised or stolen data and changing compromised passwords.

Advice from experts across AudienceProject may be sought in resolving the incident promptly and appropriately.