Clear Channel Europe

# Commercial Business Activities Privacy Notice

# Clear Channel Europe Privacy Notice

Commercial Business Activities

## Contents


Scope of this Privacy Notice ..... 3
Who are Clear Channel and how can you contact us? ..... 3
What data do Clear Channel process and where do we get it from? ..... 4
RADAR ..... 4
INTERACTIVE CAMPAIGNS ..... 7
CCTV ..... 7
CUSTOMER DATA ..... 8
Why do Clear Channel process personal data? ..... 8
What is the legal basis for processing Personal Data? ..... 9
Who do Clear Channel share Personal Data with and why? ..... 9
Transfer of personal data overseas ..... 10
How long do we keep your personal data for? ..... 10
Your rights in relation to the personal data we hold ..... 10
How do Clear Channel keep your personal data secure? ..... 10
Contacting our Data Protection Officer ..... 11
Supervisory authority ..... 11
Changes to this Privacy Notice ..... 11

## Scope of this Privacy Notice

This Privacy Notice applies to the processing of personal data in Clear Channel Out of Home advertising services.

Clear Channel provide out of home (OOH) advertising services, including digital OOH advertising. Clear Channel customers can advertise through different OOH media provided by Clear Channel, including street furniture such as bus shelters and phone kiosks; billboards including digital towers and through digital panels predominately located in malls, entertainment venues and transport hubs.

In supporting advertising customers Clear Channel help business advertise more effectively by using data to help them improve their advertising and offering interactive digital advertising products.

Much of the data Clear Channel process doesn't relate to individuals, but rather to geographic areas, data about patterns of movement, etc. However, some data processed as part of the Clear Channel services may include elements or functionality that can identify individuals to allow Clear Channel to create products and services that help our customers improve their advertising. This data is known as "personal data". Individuals whose personal data is processed have a right to be informed about the collection and use of their personal data. This is a key transparency requirement under data protection legislation.

This Clear Channel Privacy Notice is intended to provide information about how Clear Channel process personal data when providing OOH advertising services. Clear Channel process personal data for other purposes in addition to the provision of OOH advertising services such as business operational activities including third party relationship management, sales and marketing purposes and other Clear Channel Europe group management activities. Different Privacy Notices apply to these activities.

If you have a question or wish to find out more about Clear Channel products and services generally this can be found on our website https://www.clearchannel.co.uk/ and https://www.clearchanneleurope.com

## Who are Clear Channel and how can you contact us?

When we refer to Clear Channel in this Privacy Notice, we mean the various affiliated and subsidiary companies of Clear Channel International Limited (trading as Clear Channel Europe) whose registered office is 33 Golden Square, London W1F 9JT, United Kingdom. Clear Channel Europe is a group of affiliated companies and a division of Clear Channel Outdoor Holdings Inc (CCOH) which is listed on the New York Stock Exchange.

Each of the Clear Channel companies in the Clear Chanel Europe division is an independent data controller for personal data processed to support and provide OOH advertising services. For more information on Clear Channel Europe and the different affiliated and subsidiary companies in the Clear Channel Europe division can be found https://www.clearchanneleurope.com/

For any questions about how companies in the Clear Channel Europe division process personal data or any queries about information in this Privacy Notice you can contact our Data Protection Officer (DPO) at mydata@clearchannelint.com

## What data do Clear Channel process and where do we get it from?

Clear Channel process data including in some circumstances personal data, that is data that can identify individuals, to create products and services serving our advertising customers' needs for creativity, flexibility and accountability. The types of data that Clear Channel process in OOH campaigns falls into 4 categories, described in more detail below.

- RADAR – Data used to support contextualised advertising in OOH services.
- Creative campaigns – data collected and used in interactive campaigns.
- Video Surveillance including CCTV – data may be collected using cameras for security and crime prevention purposes or for the legitimate interests of Clear Channel or third parties.
- Customer data – our customers may supply data and instruct Clear Channel to process it on their behalf. In these circumstances Clear Channel act as a data processor on the customers behalf.

Where Clear Channel process data for RADAR services, in creative campaigns, and for video surveillance, including the use of CCTV, a data protection by design and default approach is followed and a Data Protection Impact Assessment (DPIA) is carried out.

The DPIA is part of a process to embed data protection by design and by default and as part of the assessment, the DPIA is used to understand the potential privacy risks, record the considerations and mitigations in place to minimise the risks. It is carried out and reviewed with the Clear Channel Privacy team under the responsibility of the DPO. Default settings limit the processing of personal data to that necessary to provide the advertising services and data is not retained longer than is necessary. All processing is subject to security controls to ensure that Personal Data is adequately protected.

## RADAR

**What data do we process?**

Clear Channel in providing DOOH services are a mass market medium and as such do not target specific individual people. Data is used to understand the audience our panels reach so that this mass market audience can be shown content they find relevant. The aim is to create engaging content with the millions of people who walk past Clear Channel panels daily. It is about using data to ensure audiences see contextually relevant messages that resonate with what they are doing at specific moments in specific places.

DOOH campaigns combine external data sources to provide relevant content to their audiences. Data is used throughout the advertising campaign journey.

- **Pre-campaign:** to accurately plan campaigns to reach target audiences.
- **Mid-campaign:** to track audience delivery, optimise campaigns, customise creative.
- **Post-campaign:** to measure results and the attribution value of OOH.

Examples of the type of data used are

- date, e.g., times of year, day of the week;
- time of day, e.g., morning, rush hour;
- different format of digital screens;
- data triggers such as local weather, pollen count, social trends, traffic flow;
- site location of the digital screen, e.g. city or postcode,
- site environment, e.g., airport, roadside, pedestrian area, and

- audience data, e.g., data collected through audience behavioural measurement tools. Clear Channel receive audience data in aggregated form, so that individuals cannot be identified, the data is used to provide demographic information and similar information about audiences.

For audience data collected through audience behavioural measurement tools we rely primarily on aggregated, anonymised data that comes from data partners. This data helps us understand the audience of our OOH adverts. It may include information about demographics and interests of the types of people who will see the advertisements. Clear Channel do not seek to profile or track individuals.

The following are methods used in the advertising eco system by our data partners and others to allow advertisers to understand their audience.

**SDK and Mobile data**
From time to time, we engage with data partners who provide insights with anonymised and aggregated data, the data source to create the aggregated data is from SDKs in apps, GPS data or other data obtained from a mobile device's IP address. "SDK" stands for "software development kit". It is a piece of code that is built into an app, and that facilitates the app to collect geolocation and other statistical data. When an individual user installs those apps on their device, the individual user has the option of giving their consent to enable the collection of limited elements of their data including Personal Data to enhance their app usage and to share with the app provider's commercial partners. Individuals can revoke consent to share data at any time in the apps' settings. Data partners then aggregate this data before it is supplied to Clear Channel.

**SDK and Cellular signal data**
Mobile phone networks may supply anonymized, aggregated data insights collected from triangulated cellular signals from phones using their network. These insights give us insights into group level audience behaviours within the vicinity of our ad locations.

Clear Channel receives anonymised, aggregated datasets from carefully chosen data partners. This data provided helps us provide insight into large scale audience behaviour to our advertisers to understand the efficacy of our advertisements.

**Wi-Fi sensors ("sniffers")**
Devices installed on some Clear Channel structures to detect the presence of devices searching for a Wi-Fi signal such as phones. These devices do not detect any personally identifiable information (including MAC ID or MAID (Mobile Advertising IDs)) but simply give a "count" of the number of devices at any given time which can be used to assist with campaign targeting.

**Mobile retargeting** - the individual user has the option of giving their consent to enable the collection of limited elements of their data including Personal Data and location data which can be shared with the app provider's commercial partners. Individual users can then receive targeted advertising on their mobile device. Individuals can revoke consent to share data at any time in the apps' settings. Clear Channel do not directly send mobile retargeting adverts in Europe. Third parties instructed by advertising customers send targeted adverts and may do so as part of a wider advertising campaign based on the location of a particular OOH display.

**Geofencing**
Geofencing" is a location-based service in which an app or other software uses GPS, RFID, Wi-Fi or cellular data to trigger a pre-programmed action when a mobile device or RFID tag enters or exits a virtual boundary set up around a geographical location, known as a geofence.

**Bluetooth beacons**
Beacons are installed on Clear Channel panels in a few of our sites. These beacons passively transmit a location signal inside its "geofence" which can be detected by mobile devices. If an individual has given permission for your mobile device to connect to beacons, via an app or through the device settings, the individual's mobile device may try to connect to the beacon installed in those billboards and share its geographical information with those beacons when you come within the beacon's geofence.

This information about the location of the individual's mobile device is not used by Clear Channel. Clear Channel use information in aggregated and anonymised form. However, the information about the location of an individual's mobile device may be used by others in the advertising ecosystem such as Clear Channel advertising customers or others acting on their behalf to send targeted messages to individuals if the individual user of the mobile device has permitted this though app and device settings. Clear Channel do not send targeted messages to individuals; however, these messages may be sent by other parties in the digital ecosystem. Users can revoke consent to share geolocation data with beacons at any time in the settings on their phones.

As an example, Clear Channel may have a digital panel which contains a beacon with a beacon geo fence. The digital panel displays at a certain time an advert for a retail customer. The retail customer may use the details of when their advert is being displayed on the DOOH panel as part of the wider advertising campaign. The retail customer may send targeted messages to individuals who have consented through their device settings and who may come within the geofence. Clear Channel do not send these messages to the individual. Clear Channel provide the retail customer with information about when the specific advert was displayed to enable the retail customer to use this information as part of a wider coordinated advertising campaign.

**Where do we obtain the data from?**
We obtain data from several sources.

- Third party data partners – we enter into agreements with third party data partners to provide us with various data sets. Due diligence is carried out on all third-party data partners with a DPIA carried out where Clear Channel obtain audience data that may be aggregated data originally collected from individuals.
- Public information – we may obtain data form publicly available sources which can often be freely used, reused and redistributed by anyone.
- Wi-Fi sniffers and similar technology embedded in some screens under the responsibility of Clear Channel, these are used to detect enabled devices within a certain area. Any data collected through technology on Clear Channel screens is subject to a DPIA and data collected is in anonymised aggregated form.

Clear Channel obtain audience data from various data partners. Data partners collect data from different sources. We undertake due diligence on our data partners to understand how data is collected by the providers even though data received by Clear Channel is in aggregated form and the detailed due diligence we carry out is not a legal requirement to comply with applicable data protection laws.

We use providers who are committed to providing individuals with relevant notice and consent options and offer controls to ensure individuals cannot be identified.

## INTERACTIVE CAMPAIGNS

**What data do we process?**

Interactive campaigns using computer vision software, audio software and similar technologies that allow interaction with digital screens are in standard use across the Out of Home Advertising industry to allow individuals to interact with creative and flexible campaigns. This technology can use cameras installed within the screen which when the camera is enabled can be set to recognise defined items, or audio functionality that can detect certain sounds. What the technology recognises, whether it is an image, sound or other input will be dependent on the software settings. Computer vision software could be programmed to identify an image of an inanimate object such as a piece of fruit, or it can be set to recognise basic characteristics of individuals (for example it may detect motion in front of the screen, height, or hair colour etc.). Using the software in this way would allow an individual looking at the screen to personalise interactions with the advertisement they see. An interactive advertisement might show a character move around in accordance with the motion of the person in front of it, or software settings may be set to capture apparent engagement with the advertisements such as the length of time someone looked at the advertisement, or expressions of individuals looking at the adverts.

When interactive campaigns are developed, including those where technology is used that can capture images, software deployed that can record or recognise sound, or other interactive campaigns such as touch screens are developed that may process personal data, the campaign is subject to a DPIA, Data Protection Impact Assessment. Clear Channel use this process to embed data protection by design and by default. The DPIA is carried out and reviewed with the Clear Channel Privacy team under the responsibility of the Clear Channel DPO to understand the potential privacy risks and put in the necessary mitigations to provide adequate protections. The default settings of the software are designed to only permit the processing of Personal Data necessary to provide the advertising services, data is not retained longer than is necessary, for example most data is processed for the time of the interaction with the advert and then securely deleted. All processing is subject to security controls to ensure that Personal Data is adequately protected.

**Where do we obtain the data from?**

Personal data collected and processed through the interactive campaign is collected from individuals who interact with the digital screens.

## CCTV

**What data do we process?**

CCTV and other video surveillance operates on some panels for security and safety purposes. Cameras can also be used to provide evidence of proof of play. Where CCTV or any other cameras are used before they are deployed, a DPIA, Data Protection Impact Assessment is carried out. Clear Channel use this process to embed data protection by design and by default. The DPIA is carried out and reviewed with the Clear Channel Privacy team under the responsibility of the Clear Channel DPO to understand the potential privacy risks and put in the necessary mitigations to provide adequate protections. The default settings are designed to only capture data that is necessary for the purposes the camera has been installed, the images are not retained longer than is necessary and then securely deleted when the images are no longer required. All processing is subject to security controls to ensure that Personal Data is adequately protected.

**Where do we obtain the data from?**
Personal data collected and processed by CCTV and other cameras used will be collected from individuals who may come in the range of the camera.

## CUSTOMER DATA

**What data do we process?**
Advertising Customers may ask Clear Channel to process personal data on their behalf, an example would be the display of an advert of an image of an identifiable individual. In these situations, Clear Channel act as a data processer on the customers behalf and do not use any of this information for any purposes other than to provide the services as instructed to by the Advertising customer, e.g., to display the advert.

**Where do we obtain the data from?**
Advertising Customers provide Clear Channel with the personal data, and it is processed on behalf of the relevant Clear Channel customer.

## Why do Clear Channel process personal data?

Clear Channel provide out of home (OOH) advertising services, including digital OOH advertising. Clear Channel customers can advertise through different OOH media provided by Clear Channel, including street furniture such as bus shelters and phone kiosks; billboards including digital towers and through digital panels predominately located in malls, entertainment venues and transport hubs.

We obtain and process data including in some circumstances personal data to create products and services serving our advertising customers' needs for creativity, flexibility and accountability. The types of data that Clear Channel process in OOH campaigns falls into 4 categories, described in more detail in the section above

- RADAR – Data used to support contextualised advertising in OOH services
- Creative campaigns – data collected and used in interactive campaigns.
- Video Surveillance including CCTV – data may be collected using cameras for security and crime prevention purposes or for the legitimate interests of Clear Channel or third parties.
- Customer data – our customers may supply data and instruct Clear Channel to process it on their behalf.

Other purposes

From time to time, we may use the personal data that we obtain for other purposes. These include

- To analyse, develop and improve the use function, and performance of our products and services, including testing the quality of any new data collected from third parties
- To manage the security of our sites, networks and systems and to operate our business
- To maintain our records and other administrative purposes, including record keeping and general administrative purposes, including for business transactions (including M&A), to include information sharing with potential transactional partners or other third parties in connection with the consideration, negotiation or completion of a transaction in which Clear Channel are

acquired by or merged with another company or there is a sale, liquidation or transfer all or a portion of assets including any bankruptcy or corporate reorganisation.

- To comply with legal obligations, to respond to legal processes or requests for information from government authorities, law enforcement or other third parties
- Manage any complaints or dispute resolution.
- To protect the rights and interests of Clear Channel, our employees and others as required and permitted by applicable law.

## What is the legal basis for processing Personal Data?

Data Protection law means that every organisation must have a lawful ground or reason for processing any personal data about an individual.

To create products and services serving our advertising customers' needs, we process personal data under a lawful ground called “legitimate interest”. As an organisation providing an OOH medium to advertisers our business is dependent on us being able to process limited personal data to build the products and services to help our customers serve creative and contextual advertising through understanding the audience our panels reach so that the audience can be shown relevant content. Clear Channel use aggregated, anonymised data to understand the demographics of the audience of the panels and as such do not target specific individuals.

When we process personal data under legitimate interest, we carry out an assessment (DPIA) to consider your rights under data protection laws as well as any potential impact to you. The DPIA is part of a process to embed data protection by design and by default and as part of the assessment, the DPIA is used to understand the potential privacy risks, record the considerations and mitigations in place to minimise the risks. It is carried out and reviewed with the Clear Channel Privacy team under the responsibility of the DPO. A key objective of the DPIA is to assess how data is collected and ensure that only data necessary for the purpose is processed. Where personal data is used to support the interactive campaigns, this is limited to that necessary to provide the advertising services and data is not retained longer than is necessary. All processing is subject to security controls to ensure that Personal Data is adequately protected.

## Who do Clear Channel share Personal Data with and why?

Personal data is shared with individuals and organisations who need to handle it so that Clear Channel can provide the OOH advertising services. Clear Channel take steps to allow access to personal data only to when required to perform identified tasks and duties and to third parties who have a legitimate purpose for accessing it. Where a third party is granted access to personal data appropriate measures are put in place to ensure that the security and confidentiality of the information is maintained.

It is also shared with

- Clear Channel group companies who may manage or support some parts of the services;
- Service provides we have engaged to support our business who receive or have access Clear Channel systems and data as part of providing services. These Clear Channel group companies and service providers may be located overseas.

## Transfer of personal data overseas

Clear Channel Europe are a group of companies located mainly in the UK and European Economic Area and as such any personal data will usually remain within the UK or the European Economic Area. Clear Channel group companies and service providers who may support these services also operate elsewhere, in and outside the European Economic Area, so data may be accessed from and transferred to these locations as well. Where data is transferred overseas, we will ensure that any personal data is adequately protected. There are different ways that this can be achieve, for example where it is transferred to a country which has been approved by the European authorities as having adequate protection in place or by putting contracts in place that has been approved by the European commission with the recipient of the personal data that provides a suitable level of protection.

## How long do we keep your personal data for?

Clear Channel keep personal data for as long as there is a continuing need to do so and in accordance with the Clear Channel data retention and destruction policy. Data that is no longer required will be securely disposed of.

Information may be retained to comply with our legal obligations, resolve any disputes and enforce our rights. These reasons can vary and will depend on the type of data processed, so the amount of time we may keep personal data may vary.

## Your rights in relation to the personal data we hold

Data protection laws give individuals a number of rights in relation to personal data. These include

- Right of access – see what information we hold about you
- Right to rectification – correct any information you think is wrong
- Right to object – ask us to stop using your data
- Right to be informed – understand what happens to your personal data
- Right to restrict processing – change how your data is used
- Right of portability – move your data
- Rights in relation to automated decision making and profiling
- Right to erasure or right to be forgotten,

Clear Channel will consider all data subjects requests individually and on a case-by-case basis. Not all the rights apply to the data processed by Clear Channel in the provision of OOH advertising services.

To exercise any of these rights, or to find out if they apply or if you require further information on your rights or our use of your Personal Data, please contact us at mydata@clearchannel.com.

## How do Clear Channel keep your personal data secure?

Clear Channel use a variety of the latest technologies and organisational measures to protect data from unauthorised access, destruction, use or disclosure.

Clear Channel have an information security framework based on internationally recognised standards of security. The cyber security measures protecting data include appropriate technical and organisational measures aligned to ISO 27k requirements and CIS controls. Clear Channel have a dedicated cyber security investigations team who safeguard Clear Channel key assets and systems.

This team identify and effectively manage any security developments that may threaten Clear Channel people, processes or technology.

## Contacting our Data Protection Officer

If you have any questions, concerns or issues about the way we are handling your personal data or want to exercise any of your data subject rights (or find out if they apply) please contact our DPO by email at mydata@clearchannelint.com .

If you would prefer to contract us by post, please address this to The Data Protection Officer c/o Clear Channel International Limited, 33 Golden Square, London W1F 9JT, United Kingdom

## Supervisory authority

Having contacted Clear Channel if you are still unhappy with any aspect of how we handle your personal data you have the legal right to lodge a complaint with the supervisory authority of the relevant Clear Channel entity that is the data controller for personal data processed when providing OOH advertising services. Each of the Clear Channel companies in the Clear Chanel Europe division is an independent data controller for personal data processed when providing OOH advertising services.

Information Commissioners Office (ICO) the supervisory authority that regulates handling of personal data in the UK is the supervisory authority for Clear Channel International Limited. You can contact them by going to their website at www.ico.org.uk

## Changes to this Privacy Notice

Clear Channel may update this Privacy Notice from time to time and ideally you should check it regularly for updates. Previous versions of Clear Channel privacy notices are available upon request.

Last Updated – October 2023