

Clear Channel International Privacy and Cookies Notice

Clear Channel International Privacy and Cookies Notice

Contents

- To which Clear Channel entity does this Notice apply? 2
- Why is this Notice important? 2
- How do we collect Personal Data and why? 3
- What Personal Data do we collect?..... 4
- Sensitive or “Special Category” Personal Data 5
- Audience Behavioural Measurement** 5
- Your Rights 7
- Transfer of Personal Data 8
- Retention of Personal Data 9
- Cookies 10
- Contact us 13
- Changes to this Notice 13

To which Clear Channel entity does this Notice apply?

This Privacy and Cookies Notice (“**Notice**”) applies to the websites of Clear Channel International including www.clearchannelinternational.com with the registered address: 33 Golden Square, London W1F 9JT, United Kingdom; and any other website of Clear Channel International group subsidiary or affiliated companies which can [be viewed here](#) (“**Clear Channel**”, “**we**,” “**us**,” or “**our**”) as well as any Mobile Apps, online forms and subscriptions, products or services, and social media channels controlled by Clear Channel where a link to this Notice is provided (each, the “**Platform**” and together, the “**Platforms**”).

Each Platform is controlled by the individual Clear Channel entity as defined in its terms of use.

Why is this Notice important?

Clear Channel are committed to protecting your Personal Data in accordance with our internal policies and applicable European legislation

This Notice informs you of our practices with respect to the collection, use and disclosure of Personal Data which you provide to us via our Platforms, in relation to any promotions, competitions, offers or marketing campaigns we carry out or which you provide for your potential employment with us. It also describes your data protection rights, including a right to object to some of the processing which Clear Channel carries out. More information about your rights, and how to exercise them, is set out in the “Your Rights” section.

“**Personal Data**” means personal information that identifies you as an individual or relates to an identifiable individual as defined under applicable European legislation (and in particular, the General Data Protection Regulation).

How do we collect Personal Data and why?

The **Data Controller** is Clear Channel International.

We may collect your Personal Data in the following circumstances:

1. With your consent:

- when you subscribe to our marketing lists, social media pages, (promotions, competitions, offers or marketing campaign communications (together, “Marketing and Promotions”) will be provided to you by Social Media Channels, email, post or other communication channels); and
- If you choose to actively engage in an experiential campaign via, for example, a QR code on an interactive advertisement or competition and we need to know your identity or request your contact details, we will obtain your consent and tell you at the time of requesting that consent, how we will use that data.

2. To perform our contractual obligations:

- under our terms when you register for our Products or Services;
- to verify your identity;
- when you register to attend a Clear Channel event;
- provide customer service related to our Products and Services;
- when forming leasing or similar arrangements over assets; and
- if you apply to work for a Clear Channel business, we may need to take steps that are necessary prior to entering into an employment contract with you such as checking you’re your qualifications or your right to work in the country you applied for a role.

3. For our legitimate business interests, which include:

- sending you communications about Marketing and Promotions if we do not need your consent
- to provide you with access to Products and Services or specific materials or information from our Platforms that you request;
- processing your feedback and contributions to customer surveys, competitions, offers or questionnaires;
- recording telephone calls with you for training and/or monitoring purposes;
- reviewing your queries so we can better help you or investigate any complaints received by you;
- to improve our service to analyse trends to administer our Platforms;
- to monitor our diversity and inclusivity; and
- to help identify you for administrative purposes.

4. For **compliance, legal or regulatory purposes**:

- to verify your identity as part of the employment screening process, and for money laundering regulation purposes; and
- to report any activity which we suspect breaches any relevant laws or regulations to the appropriate authority.
- for the protection of vital interests and information security, fraud prevention and service provision (for example, managing abuse of the service).
- to comply with EU or member state law for the prevention, investigation, detection or prosecution of criminal offences or prevention of threats to public security.

What Personal Data do we collect?

Types of Personal Data

Personal Data we may process includes but is not limited to combinations of information about:

- Your name, postal address, email address phone number, occupation and other contact information;
- If you are a landlord, the details of your ownership of assets;
- Sensitive Personal Data such as race or gender, when applying for a position with us – please see the **Sensitive Personal Data** section below;
- where you heard about us;
- details of complaints;
- any information you may voluntarily submit to us by completing any form on our Platforms, such as a “free text” boxes on our Platforms (i.e. blank spaces where you are free to insert comments);
- your dealings with us including information regarding your personal or professional interests, needs or opinions, demographics, experiences with our Products or Services and contact preferences;
- if you are a job applicant your CV details and any background information we may receive from your referees, your LinkedIn profile, the recruitment agency that you work with (if any);
- details of financial or accounting transactions carried out on our Platforms or otherwise, including credit/debit card information, billing information and/or delivery address information (if you pay for anything on our websites);
- demographic and contact information from other sources, such as public databases, joint marketing partners, social media platforms (including from people with whom you are friends or otherwise connected) and from other third parties;
- technical information, including location information, the Internet Protocol (**IP**) address used to connect your computer to the Internet, your login information, browser type and version, time zone setting, browser plug-in types and versions, operating system and platform;
- your online browsing behaviour on our Platforms; including the Uniform Resource Locators (**URL**) clickstream to, through and from our Platforms or Social Media Channels (including date and time), download errors, lengths of visits to certain pages, page interaction information (such as scrolling, clicks and mouse-overs), email marketing interaction (including if and when an

email is opened and how many times it is opened); and methods used to browse away from the page; and/or any devices you have used to access our Products and Services (including the make, model and operating system, IP address, browser type and mobile device identifiers).

In some circumstances, we request additional Personal Data to help us to provide you with the most appropriate response. If you do not provide the Personal Data where requested, your access to the service, or our ability to assist you, may be restricted.

Sensitive or “Special Category” Personal Data

“Sensitive or “Special Category” Personal Data” means Personal Data which may relate to: racial or ethnic origin, political opinions, trade union memberships, physical or mental health conditions or genetic or biometric data that uniquely identifies you, your sex life or sexual orientation, religious or philosophical beliefs and the commission or alleged commission of any offence or related proceedings. Where you do provide Sensitive Personal Data, we will keep it securely and for a proportionate amount of time, and only use that information in connection with the purpose for which it has been provided.

We may ask, if your local law allows, for your voluntary provision of race, religion and other Sensitive Personal Data as part of the Clear Channel recruitment process, to monitor our equality and diversity obligation (you can always decline to tell us).

Where permitted or required by law (which varies by jurisdiction), we may request that you self-declare pertinent current health conditions in order to allow you access to our premises, in accordance with government guidelines on public health. We keep our procedures under review to ensure they comply with recommendations in your jurisdiction.

If we are required to process your Sensitive Personal Data for any other purpose, we will, where required by law, ask for your explicit consent.

Audience Behavioural Measurement

Use of Anonymised Data

We may purchase, or collect, anonymised, aggregated datasets relating to the performance of our Out of Home advertising (such as billboards, street, roads, highways, transit etc.), or anonymised and aggregated transaction and purchase history from data providers. We do this to better understand the types of people who will see the advertisements we promote, on behalf of our advertisers. We do not seek to analyse Personal Data on an individual level.

SDK and Mobile Data

From time to time we engage with data partners which use data obtained from SDKs in apps, GPS data or other data obtained from a mobile device’s IP address (if the user has consented for this data to be shared). This data provided helps us provide insight into large scale audience behaviour.

Cellular signal and SDK data

Where users consent, mobile phone networks may supply insights based on anonymized, aggregated data 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.

“SDK” stands for **“software development kit”**. It is a piece of code that is built into an app, and that facilitates that app to collect geolocation and other statistical data. When a user installs those apps on

their device, the 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. Users can revoke consent to share data at any time in the apps' settings.

Clear Channel receives anonymised, aggregated datasets from carefully chosen GDPR-compliant data partners that helps us, and our data partners best understand consumer demographics and engagement in the real world.

Geofencing (including mobile retargeting)

“**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**.

Beacons are installed on Clear Channel panels in a number of our sites. These beacons passively transmit a location signal inside its “geofence” which can be detected by mobile devices. If you have given permission for your mobile device to connect to beacons, via an app or your device settings, then your 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.

Clear Channel and our business partners may use that information to understand audience behaviour, and business partners may send targeted messages to consenting devices relating to the content of nearby advertisements when those devices are in the vicinity of our panels. Users can revoke consent to share geolocation data with beacons at any time in the settings on their phones. If you have not given consent for your mobile devices to share data, it will not be shared.

All data used by or shared with Clear Channel by its partners, are aggregated and anonymous and we do not retain information on individuals, nor do we identify, track, profile or target individual people.

Computer vision software on our panels

Computer vision software is in standard use across the Out of Home Advertising industry (such as billboards, street, roads, highways, transit etc.). When computer vision technology is used, including if it is used for a campaign by Clear Channel or its partners, a camera installed within the screen is enabled which can recognise the basic characteristics of people (for example it may detect motion in front of the screen, or height, gender or hair colour etc.) looking at the screen in order to personalise interactions with the advertisement they see. For example, an interactive advertisement might show a pair of sunglasses on a female or male character depending on the gender of person looking at the screen, or move around in accordance with the motion of the person in front of it. It may also capture apparent engagement with the advertisements we promote (such as the length of time someone looked at the advertisement, or expressions).

If Clear Channel or our partners use computer vision technology, any Personal Data captured by it is only captured and stored temporarily. Software used is subject to strict deidentification, information security and almost immediate memory wiping procedures. We engage software providers that have been subject to data privacy impact assessments and signed terms agreeing to abide by Applicable Data Protection Legislation. Clear Channel do **not** attempt to identify you from Computer Vision software. We are not interested in profiling individuals. We and our data partners instead anonymise and aggregate any information into large scale datasets for us to better understand demographic audience reactions to the advertisements we promote, on behalf of our advertisers.

Your Rights

Under the GDPR and other applicable legislation, you have rights over your Personal Data. Those rights include (subject to legal and regulatory requirements):

Right to Rectification of Personal Data

If you advise us that your Personal Data is no longer accurate, we will amend or update it (where practical and lawful to do so).

Right to Erasure or Restriction of Processing of Personal Data

You can ask us to delete or restrict processing of your Personal Data in some circumstances such as where we no longer need it, or you withdraw your consent (if we rely on your consent for processing). If we've shared it with others, where possible, we'll let them know about the erasure.

Right to Withdraw Consent

You have an absolute right to opt-out of direct marketing, or profiling we carry out for direct marketing, at any time. If, at any time, you have consented to us processing your Personal Data in the circumstances or purposes described above, and you no longer wish to have your Personal Data processed in this way, you may unsubscribe by pressing any unsubscribe facility or by emailing mydata@clearchannelint.com.

Right to Portability

You can ask us to provide you with your personal data (that you provided to us or that we observed through your activities on our Platforms) in a commonly used and machine-readable format to send it to another controller.

Right to Object

You can object to the processing of your personal data in some circumstances (in particular, where we don't have to process the data to meet a contractual or other legal requirement, or where we are using the data for direct marketing if we are not relying on your consent).

Rights in relation to Automated Decision-making and Profiling

You have the right not to be subject to a decision when it's based solely on automated processing or profiling which produces a legal or similarly significant effect on you. We only carry out this type of decision-making where the decision is necessary for the entry into or performance of a contract; or authorised by Union or Member state law applicable to us; or based on your explicit consent.

We will always tell you if we do any such activity using your Personal Data.

Right to Access Personal Data

Where permitted by law, you may have the right to contact us to request a copy of Personal Data that we hold about you. Before responding to your request, we may ask you to (i) verify your identity and (ii) provide further details so we can better respond to your request.

These **rights may be limited**, for example if fulfilling your request would reveal personal data about another person, where they would infringe the rights of a third party (including our rights) or if you ask us to delete information which we are required by law to keep or have compelling legitimate interests in keeping. Relevant exemptions are included in both the GDPR and in the Data Protection Act 2018. We will inform you of relevant exemptions we rely upon when responding to any request you make.

To exercise any of these rights, or to obtain other information, such as a copy of a legitimate interests balancing test, you can get in touch with us using the details set out below.

If you require further information on your rights or our use of your Personal Data, please contact us at mydata@clearchannelint.com. If you have unresolved concerns, you have the **right to complain** to an EU data protection authority where you live, work or where you believe a breach may have occurred.

Children's Personal Data

Our Platforms are not intended to target children under the age of 16. We will not knowingly collect or process Personal Data belonging to children via our Platforms.

Third Party Goods and Services

We will not send you information relating to third party goods and services from outside Clear Channel unless specifically requested.

Third Party websites

Where links from our Platforms are provided to non-Clear Channel websites, we are not responsible for those websites and nor do we imply endorsement of any linked third-party websites. These third-party websites will be governed by different terms of use, depending on the owner and data controller of those websites (including privacy notices) and you are solely responsible for viewing and using each such website in accordance with their own applicable terms of use. We are not responsible for how your Personal Information is handled by such third-party websites and they are not covered by this Notice.

Transfer of Personal Data

Third Parties

We transfer your personal data where we use third party service providers to help us process Personal Data for the purposes described in this notice, these will include customer management and intelligence solution providers, aggregated data analytics partners, web hosting facilities, audit and compliance partners.

Data Controller Intragroup Transfer

Clear Channel International is the lead entity for a Group of businesses, Clear Channel International Limited, registered address, 33 Golden Square, London W1F 9JT. The Parent company of Clear Channel International is Clear Channel Outdoor, a publicly listed Company in the United States. From

time to time, it may be necessary for our legitimate interests to transfer Personal Data collected by Clear Channel amongst the Clear Channel Group and its US parent company together with their data processors.

Transfers outside the European Union

Non-European countries may have data protection laws that are less protective than the legislation where you live. Where this is the case, (such as the United States), our transfers of Personal Data will be regulated by the EU Commission's standard contractual clauses relating to the transfer of Personal Data outside of the European Union (or outside of jurisdictions deemed "adequate" for data privacy by the European Commission. The jurisdictions to which Personal Data are transferred may be conditional on your nationality or location.

Sale or Merger

If Clear Channel or its assets are sold to or merge with another entity outside Clear Channel, you should expect that some or all of the Personal Data collected by Clear Channel may be transferred to the buyer/surviving company.

Retention of Personal Data

If you have provided us with Personal Data, your Personal Data will be retained for the duration of your relationship with us to fulfil the purposes for which we collected it. This includes, the length of time required to satisfy any legal, regulatory, accounting and reporting requirements , and to process personal information on you in order to establish or defend legal claims (and we or our third party data processors will dispose of your Personal Data at the end of the relevant retention period).

In determining the appropriate retention period we consider the purpose for which we process your Personal Data, the volume, type and context of the Personal Data, local legal requirements, the risk of harm to the data protection rights of the individual and whether the purpose for processing Personal Data can be established through an alternative method.

For further information regarding the specific retention periods we apply to your Personal Data please contact us at mydata@clearchannelint.com

Personal data collected from applicants who are unsuccessful will be deleted or, if that individual may be of interest for other roles, kept until one year after the applicant submits their application.

Where we process personal data for marketing purposes or with your consent, we process the data until you ask us to stop and for a short period after this (to allow us to implement your requests). We also keep a record of the fact that you have asked us not to send you direct marketing or to process your data so that we can respect your request in future.

Where we process personal data in connection with performing a contract or for a competition, we keep the data for 6 years from your last interaction with us.

Cookies

What Cookies we and third parties use, why are they used, and how they impact you

A cookie is a small text file, typically of letters and numbers (with an ID tag), which may be placed on your computer or mobile when you access our Platforms. Cookies generally allow a website to recognise your device and browsing activity if you return to it, or if you visit another website which recognises the same cookies.

Different cookies perform different functions. Necessary cookies help you navigate through pages, “storing preferences” information and functionality cookies generally make the website easier to use. They exist just for the life of your current visit whilst you have your browser open. They are not stored on your hard disk and are erased when you exit your web browser.

Others, such as targeting and advertising cookies, identify products, goods or services you may be interested in and are used to provide you with tailored advertising and performance cookies help us collect aggregated information on how people use our Platforms.

When you visit our Platforms, we request your consent for the non-necessary cookies to be placed on your device. To opt out of cookies, please see details below.

The table below explains the cookies we use, their purpose and duration:

Cookie	Name	Purpose	Default expiration time
Cookies allowed	exp_cookies_allowed	This cookie is necessary and is used to remember a user’s choice about cookies on our site. This cookie is, by default, set on arrival to the site with a value of ‘y’.	1 year
Cookies declined	exp_cookies_declined	This cookie is necessary and is used to remember a user’s choice about cookies on our site. This cookie is set after a visitor chooses to opt out of receiving cookies, replacing the exp_cookies_allowed cookie.	1 year

Content management system	exp_last_visit exp_tracker exp_last_activity exp_stashid	These cookies are first party analytics cookies set by our content management system upon arrival to our site. Some of these cookies are deleted when a user closes their browser, the others have a variable expiry date.	1 year: exp_last_visit exp_last_activity Session: exp_tracker exp_stashid
Google Analytics	__utma __utmb __utmc __utmt __utmz _gat _ga	These cookies are analytics cookies and are used to collect information about how visitors use our site. We use the information to compile reports and to help us improve the site. The cookies collect information in an anonymous form, including the number of visitors to the site, where visitors have come to the site from and the pages they visited. Click here for an overview of privacy at Google	__utma - 2 years from set/update __utmb - 30 mins from set/update __utmt - 10 minutes __utmz - 6 months from set/update __utmc - End of browser session
Vimeo	_ga _gid player vimeo_gdpr_optin vuid __cf_bm (session)	These are functionality cookies and are used by Vimeo on website pages using embedded Vimeo videos. Please see the Vimeo cookie policy for further information. Vimeo may set other cookies in addition to those listed here (see full list of cookies used by Vimeo) .	2 years 24 hours 1 year 10 years 2 years End of browser session
ShareThis	st_samesite __stid __stidv	These are functionality cookies and are used by ShareThis on website pages using ShareThis plugin.	End of browser session
ID5-sync	gdpr CookieConsent	These are functionality cookies and are used by ID5 cookie and other consent boxes on website.	gdpr - 1 day CookieConsent - 1 year

Filemail	ASP.NET_SessionId jStorage jStorage_update	These are functionality cookies and are used by Filemail on website pages using Filemail plugin.	End or browser session Persistent
----------	--	--	--

Social buttons

On many of the pages of our website you will see ‘social buttons’. These allow you to share or bookmark pages on our site.

Social media sites such as Twitter, Google, Facebook, and LinkedIn may collect information about your internet activity. They may record if you visit our Platforms and the specific pages you are on if you are logged into their services, even if you don’t click on the button. Where this happens, we may be joint controllers with the social media site over the data transmitted to them from our website. However, they will be a separate controller for any subsequent use of your data. You can exercise your rights in relation to jointly controlled data against either us or the social media partner.

For their subsequent use, you should check the privacy and cookies policies of each of these sites to see how exactly they use your information and to find out how to opt out, or delete, such information.

Further information

1. [Facebook cookies](#)
2. [Twitter cookies](#)
3. [Google cookies](#)
4. [LinkedIn cookies](#)

Manually managing cookies

There are a number of ways you can manually manage cookies on your computer/device. Read more on the [About Cookies website](#).

If you access the Internet from more than one computer/device, it is important to ensure each browser is configured to suit your cookie preferences.

Do Not Track

If you wish to block all cookies all the time you can set your browser to do this. It is important to note that blocking cookies may result in some parts of our site not working properly. This may affect your browsing experience.

Our Platforms respect a DNT:1 signal as a valid browser setting communicating your preference.

How does Clear Channel ask for Cookies consent?

Clear Channel complies with applicable legislation on cookies. Where we need your consent a popup box will appear when you first access our Platform. This will ask you whether you consent to our use of not necessary cookies. If you do not consent to cookies, they will be disabled on your behalf. You are also free to disable cookies at any time through your browser's settings, (for more information on how to do this please see the "how to delete cookies" tab at www.allaboutcookies.org/cookies).

If you choose to disable cookies, please be aware that some parts of our Platforms may not work properly and it is likely that your Platform usage won't be counted and measured as described above, so we won't be able to take your actions into account when analysing data or when seeking to improve our service based on that analysis.

Contact us

Should you wish to make any comments, complaints, enquiries or if you have any questions relating to this Notice, your rights, the Platform, our Marketing and Promotion materials or Products or Services we provide, you may contact the Clear Channel Chief Data Privacy Officer by emailing or writing to the Privacy Office:

The Chief Data Privacy Officer

Privacy Office

Clear Channel International

33 Golden Square

London, UK

W1F 9JT

Email: mydata@clearchannelint.com

You may also contact the Data Protection Authority where you live work or believe the breach has happened. A list of the European Supervisory Authorities can be found [here](#). If you are in the UK the Data Protection Authority will likely be the [UK Information Commissioner's Office](#). You may contact them [here](#).

Changes to this Notice

This **Notice** is subject to periodic review to ensure it is in line with applicable legislation.

We retain all applicable ownership rights to information we collect. We reserve the right to change, modify, add or remove provisions of this Notice. Any changes to this Notice will be posted here, and we encourage you to check back from time to time. If the changes are substantial, we will notify the changes to you.