



# **Politik for beskyttet offentliggørelse (whistleblowing)**

## Politik for beskyttet offentliggørelse (whistleblowing)

Ejer af denne politik: Clear Channel Outdoor Holdings, Inc. Chief Compliance Officer

Ikrafttrædelsesdato: 6. december 2021

Forespørgsler om dette charter: kontakt [compliance@clearchannelint.com](mailto:compliance@clearchannelint.com)

### Funktionen af denne politik.

Denne politik er udarbejdet i samråd med nødvendige interessenter og er godkendt af ledelsen i Clear Channel Outer Holdings, Inc. "Clear Channel") og gennemgås regelmæssigt for at sikre overholdelse med den relevante lovgivning om beskyttelse af personlige oplysninger og data.

Alle Clear Channels overholdelsespolitikker understøtter funktionen af **Clear Channels adfærdskodeks og forretningsetik**.

**Clear Channels bestyrelse** er ultimativt ansvarlig for at sikre, at Clear Channel opfylder sine forpligtelser under denne politik under ledelse af **Clear Channels revisionsudvalg**.

**Chief Compliance Officer** har det daglige opsyn med denne politik. Kontakt compliance på [compliance@clearchannelint.com](mailto:compliance@clearchannelint.com), hvis du konstaterer eventuelle problemer med overensstemmelsen i denne politik og reglerne i din retskreds, ønsker at drøfte den eller få forklaringer eller har betænkeligheder i forbindelse med denne politik.

### Lokale variationer.

Det forventes, at du overholder både denne politik og alle lokale variationer af denne politik, hvor de er i kraft tillige med gældende love og bestemmelser, herunder dem, der vedrører de statsborgere, der er indberetningspligtige under denne politik, disse overholdelsesprogrammer og/eller ansættelses- eller arbejdsretten ("**gældende love**"). Gældende love kan i visse tilfælde være mere restriktive end denne politik. Hvor dette er tilfældet, skal de mere restriktive regler følges.

### Undtagelser og dispensationer.

Lokale politikker, der udarbejdes af forretningsenheder, skal være på linje med denne politik. Enhver anmodning om en dispensation eller en ændring af denne politik skal sendes med e-mail til Clear Channels Compliance Officer ([compliance@clearchannelint.com](mailto:compliance@clearchannelint.com)), som har bemyndigelse til efter eget skøn at give en dispensation eller foretage en ændring.

## POLITIK FOR BESKYTTET OFFENTLIGGØRELSE (WHISTLEBLOWING)

### 1. Introduktion til denne politik.

Clear Channel Outdoor Holdings, deres filialer og datterselskaber, er forpligtede til at overholde gældende lovgivning og regler, deres adfærdskodeks og firmapolitikker, samt opretholde de højeste standarder for overholdelse, etik, integritet, åbenhed og ansvarlighed i deres forretningsmæssige aktiviteter.

For at sikre en sådan overholdelse og at vise sin forpligtelse til åben og ansvarlig ledelse har Clear Channel udviklet denne politik for beskyttet offentliggørelse (whistleblowing) ("**denne politik**"), der vejleder i at foretage en **beskyttet offentliggørelse**.

### 2. Hvad er beskyttet offentliggørelse?

Beskyttet offentliggørelse er offentliggørelse af information om forseelser på arbejdspladsen eller i en arbejdsrelateret sammenhæng.

Du kan foretage en beskyttet offentliggørelse via Clear Channels rapporteringskanaler, hvor du har grund til at formode at en eller flere af følgende foregår, er foregået eller er sandsynligt vil foregå i fremtiden:

1. Enhver mistanke om eller faktisk overtrædelse af loven og/eller regler, herunder, men ikke begrænset til, begået kriminalitet (f.eks. bedrageri), brud på en juridisk forpligtelse, juridiske fejl osv.
2. Enhver form for forseelse og alvorlig uredelighed, der udgør ulovlig eller uetisk adfærd på arbejdspladsen, såsom mistanke om eller faktisk overtrædelse af politikker, fejl i en forretningsproces, alvorlig overtrædelse i forhold til Clear Channels adfærdskodeks og politik om forretningsetik osv.
3. Fare for enhver enkeltpersons sundhed og sikkerhed eller skade på miljøet.

### 3. Hvem gælder denne politik for?

Denne politik gælder for enhver, der vælger at bruge Clear Channels interne whistleblower-system til at indberette visse former for forseelser, fra mistanke om eller faktiske overtrædelse af gældende lovgivning og regler til brud på virksomhedens politik og etiske rammer i henhold til denne politik og via Clear Channels rapporteringskanaler.

Denne politik gælder især for:

1. Interne brugere som har fået information om arbejdsrelaterede overtrædelser i sammenhæng med Clear Channel, herunder følgende:
  - (a) Ansatte, underleverandører og selvstændige, der arbejder med Clear Channel, frivillige og betalte og ubetalte praktikanter og alle personer, der arbejder under tilsyn af leverandører og underleverandører.
  - (b) Personer tilhørende Clear Channel's administrative, ledelsesmæssige eller tilsynshavende organer, herunder menige bestyrelsesmedlemmer (samlet benævnt "interne brugere").
2. Eksterne brugere, der indberetter eller offentliggør information om overtrædelser, der er erhvervet i et arbejdsrelateret forhold, som:
  - (a) Siden er ophørt.
  - (b) Omfatter overtrædelser i løbet af ansættelsesprocessen eller andre præ-kontraktmæssige forhandlinger inden den arbejdsmæssige relation påbegyndes.
  - (c) Er aktieindehavere i vores børsnoterede selskaber.
  - (d) Er tredjeparter med forbindelse til den indberettende part og som kunne lide under represalier i en arbejdsmæssig sammenhæng, såsom kolleger eller familie til indberetteren.
  - (e) Er juridiske enheder, som indberetteren ejer, arbejder for eller på anden måde står i forbindelse med i en arbejdsrelateret sammenhæng (samlet benævnt "eksterne brugere").

Clear Channels whistleblower-hotline er ikke designet til at blive brugt af medlemmer af offentligheden eller enkeltpersoner, der ikke er relateret til Clear Channel som nævnt herover.

Hvis du ønsker at udtrykke en bekymring eller foretage en klage, og du ikke er en intern eller ekstern bruger som beskrevet herover, så kontakt Clear Channels kundeansvarlige eller [compliance@clearchannelint.com](mailto:compliance@clearchannelint.com).

Interne brugere bør følge procedurerne i denne politik under ansættelsen eller beskæftigelsen hos Clear Channel, og foretage en beskyttet offentliggørelse, hvis den pågældende er bekymret over en adfærd, som vedkommende er vidne til eller får kendskab til, og som menes at udgøre en alvorlig forseelse (som beskrevet herunder).

#### 4. Hvem er beskyttet under denne politik?

Enhver, som er omfattet af denne politik.

#### 5. Hvilken af Clear Channels indberetningskanaler skal jeg anvende ?

Hvis du er intern bruger og ikke ønsker at tale med din leder eller en lokal repræsentant for personaleafdelingen, juridisk afdeling eller afdelingen for overholdelse, bedes du anvende følgende af Clear Channels indberetningskanaler afhængigt af graden af den alvorlige forseelse, du ønsker at indberette. Hvis du stadig er i tvivl, kan du kontakte [compliance@clearchannelint.com](mailto:compliance@clearchannelint.com) for hjælp.

#### Clear Channels indberetningskanaler for interne brugere for forskellige kategorier af alvorlige forseelser.

Overholdelse kategori	Beskrivelse af alvorlige forseelser	Clear Channels indberetningskanal
<b>Rimelig indberetning (herunder finansielle og Sarbanes Oxley Act-kontroller)</b>	Tyveri, underslæb, hvidvaskning af penge, skatteunddragelse, manipuleret bogføring, alle slags økonomisk bedrageri, økonomisk eller kontraktligt dokumentfalsk, manglende overholdelse af finansforordninger eller interne kontrolprocedurer.  Enhver tilsigtet forvanskning af oplysninger, utilbørlig påvirkning eller problemer med upartiskhed i forbindelse med interaktioner med eksterne eller interne revisorer eller forsømmelse af revisionsfunktioner for aktiviteter, herunder forkerte oplysninger om indtægter, forkerte oplysninger om udgifter, forkerte oplysninger om aktiver, forkert brug af bogføringsprincipper eller andre urigtige transaktioner.	Global Legal på adressen <a href="mailto:legal@clearchannelint.com">legal@clearchannelint.com</a>  Global Compliance på adressen <a href="mailto:compliance@clearchannelint.com">compliance@clearchannelint.com</a>  Via hotlinen for whistleblowing (se bilag 1).
<b>God forretningsetik (herunder kontrol af økonomisk kriminalitet)</b>	Betaling af bestikkelse eller smørepenge til privatpersoner eller offentligt ansatte, korruption, uretmæssige sponsorater, donationer, gaver og underholdning, brud på konkurrence/monopollove eller insiderhandel, interessekonflikter, returkommissioner, bedrageri, pengeafpresning, uretmæssig tilegnelse af virksomhedsaktiver, forfalskninger af kontrakter, rapporter eller poster.	Global Legal på adressen <a href="mailto:legal@clearchannelint.com">legal@clearchannelint.com</a>  Global Compliance på adressen <a href="mailto:compliance@clearchannelint.com">compliance@clearchannelint.com</a>  Via hotlinen for whistleblowing (se bilag 1).
<b>Reelle forhold (herunder misbrug af</b>	Slaveri, menneskehandel, fysisk eller mentalt misbrug, diskrimination eller chikane på grund af en beskyttet karakteristik i henhold til loven, som ikke er dækket af den lokale klagepolitik	Global Compliance på adressen <a href="mailto:compliance@clearchannelint.com">compliance@clearchannelint.com</a>  Via hotlinen for whistleblowing (se bilag 1).

<b>menneskeret tigheder)</b>	eller gengældelse for at have foretaget en beskyttet offentliggørelse.	
<b>Beskyttelse af reelle oplysninger</b>	Databrud, industrispionage, computervira, sabotage eller netkriminalitet.	<b>du SKAL først benytte proceduren for informationssikkerhedsbrud for hastesager på <a href="mailto:informationsecurity@clearchannelint.com">informationsecurity@clearchannelint.com</a></b>
<b>Reel behandling</b>	Et brud på databeskyttelsesloven.	Privacy Office på <a href="mailto:mydata@clearchannelint.com">mydata@clearchannelint.com</a>
<b>Reelt miljø</b>	Miljøforurening, alvorlig mangel på overholdelse af sikker arbejdspraksis, usikre arbejdsforhold og virksomhedsovertrædelser, der indvirker på de ansattes sundhed og sikkerhed. Vold eller trusler mod personsikkerheden.	En leder i forretningsenheden eller Clear Channels hovedkvarter.  Personaleafdelingen i forretningsenheden.  Miljøteamet på <a href="mailto:jade@clearchannelint.com">jade@clearchannelint.com</a>  Via hotlinen for whistleblowing (se bilag 1).
<b>Andre alvorlige forseelser</b>	Andre alvorlige forseelser forudsat, at de relaterer til: en fejl i en forretningsproces der faktisk kan være systemisk, en forbrydelse eller en forseelse, en alvorlig lovovertrædelse af bestemmelser eller politik, et justitsmord, eller hvis forseelsen udgør en alvorlig trussel eller er til skade for almenvellet.	Din lokale eller regionale juridiske afdeling (eller Global Legal på adressen <a href="mailto:legal@clearchannelint.com">legal@clearchannelint.com</a> )  Din lokale Compliance Officer (eller Global Compliance på adressen <a href="mailto:compliance@clearchannelint.com">compliance@clearchannelint.com</a> )  Via hotlinen for whistleblowing (se bilag 1).
<b>Andre anliggender</b>	For alle andre anliggender vedrørende sager, der normalt behandles under procedureerne for klagepolitik og personalefunktioner eller eventuelle problemer omkring forretningsmæssige eller strategiske beslutninger, der er truffet af Clear Channel, som ikke indeholder mistanker eller påstande om alvorlige forseelser.	Din leder.  Teamet i den lokale personaleafdeling.  Den øverste ledelse i Clear Channel.

## 6. Må jeg indberette al beskyttet offentliggørelse via hotlinen for whistleblowing ?

Nogle sager haster. Indberetninger fra hotlinen for whistleblowing når os muligvis ikke med det samme. Brug derfor **IKKE** hotlinen for whistleblowing til at indberette:

- ✗ Hvis dit liv er i overhængende fare. Kontakt den lokale nødtjeneste.
- ✗ Brud på informationssikkerheden (som skal gå direkte og umiddelbart til [informationsecurity@clearchannelint.com](mailto:informationsecurity@clearchannelint.com)).
- ✗ Sager, der er begrænset ved lov i dit land:
  - a. **Sverige:** Sverige tillader kun indberetninger om 'nøglepersoner' i virksomheden. Vi mener, at dette omfatter alle på mindst lederniveau eller højere.
  - b. **Frankrig:** Anonyme indberetninger er exceptionelle og håndteres med specifikke garantier (etablering af alvorlighedsgraden af den indberettede overtrædelse, eksisterende faktiske elementer og forudgående undersøgelse af den første modtager, inden yderligere undersøgelser iværksættes). Du må dog ikke indberette sager i relation til vilkår og betingelser for ansættelse (f.eks. løn, klager, frynsegoder, optjent ferie, arbejdstid, sygdom, opsigelse, chikane, barselsorlov osv.).

Kontakt din lokale complianceansvarlige for yderligere information i relation til specifikke regler, der er gældende for dit locale område.

## 7. Ekstern rapportering

Eksterne rapporteringskanaler for whistleblowing-klager varierer afhængigt af lokale love. Yderligere oplysninger om rapportering af sager til eksterne myndigheder kan findes i tillæg 3.

## 8. Vores forpligtelser over for dig.

Clear Channel vil:

### ✓ Undersøge beskyttede offentliggørelser på en reel måde.

Når Clear Channel efter eget skøn afgør, at der skal foretages en undersøgelse, vil vi i givet fald tale med de relevante parter, gennemgå fakta på en upartisk måde og foretage undersøgelsen i overensstemmelse med **Clear Channels undersøgelsesprotokol** og gældende love og regler.

Undersøgelser kan omfatte interne eller eksterne ressourcer med emneekspertise, alt efter behov eller relevans. Alle beskyttede offentliggørelser vil blive holdt fortrolige og tilstrækkeligt sikrede. Clear Channel beskytter enhver whistleblowers identitet og tolererer ikke nogen form for gengældelse imod dem.

### ✓ Behandle anonyme offentliggørelser på en reel måde.

Vi vil altid læse anonyme offentliggørelser, forudsat at dit land tillader anonyme indberetninger (anonyme indberetninger afvises ikke i Portugal, mens Frankrig har implementeret særlige regler for anonymitet – se afsnit 6).

Clear Channel opfordrer dig dog til at identificere dig selv, når du foretager en beskyttet offentliggørelse. Clear Channel vil altid beskytte whistleblowers identitet. Clear Channel er i stand til at foretage en effektiv og troværdig undersøgelse, hvis de kender din identitet.

Clear Channel kan imidlertid beslutte efter eget rimelige skøn, og efter at have foretaget en passende research, at begrænse sin undersøgelse af anonyme indberetninger og ikke gå videre, hvis den alvorlige forseelse, der indberettes om i den pågældende anonyme indberetning ikke indeholder dokumentation eller andre underbyggende beviser til støtte for beskyldningen. I sådanne tilfælde vil Clear Channel prøve på at kontakte den pågældende enkeltperson, der foretog indberetningen om sin beslutning om at begrænse undersøgelsen.

Hvis du er bekymret om, hvorvidt din identitet afsløres, så kontakt CDPO her: [mydata@clearchannelint.com](mailto:mydata@clearchannelint.com)

### ✓ Sørge for tilstrækkelige sikkerhedsforanstaltninger for whistleblowers.

Clear Channel vil i rimeligt omfang bestræbe sig på at sørge for beskyttelse af alle whistleblowers, som i god tro indberetter deres sager under denne politik. Clear Channel vil beskytte personlige oplysninger, identiteten og fortroligheden for relevante parter og overholde retssikkerheden med hensyn til de anklagede parter.

Din identitet vil ikke blive offentliggjort for nogen, undtagen i de tilfælde hvor offentliggørelse er nødvendig (f.eks. til en korrekt undersøgelse af den beskyttede offentliggørelse, af juridiske årsager, til offentliggørelse for retshåndhævende myndigheder eller tilsynsmyndigheder, til forfølgelse eller forsvar for retskrav eller retspleje) eller med dit samtykke. Hvis vi skal offentliggøre din identitet, vil vi sørge for at sikre, at ingen beskyttet offentliggørelse forårsager gengældelse.

Clear Channel tolererer ikke chikane, gengældelsesaktioner eller forfølgelse af nogen, der foretager en beskyttet offentliggørelse i god tro og alle, der er ansvarlig for skadelig adfærd mod en whistleblower kan underkastes disciplinære sanktioner, der kan omfatte afskedigelse. Hvis du mener, at du har lidt nogen form for skade for at have foretaget en beskyttet offentliggørelse, er det vigtigt, at du informerer compliance så hurtigt som muligt på [compliance@clearchannelint.com](mailto:compliance@clearchannelint.com).

✓ **Fastholde enhver relevant ret til retssikkerhed.**

Alle, der er involveret i en beskyttet offentliggørelse vil modtage enhver relevant ret til retssikkerhed i forhold til den lokale lovgivning, hvor de befinder sig. Dette omfatter sandsynligvis formodningen om at være uskyldige, indtil eller medmindre Clear Channel er nået et stadie, hvor beviset forpligter til efter eget skøn men med rimelige handlinger til at foretage præventive eller disciplinære handlinger over for en enkeltperson.

✓ **Beskytte persondata.**

Beskyttelse af sikkerheden, integriteten og tilgængeligheden af dine og andres **persondata** er vigtig for Clear Channel. Persondata, der opnås via proceduren for beskyttet offentliggørelse, vil blive behandlet i overensstemmelse med gældende databeskyttelseslov og -regler.

**9. Dine forpligtelser over for Clear Channel.**

**DU SKAL:**

✓ **Omgående at lade os det vide, hvis du har problemer.**

Vi er alle forpligtet til at sikre, at vi opererer etisk og inden for lovens rammer. For at sikre at vi overholder juridiske, lovmæssige og selskabsforpligtelser, kræver Clear Channel, at alle interne brugere, og opfordrer eksterne brugere, til at indberette og udtrykke deres bekymringer i forbindelse med alvorlige forseelser, enten fortroligt, eller hvis din retskreds tillader det, anonymt og uden frygt for straf eller en unfair behandling.

I de fleste tilfælde forventer vi, at du foretager en beskyttet offentliggørelse så hurtigt som muligt og inden for tre måneder af den indberettede handling.

✓ **At foretage alle offentliggørelser i god tro.**

Alle interne brugere, som rejser en sag i ond eller skadelig hensigt, eller hvis de ved, at det ikke er sandt, kan risikere disciplinære sanktioner op til og inklusive afskedigelse.

Eksterne brugere, som rejser en sag uden begrundet mistanke om, at det er sandt, mister efter al sandsynlighed enhver juridisk beskyttelse, der ellers ville være tilfældet under whistleblower-lovgivning.

✓ **At anvende den mest relevante Clear Channel-indberetningskanal.**

Interne brugere opfordres til at rejse eventuelle sager via deres forretningsenheds interne klage- og indberetningsprocedurer, som beskrevet i afsnit 5 herover.

Eksterne brugere bør kontakte deres kunderelationsansvarlige eller [compliance@clearchannelint.com](mailto:compliance@clearchannelint.com).

Hvis dette ikke er muligt, anmodes både interne og eksterne brugere omgående indberette den beskyttede offentliggørelse via hotlinen (se bilag 1).

✓ **Ikke gøre gengæld\* mod nogen, som foretager en beskyttet offentliggørelse.**

Hvis du bliver opmærksom på en potentiel beskyttet offentliggørelse, som foretages af andre, enten om dig selv eller andre personer i Clear Channel, skal du kontakte [compliance@clearchannelint.com](mailto:compliance@clearchannelint.com) for at få råd.

Det er vigtigt, at du ikke skaber ulempe for den pågældende person for at have indgivet en klage eller en sag. Hvis du gør det, kan du pålægges disciplinære sanktioner op til og inklusive afskedigelse.

#### **10. Hvad sker der, efter jeg har foretaget en beskyttet offentliggørelse?**

Hvis du har foretaget en beskyttet offentliggørelse under din egen identitet, kan Clear Channel kontakte dig for at få flere oplysninger.

Clear Channel vil, når det er muligt, bestræbe sig på at opdatere dig om udviklingen af enhver undersøgelse vedrørende en beskyttet offentliggørelse, der er relateret til dig. Clear Channel vil dog ikke nødvendigvis være i stand til at bevilge adgang for eller underrette enkeltperson(er), der har foretaget en beskyttet offentliggørelse, eller mistænkte eller implicerede parter, om statussen eller indholdet af den undersøgelsen, der er i gang.

Hvis Clear Channel har brug for, at du afgiver et vidneudsagn, vil vi underrette dig ved først givne lejlighed.



## BILAG 1

### Clear Channels hotline for whistleblowing.

Hotlinen for whistleblowing er et fortroligt (eller anonymt, hvor det er tilladt ifølge loven) web- og telefonbaseret indberetningsværktøj. Den opretholdes af en selvstændig udbyder, [Navex EthicsPoint](#).

### Hvor sendes indberetninger fra hotlinen for whistleblowing hen?

Beskyttede offentliggørelser, der foretages via hotlinen for whistleblowing, vil blive sendt til Clear Channels chefjurist, Chief Compliance Officer og chefrevisoren. Disse personer kan uddelegere ansvaret for undersøgelse af den beskyttede offentliggørelse i overensstemmelse med [undersøgelsesprotokollen](#).

### Hvordan benytter jeg hotlinen for whistleblowing?

Der er to tilgængelige indberetningsmuligheder via hotlinen for whistleblowing:

- **Websiden for hotlinen for whistleblowing**

Du kan sende en online indberetning via [EthicsPoint web link](#)

([clearchannel.navexone.eu/](http://clearchannel.navexone.eu/)).



Hvis du ønsker det, kan du give oplysningerne på dit modersmål, som derefter vil blive oversat. Du kan også vedhæfte eventuelle beviser, som du har samlet til støtte for din beskyttede offentliggørelse ved hjælp af uploadfunktionen.

- **Ring til hotlinen for whistleblowing**

Du foretrækker måske at foretage din indberetning via telefon ved at tale direkte og fortroligt på dit eget sprog med en Navex-sagsbehandler ved at kontakte hotline-telefonnummeret ud for dit land herunder. Hvis det er nødvendigt, vil din beskyttede offentliggørelse bliver oversat til engelsk på dine vegne. Navex-sagsbehandlerne vil også kunne hjælpe dig med at uploade bevis til støtte for din beskyttede offentliggørelse eller besvare eventuelle proceduremæssige spørgsmål.

Visse numre virker ikke fra visse mobiltelefoner på grund af restriktioner fra landets egne netværksudbydere. Hvis det er tilfældet, bedes du benytte det online indberetningsværktøj.

Læs [FAQs](#) (ofte stillede spørgsmål) på Navex' website for at få flere oplysninger om hotlinen for whistleblowing.

## Hotlinens telefonnumre

<b>Indberet (globalt):</b>	<b>online</b>	<a href="http://clearchannel.navexone.eu">clearchannel.navexone.eu</a>
<b>Land</b>	<b>Telefonnumre:</b> Hvert land har fået tildelt et ettrinsgratisnummer.	
<b>Belgien</b>	0800 79 562	
<b>Danmark</b>	80830187	
<b>Estland</b>	8000 100 374	
<b>Finland</b>	0800 416143	
<b>Frankrig</b>	0 800 90 53 77	
<b>Irland</b>	1800851826	
<b>Italien</b>	800725910	
<b>Letland</b>	80205326	
<b>Litauen</b>	880000038	
<b>Holland</b>	0800 0232873	
<b>Nordirland</b>	0800 048 5538	
<b>Norge</b>	800 62 458	
<b>Polen</b>	800005124	
<b>Singapore</b>	8008526927	
<b>Spanien</b>	900876038	
<b>Sverige</b>	0200889632	
<b>Schweiz</b>	0800 000 619	
<b>Storbritannien</b>	0800 048 5538	
<b>USA</b>	(844) 715-9350	
<b>Peru</b>	80078572	
<b>Brasilien</b>	0800 000 0364	
<b>Mexico</b>	8006816910	
<b>Chile</b>	800914365	
<b>Kina</b>	4001200407	

## BILAG 2

### Ordliste

**Undersøgelingsprotokol** betyder Clear Channels overholdelsesdokument, som beskriver de procedurer, der skal følges i undersøgelser af beskyttede offentliggørelser. Den kan leveres på forlangende fra compliance på [compliance@clearchannelint.com](mailto:compliance@clearchannelint.com)

**Legitime forretningsårsager:** indeholder håndtering af virksomhedskriminalitet, der involverer Clear Channel, herunder bedrageri, korruption, overtrædelser af skattelovgivningen eller sanktioner, beskyttelse af vores forretningsintegritet og -omdømme, beskyttelse og varetagelse af vores medarbejdere, samt overholdelse af regler og love og vores forpligtelse til regulatorisk indberetning.

**Lokal Compliance Officer (LCO):** betyder den leder, sædvanligvis den juridiske direktør eller finansdirektør, som er udpeget til at føre tilsyn med compliance i din forretningsenhed eller -region.

**Persondata:** betyder alle oplysninger, der har relation til en identificeret eller identificerbar fysisk person, dvs. en person, der kan identificeres, direkte eller indirekte, af en identifikator: ID-nummer, placeringsdata, online identifikator eller faktorer, der er specifikke for den fysiske, psykologiske, genetiske, mentale, økonomiske, kulturelle eller sociale identitet, der har relation til en person, der er i, eller sandsynligvis kommer i, Clear Channels besiddelse.

### BILAG 3

Dette tillæg giver en oversigt på højt niveau over whistleblower-lovgivningen på tværs af forskellige markeder, hvor Clear Channel opererer, og angiver kompetente myndigheder, hvortil der kan indgives eksterne rapporter, hvis en person er utilfreds med Clear Channels interne rapporteringssystem.<sup>1</sup> Bemærk, at denne liste ikke er udtømmende, og der kan eksistere andre whistleblowing-beskyttelser og rapporteringsbestemmelser i lokale love/provinslove, som ikke er indeholdt i dette tillæg.

Hvis du har brug for flere oplysninger om dine lokale whistleblowing-love og eksterne rapporteringskanaler, bedes du kontakte Clear Channel Compliance-teamet ([compliance@clearchannelint.com](mailto:compliance@clearchannelint.com))

#### Whistleblowing-love og eksterne rapporteringskanaler, der gælder for vores europæiske markeder

Land	Whistleblowing-lovgivning	Eksterne koordinerende organer/kompetente myndigheder
<b>Belgien</b>	Den belgiske lov om beskyttelse af personer, der rapporterer overtrædelser af national lovgivning eller EU-lovgivning	Føderal ombudsmand
<b>Danmark</b>	Den danske lov om beskyttelse af whistleblowere	Varierer afhængig af problemstilling. Sager i forbindelse med databeskyttelse kan f.eks. rapporteres til datatilsynet
<b>Estland</b>	TBC	TBC
<b>Finland</b>	Lov om beskyttelse af whistleblowere 1171/2022	Justitsministeriet
<b>Frankrig</b>	Dekret nr. 2022-1686 (den franske whistleblowing-lovgivning)	Forsvarsministeriet
<b>Irland</b>	Loven om databeskyttelse (ændring) 2022	Ombudsmandens kontor (OPDC, Protected Disclosures Commissioner)
<b>Italien</b>	Dekret nr. 24/2023 (den italienske whistleblowing-lovgivning)	National antikorrupsionsmyndighed (ANAC, National Anti-Corruption Authority)
<b>Letland</b>	Lov om whistleblowing	Whistleblower-kontakt i statsministeriet
<b>Litauen</b>	Lov om beskyttelse af whistleblowere i Republikken Litauen	Den offentlige anklagemyndighed i Republikken Litauen
<b>Holland</b>	Den hollandske whistleblower-lov	Den hollandske whistleblower-myndighed
<b>Norge</b>	Norsk arbejdsmiljølov (WEA, Working Environment Act) (afsnit 2A) <i>NB: Gælder kun medarbejdere</i>	Varierer afhængig af problemstilling. Der er flere offentlige tilsynsmyndigheder, der behandler anmeldelser, såsom det norske arbeidstilsyn, politiet og datatilsynet
<b>Polen</b>	Den polske lov om beskyttelse af personer, der anmelder lovbrud – TBC	Den polske ombudsmand – TBC
<b>Spanien</b>	Whistleblowing-lov 2/2023	Uafhængig myndighed til beskyttelse af whistleblowere (AAI)
<b>Sverige</b>	Den (nye) svenske whistleblower-lov (SFS 2021:890)	Flere kompetente tilsyn, herunder det svenske finanstilsyn, det svenske databeskyttelsestilsyn og det svenske arbejdsmiljøtilsyn.

<sup>1</sup> Fra 6. april 2023 (dato for udarbejdelse)

<b>UK</b>	Loven om beskyttelse af offentligt ansatte 1998	Variere efter problemstilling. For eksempel kan sager vedrørende databeskyttelse eller miljøet rettes til henholdsvis informationskommissæren eller miljøstyrelsen
-----------	---	--

#### Whistleblowing-love og eksterne rapporteringskanaler, der gælder for vores latinamerikanske markeder

<b>Land</b>	<b>Whistleblowing-lovgivning</b>	<b>Eksterne koordinerende organer/kompetente myndigheder</b>
<b>Brasilien</b>	Brasiliansk lov til bekæmpelse af kriminalitet (artikel 15 i føderal lov 13.964/2019) Lov om beskyttelse af ofre og vidner (føderal lov 9.807/1999)	Variere efter problemstilling. Omfatter administrationsrådet for økonomisk forsvar (CADE, Administrative Council for Economic Defense) og den offentlige anklagemyndighed.
<b>Chile</b>	Lov nr. 20.393/Lovdekret nr. 2 af 1976	Arbejdsnævnet eller domstolene
<b>Mexico</b>	TBC	TBC
<b>Peru</b>	Lov nr. 30424/lovgivningsdekret 1327 (artikel 2)	Ministerium for institutionel integritet

#### Whistleblowing-love og eksterne rapporteringskanaler, der gælder for vores amerikanske markeder

<b>Land</b>	<b>Whistleblowing-lovgivning</b>	<b>Eksterne koordinerende organer/kompetente myndigheder</b>
<b>USA</b>	Lov om beskyttelse af whistleblowere af 1989	SEC – Office of the Whistleblower