Privacy Reglement

buma·stemra

25 mei 2018

Inhoud

1 Inleiding

Vereniging Buma/Stichting Stemra ('buma•stemra') is de auteursrechtenorganisatie van muziekauteurs en muziekuitgevers in Nederland en vertegenwoordigt de belangen van haar leden wereldwijd. Wij zorgen ervoor dat de ruim 25.000 aangesloten componisten, tekstschrijvers en uitgevers een vergoeding ontvangen als hun muziek gebruikt wordt. Daarnaast promoten wij Nederlandse muziek als internationaal product door het organiseren, financieren en sponsoren van talrijke muziekevenementen door Buma Cultuur.

Opslag en Verwerking van Persoonsgegevens is voor de uitvoering van deze taken essentieel. Dit dient met de grootste zorgvuldigheid te gebeuren omdat misbruik van Persoonsgegevens tot grote schade kan leiden voor betrokkenen, zoals rechthebbenden, muziekgebruikers en medewerkers, maar ook voor buma•stemra als organisatie. Wij hechten dan ook veel waarde aan het beschermen van de Persoonsgegevens die aan ons worden verstrekt en aan de wijze waarop Persoonsgegevens worden verwerkt.

Dit privacy beleid beschrijft hoe buma•stemra omgaat met Persoonsgegevens en welke uitgangspunten hierbij gelden. buma•stemra neemt hiermee haar verantwoordelijkheid voor de kwaliteit en de bescherming van de door haar verwerkte Persoonsgegevens, om daarmee aan alle geldende wet- en regelgeving te voldoen.

1.1 Definities

Begrip	Afkorting	Toelichting
Algemene Verordening Gegevensbescherming	AVG	Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG.
Autoriteit Persoonsgegevens	AP	Nationale toezichthouder op de AVG en andere wet- en regelgeving voor de Verwerking van Persoonsgegevens.
Betrokkene		Degene op wie een Persoonsgegeven betrekking heeft.
Bewaartermijn		Periode dat een Persoonsgegeven bewaard wordt in een vorm die het mogelijk maakt de betrokkene te identificeren.

Begrip	Afkorting	Toelichting
Bijzondere Persoonsgegevens		Gevoelige Persoonsgegevens die door de wetgever extra zijn beschermd, waaronder gegevens betreffende ras, godsdienst, gezondheid, politieke overtuiging, seksuele geaardheid, lidmaatschap vakbond of strafrechtelijk verleden.
Data-eigenaar		Degene die verantwoordelijk is voor (een deel van) de in de systemen opgeslagen Persoonsgegevens en ervoor zorgt dat deze de opslag en het gebruik van deze data in overeenstemming is met het vastgestelde Reglement en de geldende wet- en regelgeving, waaronder die op het gebied van privacy.
Datalek (Inbreuk in verband met persoonsgegevens)		Een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.
Datalek dossier		Dossier waarin alle informatie met betrekking tot een Datalek wordt vastgelegd.
Datalek register		Register waarin alle Datalek dossiers zijn opgeslagen.
Derde		Natuurlijke of rechtspersoon, niet zijnde Betrokkene, Verantwoordelijke, Verwerker of persoon die onder rechtstreeks gezag van de Verantwoordelijke of de Verwerker gemachtigd is om Persoonsgegevens te Verwerken.
Doelbinding		Een precieze en duidelijke omschrijving van een doel of verschillende samenhangende doeleinden, waarmee de Verwerkingsverantwoordelijke tot uitdrukking brengt waarvoor hij de Persoonsgegevens verwerkt.
Incident		Iedere vraag, klacht of melding die door de Service Desk geregistreerd wordt.
Incident Management Proces		Het proces dat beschrijft welke stappen bij de afwikkeling van een Incident genomen worden,

Begrip	Afkorting	Toelichting
		welke rollen hierbij betrokken zijn en hoe dit wordt vastgelegd.
Major Incident		Incident dat met de hoogste prioriteit moet worden afgehandeld.
Opt-in		Opname op verzendlijst na expliciet verzoek van betrokkene.
Opt-out		Verwijdering van verzendlijst na expliciet verzoek van betrokkene.
Persoonsgegeven		Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.
Privacy by Default		Maximale privacy-vriendelijkheid als uitgangspunt bij de inrichting van processen, systemen en applicaties
Privacy by Design		Het beheer van de gehele levenscyclus van Persoonsgegevens, vanaf het verzamelen tot het Verwerken en verwijderen, waarbij stelselmatig aandacht wordt besteed aan het borgen van nauwkeurigheid, vertrouwelijkheid, integriteit, fysieke veiligheid en verwijderingsmogelijkheid van de Persoonsgegevens.
Privacy Impact Assessment	PIA	Een methode die helpt bij het identificeren van privacy risico's en handvatten levert om deze risico’s te beheersen.
Privacy Incident		Iedere vraag, klacht of melding met betrekking tot de Verwerking van Persoonsgegevens.
Privacy Incident Response Team	PIRT	Multidisciplinair team dat door de Privacy Officer kan worden ingeschakeld om bij ernstige Privacy Incidenten snel en doortastend te kunnen handelen.
Privacy Officer	PO	Door Verwerkingsverantwoordelijke benoemde functionaris die het aanspreekpunt is voor alle privacy gerelateerde zaken, de organisatie adviseert over het voldoen aan wet- en regelgeving rondom privacy en de naleving ervan toetst. Tevens aanspreekpunt voor de Autoriteit Persoonsgegevens.
Procedure Melding Datalekken		Procedure die beschrijft hoe de melding en afwikkeling van een potentieel Datalek

Begrip	Afkorting	Toelichting
		plaatsvindt. Onderdeel van de procedure zijn de beslissingscriteria voor het al dan niet melden van een Datalek bij de Autoriteit Persoonsgegevens en bij Betrokkene.
Register van verwerkingsactiviteiten		Een register van de verwerkingsactiviteiten die onder de verantwoordelijkheid van de verwerkingsverantwoordelijke plaatsvinden en van de verwerkingsactiviteiten die in de rol van verwerker ten behoeve van verwerkingsverantwoordelijken zijn verricht.
Reglement		Reglement waarin het beleid met betrekking tot het Verwerken van Persoonsgegevens is vastgelegd.
Service Desk		Afdeling waar alle Incidenten worden gemeld en geregistreerd.
Systeemeigenaar		Degene die ervoor verantwoordelijk is dat een applicatie en bijbehorende ICT-faciliteiten een goede ondersteuning bieden aan de processen waarin deze gebruikt worden, zoveel mogelijk beantwoorden aan de eisen en wensen van de gebruikers en in overeenstemming zijn met het Privacy Regelement en de geldende wet- en regelgeving.
Verwerken/Verwerking van Persoonsgegevens		Elke handeling of geheel van handelingen met betrekking tot Persoonsgegevens, waaronder in ieder geval verzamelen, vastleggen, ordenen, bewaren, wijzigen, raadplegen, gebruiken, verstrekken en vernietigen.
Verwerker		Natuurlijke of rechtspersoon aan wie de Verantwoordelijke enige vorm van Verwerking van Persoonsgegevens heeft uitbesteed.
Verwerkingsverantwoordelijke		Natuurlijke of rechtspersoon die het doel en de middelen voor verwerking van Persoonsgegevens vaststelt.

1.2 Reikwijdte en doelstelling van het Reglement

Het Reglement heeft betrekking op het Verwerken van Persoonsgegevens van alle Betrokkenen binnen buma•stemra, waaronder in ieder geval alle leden, deelnemers, muziekgebruikers, medewerkers en externe relaties, alsmede op anderen van wie buma•stemra Persoonsgegevens verwerkt.

In het Reglement ligt de nadruk op de geheel of gedeeltelijk geautomatiseerde/systematische Verwerking van Persoonsgegevens die plaatsvindt onder de verantwoordelijkheid van buma•stemra, alsmede op de daaraan ten grondslag liggende documenten die in een bestand zijn opgenomen. Eveneens is het Reglement van toepassing op niet-geautomatiseerde Verwerking van Persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

Bij buma•stemra wordt het beschermen van Persoonsgegevens breed geïnterpreteerd. Er is een belangrijke relatie en gedeeltelijke overlap met het aanpalende beleidsterrein informatiebeveiliging, waarbij het gaat om de beschikbaarheid, integriteit en de vertrouwelijkheid van data, waaronder Persoonsgegevens. Op strategisch niveau wordt aandacht geschonken aan deze raakvlakken en wordt zowel planmatig als inhoudelijk afstemming gezocht.

Het Reglement bij buma•stemra heeft als doel om de kwaliteit van de Verwerking en de beveiliging van Persoonsgegevens te optimaliseren, waarbij een goede balans moet worden gevonden tussen privacy, functionaliteit en veiligheid. Beoogd wordt de persoonlijke levenssfeer van de Betrokkene zoveel mogelijk te respecteren. Alle gegevens die betrekking hebben op een Betrokkene dienen beschermd te worden tegen onwettelijk en ongeautoriseerd gebruik en andere vormen van misbruik, op basis van het fundamenteel recht op bescherming van zijn/haar Persoonsgegevens. Dit brengt met zich mee dat het Verwerken van Persoonsgegevens dient te voldoen aan alle relevante wet- en regelgeving en dat Persoonsgegevens veilig zijn bij buma•stemra.

Doelstelling van het Reglement:

- het creëren van bewustwording binnen buma•stemra van het belang en de noodzaak van het beschermen van Persoonsgegevens;
- het bieden van een kader: het Reglement biedt een kader om (toekomstige) Verwerkingen van Persoonsgegevens te toetsen en taken, bevoegdheden en verantwoordelijkheden te beleggen in de organisatie;
- het stellen van normen: de basis voor de beveiliging van Persoonsgegevens is vastgelegd in het IT beveiligingsbeleid van buma•stemra. Maatregelen worden genomen op basis van best practices;
- het nemen van de verantwoordelijkheid: door de uitgangspunten en de verantwoordelijkheden van alle betrokkenen bij het Verwerken van Persoonsgegevens expliciet vast te leggen;

- daadkrachtige implementatie van het Reglement door duidelijke keuzes in maatregelen te maken en actieve controle toe te passen op de uitvoering van de beleidsmaatregelen;
- compliant zijn met de Nederlandse en Europese wetgeving, waaronder de Uitvoeringswet AVG en de AVG.

2 Beleidsprincipes Verwerking Persoonsgegevens

- Algemeen beleidsuitgangspunt is dat Persoonsgegevens in overeenstemming met de relevante wet- en regelgeving op rechtmatige, behoorlijke en transparante wijze worden verwerkt. Hierbij dient een goede balans te worden aangebracht tussen het belang van buma•stemra om Persoonsgegevens te Verwerken en het belang van Betrokkene om eigen keuzes te maken met betrekking tot zijn Persoonsgegevens.
- Om aan bovenstaand beleidsuitgangspunt te voldoen gelden de volgende principes:
- Een Verwerking van Persoonsgegevens is gebaseerd op één van de wettelijke grondslagen zoals genoemd in artikel 6 van de AVG;
- Persoonsgegevens worden alleen verwerkt voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden ("Doelbinding"). Deze doeleinden zijn concreet en voorafgaand aan de Verwerking geformuleerd;
- Een Verwerking van Persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt tot de Persoonsgegevens die noodzakelijk zijn voor het specifieke doeleinde. De gegevens dienen met het oog op dat doel toereikend, ter zake dienend en niet bovenmatig te zijn;
- Verwerking van Persoonsgegevens gebeurt op de minst ingrijpende wijze en dient in redelijke verhouding te staan tot het beoogde doeleinde;
- Er worden maatregelen getroffen om zoveel mogelijk te waarborgen dat de te Verwerken Persoonsgegevens juist en actueel zijn;
- Persoonsgegevens worden adequaat beveiligd volgens de geldende beveiligingsnormen.
- Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen;
- Persoonsgegevens worden niet langer verwerkt dan noodzakelijk is voor de doeleinden van de Verwerking, hierbij worden de van toepassing zijnde bewaar- en vernietigtermijnen in acht genomen;
- Iedere Betrokkene heeft recht op inzage respectievelijk rectificatie of wissing, beperking en overdracht van de in de afzonderlijke Verwerkingen hem betreffende Persoonsgegevens, en heeft het recht van bezwaar, zoals geformuleerd in hoofdstuk 7 van dit Reglement;
- Bij alle registraties op vrijwillige basis zal aan de Betrokkene een eenduidige zogenaamde Opt-out procedure worden aangeboden.

3 Rollen en verantwoordelijkheden met betrekking tot Verwerking Persoonsgegevens

Om de Verwerkingen van Persoonsgegevens gestructureerd en gecoördineerd te laten verlopen is bij buma•stemra een aantal rollen onderkend en toegewezen aan functionarissen in de bestaande organisatie.

3.1 Directie

De directie is eindverantwoordelijk voor de rechtmatige en zorgvuldige Verwerking van Persoonsgegevens binnen buma•stemra en stelt het Reglement, de maatregelen en de procedures op het gebied van Verwerking vast, overeenkomstig de mandateringsafspraken zoals vastgelegd in het Reglement Bestuur en Directie.

De directie is tevens verantwoordelijk voor de uitvoering van het vastgestelde Reglement, maatregelen en procedures met betrekking tot de Verwerking van Persoonsgegevens binnen buma•stemra

3.2 Afdelingshoofden en managers

Afdelingshoofden en managers zijn verantwoordelijk voor integratie van het reglement in de dagelijkse bedrijfsvoering en de bewustwording en naleving van het Reglement door de medewerkers die onder hen vallen. Iedere leidinggevende heeft de taak om:

- ervoor te zorgen dat zijn medewerkers op de hoogte zijn van het Reglement;
- toe te zien op de naleving van het Reglement door zijn medewerkers;
- periodiek het onderwerp privacy onder de aandacht te brengen in werkoverleggen.

3.3 Medewerkers, Verwerkers en Derden

Alle medewerkers van buma•stemra, inclusief inhuurkrachten, zijn verantwoordelijk om kennis te nemen van het Reglement, de maatregelen en procedures op het gebied van Verwerking en deze na te leven. Verwerkers en Derden worden hierover door buma•stemra geïnformeerd.

3.4 Systeemeigenaren

Voor alle applicaties wordt een Systeemeigenaar benoemd. De Systeemeigenaar is ervoor verantwoordelijk dat de applicatie en bijbehorende ICT-faciliteiten een goede ondersteuning bieden aan de processen waarin deze gebruikt worden en voldoen aan het Reglement. Dit betekent dat de Systeemeigenaar ervoor zorgt de applicatie blijft beantwoorden aan de eisen en wensen van de gebruikers en de geldende wet- en regelgeving, waaronder die op het gebied van privacy.

3.5 Data-eigenaren

Voor alle Persoonsgegevens wordt een Data-eigenaar benoemd. De Data-eigenaar is verantwoordelijk voor (een deel van) de in de systemen opgeslagen Persoonsgegevens en zorgt ervoor dat deze de opslag en het gebruik van deze data in overeenstemming is met het vastgestelde Reglement en de geldende wet- en regelgeving, waaronder die op het gebied van privacy.

3.6 Privacy Officer

Bij buma•stemra is een Privacy Officer aangesteld. De Privacy Officer adviseert de organisatie in het voldoen aan de geldende en toekomstige wet- en regelgeving rondom privacy en gegevensbescherming en is intern en extern het aanspreekpunt over alle privacy gerelateerde zaken. De Privacy Officer is deskundig op het gebied van privacyregelgeving, onafhankelijk en rapporteert direct aan de directie.

Om zijn of haar taken goed te kunnen uitoefenen, beschikt de Privacy Officer, voor zover noodzakelijk is voor de uitoefening hiervan, over de bevoegdheid om ruimtes te betreden (inclusief serverruimtes), de bevoegdheid om inlichtingen en inzage te vragen en de bevoegdheid om zaken te onderzoeken.

Tot de taken van de Privacy Officer behoort:

- het inventariseren van de binnen buma•stemra verwerkte Persoonsgegevens, het bijhouden van een register hiervan en, indien wettelijk verplicht, het zorgdragen voor de aanmelding van registraties bij de Autoriteit Persoonsgegevens;
- toezien op de naleving van de wettelijke regels over het Verwerken van Persoonsgegevens binnen buma•stemra;
- het bijhouden van een Incidenten register, het doen van wettelijk verplichte meldingen met betrekking tot Incidenten aan de Autoriteit Persoonsgegevens en/of Betrokkenen en het bijhouden van dossiers over deze Incidenten;
- het geven van voorlichting en advies met betrekking tot de omgang met Persoonsgegevens in de context van de eigen organisatie en werkprocessen;
- het adviseren bij het vaststellen en realiseren van een passend niveau van informatiebeveiliging;
- de behandeling van klachten over het gebruik van Persoonsgegevens, onderzoeken uitvoeren of bemiddelen tussen klager en Verwerkingsverantwoordelijke;
- het ontwikkelen van interne normenkaders met betrekking tot de omgang met Persoonsgegevens;
- het zorgdragen voor blijvende bewustheid van privacy risico's bij de medewerkers.

4 Implementatie van het Reglement

De directie van buma•stemra is verantwoordelijk voor Verwerkingen van de Persoonsgegevens en stelt hiervoor het doel en de middelen vast. Zij wordt aangemerkt als de Verwerkingsverantwoordelijke in de zin van de Algemene Verordening Gegevensbescherming. De feitelijke Verwerking van Persoonsgegevens wordt op de organisatieniveaus eronder uitgevoerd.

Het goed, efficiënt en verantwoord leiden van een organisatie wordt aangeduid met de term governance. Onderdeel hiervan is de relatie van de Verwerkingsverantwoordelijke met de belangrijkste belanghebbenden van buma•stemra, waaronder de interne en externe toezichthouders, leden, deelnemers, muziekgebruikers, medewerkers en externe relaties, alsmede anderen van wie buma•stemra Persoonsgegevens verwerkt. Een goed corporate governance-beleid draagt zorg voor de rechten van alle belanghebbenden.

4.1 Verdeling van de verantwoordelijkheden

Het zorgvuldig Verwerken van Persoonsgegevens is een lijnverantwoordelijkheid. Dit betekent dat afdelingshoofden en managers als lijnmanagers de primaire verantwoordelijkheid dragen voor een zorgvuldige Verwerking van Persoonsgegevens op hun afdeling. Dit omvat ook de keuze van maatregelen en de uitvoering en handhaving ervan. Onder de lijnverantwoordelijkheid valt ook de taak om het Reglement met betrekking tot de Verwerking van Persoonsgegevens te communiceren met alle relevante partijen, zoals bijvoorbeeld contractspartijen.

Het zorgvuldig omgaan met Persoonsgegevens is tevens ieders eigen verantwoordelijkheid. Van medewerkers wordt verwacht dat ze zich integer gedragen. Daaronder wordt mede verstaan dat de privacy van anderen wordt gerespecteerd. Niet acceptabel is dat door al dan niet opzettelijk gedrag van medewerkers onveilige of anderszins ongewenste situaties ontstaan, die kunnen leiden tot schade en/of imagoverlies van buma•stemra of van individuen.

4.2 Overlegstructuren

Om de samenhang in de organisatie met betrekking tot gegevensbescherming goed tot uitdrukking te laten komen en de initiatieven en activiteiten op het gebied van Verwerking van Persoonsgegevens binnen de verschillende onderdelen op elkaar af te stemmen, is het belangrijk om gestructureerd overleg te voeren over het onderwerp privacy op verschillende niveaus.

Op strategisch niveau wordt richtinggevend gesproken over governance en compliance, alsmede over doelen, scope en ambitie op het gebied van privacyaspecten. Het strategisch niveau wordt ingevuld in de directie.

Op tactisch niveau wordt de strategie vertaald naar plannen, te hanteren normen, en evaluatiemethoden. Deze plannen en instrumenten zijn sturend voor de uitvoering. Het tactisch niveau wordt ingevuld in de directie en overleg met de managers.

Op operationeel niveau worden de zaken besproken die de dagelijkse bedrijfsvoering (uitvoering) aangaan. Het operationeel niveau wordt ingevuld in de afdelingsoverleggen.

4.3 Bewustwording en training

Teneinde de risico's op het terrein van het Verwerken van Persoonsgegevens zo veel mogelijk te beheersen, is naast het opstellen en implementeren van beleid en uitvoeringsmaatregelen tevens doorlopende aandacht nodig voor het risicobewustzijn van medewerkers. Onderdeel van het beleid is dan ook het nemen van maatregelen om dit risicobewustzijn te bevorderen, zodat kennis van risico's wordt verhoogd en (veilig en verantwoord) gedrag wordt aangemoedigd, onder andere door regelmatig terugkerende bewustwordingscampagnes voor medewerkers.

Doorlopende aandacht voor het risicobewustzijn van medewerkers is één van de taken van de Privacy Officer.

4.4 Interne audit

Audits maken het mogelijk het Reglement vastgelegde beleid en de genomen maatregelen te controleren op effectiviteit. De Privacy Officer initieert gezamenlijk met de IT Security Officer en het Hoofd Audit de controle op het rechtmatig en zorgvuldig Verwerken van Persoonsgegevens.

Eventuele externe controles worden uitgevoerd door onafhankelijke accountants. Dit is gekoppeld aan het jaarlijkse accountantsonderzoek en wordt zoveel mogelijk geïntegreerd in de reguliere Planning & Control cyclus.

Mocht de naleving van het beleid en/of de bescherming van data- en privacygegevens ernstig tekort schieten, dan kan de directie de betrokken verantwoordelijke medewerkers een sanctie opleggen, binnen de kaders van de CAO en de wettelijke mogelijkheden.

5 Rechtmatige, behoorlijke en transparante Verwerking van Persoonsgegevens

5.1 Grondslag, doelbinding en belangenafweging

Het Verwerken van Persoonsgegevens moet gebaseerd zijn op een van de wettelijke gronden zoals beschreven in artikel 6 van de AVG. De Verwerkingsverantwoordelijke omschrijft vooraf de doeleinden voor de Verwerking. Deze doeleinden zijn concreet en specifiek geformuleerd. Bij elke Verwerking wordt getoetst in hoeverre het Verwerken van Persoonsgegevens noodzakelijk is. Hierbij worden de verschillende belangen afgewogen en wordt gekeken naar de doelmatigheid, proportionaliteit en subsidiariteit. Persoonsgegevens worden niet verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen.

buma•stemra treft de nodige maatregelen om te zorgen dat Persoonsgegevens, gelet op de doeleinden waarvoor zij worden verzameld of Verwerkt, juist en nauwkeurig zijn.

Een overzicht van de door buma•stemra verwerkte categorieën Persoonsgegevens is opgenomen in de Bijlage. Per categorie is aangegeven wat hiervoor de wettelijke grondslag en de doelbinding is, wat de maximale bewaartermijn is en wie de rol van Data-eigenaar heeft.

5.2 Bij nieuwe projecten en wijzigingen: uitvoeren Privacy Impact Assessment (PIA)

Bij (onderzoeks)projecten, infrastructurele wijzigingen of de aanschaf van nieuwe systemen, wordt vanaf de start rekening gehouden met de inrichting van privacy door een Privacy Impact Assessment (PIA) uit te voeren. Het is de taak van de Privacy Officer de PIA goed te keuren. buma•stemra hanteert bij de implementatie de principes Privacy by Design en Privacy by Default.

Een PIA is ook wettelijk verplicht indien een beoogde nieuwe verwerking een *hoog risico* voor betrokkenen met zich meebrengt. Dan moet de PIA aan een aantal eisen voldoen. Of sprake is van een *hoog risico* kan worden uitgemaakt aan de hand van de 9 door de Artikel 29-werkgroep gepubliceerde criteria.[1] Een PIA is met name wettelijk verplicht indien een verwerking betrekking heeft op (art. 35, lid 3, AVG):

- ‘een systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen, die is gebaseerd op geautomatiseerde verwerking, waaronder profilering, en waarop besluiten worden gebaseerd waaraan voor de

[1] *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679 (WP248rev.01), Artikel 29-werkgroep april 2017.*

natuurlijke persoon rechtsgevolgen zijn verbonden of die de natuurlijke persoon op vergelijkbare wijze wezenlijk treffen;
- grootschalige verwerking van bijzondere categorieën van persoonsgegevens […] of van gegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten […]; of
- stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten'.

5.3 Melden en documenteren van Verwerkingen

De Verwerking van Persoonsgegevens wordt door afdelingshoofden bij de Privacy Officer gemeld voor opname in het Register van de Verwerkingsactiviteiten van buma•stemra.

De Verwerkingen worden gemeld aan de Privacy Officer onder opgave van de volgende gegevens:

	Rol van buma•stemra	
	Verwerkings-verantwoordelijke	Verwerker
Naam en contactgegevens verantwoordelijke(n)	X	X
Naam en contactgegevens van de verwerker(s)		X
Verwerkingsdoeleinden	X	
Categorieën van betrokkenen en van gegevens	X	
Categorieën van ontvangers (onder andere in derde landen)	X	
Doorgiften aan een derde land (inclusief passende waarborgen)		X
Bewaartermijnen	X	
Algemene beschrijving van technische en organisatorische maatregelen	X	X

5.4 De organisatie van de beveiliging

buma•stemra draagt zorg voor een adequaat beveiligingsniveau en legt passende technische en organisatorische maatregelen ten uitvoer om Persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige Verwerking. Deze maatregelen zijn er mede op

gericht onnodige c.q. onrechtmatige verzameling en Verwerking van Persoonsgegevens te voorkomen.

Een risicoanalyse op privacybescherming en informatiebeveiliging maakt deel uit van het intern risicobeheersings- en controlesysteem van buma•stemra.

5.5 Geheimhouding

Bij buma•stemra worden alle Persoonsgegevens als vertrouwelijk geclassificeerd. Een ieder behoort de vertrouwelijkheid van Persoonsgegevens te kennen en daarnaar te handelen.

Ook personen voor wie niet reeds uit hoofde van ambt, beroep of wettelijk voorschrift een geheimhoudingsplicht geldt, zijn verplicht tot geheimhouding van de Persoonsgegevens waarvan zij kennis nemen, behoudens voor zover enig wettelijk voorschrift hen tot mededeling verplicht of uit hun taak de noodzaak tot mededeling voortvloeit.

5.6 Bewaartermijnen/ vernietigingstermijnen per soort gegeven

Persoonsgegevens worden niet langer bewaard dan noodzakelijk is voor de doeleinden waarvoor zij zijn verzameld of worden gebruikt. Hoe lang bepaalde gegevens worden bewaard, is afhankelijk van de aard van de gegevens en de doeleinden waarvoor zij worden verwerkt. De bewaartermijn kan dus per doel verschillen. buma•stemra zal de Persoonsgegevens na het verlopen van de bewaartermijn vernietigen of, indien de Persoonsgegevens bestemd zijn voor historische, statistische of wetenschappelijke doeleinden, in een archief bewaren en passende waarborgen bieden, waaronder anonimisering en/of pseudonimisering indien mogelijk.

5.7 Bijzondere Persoonsgegevens

Onder bijzondere Persoonsgegevens vallen gegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging en strafrechtelijke gegevens.

buma•stemra legt in principe geen bijzondere Persoonsgegevens vast, tenzij dit strikt noodzakelijk is en de Verwerking van deze gegevens geschiedt op basis van een wettelijke grondslag, uitdrukkelijke toestemming van de Betrokkene of een zwaarwegend algemeen belang.

Bij de Verwerking van bijzondere Persoonsgegevens kan door de Privacy Officer geoordeeld worden dat voor deze gegevens, in aanvulling op het algemene beveiligingsniveau, extra beveiligingsmaatregelen nodig zijn.

5.8 Doorgifte van Persoonsgegevens aan Derden

5.8.1 Uitbesteden van Verwerking aan een Verwerker

- Indien buma•stemra Persoonsgegevens laat Verwerken door een Bewerker, wordt de uitvoering hiervan geregeld in een verwerkersovereenkomst. Dit is een schriftelijke overeenkomst tussen buma•stemra als Verwerkingsverantwoordelijke en de Verwerker.
- In een verwerkersovereenkomst is in ieder geval opgenomen dat de verwerker:
- de persoonsgegevens uitsluitend verwerkt op basis van schriftelijke instructies van de verwerkingsverantwoordelijke;
- alleen met schriftelijke toestemming van buma•stemra de gegevens zal doorgeven aan een derde land of een internationale organisatie, tenzij een op de verwerker van toepassing zijnde Unierechtelijke of lidstaatrechtelijke bepaling hem tot verwerking verplicht; in dat geval stelt de verwerker buma•stemra, voorafgaand aan de verwerking, in kennis van dat wettelijk voorschrift, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt;
- ervoor zorgt dat alle bij de verwerking betrokken personen verplicht zijn vertrouwelijkheid in acht te nemen;
- alle overeenkomstig artikel 32 AVG vereiste technische en organisatorische maatregelen neemt;
- d) aan de in de leden 2 en 4 bedoelde voorwaarden voor het in dienst nemen van een andere verwerker voldoet;
- buma•stemra bijstand verleent bij het vervullen van diens plicht om verzoeken om uitoefening van rechten van betrokkenen te beantwoorden;
- buma•stemra bijstand verleent bij het doen nakomen van de verplichtingen uit hoofde van de artikelen 32 tot en met 36 AVG;
- na afloop van de overeenkomst alle gegevens wist of deze aan buma•stemra terugbezorgt, en bestaande kopieën verwijdert, tenzij opslag van de persoonsgegevens Unierechtelijk of lidstaatrechtelijk is verplicht;
- aan buma•stemra alle informatie ter beschikking stelt die nodig is om de nakoming van verplichtingen van buma•stemra met betrekking tot de verwerking aan te tonen en audits, waaronder inspecties, door buma•stemra of een door buma•stemra gemachtigde controleur mogelijk maakt en eraan bijdraagt.

5.8.2 Doorgifte Persoonsgegevens binnen de Europese Unie[2]

Omdat in alle lidstaten van de Europese Unie de Algemene Verordening Gegevensbescherming geldt, is binnen de EU het niveau van gegevensbescherming gelijk. De EU is daarom één rechtsgebied bij de bescherming van Persoonsgegevens.

buma•stemra wisselt alleen Persoonsgegevens uit indien noodzakelijke en/of in het belang van de Betrokkene ("need to know" principe).

5.8.3 Doorgifte Persoonsgegevens buiten de Europese Unie

buma•stemra verstrekt Persoonsgegevens alleen aan Derden die zich in een land buiten de Europese Unie bevinden, indien dat land in zijn geheel of de betreffende organisatie specifiek een passend beschermingsniveau waarborgt. Hiertoe moet ten minste aan een van de volgende voorwaarden zijn voldaan:

- Het beschermingsniveau van een land wordt als adequaat aangemerkt als het land is opgenomen op de lijst van landen waarvoor de Europese Commissie een adequaatheidsbesluit heeft genomen.
- Het beschermingsniveau van een organisatie wordt ook als passend aangemerkt als zij beschikt over door een Europese toezichthouder goedgekeurde en op deze verwerking betrekking hebbende Binding Corporate Rules.
- Verwerking is mogelijk door gebruik van door de Europese Commissie goedgekeurde 'standaardbepalingen inzake gegevensbescherming' in een overeenkomst tussen buma•stemra en de betreffende organisatie in het derde land.

Daarnaast vindt momenteel Verwerking van gegevens plaats in landen of door organisaties zonder passend beschermingsniveau op basis van een onder art. 77, lid 2 van de Wet bescherming persoonsgegevens (Wbp) gemaakte uitzondering. De uitzondering is toegestaan middels een vergunning van de Minister van Veiligheid & Justitie, welke op grond van art. 46, lid 5 van de AVG van kracht blijft na het van toepassing worden van de AVG en intrekking van de Wbp op 25 mei 2018.

buma•stemra wisselt alleen Persoonsgegevens uit indien noodzakelijke en/of in het belang van de Betrokkene ("need to know" principe).

[2] *Met EU-landen worden in dit Reglement gelijk gesteld de niet-EU-landen uit de Europese Economische Ruimte, te weten Noorwegen, IJsland en Liechtenstein*

6 Incidenten met betrekking tot Persoonsgegevens

Iedere vraag, klacht of melding met betrekking tot de Verwerking van Persoonsgegevens binnen buma•stemra is een Incident. Dit hoofdstuk beschrijft het beleid met betrekking tot de melding, registratie en afhandeling van Incidenten of het vermoeden van Incidenten in de reguliere bedrijfsvoering en in bijzondere omstandigheden.

6.1 Melding en registratie

Incidenten met Persoonsgegevens worden gemeld bij de service desk of, indien vertrouwelijkheid gewenst is, bij de Privacy Officer. In voorkomend geval vindt registratie van het Incident bij de service desk plaats op naam van de Privacy Officer. Van elk Incident en de afhandeling daarvan wordt een registratie bijgehouden. Een Incident kan gemeld worden door een Betrokkene, een Verwerker of een Derde, waaronder ook de medewerkers van buma•stemra.

6.2 Afhandeling

Incidenten worden binnen buma•stemra afgehandeld conform de vastgestelde Incident management procedure. Is sprake van een Incident waarbij mogelijk Persoonsgegevens zijn gecompromitteerd, dan wordt het Incident door de servicedesk gekenmerkt als “Privacy Incident” en verder verwerkt volgens de Procedure Melding Datalekken. Bij deze procedure worden de volgende uitgangspunten gehanteerd:

- Datalekken worden per definitie geclassificeerd als “Major Incident”;
- de regie bij de afwikkeling van een Datalek wordt gevoerd door de Privacy Officer;
- bij ernstige Incidenten wordt een Privacy Incident Response Team ingesteld (PIRT);
- de beslissing of bij een Incident melding nodig is (binnen 72 uur) bij de Autoriteit Persoonsgegevens en/of (onverwijld) bij betrokkenen wordt genomen door de Directie, op advies van de Privacy Officer en, indien van toepassing, de andere leden van het PIRT;
- van elk Incident wordt door de Privacy Officer een dossier bijgehouden.

6.3 Evaluatie

buma•stemra hecht grote waarde aan het leren van Incidenten. Jaarlijks vindt rapportage plaats van de Privacy Office met betrekking tot de in de verslagperiode voorgekomen Incidenten, de afwikkeling ervan en de verbeteringen die zijn of kunnen worden doorgevoerd. De rapportage van Privacy Incidenten maakt daarom een vast onderdeel uit van de jaarrapportage van de directie.

6.4 Bijzondere omstandigheden

Ingeval zich een ernstig Incident voordoet kan een Privacy Incident Response Team (PIRT) team worden ingesteld. Dit team heeft als taak om te acteren bij ernstige Incidenten met

Persoonsgegevens, in gevallen waarin de staande organisatie een Incident niet via de standaard procedures kan oplossen.

Het besluit over het inschakelen van een PIRT dient te worden genomen door de Directie, waarbij de Privacy Officer een adviserende rol heeft. In het PIRT hebben ieder geval zitting de Data-eigenaar, de Privacy Officer en een vertegenwoordiger van de directie. Afhankelijk van het type Incident kunnen daarnaast een externe jurist, vertegenwoordigers van ICT, JAZ, communicatie of andere deskundigen in het team worden opgenomen.

Het PIRT werkt volgens een door de directie vastgestelde procedure. Onderdeel hiervan is een evaluatie van de afgehandelde Incidenten, waarbij het PIRT achteraf verantwoording aflegt over de wijze waarop het team van zijn mandaat gebruik heeft gemaakt.

7 Rechten van Betrokkenen

7.1 Informatieplicht

Het privacy beleid van buma•stemra is vastgelegd in onderhavig Reglement. Voorts informeert buma•stemra betrokkenen over de Verwerking van Persoonsgegevens door middel van een privacy statement op haar website. buma•stemra respecteert alle wettelijke rechten van Betrokkenen waarmee zij de op hen betrekking hebbende Persoonsgegevens kunnen beschermen.

Teneinde blijvende rechtmatige, behoorlijke en transparante Verwerking te waarborgen, zal bij ingrijpende wijzigingen van het Reglement hiervan melding worden gemaakt aan Betrokkenen.

7.2 Recht van inzage

Verzoek tot inzage

Iedere Betrokkene heeft recht op inzage in de van hem verwerkte Persoonsgegevens. Een verzoek hiertoe kan schriftelijk worden ingediend bij de Privacy Officer. De contactgegevens van de Privacy Officer zijn opgenomen in hoofdstuk 8 van dit Reglement.

Termijn

Op het verzoek wordt zo spoedig mogelijk, doch uiterlijk binnen vier weken na indiening schriftelijk gereageerd. buma•stemra draagt hierbij zorg voor een deugdelijke vaststelling van de identiteit van de verzoeker.

Mededeling

Indien gegevens worden verwerkt, bevat de mededeling van buma•stemra een volledig overzicht daarvan in begrijpelijke vorm, een omschrijving van de doeleinden van de Verwerking, de categorieën van gegevens waarop Verwerking betrekking heeft en de categorieën van ontvangers, alsmede beschikbare informatie over herkomst van de gegevens, de termijn van bewaring van gegevens en het recht om een klacht in te dienen bij de Autoriteit Persoonsgegevens. Ook wijst de mededeling van buma•stemra de betrokkene op het recht van rectificatie of wissing, beperking, overdracht en indien verwerking op grond van gerechtvaardigd belang plaatsvindt ook op het recht van bezwaar.

Voor zover gegevens verwerkt worden in een derde land heeft de betrokkene het recht geïnformeerd te worden over de geboden passende waarborgen om de gegevens te beschermen.

7.3 Recht op rectificatie of wissing, beperking en overdraagbaarheid

Verzoek

Iedere Betrokkene kan met betrekking tot over hem opgenomen Persoonsgegevens bij buma•stemra van deze gegevens verzoeken die te rectificeren of te wissen of (onder voorwaarden) de verwerking ervan te beperken, of over te dragen aan de betrokkene.

Termijn

buma•stemra deelt binnen vier weken na ontvangst van het verzoek schriftelijk aan de Betrokkene mede of zijn verzoek gegrond is.

Kennisgeving

Indien opgenomen Persoonsgegevens van de Betrokkene feitelijk onjuist zijn, voor het doel of doeleinden van de Verwerking onvolledig of niet ter zake dienend zijn dan wel anderszins in strijd met een wettelijk voorschrift zijn verwerkt, verbetert de gegevensbeheerder deze gegevens.

Bovendien worden Derden aan wie de gegevens, voorafgaand aan de correctie, zijn verstrekt hiervan in kennis gesteld. De verzoeker mag opgave verzoeken van degene aan wie buma•stemra deze mededeling heeft gedaan.

Termijn voor uitvoering

De gegevensbeheerder zorgt ervoor dat een beslissing tot verbetering, aanvulling, verwijdering of afscherming zo spoedig mogelijk wordt uitgevoerd.

7.4 Recht van bezwaar

Gronden voor bezwaar

In verband met zijn of haar persoonlijke omstandigheden, mag iedere Betrokkene bezwaar aantekenen tegen Verwerking bij buma•stemra, als deze Verwerking plaatsvond op grond van a) de vervulling van een publiekrechtelijke taak van de gegevensbeheerder of b) de behartiging van het gerechtvaardigd belang van buma•stemra of van een Derde aan wie de gegevens worden verstrekt.

Termijn

buma•stemra beoordeelt binnen vier weken na ontvangst van het bezwaar of deze gerechtvaardigd is. Indien het bezwaar gerechtvaardigd is, treft buma•stemra maatregelen die nodig zijn om de Verwerking de beëindigen.

7.5 Rechtsbescherming

Algemene klachten

Indien de Betrokkene van mening is dat de wettelijke bepalingen inzake de privacybescherming dan wel de bepalingen van dit Beleid jegens hem niet correct worden gehandhaafd, kan hij een schriftelijke klacht indienen bij de Privacy Officer van buma•stemra. De contactgegevens van de Privacy Officer zijn opgenomen in hoofdstuk 8 van dit Reglement.

Op elk gewenst moment - voor, tijdens of na het bovenstaande klachtenproces – kan een betrokkene eveneens een klacht indienen bij de Autoriteit Persoonsgegevens.

Bezwaarmogelijkheden na indienen algemene klacht

Indien het antwoord van buma•stemra voor de Betrokkene niet leidt tot een voor hem acceptabel resultaat, heeft de Betrokkene de mogelijkheid een verzoekschriftprocedure te starten bij de kantonrechter.

Beroepsmogelijkheden na afwijzing van een verzoekschrift tot inzage

Indien buma•stemra afwijzend heeft beslist op een verzoek tot inzage in of verbetering, aanvulling, verwijdering of afscherming van Persoonsgegevens, of buma•stemra heeft het verzoek van de Betrokkene afgewezen, heeft de Betrokkene de mogelijkheid een verzoekschriftprocedure te starten bij de kantonrechter.

Termijn indienen bezwaar

Het bezwaarschrift dient binnen zes weken na ontvangst van het antwoord van buma•stemra ingediend te worden bij de kantonrechter. Indien buma•stemra niet binnen de gestelde termijn heeft geantwoord, moet het verzoekschrift binnen zes weken na afloop van die termijn worden ingediend.

8 Vaststelling en aanpassing beleid

Onderhavig Privacy Reglement is vastgesteld door de Directie van buma•stemra d.d. 25 mei 2018.

Een review van het Privacy Reglement maakt onderdeel uit van de jaarlijkse plan-do-check-act cyclus van de Privacy Officer. Daarin is ook een controle op de effectiviteit van de maatregelen opgenomen.

De meest recente versie van het Privacy Reglement wordt gepubliceerd op het intranet van buma•stemra. De voor externe stakeholders relevante informatie uit het Reglement zal worden opgenomen in een Privacy Statement op de portals voor rechthebbenden en eventuele andere specifieke doelgroepen.

Voor vragen of opmerkingen met betrekking tot dit document kunt u terecht bij de Privacy Officer van buma•stemra via:

buma•stemra
t.a.v. de Privacy Officer
Postbus 3080
2130 KB Hoofddorp
T: (023) 799 79 99
E: privacyofficer@bumastemra.nl

BIJLAGE: door buma•stemra verwerkte categorieën Persoonsgegevens

Verwerkingen als Verantwoordelijke		
categorie	type gegevens	doelbinding
medewerkers	contactgegevens	algemene bedrijfsvoering en nakoming wettelijke verplichtingen
medewerkers	personeelsdossier	het voeren van personeelsbeleid en de van nakoming wettelijke verplichtingen
medewerkers	loongegevens	het voeren van een loonadministratie en de nakoming van wettelijke verplichtingen
medewerkers	betalingsgegevens	het voeren van een financiële administratie, het verwerken van in- en uitgaande betalingen en de nakoming van wettelijke verplichtingen
medewerkers	sollicitantengegevens	het werven en selecteren van gekwalificeerd personeel
leveranciers/relaties	contactgegevens	registratie relatiegegevens t.b.v. uitvoering overeenkomst, marketing en communicatie
leveranciers/relaties	betalingsgegevens	het voeren van een financiële administratie, het verwerken van in- en uitgaande betalingen en de nakoming van wettelijke verplichtingen
leveranciers/relaties	service calls	het afhandelen van vragen en incidenten en het verzamelen van informatie hierover t.b.v. marketing en beleidsontwikkeling
gebruikers parkeergarage	camerabeelden	beveiliging van het pand en de hierin aanwezige zaken en personen
leden/rechthebbenden	contactgegevens	uitvoering overeenkomst, marketing en communicatie
leden/rechthebbenden	repertoire	uitvoering overeenkomst, marketing en communicatie
leden/rechthebbenden	betalingsgegevens	het voeren van een financiële administratie, het verwerken van in- en uitgaande betalingen en de nakoming van wettelijke verplichtingen
leden/rechthebbenden	service calls	het afhandelen van vragen en incidenten en het verzamelen van informatie hierover t.b.v. marketing en beleidsontwikkeling
muziekgebruikers	contactgegevens	registratie relatiegegevens t.b.v. uitvoering overeenkomst, marketing en communicatie
muziekgebruikers	licenties	uitvoering overeenkomst, marketing en communicatie
muziekgebruikers	betalingsgegevens	het voeren van een financiële administratie, het verwerken van in- en uitgaande betalingen en de nakoming van wettelijke verplichtingen
muziekgebruiker	service calls	het afhandelen van vragen en incidenten en het verzamelen van informatie hierover t.b.v. marketing en beleidsontwikkeling