Privacy Rules

buma•stemra

22 November 2018

Content

1. Introduction

Vereniging Buma/Stichting Stemra ('buma•stemra') is the collecting society for music authors and music publishers in the Netherlands and represents the interests of its members worldwide. We ensure that the more than 25,000 affiliated composers, writers and publishers receive remuneration when their music is used. In addition, we promote Dutch music as an international product by organising, financing and sponsoring a variety of music events through 'Buma Cultuur'.

The storage and processing of Personal Data are essential for carrying out these tasks. This must occur with the utmost care because misuse of Personal Data can lead to considerable damage for Data Subjects, such as the rightholders, music users and employees, but also for buma•stemra as an organisation. We therefore highly value the protection of the Personal Data that is provided to us and how the Personal Data is processed.

This privacy policy describes how buma•stemra handles the Personal Data and which basic principles apply. buma•stemra hereby accepts its responsibility to comply with all the applicable laws and legislation for the quality and protection of the Personal Data it processes.

1.1. Definitions

Term	Abbreviation	Explanation
General Data Protection Regulation	GDPR	Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 concerning the protection of natural persons in connection with the processing of personal data and concerning the free trafficking of that data and the revocation of Directive 95/46/EU.
Personal Data Authority	PDA	The national supervisor of the GDPR and other laws and legislation for the Processing of Personal Data.
Data subject		The person to whom the Personal Data relates.
Storage term		Period of time that Personal Data is stored in a form that makes it possible to identify the data subject.
Special Personal Data		Sensitive Personal Data that enjoys extra protection from the authorities, including data concerning race, religion, health, political beliefs, sexual orientation, union membership or criminal history.
Data Owner		The person who is responsible for (a part of) the Personal Data stored in the systems and who ensures that the storage and the use of this data is in compliance with the established Rules and the applicable laws and legislation, including those in the area of privacy.
Data leak (Breach in relation to personal data)		A breach of the protection which results, whether accidentally or due to unlawful action, in the destruction, loss, change or the unauthorised distribution or the unauthorised access to the transferred, stored or otherwise processed data.
Data leak file		File in which all the information that concerns a Data leak is recorded.
Data leak register		Register in which all the Data leak files are stored.
Third party		Natural or legal person, not being the Data Subject, Controller, Processor or person who is authorised under the immediate authority of the Controller or the Processor to Process Personal Data.
Principle of Purpose		A precise and clear description of a purpose or various correlating purposes in which the Controller expresses why it processes Personal Data.

Term	Abbreviation	Explanation
Incident		Every question, complaint or report that is registered by the Service Desk.
Incident Management Process		The process that describes which steps will be taken in handling an Incident, which roles are involved in this and how this will be recorded.
Major Incident		Incident that must be handled with the highest priority.
Opt-in		Inclusion on mailing list after explicit request by the data subject.
Opt-out		Removal from a mailing list after the explicit request of the data subject.
Personal Data		All data concerning an identified or identifiable natural person.
Privacy by Default		Maximum privacy-friendliness as basic principle with the arrangement of processes, systems and applications
Privacy by Design		The management of the entire life-cycle of Personal Data, starting from the collection and up to the Processing and removal, whereby systematic attention is paid to safeguarding the accuracy, confidentiality, integrity, physical protection and removal possibility of the Personal Data.
Privacy Impact Assessment	PIA	A method that helps with the identification of privacy risks and provides tools to manage these risks.
Privacy Incident		Every question, complaint or report concerning the Processing of Personal Data.
Privacy Incident Response Team	PIRT	Multi-disciplinary team that can be engaged by the Privacy Officer in order to handle serious Privacy Incidents quickly and effectively.
Privacy Officer	PO	The officer named by the Controller who is the point of contact for all privacy-related matters, and who advises the organisation on compliance to the laws and legislation concerning privacy and monitors the observance thereof. Also the point of contact for the Personal Data Authority.

Term	Abbreviation	Explanation
Date leaks reporting procedure		Procedure that describes how the report and handling of a potential Data Leak occurs. Part of the procedure includes the decision criteria of whether or not to report a Data leak to the Personal Data Authority and the Data Subject.
Register of processing activities		A register of the processing activities that take place under the responsibility of the Controller and of the processing activities that are carried out in the role of processor on behalf of the Controllers.
Rules		Rules in which the policy concerning the Processing of Personal Data is established.
Service Desk		Department where all Incidents are reported and registered.
System owner		The person responsible for ensuring that an application and accompanying IT facilities offer good support to the processes in which these are used, that theses meet the needs and wishes of users as much as possible and are in accordance with the Privacy Rules and the applicable laws and legislation.
Processing/Processing of Personal Data		Every action or series of actions concerning Personal Data, including in any case, collection, establishment, organisation, storage, consultation, use, distribution and destruction.
Processor		Natural or legal person to whom the Controller has outsourced any form of Processing of Personal Data.
Controller		Natural or legal person who establishes the purpose and the means for processing Personal Data.

1.2. Scope and purpose of the Rules

These Rules concern the Processing of Personal Data of all Data Subjects within buma•stemra, including in any case, all members, participants, music users, employees and external relations, as well as those individuals whose Personal Data buma•stemra processes.

In the Rules, the emphasis lies on the entire or partial automated/systematic Processing of Personal Data that occurs under the responsibility of buma•stemra, as well as the underlying documents that have been included in the file. The Rules also apply to the non-automated Processing of Personal Data that has been included in a file or has been deemed to be included in the file.

At buma•stemra, the protection of Personal Data is interpreted broadly. There is a significant correlation and partial overlap with the related policy terrain of information protection, whereby it concerns the availability, integrity and confidentiality of data, including Personal Data. At a strategic level, attention is paid to these areas and both systematic and substantive coordination is sought.

At buma•stemra, the Rules have the purpose of optimising the quality of the Processing and the Protection of Personal Data, whereby a good balance must be struck between privacy, functionality and security. The intention is to respect the privacy of the Data Subject as much as possible. All data that concerns the Data Subject should be protected against unlawful and unauthorised use and other forms of misuse, based on the fundamental right to the Protection of his/her Personal Data. This means that the Processing of Personal Data must be in compliance with all the relevant laws and legislation and that the Personal Data is protected by buma•stemra.

Purpose of the Rules:

- to create awareness within buma•stemra for the importance of and need to protect Personal Data;
- to provide a framework: the Rules provide a framework to monitor (future) Processing of Personal Data and to assign tasks, authorities and responsibilities in the organisation;
- to establish standards: the foundation for the protection of Personal Data is established in the IT security policy of buma•stemra. Measures are taken as based on best practices;
- to take responsibility: by explicitly establishing the basic principles and responsibilities of the parties involved in the Processing of Personal Data;
- resolute implementation of the Rules by making clear choices in terms of measures to be taken and applying active control on the execution of policy measures;
- ensuring compliance with Dutch and European legislation, including the GDPR Implementation law and the GDPR itself.

2. Processing Personal Data Policy Principles

The basic policy principle is that Personal Data is processed in accordance with the relevant laws and legislation in a legal, proper and transparent fashion. In doing so, a good balance must be created between the interest of buma•stemra to Process Personal Data and the interest of the Data Subject to make their own choice concerning their Personal Data.

In order to satisfy this basic policy principle, the following tenets apply:

- Processing Personal Data is based on one of the legal grounds as stated in Article 6 of the GDPR;
- Personal Data is only processed for specific, expressly described and justified purposes ("Principle of Purpose"). These purposes are concrete and have been formulated in advance of Processing;
- when Processing Personal Data, the quantity and type of data is limited to the Personal Data that is necessary for the specific purpose. The data should adequately match the purpose, serve the purpose and should not be excessive;
- Processing Personal Data should occur in the least intrusive manner and should be within reasonable proportion to the intended purpose;
- measures are taken to safeguard that the Processing of Personal Data is accurate and up-to-date as much as possible;
- Personal Data is adequately protected according to the applicable protection standards.
- Personal Data is not further processed in a manner that is not in line with the purposes for which it was acquired;
- Personal Data is not processed for longer than is necessary for the purposes of the Processing and the applicable storage and destruction periods are honoured;
- every Data Subject has the right to access, rectify, erasure, restrict and transfer the Personal Data that concerns them in each of the individual Processing actions and also has the right of objection as formulated in section 7 of these Rules;
- with all voluntary registrations, the Data Subject shall be offered a unilateral so-called Opt-out procedure.

3. Roles and responsibilities concerning the Processing of Personal Data

In order to ensure that the Processing of Personal Data is carried out in a structured and coordinated fashion, buma•stemra has assigned a number of roles and designated officers within its current organisation.

3.1. Board

The Board is ultimately responsible for the lawful and diligent Processing of Personal Data within buma•stemra and establishes the Rules, the measures and the procedures in the area of Processing.

The Board is also responsible for the execution of the established Rules, measures and procedures concerning the Processing of Personal Data within buma•stemra.

3.2. Department heads and managers

Department heads and managers are responsible for integrating the Rules into the daily business operations and the awareness of and compliance with the Rules by the employees and their subordinates. Every manager is tasked with:

- making sure that their employees are well-informed about the Rules;
- making sure their employees comply with the Rules;
- periodically introducing the subject of privacy at work consultations.

3.3. Employees, Processors and Third Parties

All employees of buma•stemra, including temporary staff, are expected to be aware of the Rules, measures and procedures in the area of Processing and to comply with these. Processors and Third Parties will be informed about this by buma•stemra.

3.4. System Owners

All applications will be assigned a System Owner. The System Owner is responsible that the application and the corresponding ICT facilities offer good support to the processes in which they are used and are in compliance with the Statement. This means that the System Owner ensures that the application continues to meet the needs and wishes of users and is in accordance with the applicable laws and legislation in the area of privacy.

3.5. Data Owners

All Personal Data will be assigned a Data Owner. The Data Owner is responsible for (part of) the Personal Data that is stored on the systems and ensures that this storage and the use is in accordance with the established Rules and the applicable laws and legislation, including those in the area of privacy.

3.6. Privacy Officer

buma•stemra has appointed a Privacy Officer. The Privacy Officer advises on compliance with the applicable and future laws and legislation concerning privacy and the protection of data and is the internal and external point of contact for all privacy-related matters. The Privacy Officer is competent in the area of privacy legislation, independent and reports directly to the Board.

In order to be able to carry out his/her tasks properly, the Privacy Officer has the authority, insofar as is necessary to be able to do this, to enter rooms (including server rooms), to ask for information and access and to investigate matters.

The tasks of the Privacy Officer include:

- taking inventory of the Personal Data that is processed within buma•stemra, maintaining a register of that data, and, if legally required, to report registrations to the Personal Data Authority;
- supervising the compliance to the statutory regulations concerning the Processing of Personal Data within buma•stemra;
- maintaining an Incidents register, making legally required reports concerning Incidents to the Data Protection Authority and/or Data Subjects and maintaining files about these Incidents.
- providing information and advice concerning the handling of Personal Data in the context of their own organisation and work processes;
- providing advice and establishing and realising a fitting level of information protection;
- dealing with complaints about the use of Personal Data, carrying out investigations or negotiating between the complainant and the Controller;
- developing internal standards concerning the handling of Personal Data;
- ensuring continued awareness of privacy risks among employees.

4. Implementation of the Rules

The Board of buma•stemra is responsible for the Processing of Personal Data and establishes the purpose and tools for this. The Board is designated as the Controller as intended in the General Personal Data Processing Regulation. The actual Processing of Personal Data occurs at the lower organisational levels.

The proper, efficient and responsible leadership of an organisation is indicated by the term governance. A part of this is the relation of the Controller with the most important stakeholders of buma•stemra, including the internal and external supervisors, members, participants, music users, employees and external relations, as well as those individuals whose Personal Data buma•stemra processes. Good corporate governance policy safeguards the rights of all stakeholders.

4.1. Division of responsibilities

The diligent Processing of Personal Data is a line responsibility. This means that department heads and managers have the primary responsibility, as line managers, for the diligent Processing of Personal Data at their departments. This also includes the choice of measures to be taken and the enforcement thereof. Under line responsibility also falls the task of communicating the Rules concerning the Processing of Personal Data to all the relevant parties, including, for example, the contract parties.

The diligent handling of Personal Data is also everyone's own responsibility. Employees are expected to act with integrity. That also means that the privacy of others must be respected. It is not acceptable that, due to the behaviour of employees, whether deliberate or not, unsafe or otherwise undesired situations arise that could lead to damage and/or loss of reputation of buma•stemra or individuals.

4.2. Consultation structures

In order to ensure the cohesion within the organisation concerning the protection of data and coordinate the activities in the area of Processing Personal Data within the various compartments, it is important to carry out structured consultation about the subject of privacy at different levels.

At a strategic level, a focused discussion takes place about governance and compliance, as well as about purposes, scope and ambition in the area of privacy aspects. The strategic level is handled by the Board.

At a tactical level, the strategy is translated into plans, standards to uphold, and methods of evaluation. These plans and instruments guide the implementation. The tactical level is handled by the Board in consultation with the managers.

At an operational level, matters are discussed that concern the (carrying out of) daily business operations. The operational level is handled during the departmental consultations.

4.3. Awareness and training

In order to manage the risks in the area of Processing Personal Data as much as possible, in addition to the creation and implementation of policy and measures, ongoing attention is needed for the risk awareness level of employees. Therefore, part of this policy also includes measures to help stimulate this risk awareness so that the knowledge of risks is enhanced and (safe and responsible) behaviour is encouraged by, among others, regular repeating awareness campaigns for employees.

The constant attention for risk awareness among the employees is also one of the tasks of the Privacy Officer.

4.4. Internal audit

Audits make it possible to verify whether the policy established in the Rules and the measures taken are effective. The Privacy Officer initiates, together with the IT Security Officer and the head of the Audit department, the verification of the lawful and diligent Processing of Personal Data.

Any external audits are carried out by independent accountants. This is linked to the annual audit and is integrated into the normal Planning & Control cycle as much as possible.

If compliance to the policy and/or the protection of data and privacy information grievously falls short, the Board could put a sanction on the employees responsible as long as it within the framework of the CLA and statutory possibilities.

5. Legal, proper and transparent Processing of Personal Data

5.1. Grounds, principle of purpose and balance of interest

The Processing of Personal Data must be based on one of the grounds as described in Article 6 of the GDPR. The Controller describes the purposes in advance of the Processing. These purposes have been concretely and specifically formulated. All Processing is reviewed to examine whether the Processing of Personal Data is necessary. In doing so, the various interests will be weighed and the efficiency, proportionality and subsidiarity are considered. Personal Data is not processed in a manner that is incompatible with the purposes for which it was obtained.

buma•stemra shall take the necessary measures to ensure that the Personal Data, considering the purposes for which it was collected or Processed, is correct and accurate.

An overview of the Personal Data categories that are processed by buma•stemra can be found in the Annexe. Per category, it has been indicated what the legal basis and principle of purpose is, what the maximum storage period is and who has the role of Data Owner.

5.2. For new projects and changes: carry out Privacy Impact Assessment (PIA)

For (research) projects, infrastructural changes or the acquisition of new systems, the establishment of privacy should be taken into account from the beginning by way of carrying out a Privacy Impact Assessment (PIA). The Privacy Officer is tasked with approving the PIA. buma•stemra, upon implementation, shall uphold the Privacy by Design and Privacy by Default principles.

A PIA is also legally required if a proposed new processing brings about high risk for data subjects. In these cases, the PIA must meet several requirements. To determine whether high risk is involved, the 9 published criteria by the Article 29 work group can be used.[1] A PIA is legally required specifically when the processing concerns (Art. 35, paragraph 3, GDPR):

- 'a systematic and expansive assessment of personal aspects of natural persons that is based on automated processing, including profiling and upon which decisions are based which have legal consequences for the natural person or effect the natural person in a similar fashion;
- large-scale processing of special categories of personal data [...] or of data concerning criminal convictions and offences [...]; or
- systematic and large-scale monitoring of publicly accessible areas.'

---

1 *Guidelines for the 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), Article 29 work group April 2017.*

5.3. Reporting and documenting Processing

The Processing of Personal Data is reported by the department heads to the Privacy Officer for inclusion in the buma•stemra Register of Processing activities.

The Processing is reported to the Privacy Officer stating the following information:

	Role of buma•stemra	
	Controller	Processor
Name and contact information of Controller(s)	X	X
Name and contact information of the processor(s)		X
Processing purposes	X	
Categories of data subjects and of data	X	
Categories of recipients (in third countries, among others)	X	
Transfers to a third country (including appropriate warranties)		X
Storage terms	X	
General description of technical and organisational measures	X	X

5.4. The organisation of the protection

buma•stemra ensures that there is an adequate protection level and shall take appropriate technical and organisational measures to protect the Personal Data against loss or any form of unlawful Processing. These measures are also partially focused on the prevention of unlawful collection and Processing of Personal Data.

A risk analysis of privacy protection and information protection is part of the internal risk management and control system of buma•stemra.

5.5. Confidentiality

At buma•stemra, all Personal Data is classified as confidential. Everyone should be aware of the confidentiality of the Personal Data and act accordingly.

Persons who do not have a confidentiality obligation due to their function, profession or legal requirement, are also obliged to maintain confidentiality when it comes to the Personal Data they handle, except insofar as any legal requirement makes it mandatory or the need to report arises from their task.

5.6. Storage terms / destruction periods per type of data

Personal Data is not stored longer than necessary for the purposes for which it was collected or used. How long certain data is stored is dependent on the nature of the data and the purposes which it was processed. Hence, the storage term can vary per purpose. buma•stemra shall destroy the Personal Data after the expiry of the storage term or, if the Personal Data is intended for historical, statistical or scientific purposes, shall store the data in an archive that offers fitting safeguards, including anonymisation and/or pseudonimisation if at all possible.

5.7. Special Personal Data

Under special Personal Data we mean data that concerns someone's religion or life conviction, race, political beliefs, health, sexuality, membership of a trade union or criminal data.

In principle, buma•stemra does not record any special Personal Data, unless it is strictly necessary and the Processing of this data takes place on the basis of legal grounds, the express permission of the Data Subject or a considerable general interest.

With the processing of special Personal Data, the Privacy Officer can determine that this data requires extra protection measures in addition to the general protection level.

5.8. Transfer of Personal Data to Third Parties

1. Outsourcing of Processing to a Processor

If buma•stemra has Personal Data processed by a Processor, the execution thereof shall be arranged in a processing agreement. This is a written agreement between buma•stemra as Controller and the Processor. The processing agreement shall include, in any case, that the processor:

- only processes the personal data based on the written instructions of the Controller;
- shall only pass on the data with the written permission of buma•stemra to a third country or an international organisation, unless the processor is required to perform the processing due to a legal obligation arising from a Union or member state provision; in that case, the processor shall inform buma•stemra in advance of the processing of this legal prerequisite, unless that legislation prohibits this notification for serious reasons of general interest;
- ensures that with all processing, the persons involved are required to respect their confidentiality;
- takes all the required technical and organisational measures in accordance with Article 32 GDPR;
- meets the conditions of paragraphs 2 and 4 for the hiring of outside processors;
- provides support to buma•stemra in carrying out its obligation to answer requests from Data Subjects to exercise their rights;

- provides support to buma•stemra in its compliance with the obligations of Articles 32 through 36 of the GDPR;
- ensures that all data is deleted or returned to buma•stemra after the expiry of the agreement, and removes existing copies, unless storage of the Personal Data is statutorily required by a Union or member state;
- makes all information available to buma•stemra that is necessary to demonstrate the compliance of buma•stemra to its obligations concerning the processing and makes audits, including inspections by buma•stemra or an authorised inspector of buma•stemra possible and contributes to these.

2. Transfer of Personal Data within the European Union[2]

Because the General Personal Data Regulation applies to all member states of the European Union, the level protection within the EU is the same. The EU is therefore one jurisdiction for the protection of Personal Data.

buma•stemra only exchanges Personal Data when necessary and/or it is in the interest of the Data Subject ("need to know" principle).

3. Transfer of Personal Data outside the European Union

buma•stemra only provides Personal Data to Third Parties that are located outside the European Union if that country in general, or the organisation specifically, can safeguard an appropriate level of protection. For this, at least the following conditions must be met:

- The protection level of a country is designated as adequate when that country is included on the list of countries for which the European Commission has made an adequacy assessment.
- The protection level of an organisation is only designated as adequate if it possesses Binding Corporate Rules that concern this processing and which have been approved by a European supervisor.
- Processing is possible with the use of the 'standard conditions concerning data protection' approved by the European Commission in an agreement between buma•stemra and the organisation concerned in the third county.

In addition, Processing of data currently takes place in countries or by organisations without an appropriate protection level on the basis of the exception made under Art. 77, paragraph 2 of the Personal Data Protection Act (DPPA). The exception is permitted by way of a permit provided by the Ministry of Safety & Justice and on the grounds of Art. 46, paragraph 5 of the GDPR this stays in effect after the revocation of the DPPA on 25 May 2018.

buma•stemra only exchanges Personal Data when necessary and/or it is in the interest of the Data Subject ("need to know" principle).

---

[2] *In these Rules, the countries that are considered equal to EU countries, are those countries in the European Economic Region, namely, Norway, Iceland and Liechtenstein*

6. Incidents concerning Personal Data

Every question, complaint or report concerning the Processing of Personal Data within buma•stemra is an Incident. This section describes the policy concerning the reporting, registration and handling of Incidents or the suspected Incidents in the normal business operations and during special circumstances.

6.1. Reporting and registration

Incidents with Personal Data are reported to the service desk, or if confidentiality is desired, the Privacy Officer. In some cases, the registration of the Incident takes place at the service desk and in name of the Privacy Officer. A registration is made of every Incident and treatment thereof. An Incident can be reported by Data Subject, a Processor or a Third Party, also including the employees of buma•stemra.

6.2. Handling

Incidents are handled within buma•stemra in accordance with the established Incident Management Procedure. If an Incident arises that may possibly compromise Personal Data, the Incident will be designated as a "Privacy Incident" by the service desk and further processed according to the Procedure for Reporting Data Leaks. The following basic principles apply to this procedure:

- Data leaks are, by definition, classified as "Major Incidents";
- the Privacy Officer is in charge of the investigation that ensues with a Data leak;
- with serious Incidents, a Privacy Response Team (PIRT) will be implemented;
- the decision of whether an Incident needs to be reported (within 72 hours) to the Personal Data Protection Authority and/or (immediately) to the Data Subjects, is made by the Board acting on the advice of the Privacy Officer and, if applicable, the other members of the PIRT;
- the Privacy Officer will maintain a file of every Incident.

6.3. Evaluation

buma•stemra highly values learning from Incidents. Annual reporting shall take place by the Privacy Officer concerning the Incidents that occurred in the period, how they were handled and the improvements that can be implemented. That is why the reporting of Privacy Incidents is a permanent feature of the annual reporting by the Board.

6.4. Special circumstances

In the event a serious Incident takes place, a Privacy Incident Response Team (PIRT) can be implemented. This team is tasked with responding to serious Incidents involving Personal Data, in cases where the standing organisation cannot solve an Incident via the standard procedures.

The decision to engage a PIRT should be made by the Board, whereby the Privacy Officer has an advisory role. The PIRT shall be composed of, in any case, the Data Owner, the Privacy Officer and a representative of

the Board. Depending on the type of Incident, an external lawyer, representatives of ICT, JAZ, communication or other experts can also be included in the team.

The PIRT works according to a procedure that is established by the Board. A part of this includes an evaluation of the Incidents that have been handled, whereby the PIRT clarifies the manner in which the team has used the mandate to the Board afterwards.

7. Rights of Data Subjects

7.1. Information requirement

The privacy policy of buma•stemra is established in these present Rules. buma•stemra then informs the Data Subjects about the Processing of Personal Data by way of a privacy statement on its website. buma•stemra respects all the legal rights of Data Subjects which can offer them protection concerning the Personal Data.

For the purpose of safeguarding continued rightful, proper and transparent Processing, profound changes to the Rules shall be communicated to the Data Subjects.

7.2. Right of access

Request to access

Every Data Subject has the right to access their processed Personal Data. A written request for access can be submitted to the Privacy Officer. The contact information of the Privacy Officer has been included in section 8 of these Rules.

Term

The request should be responded to as quickly as possible, but ultimately within four weeks and in writing. buma•stemra herein ensures the proper establishment of the identity of the requester.

Report

If data is processed, the buma•stemra report shall contain a complete, easy to understand overview of the processing, a description of the purposes of the Processing, the categories of the data that concerns the Processing and the categories of recipients, as well as any available information about the origin of the data, the storage term of the data and the right to submit a complaint to the Personal Data Authority. The report of buma•stemra also informs the Data Subject of the right to rectify, erasure, restrict, data portability and if the processing takes place on the grounds of justified interest, also the right of objection.

Insofar as data is processed in a third country, the Data Subject has the right to be informed about the appropriate safeguards offered to protect the data.

7.3. Right to rectification or erasure, restriction and data portability

Request

Every Data Subject can request to have the Personal Data that concerns them and is included by buma•stemra rectified or erased or (under certain conditions) restricted in the processing thereof, or to transfer the data to the Data Subject.

Term

Within four weeks after receipt, buma•stemra shall inform the Data Subject in writing whether the request is founded.

Notification

If the included Personal Data of the Data Subject is factually incorrect for the purpose or purposes of the Processing, or is incomplete or not relevant or otherwise in conflict with a legal prerequisite for processing, the data manager shall improve the data.

Third Parties to whom the data has been provided prior to the correction, should also be notified of this. The requester may request specification of the party whom buma•stemra has notified.

Term of execution

The data manager ensures that a decision to improve, supplement, remove or shield the data is carried out as quickly as possible.

7.4. Right of objection

Grounds of objection

In relation to his/her personal circumstances, every Data Subject may object to the Processing by buma•stemra, if this Processing took place on the grounds of a) the fulfilment of a legal public task of the data manager or b) the representation of the justified interest of buma•stemra or of the Third Party to whom the data is provided.

Term

Within four weeks after receipt, buma•stemra shall assess whether the objection is justified. If the objection is justified, buma•stemra shall take the necessary measures to end the Processing.

7.5. Protection of rights

General complaints

If the Data Subject is of the opinion that the legal conditions concerning the protection of privacy or the conditions of this Policy are not properly upheld, he can submit a written complaint to the Privacy Officer of buma•stemra. The contact information of the Privacy Officer has been included in section 8 of these Rules.

At any given moment - before, during or after the complaint process stated above - the Data Subject can also submit a complaint to the Personal Data Authority.

Opportunities to object after submission of a general complaint.

If the answer by buma•stemra does not yield an acceptable result for the Data Subject, the Data Subject also has the option of starting a petition procedure with the sub-district court judge.

Possibilities to appeal after refusal of a petition to have access

If buma•stemra has decided to deny a request to access, improve, supplement, remove or shield the Personal Data, or if buma•stemra has refused the request, the Data Subject has the possibility to start a petition procedure with the sub-district court judge.

Terms for submitting an objection

The notice of objection must be submitted to the sub-district court judge within six weeks after receipt of the answer from buma•stemra. If buma•stemra fails to respond within the stated term, the petition must be submitted within six weeks after the end of the term.

8. Establishment and adjustment of policy

The present Privacy Rules were established on 25 May 2018 and were last adjusted by the Board of buma•stemra on 22 November 2018.

A review of the Privacy Rules is part of the annual plan-do-check-act cycle of the Privacy Officer. This also includes checking the effectiveness of the included measures.

The most recent version of the Privacy Rules is published on the intranet of buma•stemra. Information of the Rules that is relevant to external stakeholders shall be included in a Privacy Statement on the portals for interested parties and possibly other specific target groups.

For questions or comments concerning this document, you can reach the Privacy Officer of buma•stemra at:

buma•stemra
Attn. The Privacy Officer
Post box 3080
2130 KB Hoofddorp, the Netherlands
T: +31 (0)23 799 79 99
E: privacyofficer@bumastemra.nl

Annexe: Categories of Personal Data processed by buma•stemra

Processing as Controller		
category	type of data	Principle of Purpose
employees	contact information	general business operations and compliance with legal obligations
employees	personnel file	conducting staff policy and compliance with legal obligations
employees	wage information	maintaining wage administration and compliance with legal obligations
employees	payment details	conducting financial administration, processing in and outgoing payments and compliance with legal obligations
employees	applicants data	recruitment and selection of qualified personnel
suppliers/relations	contact information	registration contact information for execution of agreement, marketing and communication
suppliers/relations	payment details	conducting financial administration, processing in and outgoing payments and compliance with legal obligations
suppliers/relations	service calls	the handling of questions and incidents and the collection of resulting information for marketing and policy development
car park users	camera footage	building security and security for all persons and matters present inside the building
members/rightholders	contact information	execution agreement, marketing and communication
members/rightholders	repertoire	execution agreement, marketing and communication
members/rightholders	payment details	conducting financial administration, processing in and outgoing payments and compliance with legal obligations
members/rightholders	service calls	the handling of questions and incidents and the collection of resulting information for marketing and policy development
music users	contact information	registration contact information for execution of agreement, marketing and communication
music users	licences	execution agreement, marketing and communication
music users	payment details	conducting financial administration, processing in and outgoing payments and compliance with legal obligations
music users	service calls	the handling of questions and incidents and the collection of resulting information for marketing and policy development