THE MEKONG RIVER COMMISSION SECRETARIAT
GUIDELINES FOR THE PROTECTION OF PERSONAL DATA

ROLES AND RESPONSIBILITIES

ADMINISTRATION DIVISION

HR

- Be responsible for the PPD of Human Resources Management processes,
- Be the focal point to facilitate the personal data's access, correction, or update processes.

Finance and Procurement

- Be responsible for the PPD of financial and procurement management.

IT

- Be responsible for the IT's PPD tasks regarding the protection of privacy, secured use of emails and email accounts, IT systems' virus and threat protection, etc.
- In charge of authentication and encryption of personal data as and when requested.
- Be responsible to make available stable and up-to-date facilities and platforms for the protection of personal data at the MRCS.

Administration

- Be responsible for the PPD of administrative and governance related routines.

TECHNICAL DIVISIONS AND OFFICE OF CEO

Technical Divisions

- Be responsible for the Division's PPD and are to comply to the requirements of the PPD rules and procedures as and when applicable in technical briefings, reports, workshops, and in divisional filing administration.

OCEO

- Be responsible for the PPD at OCEO and is to comply with the requirements of the PPD rules and procedures as and when applicable in M&E, Reporting and Internal Auditing.
- Have the overall responsibilities for the MRC's PPD in press releases, international meetings and

CONTEXT AND OBJECTIVES OF THE GUIDELINES

In the course of its operations, the Secretariat of the Mekong River Commission (MRC Secretariat or MRCS) obtains, stores and processes information, sometimes including data of a personal nature. Many parties involved with and connected to the Mekong River Commission have an interest in ensuring that the MRC Secretariat has appropriate policies, processes and procedures in place to adequately protect personal data, including members of the MRC Council and the Joint Committee, Government Line Agencies, MRC Employees and applicants, Development Partners, Dialogue Partners and suppliers, consultants or service providers.

The MRC Secretariat is committed to respecting the dignity and privacy of the individuals, while balancing such rights with the MRC Secretariat's ability to carry out its mission. These Personal Data Protection Guidelines (the Guidelines) set out appropriate requirements and outline the processes and procedures to be followed by the MRC Secretariat to ensure that it can carry out its mandate while abiding by internationally recognised standards for protecting personal data.

The basic concept of personal data protection is to protect certain rights of individuals to control what information about them is available to third parties and how such data is then used or shared. Personal data protection laws and policies are intended to help protect an individual's rights to privacy while seeking to ensure that legitimate business and governance activities can be conducted within certain parameters.

SCOPE

These Guidelines apply to all MRC Employees who receive, store and/or process any Personal Data (as defined below) and relate to all Personal Data received, stored and/or processed by the MRC Secretariat. The Guidelines apply only to Personal Data and attention should be paid to other MRC rules and regulations that may apply to the collection, retention and processing of other data, for example other confidential documentation.

DEFINITIONS

The following definitions apply for the purpose of these Guidelines:

Consent: Any freely given, specific, informed and unambiguous indication of an agreement by a Data Subject to the processing of their Personal Data, which may be given by a written or oral statement or by a clear affirmative action.

Data Controller: the natural or legal person which, alone or jointly with others, determines the purposes and means of the processing of Personal Data. For the purposes of these Guidelines, the Mekong River Commission will be considered the Data Controller.

Data Processor: a natural or legal person, agency, public authority or any other body that is engaged in processing Personal Data on behalf of the Data Controller.

Data Subject: a natural person that can be identified, directly or indirectly, in particular by reference to Personal Data. Examples of potential Data Subjects may include MRC Employees or members of the MRC governance bodies, Member Country representatives, Development Partners, Dialogue Partners, Suppliers, or any individuals whose Personal Data is included in information collected from any of the foregoing.

conferences, publication, websites management, outreach activities with communities, etc.

PERSONAL DATA ENTRIES

The MRC normally receives, stores, uses, discloses, or disposes personal information and data through the following key inventories:

FINANCE:
- Staff's payroll disbursement vouchers,
- Staff's provident fund data,
- Journal vouchers,
- Receipt vouchers,
- Communication regarding fraudulent, whistle blowing, fraud and corruption cases.

PROCUREMENT
- Tenders' profiles and contracts,
- Evaluation, comparison and rejection or termination of bids and contracts,
- Publication of award of contracts,
- Resolution of disputes,
- Procurement records and files.

HUMAN RESOURCES
- Staff personal files that include application, CVs/Resume, health, genetic and biometric data, personal status including marriage and gender preferences, etc.,
- Salary data and payroll information,
- Summary dismissal, termination of appointment,
- Exit procedures including interview reports and handover notes,
- Attendance records,
- Disciplinary measures and dispute and conflict resolutions,
- Whistle blowing, harassment, misconduct, violence and abuse cases.

ADMINISTRATION
- Conferences, workshops and Governance meetings' proceedings and records/minutes,
- Filing systems and document centres that contain personal data,
- Telephone directories and name cards.

INFORMATION TECHNOLOGY
- Personal laptop/desktop passwords,
- CCTV systems and records,
- Office email accounts.

AUDITING: Internal and external audit reports (both drafts and final) that include Personal Data.

M&E AND REPORTING
- (personal) success stories and case studies.

Data Transfer: any act that makes Personal Data accessible, whether on paper, via electronic means or the internet or any other method, to a Third Party. To "transfer" Personal Data means undertaking a Data Transfer of such Personal Data.

Information Owner: the owner accountable for specific MRC Secretariat information, which for the purpose of these Guidelines are the Division Directors who should be considered Information Owners of all information generated by or entrusted to their respective divisions. Division Directors may delegate their responsibilities as Information Owners to individual(s) within their Divisions, as they deem appropriate. Such individuals must be clearly identified to the other Division Directors (e.g., through an email from the applicable Director).

Joint Controller: Two or more Data Controllers that jointly determine why and how to process personal data.

MRC Employees (as defined in the HR Manual)**:** all staff categories, including fixed-term staff and other employees working under Service Contracts, Special Agreements or Special Service Agreements such as consultants, Junior Riparian Professionals, Associates, Seconded Staff, Junior Program Officer (JPO), Fellows, Interns, etc.

Personal Data: any information relating to a natural person who can be identified by such data, from such data and other information, or by means reasonably likely to be used related to such data. This can include biographical data, such as name, sex, marital status, date and place of birth, country of origin, country of asylum, individual registration number, identification number, occupation, religion, ethnicity, sexual orientation, biometric data such as a photograph, fingerprint, facial or iris image, location data, an online identifier, or information that is linked specifically to the physical, physiological, genetic, mental, economic, cultural or social identity of the person.

Personal Data Breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

Processing: any operation or set of operations that is performed on Personal Data, such as collecting, recording, organizing, structuring, storing, adapting or altering, retrieving, consulting, using, disclosing by transmission, disseminating or otherwise making available, aligning or combining, blocking, erasing or destroying. "processed" means having undertaken the act of processing.

Sensitive Personal Data: Personal Data which form part of the core area of private life, such as racial or ethnic origin, political affiliations or opinions, religious or philosophical beliefs, trade-union membership, health status (including medical, biological or biometric data), financial or family/relationship situation (including marital status, sexual orientation or preference or sex life and dependents) of a data subject. Sensitive data also include some employment records of MRC Employees, such as those relating to their performance and conduct.

Data Breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

Supplier (as defined in the Procurement Manual): a person, firm, company, or organization that provides works, goods, or non-consultant services against a contract.

Third Party: any natural or legal person, public authority, agency or any other body other than the Data Subject, the Data Processor and the MRC Secretariat (as the Data Controller) and the persons under the direct authority of the Data Processor and the Data Controller. Examples of Third Parties are Member Countries and their

RELATED DOCUMENTS

MRC Administration Manual

governments, other national governments, international governmental or non-governmental organizations, and private sector entities and individuals.

Defined terms used in these Personal Data Protection Guidelines not defined above have the meaning as provided in the relevant MRC Operational Manual.

PRINCIPLES FOR PERSONAL DATA PROCESSING AT THE MRCS

The MRC Secretariat shall respect and apply the following principles when processing Personal Data:

Fair and Legitimate Processing:
Personal Data should be processed in a fair and transparent manner and only if there is a legitimate basis for doing so. Legitimate bases include:

- The Data Subject has given Consent to the processing of their personal data for one or more specific purposes
- In the best interest of the Data Subject or another person
- To ensure the safety and/or security of individuals
- The public interest
- To enable the MRC Secretariat to carry out its mandate under the 1995 Agreement, the MRCS ROPs and any approved work plans (MRC's legitimate interest)
- Performance of a contract
- Compliance with a legal obligation
- Defence of legal claims.

The MRC Secretariat shall take particular care in processing Sensitive Personal Data. Sensitive Personal Data shall only be processed where the Data Subject has given his or her explicit consent except:

- as is necessary for the purposes of carrying out the obligations and specific rights of the MRC Secretariat under applicable employment law; or
- where processing is carried out in the course of the MRC Secretariat's legitimate interests on the condition that the processing relates solely to MRC Employees or to persons who have regular contact with the MRC Secretariat in connection with its purposes, and that the Sensitive Personal Data are not disclosed to a Third Party without the consent of the Data Subjects.

Limitation to a Purpose:
Personal Data may be processed only for one or more specific and legitimate purposes and may not be further processed in a manner incompatible with such purpose(s). The MRC Secretariat may process Personal Data for purposes other than those specified at the time of collection if such further processing is compatible with those original purposes and, in particular, where the processing is necessary for historical, statistical or scientific purposes, or accountability of humanitarian action. However, further processing is not permissible if the risks for the Data Subject outweigh the benefits of further processing.

Data Minimisation:
The processing of Personal Data should be necessary and proportionate to the purpose(s) for which it is being processed. Therefore, Personal Data that is being collected and processed should be adequate and relevant to the identified purpose and should not exceed that purpose.

Accuracy:
Personal Data should be recorded as accurately as possible and, where necessary, updated to ensure it fulfils the purpose(s) for which it is processed. Data Subjects should be made aware of the importance of providing accurate and complete information,

including updating such information as applicable. Every reasonable precaution and effort must be taken to ensure that inaccurate Personal Data are corrected or deleted without undue delay (taking into account the purpose(s) for which they are processed, as well as the principles of data minimization and storage limitation).

Storage Limitation:
Personal Data must be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purpose(s) for which the Personal Data are processed. Personal Data may be stored for longer periods insofar as the Personal Data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

Maintaining Security and Confidentiality:
Personal Data must be processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures. In particular, the MRC Secretariat shall ensure that Sensitive Personal Data will be handled with the highest levels of care so as to preserve confidentiality.

Taking into account the available technology and cost of implementation, the MRC Secretariat shall implement appropriate organisational and technical measures to ensure that the processing of Personal Data meets the requirements of these Guidelines, including implementing protection-enhancing technologies and tools to enable Data Processors to better protect Personal Data.

To the maximum extent feasible, the MRC Secretariat shall make available to all MRC Secretariat Employees, and train such Employees, as appropriate on standard operating procedures related to data protection and security.

The below data are considered Personal Data and as such confidential by nature under the relevant MRCS Manuals and procedures. As such, the collection and processing must be handled strictly following these Guidelines as well as the MRCS Manuals and procedures applicable to confidential data, in particular relying only on the legitimate bases set out above:

- Personal information (Date of births, ID and passport numbers, gender and gender preferences, marital status, children, etc.),
- Personal contacts (email, addresses, phone numbers, etc.),
- Personal pictures and recorded video clips,
- Personal profiles such as resumes, curriculum vitae, and bio,
- Biometrics data such as fingerprints, eye scans,
- Staff and consultants' work performances, case studies, profiling of individuals, accreditation of writers, exit interviews, reference checks, etc.
- Personal health information including sick leave reports, health statement, health check records, health insurance claim records, etc.
- Personal financial data including salary, account details, pay rates, allowances, provident fund, personal advance purposes, insurances, benefits, separation, and designations, etc.
- Announced business including bidding data and business disclosure,
- Disputes and grievances,
- Dismissal or related disciplinary measures.

RIGHTS OF DATA SUBJECTS

Access:
Any person will be entitled to request information about their Personal Data. Except in the circumstances listed in this section below, a Data Subject will be entitled to receive from the MRCS:

- Confirmation as to whether or not Personal Data related to him or her has been, is being or is expected to be processed;
- Information on the Personal Data being processed, the purpose(s) for processing such data and any third parties to whom such data has been, is being, or is expected to be transferred.

The MRC Secretariat will make information publicly available regarding the rights of Data Subjects under these Guidelines to access, correct, transfer and/or delete their Personal Data, including the means by which such a request can be made. In the event of such a request from a Data Subject, all applicable Information Owners within the MRC Secretariat will cooperate to compile the relevant information in a reasonable timeframe to be determined and agreed in coordination with the Data Subject, taking into account factors such as the urgency and scope of the request.

The MRC Secretariat should not reveal any information about Data Subjects under this provision unless they are provided with sufficient proof that the person asking for the information is, in fact, the Data Subject. Any information which would reasonably lead to the identification of a whistle-blower must not be disclosed without such person's explicit consent.

The right of Data Subjects to access information does not apply or may be limited when important public interest requires that access be denied. These interests may include:

- Upholding confidentiality, such as that of whistle-blowers;
- Ensuring the viability of programs and work-plans being carried out under the MRC Secretariat's mandate;
- Preserving the confidentiality of MRC Employees' views or line of reasoning, which, if breached, might jeopardize MRCS' operations and/or disclose Personal Data of MRC Employees;
- Preventing retaliation;
- Maintaining the privileges and immunities afforded to the MRC;
- Maintaining the solicitor-client or other type of legally-protected privilege;
- Defence of legal claims and compliance with legal obligations;
- Ensuring the integrity of audit, investigation or judicial processes; and
- The rights and freedoms of others that override the data-protection interests of the Data Subject.

The MRC Secretariat may also limit Data Subjects' right to access information if the Data Subjects' requests are manifestly excessive.

Correction and Deletion

A Data Subject may request the correction or deletion of Personal Data that is inaccurate, incomplete, unnecessary or excessive, and the MRC Secretariat should correct or delete the Personal Data, as applicable, without undue delay.

Where a Data Subject requests the correction or deletion of his or her Personal Data, the MRC Secretariat should request proof relating to the inaccuracy or incompleteness, as appropriate. If there is a dispute as to whether the Personal Data is unnecessary or excessive, the Information Owner shall be consulted and the final determination will be made by the CEO (or designee)

However, data may be retained in its original form if it pertains to historical records or other auditable information.

Portability

A Data Subject may at any time request a copy of their Personal Data (in an easily accessible format) and/or request to have their personal data transmitted from the MRC Secretariat to another data controller.

Objection
A Data Subject may object at any time, on compelling legitimate grounds relating to their particular situation, to the processing of Personal Data concerning him or her.

An objection of this kind will be accepted if the fundamental rights and freedoms of the Data Subject in question outweigh the MRC Secretariat's legitimate interests, or the public interest, in processing. If such objection is accepted, the MRC Secretariat should no longer process the Personal Data concerned. If there is a dispute with respect to an objection, the Information Owner shall be consulted and the final determination will be made by the CEO (or designee).

General
The MRC Secretariat shall take due care to respond in a timely and reasoned manner to any requests by Data Subjects for access, correction, deletion and transmittal or to any objections received by Data Subjects.

PROTECTION OF PERSONAL DATA RULES AND PROCEDURES AT THE MRCS

DATA COLLECTION AND PROCESSING BY MRCS

Collecting Data from Data Subjects
When collecting Personal Data directly from a Data Subject, the MRC Secretariat should inform the Data Subject of the following in a manner and language that is understandable to the Data Subject:

- The specific purpose(s) for which the Personal Data or categories of Personal Data will be processed;
- Whether such Personal Data is intended to be transferred to a Third Party (including being made public);
- The importance of the Data Subject providing accurate and complete information, including updating such information as applicable; and
- The existence of these Guidelines and the means by which the Data Subject may request information or exercise his or her rights as provided under these Guidelines.

Where possible, the Data Subject should be asked to acknowledge that they have received the above information and that by providing their Personal Data, they consent to the collection for the purpose articulated and the potential transfer, if applicable.

Processing of Data by the MRCS
Decisions should not be made about individuals using entirely automated processes. Careful consideration shall be given before any techniques that will result in decisions being made about individuals through purely automated means, to ensure appropriate manual reviews are embedded into the decision-making process.

Suppliers
Where the collection and processing of Personal Data is one of the responsibilities of a Supplier, the MRC Secretariat shall endeavour to ensure that such Supplier undertakes and respects (or ensures that any Supplier with whom it contracts to collect or process Personal Data undertakes and respects) the same or comparable standards and basic principles of Personal Data protection as contained in these Guidelines.

When there is a reasonable expectation that the MRC Secretariat may collect or seek to collect Personal Data that is held by a Supplier, the MRC Secretariat should, as early as practicable, seek to ensure that such Supplier (i) is aware that the MRC Secretariat may collect or seek to collect data, which may include Personal Data, and knows the purpose for such potential collection, and (ii) has undertaken prior to collection and thereafter whatever is required under the laws applicable to such Supplier, as applicable, to ensure that the Personal Data may be transferred to the MRC Secretariat for such purpose upon request.

Confidentiality and Security of Personal Data
The MRC Secretariat shall treat all Personal Data classified as confidential. All Personal Data must be processed, handled, filed and stored in order to ensure and respect confidentiality.

The MRC Secretariat must ensure and implement a level of data security that is appropriate to the risks presented by the nature and processing of Personal Data, the availability and quality of the necessary equipment, the cost and the operational feasibility. In particular, the MRC Secretariat must ensure that Sensitive Personal Data is appropriately handled so as to preserve confidentiality.

The MRC Secretariat's data security measures must be designed and implemented to protect Personal Data against the risk of accidental or unlawful/illegitimate destruction, loss, alteration, or unauthorized disclosure of, or access to, Personal Data.

Taking into account the available technology and cost of implementation, the MRC Secretariat must implement appropriate organizational and technical measures to ensure that Personal Data processing meets the requirements of these Regulations, including implementing data protection-enhancing technologies and tools to enable Data Processors to better protect Personal Data.

The MRC Secretariat must make available to all MRC Employees, and train MRC Employees as appropriate, on standard operating procedures related to data protection and security.

The MRC Secretariat must maintain computer and information technology (IT) security that facilitate compliance with these Guidelines and any other relevant Operational Manuals, Procedures or Guidelines.

Ensuring Accuracy of Personal Data
MRC Employees must ensure that the MRC Secretariat has his or her latest personal information, as requested by the Human Resources Team. MRC Employees must provide notice of any changes as soon as possible to ensure accuracy of personal records at all times.

The MRC Secretariat should correct or delete Personal Data held on its systems when it becomes known that such Personal Data is inaccurate, incomplete, unnecessary or excessive. Where feasible and appropriate, confirmation from the Data Subject as to any correction should be obtained.

The MRC Secretariat should update Personal Data records when necessary and periodically verify them.

When Personal Data is corrected or deleted in the MRC Secretariat's systems as a result of having been inaccurate, the MRC Secretariat should notify, as soon as reasonably practical, any Third Parties to whom the relevant Personal Data was transferred, to the extent relevant and appropriate taking into account factors such as the original purpose of the transfer, whether the purpose is continuing and whether such notification would continue to be in compliance with the principles contained in these Guidelines.

Notification of a Data Breach
MRCS Employees are required to notify the Information Owner and the Information Technology (IT) Officer as soon as possible upon becoming aware of a Personal Data Breach or suspected breach and to properly record the breach. If Sensitive Personal Data has been or may have been compromised (e.g. unauthorized or unintended loss, modification, access or distribution), then this must be reported immediately and highlighted when reporting the incident.

If a Personal Data Breach is likely to result in personal injury or harm to a Data Subject, the Information Owner, or someone designated on his or her behalf within the MRC

Secretariat, should use his or her best efforts to communicate the Personal Data Breach to the Data Subject and take mitigating measures as appropriate without undue delay, unless:

- doing so would involve disproportional effort, owing to logistical circumstances or security conditions or the number of cases involved. In such cases, the Information Owner must consider whether it would be appropriate to issue a public statement or similar measure whereby the Data Subjects are informed in a manner that is reasonably expected to be effective;
- doing so would result in a breach of a legal obligation;
- doing so would jeopardize the privileges and immunities afforded to the MRC;
- doing so would be a violation of the solicitor-client or other type of legally-protected privilege;
- it is necessary not to in order to defend legal claims;
- doing so would adversely affect a matter of substantial public interest, such as the viability of MRC Secretariat's activities; or
- approaching the Data Subjects, because of the security or political conditions, could endanger them or cause them severe distress.

Retention

Personal Data should not be retained to a greater extent or for a longer period than is necessary for the purpose(s) for which it was collected.

The precise length of time will depend on the type of Personal Data, the purpose for which it has been processed and other obligations under MRCS' Operational Manuals Procedures and Guidelines that may require the MRCS to retain it for certain specified periods (see in particular Section 5.2 of the Administration Manual on document retention).

DATA PROCESSING BY THIRD PARTIES

Contractual Basis

If the MRC Secretariat cooperates with a Third Party in processing Personal Data, the responsibilities of both parties should be clearly defined and set out in a contract or other legally binding arrangement between the MRC Secretariat and such other entity so as to allow the MRC Secretariat to ensure that confidentiality is maintained, to specify the specific purpose(s) and legitimate basis for the processing of Personal Data and to ensure continuing compliance with the standards and basic principles of these Guidelines.

Irrespective of any obligations set forth in an agreement, the MRC Secretariat should verify, prior to transferring Personal Data to a Data Processor or engaging a Data Processor in the collection and processing of Personal Data, that the processing of Personal Data by the Data Processor satisfies the standards and basic principles of these Guidelines and ensure the protection of the rights of Data Subjects.

In sum, the MRC Secretariat shall only use Data Processors that provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing with meet the requirements and standards of these Guidelines and ensure the protection of the rights of Data Subjects. Appropriate contractual arrangements will be put in place to ensure such compliance.

DATA TRANSFERS BY THE MRCS

Limitations on Data Transfers

The MRC Secretariat may transfer Personal Data to Third Parties on the condition that the Third Party affords a level of data protection the same or comparable to the standards set out in these Guidelines, and Data Subjects have been made aware that their Personal Data may be transferred. In particular, and without limitation to the foregoing, Data Transfers are subject to the following conditions:

- The Data Transfer must be based on one or more legitimate bases;
- The Data Transfer must be for one or more specific and legitimate purpose(s);
- Processing by the Third Party must be restricted as much as possible to the specific purpose(s);
- The amount and type of Personal Data to be transferred is strictly limited to the Third Party's need to know for the specified purposes intended;
- The Data Transfer should not be incompatible with the reasonable expectations of the Data Subject; and
- The Data Transfer fulfils the applicable conditions set out in the Section on Safeguards below.

Depending on the sensitivity of the transfer and the risks it presents to individuals, additional protections may be necessary. In all cases, any potential negative impact on the safety and security of MRC Employees or other Data Subjects or the effective functioning of the MRC Secretariat pursuant to its mandate should be taken into account.

Safeguards

In an effort to ensure that the limitations set out above are adhered to, appropriate safeguards should be adopted, such as:

- Ensuring that a Data Transfer is made to a Third Party that is subject to appropriate data protection legislation (in line with the standards set out in these Guidelines) or appropriate internal statutes or policies; and/or
- Using binding contractual clauses ensuring data security and appropriate levels of data protection.

While every effort should be made to ensure the above safeguards are adhered to in the case of any transfer of Personal Data, other permissible grounds for transferring Personal Data include:

- The Consent of the Data Subject (wherever possible, evidence of such Consent should be obtained and retained);
- The vital or best interests of the Data Subjects or other persons;
- The public interest, based on the MRC Secretariat's mandate;
- To ensure the safety and/or security of individuals;
- The fulfilment of a contract between the MRC Secretariat and the Data Subject; or
- Defence of legal claims or compliance with legal obligations.

In such circumstances, Consent of the Data Subject should be sought whenever practicable, even if there are other permissible grounds for the transfer. Information Owners are responsible, where applicable, for determining whether one or more of the above grounds is applicable.

To the extent possible, all parties concerned must be made aware that the MRC Secretariat cannot be obliged to disclose any information acquired in the course of its activities.

In all cases, appropriate measures should be used to safeguard the transmission or forwarding of Personal Data to Third Parties. The means of transmission, and the methods of security employed, should be consistent with the nature and sensitivity of Personal Data.

Transfers to Legal Authorities

In appropriate circumstances, the MRC Secretariat may transfer Personal Data to a national law enforcement agency, a national court or another legitimate legal authority.

Such Data Transfers may be upon request of the legal authority (which may be binding or non-binding on the MRC Secretariat) or on the MRC Secretariat's own initiative.

The MRC Secretariat may only cooperate with a non-binding request and transfer Personal Data to a legal authority or transfer Personal Data to a legal authority on its own initiative if the following conditions are met (unless Consent to the Transfer of such Personal Data by the Data Subject has been obtained):

- Such Data Transfer is necessary for the purposes of the detection, prevention, investigation or prosecution of a serious criminal offense, in particular in order to avoid an immediate and substantial risk to the safety and security of an individual or the public;
- The requesting legal authority is competent in relation to the detection, prevention, investigation or prosecution of the offense in questions;
- Such Data Transfer will substantially assist the legal authority in the pursuit of these purposes and the Personal Data cannot otherwise be obtained from other sources;
- Such Data Transfer does not disproportionately interfere with a Data Subject's or another person of concern's right to privacy or other human rights; and
- In the case of Personal Data in relation to victims and witnesses, their Consent to the transfer has been obtained.

Privileges and Immunities

Any transfer of Personal Data is and shall be without prejudice to and shall not be deemed as a waiver, express or implied, of any of the privileges or immunities of the MRC under (i) international law, including customary international law, international conventions, treaties or agreements; or (ii) any national laws.

IMPLEMENTATION

The MRC Secretariat will be responsible for the overall implementation of these Guidelines, including ensuring that MRC Employees are appropriately aware of these Guidelines and the requirements within them, and for making any required determinations hereunder. Each Information Owner is responsible for ensuring that the appropriate level of access, accuracy, availability and controls for information are maintained in accordance with these Guidelines.

FORMS TO BE USED AND PRIVACY STATEMENT FOR PROCUREMENT PROCESS

Code	Name	Effective Use of Forms
PPD-01	MRC Employee Statement on Personal Data Collection and Processing.	- This Form is used by the MRCS to ensure that MRC Employees, as Data Subjects, have read and understood the manner in which MRCS processes and collects personal data. In the Form, MRC Employees also undertake to keep their personal data up-to-date. - This Form will be signed by MRC Employees at the start of their service with the MRC, together with the signing of the Service Contracts, or at the time the Guidelines become effective and implemented.
PPD-02	Personal Data Access/Update/Correction/Erase Request	- Both fixed-term staff, consultants, or other defined third parties identified as an MRC's Data Subject can use this Form to request access to his or her personal data, correction, update or erase of it. - The Form can be sent to HR as a focal point to facilitate the access, correction, or update processes.
PPD-03	Privacy Statement for the MRC Secretariat Procurement Processes	- This Statement informs all participants and tenders and Suppliers of the MRC Secretariat about how the MRC Secretariat treats their Personal Data. - The Statement shall be part of all tender documents distributed to potential suppliers and shall also be accessible on the MRC Secretariat website in the section on Tenders.

PPD-01

Mekong River Commission
For Sustainable Development

MRC EMPLOYEE STATEMENT ON PERSONAL DATA COLLECTION AND PROCESSING

By signing this form, I acknowledge that I have read and understood the MRC Secretariat Guidelines on Personal Data Collection (the "Guidelines") (attached). Further to the Guidelines, I understand that the MRC Secretariat, and any third parties designated for that purpose, may process Personal Data for the purpose of the Mekong River Commission implementing its activities and for it to have the information available that a reasonable employer requires, including for the purpose of any benefits or other entitlements. As such, I consent to the MRC Secretariat's collection and processing of my personal data according to the Guidelines. The MRC may collect data through the forms, requests, statements, applications and other documents referred to in the Personnel File Checklist (EP-05) or such other means consistent with the Guidelines.

I understand that, as a Data Subject and in accordance with the Guidelines, I can request access, correction and deletion of my personal data by using the appropriate form (PPD-02).

I further undertake to ensure that the personal data provided shall be correct and kept updated. To this end, I will inform the HR team of any changes occurring.

_____	_____	_____
Staff's Full Name	Staff's Signature	Date

Mekong River Commission
For Sustainable Development

PERSONAL DATA ACCESS/UPDATE/CORRECTION/ERASURE REQUEST

Any Data Subject under the MRC Secretariat Guidelines for the Protection of Personal Data can use this form to request access to his or her personal data, or to request for correction, updating or removing it. The Form can be sent to HR as a focal point to facilitate the access, correction, updating, or removal processes.

Requester's Name:		**Agency/Division if applicable:**	
Type of Request:	☐ **Access** ☐ **Correction** ☐ **Updating** ☐ **Erasure*** ** Personal Data provided by MRC Employees that are related to benefits provided by the MRC or otherwise needed for reasonable HR purposes cannot be erased.*		
Purpose:			
Data:	**Personal Data covered by the request:** ☐ Personal information (date of birth, ID and passport number, gender and gender preference, marital status, children, etc.) ☐ Personal contact (email, residential address, phone number, etc.) ☐ Personal picture and recorded video clip ☐ Personal profile such as resume, curriculum vitae, and biography ☐ Biometrics data such as fingerprint and eye scans ☐ Disclosed businesses to the MRCS ☐ Others (please specify): _____ **Personal Financial Data:** ☐ Payment/payroll ☐ Bank details ☐ Others (please specify): _____		
Description of Request	*Please provide details on the action you are requesting and be specific about the Personal Data that is the subject of your request:*		
Requester:	Signature:		Date:
Verified by: (Division Director)	Full Name:	Signature:	Date:
Concurred by: (AD Director)	Full Name:	Signature:	Date:

Mekong River Commission
For Sustainable Development

PRIVACY STATEMENT FOR THE MRC SECRETARIAT PROCUREMENT PROCESSES (BIDDING, SELECTION AND EVALUATION PROCESSES, PROCUREMENT CONTRACTS IMPLEMENTATION AND MONITORING)

The Mekong River Commission Secretariat (hereinafter "MRC Secretariat" or "MRCS") is committed to respecting the dignity and privacy of people, while balancing such rights with the MRC Secretariat's ability to carry out its mission and activities.

1. When does this privacy statement apply?

This privacy statement explains how the MRC Secretariat may collect and use information as part of its procurement processes. The procurement process includes the submission of bids, the due diligence process, [1] selection and evaluation process of your or your organization's proposals/bids/quotes, and the implementation of any contract with you or your organization and the MRC Secretariat.

This privacy statement also explains the choices and rights available to you. We reserve the right to modify this privacy statement at any time and encourage you to stay informed by reviewing updates posted on the MRC Secretariat website.

2. Why does the MRC Secretariat process my personal data?

The MRC Secretariat may process personal information to carry out its mission and mandate as an international organization. This means the MRC Secretariat has an interest in collecting and using personal information for the following purposes:

- to assess your or your organization's capacity and suitability to provide the goods or services financed by the MRC Secretariat, including potential operational, financial and reputational risk which you or your organization (or association with your organization) may present to the MRC Secretariat,
- to assess the background and skills of you or your organization's employees or consultants who may work under a contract with the MRC Secretariat,
- to undertake regular procurement proceedings, including audit and accounting, quality assurance inspection, risk assessment and mitigation, due diligence, conflict of interest management and contract negotiation and management functions, and
- to select, manage and monitor the MRC Secretariat's suppliers, as part of its procurement process.

3. What information will be collected about me and how will it be used?

The information the MRC Secretariat will collect about you includes:

[1] As described in the MRC Secretariat Due Diligence Guidelines.

- business contact details, such as names, titles, addresses, emails, phone numbers, etc.;
- fiscal or financial information, such as financial statements, audit reports, bank details, VAT or other tax registration number, invoices including supporting documentation such as timesheets, receipts, etc.;
- professional background (skills, education, employment, qualifications, memberships and associations, partnerships etc.);
- biographical information, such as gender, date of birth, family relations, nationality, right to work or conduct business in relevant locations; and
- reports of suspected or credible links to prohibited practices, professional misconduct or unethical activities (as set out in the MRC Secretariat's Exclusion Criteria) that may present risks, including operational, financial or integrity risk, to the MRC Secretariat.

The personal information will be made available to the evaluators or members of the proposals/bids/quotes evaluation panel, the MRC Secretariat's auditors (internal and/or external), as well as the relevant employees and consultants of the requesting business unit, the MRCS HR and Procurement teams, who have a need to obtain the information to ensure compliance with the procurement process. The personal information will also be made available to the relevant teams conducting the MRCS due diligence process.

4. Where does the MRC Secretariat obtain information?

The MRC Secretariat may obtain personal data directly from individuals applying for consultancies or individuals providing their own information as representatives of bidders or suppliers. Personal data may also be obtained indirectly from organizations lawfully providing personal information for their employees, sub-contractors, consultants, etc.; MRCS may obtain information provided by bidders or suppliers, current or past employers, clients or associates, public partners such as governmental authorities or intergovernmental organizations, from public sources such as judicial records, sanctions lists, media and social media.

5. How long will the MRC Secretariat keep my information?

The MRCS retains information for up to seven (7) years.

6. How does the MRC Secretariat protect my information?

The MRC Secretariat has put in place a set of measures to protect information, including strong information security policies and controls baseline, as set out in its Personal Data Protection Guidelines (which can be accessed here: [PPD Guideline]).

7. What if I don't wish to provide my information?

You are not obliged to participate in the MRC Secretariat's procurement process as an individual consultant, or an organization. If you choose not to provide certain information about yourself, MRCS may not be able to fully assess your or your organization's capacity to perform the work and this could result in MRCS not being able to award or enter into a contract with you or your organization. If you are an employee, consultant or other contractor of a supplier, or applicant to become a supplier and you believe your employer or contractor has not lawfully provided your personal information to the MRC Secretariat please contact the MRC Secretariat at the e-mail address below.

8. Whom should I contact if I have questions about my personal information?

You may request at any time to access your personal information or that your personal information be corrected or deleted in connection with the MRC Secretariat's procurement process. In case of a request for deletion and depending on the nature of the information to be removed, the MRC Secretariat reserves the right to no longer consider a bid or proposal if the deletion results in the minimum criteria for such bid or proposal cannot be met any more.

You are invited to contact mrcshr@mrcmekong.org if you have questions about your personal information, including if you have any complaints with respect to how the MRC Secretariat treats your personal information.

For your protection, the MRC Secretariat will only implement requests with respect to the personal information associated with the particular email address that you use to send us your request, and you may need to verify your identity before the MRC Secretariat is able to implement your request. Verification may require that the MRCS asks you to provide other personal information or use certain security measures. If MRCS is unable to verify your request, it may not be able to implement the request for security reasons.

The MRC Secretariat will endeavour to comply with your request as soon as reasonably practicable. In some cases, certain information may need to be retained where important public interests require this, such as the safety and security of individuals; the rights and freedoms of others; the integrity of audit, investigation, arbitral or judicial processes; and/or recordkeeping or legal purposes.

9. Privileges and immunities

Nothing in or related to this privacy statement may be construed as a waiver, express or implied, of the privileges and immunities accorded to the MRC Secretariat under international law, including international customary law, any international conventions, treaties or agreements, or any national laws.