ICMPD
International Centre for
Migration Policy Development

Data Protection Rules and Procedure

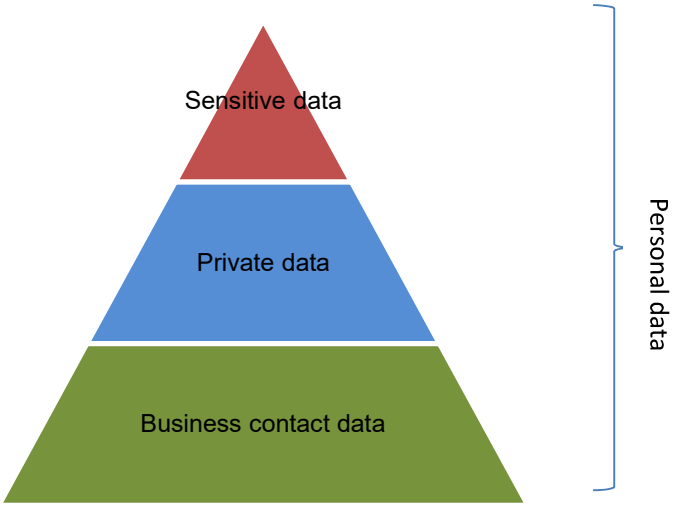
Filename: Data Protection Rules and Procedure		Distribution: ICMPD Employees	
Drafted	Approved	Released	Effective from
Pohnitzer	Rolli	Griffin Dass	25/10/2019

Table of Contents

Purpose

These rules regulate the handling of personal data of individuals and in relation to ICMPD business partners.

Data protection (DP) is a fundamental right, and ICMPD implements both technical and organisational measures to ensure that the core of the right to data protection embodied in the main principles of the General Data Protection Regulation (GDPR)[1] are adequately protected depending on the sensitivity level of the respective data.



Scope

The provisions in this document apply to all ICMPD offices, all ICMPD staff members and contractors working for ICMPD on an SSA basis. Both electronic and hard copy files processed by ICMPD are affected. If employees store or transfer private messages, files or contacts in/on equipment, systems, services, or virtual/physical spaces provided, managed and maintained by ICMPD, it is their personal responsibility to ensure consent was duly received and the rights of the Data Subject upheld.

This document stipulates the general rules applicable to personal data processed by ICMPD. Rules specific to certain processing activities[2] are stipulated in the applicable rules and procedures, and further detailed in related work instructions.

Definitions

Personal data (PD) .....any information that identifies or can be used to identify[3] a natural person ("Data Subject"), whether by itself or together with other information in ICMPD's possession.

Data Subject.....any identified or identifiable natural person, whose PD is handled by the data processor on behalf of the data controller (see definitions below). With respect to his or her PD, the Data Subject holds the rights of confirmation, access, rectification, deletion and restriction of distribution thereof.

Business contacts.....natural persons who are identifiable via their business contact details, including consultants[4] and representatives of suppliers and project partners/beneficiaries, and who have provided their details to ICMPD in their professional capacity.

---

[1] Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of the PD and the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[2] For example, recruitment, newsletter dissemination, document management and event management.

[3] PD includes name, telephone number, email address, place and date of birth, audio, photograph, video and factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a natural person.

[4] For whom business and private contact details may overlap.

Private data.....PD of natural persons who do not fall under the category of business contacts.

Sensitive personal data .....is a special category of PD that is subject to additional protection as their abuse could lead to the potential harm to or discrimination of the Data Subject or others.[5]

Consent of the Data Subject.....any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or clear affirmative action,[6] signifies agreement to the processing of PD relating to him or her; whereby informed means that they actively understand the foreseeable purpose and who will have access to their PD.

Data processing.....any operation or set of operations which is performed on PD or on sets of PD, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data controller.....the natural or legal person, public authority, agency or other body which, alone or jointly with others (e.g. implementing partners), determines the purposes and means of the processing of PD.

Data processor .....natural or legal person, public authority, agency or other body which processes PD on behalf of the controller. The definition also applies to a contractor who merely has, for the time of their engagement with ICMPD, access to certain data for which ICMPD is the data controller and who is not tasked by ICMPD with carrying out any activities related to the data.[7]

Third party.....natural or legal person, public authority, agency or body other than the Data Subject, controller, processor and natural persons who, under the direct authority of the controller or processor, are authorised to process PD.

Personal data breach.....breach of data security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, PD transmitted, stored or otherwise processed; includes, for example, equipment/documents stolen which included/stored PD.

Encryption .....the process of converting data into incomprehensible code and using a key to protect access to the original data.

Anonymisation/pseudonymisation .....the processing of PD in such a manner that the PD can no longer be attributed to a specific Data Subject without the use of additional information, provided that such additional information is stored separately and is subject to technical and organisational measures to ensure that the PD is not attributed to an identified or identifiable natural person.

---

[5] Such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, and data concerning health or a Data Subject's sexual orientation.

[6] Such as written electronically or spoken orally for business contacts, e.g. by personally handing over their business card or sending their CV.

[7] Such as hotels, interviewers, translators and IT companies updating websites holding PD.

Roles and Responsibilities

	Responsibilities	Remarks
Legal Consultant	Reviews relevant contracts deviating from standard format, and other relevant documents upon instruction of the ODP	Via PGU
Organisational DP Focal Point (ODP)	Ensures reflection of applicable international developments in the regulatory framework(s); training of new staff and personnel to create awareness; focal point for external and internal inquiries related to DP; involved in any audit and investigation related to DP; reports to the Dir ROM on any risk or breach; advises on risk assessments where sensitive data is involved	All inquiries should be directed to data.protection@icmpd.org
Data Focal Point (DFP)	Takes all measures necessary to ensure integrity of and adequate access restrictions for virtual and physical space(s) within his or her responsibility; ensures documentation of purpose and legitimate ground(s) of processing and access/disclosure for any PD stored in their space(s); upon request, ensures information/rectification deletion/destruction (if feasible) of data in the space(s) under his or her responsibility; ensures retention periods are respected in their space(s)	Process Manager; PjM; RC; HoP; HoU; HoO as per responsibility for respective space – a replacement ("Deputy DFP") must be assigned Virtual spaces include ICMPDNet, local servers, Outlook (including Public Folders), SharePoint and external virtual spaces (e.g. external file sharing and communication tools)
Application/Project Manager (AM/PjM)	Runs risk assessments related to PD processing; coordinates in a timely fashion with ICT Support and the ODP in case sensitive data or other high risks are involved; upon a project's completion, reviews which data should be retained/anonymised/pseudonymised/transferred/deleted	
HoCFM	Responsible for the archiving of audit-relevant files and definition of accounting policy	
ICT Support	Ensures adequate data security in line with this document and project-specific requirements; if required, consults with the ODP and with external providers on technical issues in case of data security breaches	
QMS Team	Consults with the ODP when updating/drafting any DP-relevant controlled documents; maintains entries in the Overview of Data Processing Activities related to its process(es)	
Staff members and contractors working on SSA basis	Treat any PD with respect in line with this normative document; follow rules and instructions related to PD as applicable to their functions; follow ICT Support rules, e.g. on strong passwords and logging out; are mindful of data quality; keep PD up-to-date in PeopleNet; in the event of any (suspected) breach or risk thereof send an email to data.protection@icmpd.org, copying the respective DFP and ICT, and/or the person responsible for office management in the respective location	

Rules

1. The following principles – in line with the GDPR – apply to any processing of personal data on behalf of ICMPD:
   1.1. Lawful and fair processing: data processing may be based on active consent of the data subject, a contract or legal obligation, vital interests or public interest, and legitimate interests of the organisation. The latter need to be weighed against the interests of the data subject;
   1.2. Transparency
   1.3. Purpose specification and limitation
   1.4. Data minimisation: collecting and processing only the data needed for the specific purpose, and only keeping it as long as needed;
   1.5. Data quality: includes ensuring integrity of data, and keeping it up-to-date;
   1.6. Accountability
2. All staff members and SSA contractors sign a confidentiality clause as part of their contract and are sufficiently instructed to carry out their responsibilities in relation to DP. Should they have any doubt regarding their responsibilities, they must address data.protection@icmpd.org.
3. Any breach of the confidentiality clause and this normative document is considered a breach of the ICMPD Code of Conduct and will result in disciplinary measures under *ICMPD Staff Regulations/*applicable rules, without prejudice to any further remedy in accordance with the applicable law.
4. All PD shall be processed in a fair and transparent manner.
5. PD shall be collected for specific, explicit and legitimate business purposes only, based on considerations of organisational need, and the needs and interests of the Data Subject. Only data relevant for the specific purpose may be collected and processed.
6. All PD shall be accurate and maintained up-to-date. When found to be inaccurate, it shall be corrected as soon as possible.
7. PD shall only be used for the specified purpose.
8. PD which is no longer used for its specified purpose nor needed for contractual/legal purposes, or is known to be inaccurate, shall be deleted/destroyed or, where deletion is not feasible, access must be restricted so that no one has access, apart from those responsible for the technical maintenance of the space in which it is saved.
9. While business contacts may be made available to all staff and personnel[8], and to implementing partners, beneficiaries and contractors as required, access to private and sensitive data is restricted to persons who need access for carrying out their respective function, and for as long as they carry out this function based on a secure authentication mechanism including strong passwords.
10. The processing activities of PD owned by ICMPD may only be performed by external parties based on the conclusion of a binding written contract that sets out the purpose and duration of the processing, and ensures that the processor meets technical and organisational requirements to ensure the effective protection of the rights of the concerned Data Subjects.

[8] Unless there are restrictions related to confidentiality

Purpose and scope

The purpose of this manual is to specify the implementation of the *Data Protection Rules*. It explains the data processing cycle, from collection of data to its destruction, as well as how data protection issues are to be handled at project and organisational level.

The Procurement and Expert Management frameworks also make reference to data protection in relation to suppliers and experts, respectively.

Knowledge and information management

In order to minimise the risk of inadequate handling of PD, training is provided to all staff and personnel to the extent necessary for them to carry out their functions.

Further details can be found in the FAQ on *Data Protection Space*, where a discussion board also provides the possibility to ask questions related to specific contexts.

Overview of organisational processing activities

At all times, process managers must maintain the entries related to the processing activities in their processes up-to-date in the *Organisational Overview Personal Data Processing*, and duly inform all affected of any changes.

Project-related personal data processing

During project development, the application manager must carry out a general risk-benefit assessment of data processing,[9] and an assessment of the specific risks related to PD processing as planned as part of the general risk assessment, and propose adequate mitigating measures.[10] Special technical and organisational measures must be discussed with the ODP and ICT Support if sensitive data is involved or a high risk has been identified. Adequate funding must be foreseen for this purpose (*Budgeting Guidelines*). The measures foreseen need to be reviewed/coordinated with the ODP and ICT Support in due time before data collection commences, taking into account the time needed for the purchase/implementation of technical and organisational measures. As a minimum measure, training is provided by the ODP to all staff members and contractors working on an SSA basis; if ICMPD is in the lead and is the data controller, the training should include contractors, implementing partners and beneficiaries. Risks should be further minimised by strict organisational and technical controls and monitoring, and need to be re-assessed by the PjM at regular intervals as part of any work plan.

In the event that risks are likely to materialise or new and high risks are identified, the ODP – and ICT Support if technical measures are concerned – must be informed without undue delay.

The DFP responsible must know, at any time, which PD is being processed and accessible by/shared with whom and by which means in their projects. For this purpose, they may use the *Project Overview Personal Data Processing Template*. For projects in which private/sensitive data is processed, documentation via a record based on this template is a requirement.

---

[9] Expected organisational benefits must be reasonable, justifiable and proportional, whereas the benefit to/limitation of the risk of harm to the Data Subject is the most important consideration.

[10] See *Risk Analysis Work Instructions*.

Data collection

When collecting PD,[11] care should be taken of social, cultural and religious attitudes of target groups and individuals. Gender, culture, language and age-specific collection methods should be used with due respect for the safety and dignity of the Data Subject. Appropriate safeguards should be in place to protect the rights and well-being specifically of vulnerable Data Subjects.[12]

Any consent for the processing of PD shall be given in a free, specific, informed and unambiguous manner. Data Subjects must be informed at the time of giving consent in an easily understandable way for the target group about:

- the purpose of data collection – including any foreseeable additional purpose;[13]
- to whom the data will be disclosed;[14] and
- the possibility to request information, and the update or deletion of the data provided by emailing the respective ICMPD focal point or data.protection@icmpd.org.

If PD is collected as part of research activities, a clear description of the objective and nature of the research, the expected role of the Data Subject, and the research methodology and output must be provided to the Data Subject, where feasible and applicable. Interviewers must be sufficiently trained.

Data Subjects should be informed of any possible consequences of not providing consent. If Data Subjects have a limited capacity to consent, their best interests must be taken into account. If data is collected from a third party for practical reasons, the third party should inform the Data Subject or their legal representative and confirm to ICMPD in writing that the data provided is valid and that the Data Subject/legal representative has been informed in line with GDPR requirements.

Consent should be given in written form. In every case, information provided and consent must be adequately documented[15] to allow verification that consent was obtained at the time of data collection.

By signing a contract with ICMPD, employees consent to the sharing of their names, business address and ICMPD telephone number, as well as the use of their current CV[16] and photographic images/recordings taken in a business context for business purposes. Photographic images/recordings may be published and stay published beyond the end of the employment contract unless the employee specifically withdraws their consent. Disclosure outside of ICMPD HRM of any other PD requires additional consent.

Providing a CV or business card to ICMPD is considered an active statement by an aspiring business partner of their interest to be represented in all relevant ICMPD contact/expert directories and be contacted by

[11] Includes taking photographs/videos.
[12] For example, minors, detainees, disabled or otherwise disadvantaged individuals and thus likely to be vulnerable to coercion.
[13] For example, for organisation of the event; research/statistical/administrative/communication purposes.
[14] If it is planned to transfer PD to a third country or international organisation for which there is no *adequacy decision by the EC*, this needs to be expressly stated.
[15] Includes recording by computer systems, voice recording or documented confirmation by staff members/contractors.
[16] As verified by themselves.

ICMPD officers within the given business context unless the Data Subject specifically limits his or her consent when providing PD.

For the dissemination of newsletters or other standardised information material, specific consent for this purpose must be obtained unless there is a contractual obligation to inform the specific target group, respective interest has been recorded or is apparent from their role. Recipients must be informed that their PD may be used to better target ICMPD communication tools in the future via tracking views/clicks, if applicable, and where respective PD is stored.[17]

Storage

All PD shall be stored in a manner and location that ensures appropriate data security and authentication mechanisms to ensure eligibility of access. Respective office rules are in place to govern physical spaces. In terms of virtual spaces, data security and integrity measures include regular updates and backup, effective recovery mechanisms and malware detection. *ICT Rules* and related work instructions, such as those related to *ICMPDnet*, govern general authentication and data storage requirements of ICMPD-controlled content.[18] Employees are specifically reminded that portable equipment must be stored in a safe and secure location at all times, strong passwords be chosen and screens locked when not in use.

PD shall exclusively be stored electronically unless there are any legal requirements to keep **hard copies**. Hard copies with private data shall be effectively destroyed after electronic archiving, e.g. by shredding. Printouts of private data shall be avoided, and, if required, the printer shall be closely monitored and documents immediately retrieved and placed in a locked cupboard whenever not in use. Special care must be taken when transporting hard copy files with private data away from an ICMPD office.

Adequate authentication mechanisms in line with *ICT Rules* must be technically ensured for all access points to **electronically stored** PD effectively controlled by ICMPD. Where systems for which data security is not fully under ICMPD's control (e.g. Dropbox) are used for storage or transfer of any PD, it may only be used from an ICMPD computer with a personal account linked to an ICMPD email address. Sensitive data must not be stored on such systems.

Storage of PD on portable storage devices, such as USB sticks, should be avoided whenever possible. If temporary storage is unavoidable, the media must be kept safe and under observation, and the respective file(s) encrypted. The file(s) must be transferred to another appropriate storage space as soon as possible and the external storage device formatted to ensure deletion of the file(s).

The responsible DFP must take adequate measures to ensure that private data stored in the space for which they are responsible is only accessible on a need-to-know basis required for fulfilling the function of the party who is granted access: respective justifications for access must be provided with the relevant request and the manager copied on the request to certify the eligibility. In addition, for third-party systems (e.g. Dropbox) in which PD is stored by ICMPD, the respective DFP is responsible for ensuring access may not be extended without his or her consent.

[17] Direct reference must be made to the service provider used.

[18] Conditions for third party file share or data base systems must be reviewed by ICT Support and a lawyer before any commitment to their usage is made in order to ensure adequate technical and legal assurances.

For this purpose, and to allow for effective retrieval/correction/deletion of PD if requested by the Data Subject, the DFP must ensure that all PD is saved in a clearly marked folder[19] or, where no folder structure exists (e.g. on SharePoint), the file is marked accordingly. Dedicated sub-folders should be created for private and sensitive PD, and applicable access restrictions set. Attention should be placed not only on read access but also edit and delete rights in order to minimise the risk of wanton manipulation/deletion. Attention must be paid that access restrictions stay intact while moving folders.

In the case of employee **off-boarding**, ICT Support and the person responsible for office management in the respective location effectively ensure that exiting employees do not have access to spaces controlled by ICMPD beyond their last day of work. The DFP is responsible for withdrawing access to file sharing and database systems used by their team (e.g. Dropbox and databases on project websites).

Transfer and transmission of PD

Legal and organisational measures

PD may only be disclosed based on a contractual relationship including adequate non-disclosure and data security assurances. *Service and Supply Contracts* include a clause on data protection, and, if sensitive data is accessible to suppliers, a more extensive *Non-Disclosure Agreement* must be considered.

Where ICMPD contractors are processing substantial amounts of personal data or process sensitive data on a regular basis, a Data Processor Contract (based on the *Data Processor Contract Template* or similar) must be signed and/or respective articles included in the general contract. Any such contract must include the type of PD, duration and purpose of the processing, a limitation on further use and disclosure, as well as a destruction requirement, and the rights and obligations of ICMPD and the processor. Ownership generally rests with ICMPD where ICMPD collected the data as data controller. ICMPD shall be granted the right to audit the facilities of the processor at any time.

Agreements/contracts exclusively related to data protection are signed by the Data Focal Point responsible. General contracts are signed as per the Procurement *Rules* and *Procedures*.

ICMPD shall only use external processors that provide sufficient guarantees to implement technical and organisational measures in such a manner that processing will meet the requirements of this normative document and ensure the protection of the rights of Data Subjects.

Records must be retained of all disclosures to third parties.

Technical measures

Transmission of PD has to be technically secured against unwanted dissemination to, or interception by, unintended/unwanted parties. It must be ensured that only those who should be granted access actually have access via appropriate authentication services.

Emails including PD must not be sent via/to any private email accounts. For the ICMPD emailing system, there are technical measures in place to prefer transport encryption based on TLS v.1.2. When transmitting private data via a messaging system, this should be done via encrypted email attachments in emails marked confidential. Passwords must have a minimum length of 12 characters consisting of at least one lower case

[19] On ICMPDnet and local servers, concerned sub-folders must include '_XDP'. On SharePoint, respective files must be marked via the document properties.

letter, one upper case letter and one digit, and must never be transmitted via email but with an end-to-end encrypted transmission system.

Web-based transfer systems have to use HTTPS protocol based on TLS (>= v.1.2) encryption.

All electronic records sent or received containing private data must be saved without undue delay on an ICMPD-maintained system and deleted from individual mailboxes, including the deleted items folder. Requirements and restrictions as to the use of services/tools mentioned in the section *Storage* apply.

Where transfer of hard copies including sensitive data is required, these must be sent by registered mail via a trusted international courier service.

Publication

Only PD (including photographs/videos) where specific written[20] consent for use has been obtained prior to publication shall be used in publications, including websites and social media, or any oral communication to the public. Where consent has not been obtained through event registration or a research/interview authorisation form, the *Publication Authorisation Form* may be used.

Anonymity shall be maintained when publishing research findings and analysis,[21] unless the Data Subject has specifically agreed.

Retention, archiving and destruction

The general **retention period** of PD at ICMPD is ten years, apart from the PD of applicants whose PD is deleted/destroyed after two years from the last update by the applicant.[22] This is notwithstanding any other legal requirements to which ICMPD must comply. Data may also be retained if a further business purpose is given. For statistical information, records shall be anonymised.

This is notwithstanding the **right of the Data Subject to request deletion** of their PD **or withdraw specific consent** at any time. The request must be complied with unless there are legal requirements to keep certain data. Data Subjects should be informed of any known consequences of withdrawing their consent. If deletion/destruction is not feasible, it must be otherwise ensured that it will not be accessible by anyone apart from those responsible for the technical maintenance of the respective storage space. If the relevant PD has been published with the consent of the Data Subject and the Data Subject requests deletion of his or her PD or withdraws consent, they must be removed[23] from all copies of the publication which, at the time of request, are still under the direct control of ICMPD, or the publication be destroyed.

When the specific purpose for which consent was given has been accomplished, the responsible DFP must review if private data may be anonymised or pseudonymised. During project closure the PjM must review all PD in the project folder, anonymise/pseudonymise it or, in case there is a further business purpose, with the approval of the relevant DFP, transfer it to another location where that business purpose is best served. Any PD needed for accounting purposes is stored in SAP and should not be kept in the project folder. Remaining PD which is no longer required for audit purposes must be deleted.

[20] Emails and recordings by computer systems are acceptable.
[21] For example, pseudonyms should be used or identifiable factors substituted.
[22] For successful applicants, only information that has a bearing on the employment relationship shall be retained and transferred to the employment records.
[23] Deleted from the file, and blackened out or otherwise made unreadable in hard copies.

Where, for technical reasons, more PD is collected than required or at a later stage not all PD is needed for the specific purpose consent was given, the data should not be retained, or PD should be anonymised where possible.[24]

Hard copies shall be anonymised, shredded or destroyed by a professional destruction company, and electronic files permanently deleted from the system[25] or anonymised. Where destruction or deletion is not feasible, because it would represent an unreasonable burden to ICMPD, any records or PD identified for destruction/deletion may not be used and shall be stored in a secure environment to which no one has access apart from those responsible for technical maintenance of the space in question, in order to ensure confidentiality in accordance with this normative document.

Any external party to which sensitive PD was disclosed must provide written confirmation/records of destruction once the contractual relationship ends, the specific purpose no longer applies or the Data Subject withdraws his or her consent. The records must be filed for future reference.

Data Quality

Data integrity

Data accuracy

Care should be taken to ensure accuracy of data collected. For this purpose, supporting documentation may be collected with the specific consent of the Data Subject. Keeping the same data in several spaces must be avoided in order to avoid the risk of inaccurate data.

PD is considered accurate unless and until any indication is received from the Data Subject that the data has become outdated, at which time it must immediately be updated in all locations, where feasible, or the usage of the outdated data prevented. Outdated files must be replaced by current files or moved to "Outdated" folders.

If the Data Subject is likely to believe that updates in one database may automatically trigger updates in any other databases, the Data Subject must be alerted if this is not the case.

Data subject requests and complaints

Requests for data information, change, withdrawal of consent or deletion must be received personally from the Data Subject.

Requests by staff, personnel and interns

Staff, personnel and interns shall have the right to obtain from ICMPD, without charge and at any time, information about their PD stored on/in ICMPD filing systems and a copy of this information by contacting HRM.

[24] For example, PD may be needed for selecting audit targets but the data set may be anonymised once the selection has been completed.
[25] Coordinate with ICT Support to ensure permanent elimination.

Requests by other parties

External parties should send their requests for data information, rectification or deletion from a specific system/document to their ICMPD focal point or in case of general requests to data.protection@icmpd.org. The ODP, based on due assurance that the request has come from the Data Subject or their legal representative, will follow up the request in cooperation with the DFPs.

Any employee who receives a PD-related request from an external party:

- acknowledges receipt of the request within 72 hours, informing the requestor that his or her request was forwarded to the appropriate authority within the organisation, without however making any commitment to the requestor other than that they will receive a response within four weeks; and
- forwards the request without delay to data.protection@icmpd.org

The ODP analyses the request, if necessary requesting documentation from the requestor to prove his or her identity, and channels it to the DFP(s) as appropriate. The DFP(s) responsible review their databases and respond to the ODP's request within five working days. If the request cannot be fully complied with, the DFP must inform the ODP within the same timeframe. The ODP informs the requestor about the action taken within a maximum of four weeks, copying the employee who received the initial request. Should it be unfeasible to comply with the request, the requestor must equally be informed within the same time period.

Before any request for deletion is processed, it must be ensured that no legal requirements are affected by such deletion. Data for which any request other than deletion is received must not be deleted within four months of the request received to allow for due investigation, if necessary.

Complaints

Any complaints related to PD processing, be they from internal or external sources, must be addressed to data.protection@icmpd.org. The ODP will ensure due recording and follow-up.

Breaches

Any perceived risks to data security or malfunctioning related to virtual or physical spaces which may result in a PD breach, must be reported to data.protection@icmpd.org, copying ICT Support or the person responsible for office management in the respective location as applicable, without delay.

Any (suspected) significant PD breach which may result in harm to any individual must be referred to the ODP, copying ICT Support and the manager responsible without any delay. The ODP calls a crisis meeting with the HoICT and other DFPs involved within 24 hours of gaining knowledge of the breach. ICT Support acts as an advisor for technical coordination with external parties, if necessary. [26] The ODP will produce a report for the Dir ROM for a decision within 48 hours of the data security breach on the steps to be taken. Without undue delay, the ODP then informs all parties concerned and monitors follow-up of the steps decided. A logging list is kept on Data Protection Space for this purpose.

Any theft or loss[27] of mobile equipment is to be handled as a potential data breach. The equipment will be remotely wiped by ICT Support.

[26] Where third party providers are involved, ICT Support will contact them without delay as input to the meeting.
[27] Equipment not retrieved within 24 hours.

Audits and investigations

Data protection audits

Dedicated audits will be carried out at least once a year based on a risk assessment and upon the identification of a risk in case of urgency, including spot checks without advance notification and monitoring missions in the field.

Investigations

ICMPD may use payroll and other PD for the prevention and detection of fraud and misconduct, and in investigations related thereto. Staff members' and personnel emails, logs of websites visited, logs of telephone calls and access logs may be checked to ensure security of systems or to investigate misconduct. Investigation proceedings shall be confidential and restricted to those employees involved in the investigation. PD will only be disclosed to third parties in accordance with the contract, ICMPD regulations and as required by law. The information disclosed shall be accessible to the employee(s) concerned.

Relevant references

Regulations, Policies and Rules

- *Staff Regulations*
- *Code of Conduct*
- *Document Management Policy*
- *ICT Policy*
- *ICMPDnet Work Instructions*
- *Budgeting Guidelines*
- *Internal Audits*

Records

- *Organisational Overview Personal Data Processing*
- *ICMPD Website Privacy Notice*

Instructions

- *How-to Tenfold*

Templates and Samples

- *Data Processor Contract Template*
- *Non-disclosure Undertaking Template*
- *Research/Interview Authorisation Form Template*
- *Publication Authorisation Form Template*
- *Database General Terms and Conditions Sample*
- *Sample Data Protection Declaration for Projects*
- *Project Overview Personal Data Processing Template*
- *Request for Disclosure*