



**POLICY ON
PERSONALLY IDENTIFIABLE INFORMATION PROTECTION
(PIIP)**

Document Classification:	Unclassified
Document Ref.:	
Issue:	3.1
Date:	11/02/2019
Document Author:	Gregor Wettberg
Document Owner:	Stefan Eberle
Document Status:	Final

Revision History

Issue	Revision Author	Summary of changes	Date
3.1	PIIPO, Head of Legal, Comments from PII Supervisor	Clarifications re basis for processing data and the scope of consent based processing; Addition of instructions re filing a complaint; Clarifications re right to deletion; Removal of “right to portability” due to lack of relevance for ECMWF; Rectifications of clerical errors	08.02.2019

Approval

Issue	Internal body/post	Date
2.9	Director of Administration	01.11.2018
2.9	Directors, Director-General	01.11.2018
3.0	Council (for information)	04.12.2018
3.1	Director-General	11.02.2019

Distribution

Issue	Department	Date
2.4	External Consultant	
2.4	Information Security Governance Board – for information	
2.4	Head of Staff Committee – for information	
2.5	Director of Administration – for approval	
2.6	Directors – for approval	
2.7	External Consultant	
2.8	Directors - for information	
2.9	Director-General - for implementation	
3	All internal departments – after approval	

3.1	Directors	11.02.2019
3.1	Director-General	11.02.2019

Related Documents

Document Title	Link/Address
Information Security Policy	R:\enterprise\InfoSec\Documents\Policies\FINAL

Contents
1. Introduction	1
2. Glossary	1
3. PII Protection Principles	2
4. Governance.....	2
5. PII Protection Officer.....	3
6. Responsibilities of Staff for Processing of PII	4
7. Responsibilities of Staff as PII Subjects.....	6
8. Rights of PII Subjects	6
9. The PII Supervisor	8
10. The PII Protection Committee	9
11. Practical Application	10

PII PROTECTION POLICY

1. Introduction

ECMWF deals with many individuals, such as members of staff, candidates to become members of staff, visiting scientists and representatives of its customers, collaborators, suppliers (including organisations, which bid to become a supplier), member states and funding bodies. ECMWF needs to store and use certain information about those individuals in order to communicate with them and carry out its business effectively.

At the same time, ECMWF is committed to protecting the rights of individuals to privacy, in line with EU Personal Data Protection Principles.

2. Glossary

In order to understand the EU Personal Data Protection Principles and this Policy on the Protection of PII (“the Policy”), a short glossary of terms is provided:

Personally Identifiable Information (PII):	means any information relating to a natural person, who can be identified from or by way of that information;
PII Subject:	means a natural person to whom PII relates;
Processing:	means any operation or set of operations which is performed upon PII, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;
Staff:	means all ECMWF staff members (Article 1(1) of the Staff Regulations), contractors including temporary agents, and visiting scientists.

3. PII Protection Principles

- a) ECMWF shall process PII for specified, proportionate and lawful purposes. ECMWF is entitled to process PII if it is necessary for any of the following purposes:
 - i. to perform a contract with the PII Subject (e.g. an employment contract) or a contract with a party, which the PII Subject represents (e.g. a user licence); or
 - ii. to achieve the purposes, objectives and activities laid down in the Convention; or
 - iii. to comply with decisions of the Council or policies and procedures enacted by the Director-General; or
 - iv. to protect its legitimate interests; or
 - v. to ensure its day-to-day operations.
- b) ECMWF shall inform PII Subjects about processing their PII, unless the circumstances are exceptional e.g. to assist the legitimate authorities to investigate allegations of fraud, crime or terrorism;
- c) In the absence of a purpose as contained in Section 3 a), ECMWF shall only obtain and process PII with the PII Subject's explicit, unambiguous consent;
- d) If PII is processed by consent only, ECMWF shall process PII for the purposes which have been made known to the PII Subject (Known Purposes) and for no other purposes, unless the circumstances are exceptional (see above);
- e) PII shall be adequate, relevant and limited to what is necessary for the Known Purposes;
- f) PII shall not be kept for longer than is necessary;
- g) PII shall be accurate and where necessary kept up to date;
- h) PII shall be kept safe from unauthorised access, accidental loss, damage or destruction;
- i) PII shall not be transferred outside the European Economic Area, or to another international organisation, unless ECMWF has determined that adequate safeguards are in place to protect the fundamental rights and freedoms of individuals over the processing of their PII.

4. Governance

ECMWF has developed this Policy to establish ECMWF's PII protection governance. The Policy will also define the roles and responsibilities of a PII Protection Officer (Section 5); a PII Supervisor (Section 9); and a PII Protection Committee (Section 10). This Policy has been approved by the Director-General at ECMWF and is one of the policies that support the ECMWF strategy.

5. PII Protection Officer

- a) The Director-General designates ECMWF staff members as PII Protection Officer and his/her deputy. They may only be relieved of his/her position as PII Protection Officer and deputy by decision of the Director General. The PII Protection Officer can designate assistants.
- b) The deputy PII Protection Officer shall perform, on an exceptional basis and under the same conditions as the PII Protection Officer, the same duties as those of the PII Protection Officer when the latter should be prevented. The following rules apply to the deputy *mutatis mutandis*.
- c) The PII Protection Officer is responsible for discharging the duties assigned to him/her under this Policy and to perform any other responsibilities assigned to him/her by the Director General.
- d) The PII Protection Officer monitors ECMWF's compliance with this Policy and acts as a point of communication for anyone who wishes to enquire or complain about how PII is processed by ECMWF. The PII Protection Officer shall investigate complaints and issue a written decision. If a PII Subject writes to ECMWF about one of the rights listed below and ECMWF can verify the identity of the PII Subject, then ECMWF shall respond without undue delay and, where practical, within one month of receiving the PII Subject's written communication.
- e) The PII Protection Officer shall also:
 - i. Maintain a list of ECMWF's primary purposes for processing PII, in line with ECMWF's activities;
 - ii. Maintain appropriate records of ECMWF's PII protection activities, including a register of third parties who receive PII from ECMWF;
 - iii. Initiate appropriate information, education and training about this Policy and ECMWF's PII protection framework;
 - iv. Assist relevant staff to undertake a PII protection impact assessment in respect of any processing, which is likely to result in a high risk to the rights or freedoms of the PII Subjects;
 - v. Assist with management of the rights and complaints of PII Subjects (see below in Section 8);
 - vi. Cooperate with the PII Supervisor as requested;
 - vii. Chair the PII Protection Committee and report annually to the Committee about his/her activities;
 - viii. Manage notifications of any breaches of this Policy;
 - ix. Manage the communications and relations, which are required to demonstrate the adequacy of this Policy, so that ECMWF can continue to process PII, in line with its activities.
- f) The PII Protection Officer may perform other functions at ECMWF, unless these functions interfere with his/her obligations under this Policy.
- g) The PII Protection Officer is responsible for discharging the duties assigned to him/her under this Policy. In the discharge of his/her duties, the PII Protection Officer
 - i. is bound to confidentiality related to PII s/he became aware of in performing his/her duties. Such obligation shall continue indefinitely after the termination of the appointment; and

- ii. shall act independently in his/her capacity as PII Protection Officer and not be subjected to instructions from ECMWF's hierarchy save that of the Director General provided such instructions are lawful.

6. Responsibilities of Staff for Processing of PII

a) *General*

- Staff who plan and design activities involving the processing of PII shall do so in such a way as to enable this Policy and the PII protection principles, listed in Section 3 above to be followed. The same staff shall make and store a written record of justification for any derogation from this norm.
- Staff who process PII for ECMWF shall comply with this Policy.
- Staff who engage third parties (including suppliers and collaborators) to process PII on behalf of ECMWF shall negotiate terms so that the PII is processed in accordance with the PII Protection Principles set out in Section 3 or to an equivalent standard.
- Staff shall avail themselves of available information, education and training about this Policy and ECMWF's PII protection activities;
- Staff shall request help from their line manager or the PII Protection Officer if they are unsure about any aspect of this Policy or how to comply with it.
- Staff shall bear in mind that PII is a form of information asset and that this Policy is supported by ECMWF's wider Information Security Policy.

b) *Storage of PII*

- If and when ECMWF introduces an information classification scheme, all documents containing PII shall be marked and treated according to such scheme.

When PII is stored on paper:

- It shall be kept in a secure place where unauthorised people cannot access it. (This may require particular consideration when paper documents are being taken away from ECMWF premises).
- Paper copies and printouts containing PII shall be shredded or disposed of securely when no longer required.

When PII is stored electronically:

- It shall be protected from unauthorised access, accidental deletion and malicious hacking attempts.
- If the electronic storage device is portable (e.g. a laptop/hard drive, mobile phone, memory stick or media disk), extra precautions shall be taken to preserve the integrity and confidentiality of the PII stored on it. (If in doubt about appropriate extra precautions, the PII Protection Officer shall be consulted.)

c) *Working with PII*

- Staff shall only work with/process PII for legitimate purposes as stated above in Section 3. If in doubt, the PII Protection Officer shall be consulted.

d) *Accuracy and retention of PII*

- It is the responsibility of all staff, who work with PII, to take reasonable steps to keep it as accurate and up-to-date as possible and to delete or dispose of it when it is no longer needed.
- PII shall be held in as few places as necessary. Staff shall not create any unnecessary, additional copies.
- ECMWF shall make it relatively easy for PII Subjects to notify changes (e.g. via the ECMWF website) so that ECMWF can keep the PII, which it holds about them up-to-date.
- PII shall be deleted or securely disposed of when it is no longer required for the purposes for which it was acquired (a pre-agreed retention period). Retention Periods shall be set by agreement with the PII Protection Officer and published.

e) *Access to and Disclosure of PII*

- PII held by ECMWF shall only be accessible to those who need it for their work.
- Staff that is accessing PII in the exercise of their work assignments may not access or process such PII for other purposes.
- Staff shall keep all PII secure, by taking sensible precautions, in line with ECMWF's Information Security Policy.
- Staff shall take precautions, so that when PII is transmitted in any form, it reaches only the correct recipient and the recipient preserves its integrity and confidentiality.
- PII shall not be disclosed to unauthorised people, either within ECMWF or externally. (Where appropriate, PII shall be redacted from copies of those documents, which must be shared for work purposes.)
- PII shall not be shared informally (e.g. mentioned or discussed in casual conversation or revealed in response to an apparently innocent enquiry);
- Before releasing PII to a third party who claims to have the PII Subject's consent, the PII Protection Officer, who will check to verify the existence of consent.

f) *When a PII Subject Makes Contact about his/her PII*

- Staff shall be familiar with the rights of PII Subjects (see below in Section 8);
- Staff shall deal directly with PII Subjects, in the normal course of ECMWF business (e.g. acquisition of consent for processing, an update or correction of PII or an informal subject access request);
- When a PII Subject submits something outside the normal course of ECMWF business (e.g. a withdrawal of consent for processing, a formal subject access request or a complaint), Staff shall consult with the PII Protection Officer, who shall either advise about or manage an appropriate response.

g) *In Case of Breach¹*

- If any Staff suspects or knows that this Policy or the principles set out above have not been or are not being followed, for instance in the case of loss, theft, misuse or unauthorised disclosure of PII, they shall report the matter by the fastest possible means to the Service Desk or directly in confidence to the PII Protection Officer. Thereafter, the circumstances of an incident will be discussed/investigated on a strictly need-to-know basis.
- Relevant staff shall assist the PII Protection Officer to assess whether the apparent breach is likely to result in a risk to the rights and freedoms of PII Subjects.
- If so, the relevant staff shall assist the PII Protection Officer to notify the PII Subjects, whose rights and freedoms may be at risk, as soon as possible.
- In any event, the relevant Staff shall assist the PII Protection Officer to rectify the breach and to amend the relevant activities, so that the breach does not reoccur.

7. Responsibilities of Staff as PII Subjects

Staff who provide PII to ECMWF, about themselves shall provide it in a complete and accurate form. Over the course of their employment, they shall assist ECMWF to keep the same PII complete, accurate and up to date.

8. Rights of PII Subjects

a) *To know*

- In most cases, ECMWF shall let PII Subjects know what PII will be processed and for what purposes at the time when they first start to deal with ECMWF or when they enter into a contract with ECMWF. It shall also provide them with the contact details of the PII Protection Officer. To this end, ECMWF shall publish privacy statements as specified in sub-section c) below.

¹ This part of the Policy is in line with ECMWF's applicable procedures on the management of *information security incidents*.

- ECMWF shall let PII Subjects know if and when it acquires any of their PII from a source other than the PII Subject themselves.

b) To give and to withdraw their consent

- In some situations, only consent will serve as legitimate basis for the processing of PII by ECMWF. Details can be found in Section 3. If that is indeed the case, ECMWF shall acquire an explicit, unambiguous, positive indication of consent of each PII Subject to its processing of their PII.
- If PII is being processed on the basis of consent, ECMWF shall keep a record of each individual indication of consent and inform PII Subjects how to withdraw consent effectively. Withdrawing consent must not require substantially different means than are employed to give consent.
- If PII is being processed on the basis of consent, ECMWF shall enable the relevant PII Subjects to withdraw their consent at any time and, in that case, ECMWF shall cease the processing of the relevant PII. However, even if consent is withdrawn, another legitimate reason for the processing of PII may have become available or may have been available in parallel. If so, the fact that consent was requested nevertheless will not invalidate such alternative reasons for processing.

c) To enquire, object or require the fulfilment of their rights

- All PII Subjects have the right to enquire or object to the processing of their PII and to require ECMWF to fulfil one or more of their rights under this Policy. In response, ECMWF can demonstrate that legitimate grounds for processing prevail or, otherwise no longer process such PII.
- Current and former Staff, including pensioners, may make enquiries about their own PII directly to HR. All other PII Subjects may contact the PII Protection Officer about their own PII.
- Any other PII related enquiries received elsewhere in ECMWF shall be referred to the PII Protection Officer as soon as they are received.
- ECMWF shall publish contact details for the PII Protection Officer, within the privacy statement, on ECMWF's staff intranet and external website, to assist all PII Subjects to submit and resolve such enquiries, complaints and requirements. The privacy statement will take immediate effect following its publication.

d) To make a formal subject access request

- All PII Subjects may make a written request for a copy of the PII, which ECMWF holds about them. This right does not extend to PII of which the PII Subject is not already aware and if

to PII the release of which would unduly infringe rights of other PII subjects or violate obligations of ECMWF. The method for making such a formal subject access request shall be publicised in ECMWF's privacy statements.

- The PII Protection Officer shall always verify the identity of anyone making a formal subject access request, before disclosing any PII.
- Only in exceptional circumstances, e.g. for the prevention or detection of crime or for the protection of the PII Subject, will ECMWF withhold certain PII from a PII Subject.

e) To rectification and erasure

- All PII Subjects have the right to ask for their PII to be corrected, completed or brought up-to-date.
- A PII Subject may ask for all or part of their PII to be erased if that information or part is no longer necessary for the processing in line with Section 3 above, has no relevant historical value, or if consent is being relied upon for processing and the PII Subject has withdrawn consent for the relevant form of processing. For the avoidance of doubt, PII will not be deleted from back-ups. However, if a back-up is played back into an operational system, ECMWF will put all reasonable effort into updating or erasing PII which have changed since the date of the backup which has been played back.

f) To object to automated decision making, including profiling

- An "automated decision" is a decision based solely on automated processing.
- "Profiling" is automated processing, for the purpose of evaluating certain personal aspects about a PII Subject, e.g. their economic circumstances, health, personal preferences, behaviour, location or movements.
- All PII subjects have the right to object to automated decision making, including profiling.
- ECMWF shall notify PII Subjects in advance, before undertaking or making arrangements for any sort of automated decision making or profiling. This shall be confirmed in ECMWF's privacy statements.

9. The PII Supervisor

- a) A PII Supervisor as well as a deputy PII Supervisor are appointed by the ECMWF Council upon a proposal from the Director-General. The deputy shall perform, on an exceptional basis and under the same conditions as the PII Supervisor, the same duties as those of the PII Supervisor when the latter should be prevented. The following rules apply to the deputy *mutatis mutandis*.
- b) The PII Supervisor has jurisdiction to hear and investigate complaints by any PII Subject against decisions by the PII Protection Officer. The PII Supervisor may replace a decision with an alternative decision of his/her own, if the decision of the PII Protection Officer affects the PII Subject's rights and if the decision is contrary to the PII Protection Policy.

- Decisions by the PII Supervisor are final. The PII Supervisor can also make additional recommendations to the PII Protection Committee.
- c) The PII Supervisor shall be an independent external expert with demonstrable data protection expertise, particularly with regard to data protection legislation of the European Union. S/he shall be a national of an ECMWF Member State or Co-operating State and is appointed for three years. Re-appointment is possible. The PII Supervisor is competent to hear complaints after the expiry of his/her term, if these complaints were lodged during that term.
 - d) The PII Supervisor shall refrain from any act or activity which is incompatible with his/her functions and is required to excuse him/herself in cases of actual or perceived conflicts of interest. The PII Supervisor is subject to the obligation of confidentiality. S/he may adopt further rules applicable to its own procedure.
 - e) Complaints are free of charge for the PII Subject. The PII Supervisor can request the Director-General to reimburse the PII Subjects for reasonable costs incurred in conjunction with a complaint. The PII Supervisor receives a fixed remuneration for each complaint and reimbursement for expenses. The remuneration shall be determined by the Council on proposal by the Director-General and reviewed at least every three years. Expenses shall consist of travel expenses and a daily subsistence allowance, both calculated on the basis of the provisions of Article 23 and Annex III of the Staff Regulations.
 - f) Complaints have to be lodged in writing within 30 days of receipt of the written decision by the PII Protection Officer. The PII Supervisor may, in exceptional cases, beyond the PII Subject's reasonable control, admit complaints lodged after 30 days. Vexatious complaints are inadmissible.
 - g) The complaint can be lodged by email or registered mail to addresses made publicly available by the Director-General. It shall substantiate the reasons for the complaint and outline the requested redress. There are no additional formal requirements for the complaint.
 - h) In order for the PII Supervisor to investigate a complaint, the PII Protection Officer has an obligation to co-operate with the PII Supervisor and to supply him/her with all requested information, unless the production of such information is grossly disproportionate to the nature and gravity of the complaint. The PII Protection Officer and the PII Subject shall be heard in the course of an investigation.
 - i) Complaints should be decided within 60 days, unless decided otherwise by the PII Supervisor.
 - j) Article 8(3) to (6) of Annex VII to the Staff Regulations apply mutatis mutandis.

10. The PII Protection Committee

- a) The PII Protection Committee is responsible for providing to the Director-General reports concerning the overall functioning of ECMWF's PII protection framework and making recommendations for improvements. The PII Protection Committee will take recommendations by the PII Supervisor into account in doing so.
- b) The PII Protection Committee is convened and chaired by the PII Protection Officer at least once every year and otherwise, on an ad-hoc basis. Meetings are minuted. The PII Protection Committee may enact further rules of procedure.

- c) The PII Protection Committee is composed of the PII Protections Officer, his/her deputy, a member of the ECMWF Legal Services and the ECMWF Information Security Officer. The PII Protection Committee can invite guests, particularly representatives from each Department, as designated by the respective Director.
- d) Decisions are taken by simple majority. In case of a draw, the vote of the PII Protection Officer is decisive.
- e) All PII Protection Committee members, ad-hoc or permanent, are bound to an obligation of confidentiality in performing their duties, particularly with regard to PII they are exposed to in performing their duties. Such obligation shall continue indefinitely after the termination of their PII Protection Committee membership.

11. Practical Application

Wherever possible, the practical application of this Policy shall support and not hinder the work of ECMWF.

Reading, 11 February 2019

The Director-General