



NATO STABILITY POLICING CENTRE OF EXCELLENCE

AND

NATO SECURITY FORCE ASSISTANCE CENTRE OF EXCELLENCE

PERSONAL DATA PROTECTION POLICY DIRECTIVE

SUMMARY

1. INTRODUCTION

2. PURPOSE

3. APPLICABILITY

4. DEFINITIONS

5. GENERAL PRINCIPLES

6. RESPONSIBILITIES

7. PERSONAL DATA PROCESSING

8. DOCUMENTATION AND RECORDS

9. DATA PROTECTION AND RISK MANAGEMENT

10. SHARING AND TRANSFER OF PERSONAL DATA

11. DATA SUBJECT RIGHTS

12. PERSONAL DATA BREACHES

13. COMPLIANCE, MONITORING AND REVIEW

14. FINAL PROVISIONS

REFERENCES

a. NATO Personal Data Protection Framework Policy.
b. C-M(2007)0118, The NATO Information Management Policy, 11 December 2007.
c. C-M(2002)49-REV1, Security Within the North Atlantic Treaty Organization (NATO), 20 November 2020.
d. C-M(2002)60, The Management of Non-Classified NATO Information, 11 July 2002.
e. AC/35-D/2020 (INV), Directive on the Protection of Communication and Information Systems (CIS) Handling Non-Classified NATO Information, 6 November 2019.
f. C-M(2015)0041-REV2 Annex 13, Data Management Policy, 14 December 2018.
g. PO(2021)0360, Data Exploitation Framework Policy, 12 October 2021.
h. C-M(2011)0043, The NATO Records Policy, 28 June 2011.
i. C-M(2008)0116-REV1 (INV), Public Disclosure of NATO Information, 13 February 2017.
j. C-M(2009)0021, Policy on Retention and Disposition of NATO Information, 6 February 2009.
k. EU General Data Protection Regulation (GDPR) 2016/679.
l. Italian Legislative Decree 30 June 2003 n. 196 and n. 101 dated 10 August 2018 which adapts the Code regarding the protection of personal data "Legislative Decree dated 30 June 2003, n. 196" to the provisions of the Regulation (UE) 2016/679.
m. Other applicable NATO directives, policies, administrative instructions, and NSPCOE NSFACOE internal directives governing information security, records management, information management, cybersecurity, human resources, procurement, and risk management.
n. Memorandum of Understanding (MOU) concerning the establishment, administration and operation of the NATO Security Force Assistance Centre of Excellence, signed 13 December 2017.
o. MOU concerning the establishment, administration and operation of the NATO Stability Policing, signed 15 April 2015.

1. INTRODUCTION

To fully understand the very peculiar personal data policy applicable to the NATO Stability Policing Centre of Excellence (NSPCOE) and the NATO Security Force Assistance COE (NSFACOE), it is appropriate to provide some preliminary information regarding their legal status.
These Centres are bodies that support NATO. The legal status of these international entities is based on Memoranda of Understanding (MoU) between the participating nations.
In particular, they:

- hold the status of a NATO international military headquarters (pursuant to Article 14 of the "*Protocol on the Status of International Military Headquarters set up pursuant to the North Atlantic Treaty*" of 28 August 1952, known as the Paris Protocol). The Centres and their personnel enjoy specific status, privileges and immunities;
- interact with the:
  . Host Nation (Italy) in which NATO data protection policy, EU General Data Protection Regulation (GDPR) and its Italian implementations apply.
  . NATO European Union (EU) countries in which NATO data protection policy and EU General Data Protection Regulation (GDPR) apply;
  . NATO non-EU countries in which NATO data protection policy apply;
  . other Countries non-member of the Alliance, International Organizations, private company, university, other different actors, individuals etc. in which the data protection legal framework on a case-by case basis apply.

2. PURPOSE

The NATO Personal Data Protection Framework Policy (Reference A), foresees each NATO body shall develop and maintain a subordinate directive, tailored to their organizational requirements, to implement the Policy.
According to that the Personal Data Protection Directive (PDPD) of the NSPCOE and NSFACOE establish a Personal Data Protection Programme and implement the NATO Personal Data Protection Framework Policy within the Centres. The document prescribes the governance, responsibilities, organizational measures, and operational requirements necessary to ensure that personal data are processed lawfully, fairly, transparently, securely, and in a manner that protects the rights and legitimate interests of data subjects while supporting the effective execution of the Centres' mission.
Under this framework the Centres have to:

- minimize data collection and gather only the specific personal information required for the purpose of the activity.
- maintain High Standards to ensure data processing aligns with the highest international standards while safeguarding sensitive information;
- handle data lifecycle, managing data securely from initial processing to eventual disposal according to the NATO Policy.

The Directive establishes the responsibilities, procedures, and oversight mechanisms necessary to ensure accountability for personal data processing activities, protect the

confidentiality, integrity, availability, and resilience of personal data, facilitate the lawful sharing and transfer of personal data, ensure compliance with the rights of data subjects, support the effective management of personal data breaches, and promote a culture of personal data protection through governance, awareness, training, monitoring, and continual improvement.
Nothing in this Directive supersedes the provisions of higher-level NATO policies, directives, or administrative instructions indicated in the references.

3. APPLICABILITY

This Directive applies to all military personnel, civilian staff, national experts, secondees, contractors, consultants, interns, temporary personnel, and any other individuals processing personal data on behalf of the Centres, irrespective of their employment status or contractual relationship with them. Compliance with this Directive is a condition for the processing of personal data within the Centres.
It applies to the processing of personal data and storage of personal data by automated and not-automated means.
This Directive does not apply to personal data processed exclusively for intelligence or counter-intelligence purposes. Where additional or more restrictive requirements apply, those requirements shall prevail on the higher-level NATO policies governing security, information management, records management, cybersecurity, or other specialized functional areas.

4. DEFINITIONS

Unless otherwise specified in this Directive, terms and definitions shall have the meanings assigned to them in the NATO Personal Data Protection Framework Policy. Where a conflict exists between a definition contained in this Directive and one contained in the NATO Personal Data Protection Framework Policy, the latter shall prevail. For the purposes of this Directive, the following definitions shall apply:

a. **Anonymization** – The irreversible processing of personal data in such a manner that the data subject is no longer identifiable. Personal data which has been anonymized is no longer personal data. See also pseudonymization.
b. **Centres** – The NATO Stability Policing Centre of Excellence (NSPCOE) and the NATO Security Force Assistance Centre of Excellence (NSFACOE).
c. **Consent** - any freely given and unambiguous permission of the data subject to process his/her Personal Data.
d. **Data subject** – Any identified or identifiable individual whose personal data is processed by a NATO body, for instance NATO International Civilians and Military assigned to NATO, their family members, members of national delegations, visitors to NATO bodies, registered users of NATO web portals and so on.
e. **Director** – The Director of the NSPCOE and NSFACOE, who has overall responsibility and accountability for implementing this Directive and ensuring that personal data processed by or on behalf of the respective Centre are protected in accordance with applicable NATO policies.

f. **Head of Organizational Element** – The head of a Branch, Section, or other organizational element responsible for ensuring that personal data processing activities within his or her area of responsibility comply with this Directive.
g. **Health Data** - personal Data related to the physical or mental health of a person.
h. **Minimization** – Collecting the minimal amount of personal data required to achieve the specified purpose of processing. Collecting the minimal amount of personal data required to achieve the specified purpose of processing.
i. **Need-to-Know** – The principle whereby access to personal data is granted only to individuals whose official duties require such access to perform authorized functions.
j. **Personal data** – Any information that relates to an identified or identifiable living individual. Personal data includes information that combined can lead to the identification of a particular person (e.g. name, surname, e-mail address, telephone number, other contact information, date of birth, address, nationality, ID numbers and validity dates, copies of any official documents necessary (e.g. official national orders of being posted to NSPCOE and NSFACOE, security clearances, copies of ID etc.).
k. **Personal data breach** – A compromise of security that leads to unauthorized disclosure, alteration or destruction of personal data. A significant compromise shall be understood as one posing a high risk to the rights of the data subject.
l. **Personal Data Protection Impact Assessment (PDPIA)** – A documented assessment conducted to identify, evaluate, and mitigate risks arising from the processing of personal data and to determine the measures necessary to ensure compliance with this Directive and the NATO Personal Data Protection Framework Policy.
m. **Personal Data Protection Programme** – The governance framework established by the Centre to implement the NATO Personal Data Protection Framework Policy through documented responsibilities, operational procedures, technical and organizational measures, monitoring, training, and continual improvement.
n. **Pseudonymization** – Processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information. The additional information is kept separately and subject to technical and organizational measures to ensure non-attribution to an identified or identifiable individual. See also anonymization.
o. **Recipient** - a natural or legal person, public authority, agency or another body, to which the Personal Data is disclosed.
p. **Record of Processing Activities (ROPA)** – The official record maintained by the Centre documenting personal data processing activities, including their purposes, legal basis, categories of personal data, categories of data subjects, recipients, retention periods, and applicable technical and organizational safeguards.
q. **Responsibility-to-Share** – The principle whereby personal data may be shared within NATO when necessary to support authorized activities, provided that such

sharing complies with the NATO Personal Data Protection Framework Policy, this Directive, and other applicable NATO policies.

r. **Sharing** (of personal data) – An act that makes a NATO body's personal data accessible to another NATO body or other NATO related entities (e.g. MOU organization) that abide by this Policy.
s. **Special categories of personal data** – Personal data compromise of which would reasonably be expected to be exceptionally detrimental to the data subject. Special categories of personal data include but is not limited to: racial origin; political or religious beliefs; physical or mental health; biometric data; sexual life; criminal convictions or the alleged commission of an offence; trade union membership.
t. **Third Party** - a natural or legal person, public authority, agency or body.
u. **Transfer** (of personal data) – Any act that makes NATO personal data accessible to 3rd parties that are not NATO bodies and do not abide by this policy.

5. GENERAL PRINCIPLES

NSPCOE and NSFACOE shall only process personal data (collect, store and utilize) as necessary for the fulfilment of its functions.
Data will be gathered, processed and accessible only on a need-to-know basis by relevant NSPCOE and NSFACOE personnel.
The gathered personal data will not be shared with any third parties, unless required to fulfil official NSPCOE and NSFACOE functions or when required by law.
The Centres shall implement a risk-based approach to the protection of personal data.
Personal data protection shall be integrated into the planning, design, acquisition, development, operation, maintenance, modification, and retirement of business processes, services, and Communication and Information Systems (CIS).
The Centres shall ensure that personal data remain accurate and, where appropriate, up to date, are retained only for as long as necessary, and are protected against unauthorized or unlawful access, disclosure, alteration, loss, or destruction through appropriate technical and organizational measures.
Accountability for the protection of personal data shall form an integral part of the Centres governance framework. All organizational elements processing personal data shall be able to demonstrate that such processing is supported through appropriate documentation, records, oversight activities, and periodic reviews.
Personal data protection shall be considered a continuous management responsibility. The Centres shall periodically review its Personal Data Protection procedures, taking into account changes in operational requirements, organizational structure, information systems, and lessons identified, in order to ensure the continued effectiveness.

6. RESPONSIBILITIES

a. Management.
The protection of personal data is a management responsibility that shall be exercised at every level of the Centres. Responsibility for ensuring compliance with this Directive rests with Heads of Organizational Elements and all personnel processing personal data within the scope of their official duties.

b. Director.
The Director is accountable for the implementation and oversight of the Centres' Personal Data Protection Directive and shall ensure that appropriate governance arrangements, organizational measures, and resources are established and maintained. The Director shall appoint a Personal Data Protection Officer (PDPO).

c. Personal Data Protection Officer.
The Personal Data Protection Officer shall advise the Director and the organizational elements on the application of this Directive and the NATO Personal Data Protection Framework Policy, monitor compliance with personal data protection requirements, maintain the records and registers prescribed by this Directive, coordinate the management of data subject requests and personal data breaches, provide advice on Personal Data Protection Impact Assessments, support awareness and training activities, and prepare the annual review of the Centres' Personal Data Protection Directive and procedures.

d. Heads of Organizational Elements
Heads of Organizational Elements are responsible for ensuring that personal data processing activities within their areas of responsibility comply with this Directive. They shall ensure that processing activities are identified and documented, that appropriate technical and organizational safeguards are implemented, that personal data are processed only for authorized purposes, and that the PDPO is informed of any new activity, significant modification, or incident that may affect the protection of personal data.

e. Collective.
All personnel shall exercise due care in protecting personal data from unauthorized access, disclosure, alteration, loss, or destruction and shall immediately report any suspected or confirmed personal data breach to PDPO.

7. PERSONAL DATA PROCESSING

It refers to any activity or set of activity which are performed on Personal Data, whether by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Personal data shall be processed only where such processing is necessary to support the functions and activities of the Centres. Before commencing any processing activity, the responsible Organizational Element shall identify and document the purpose of the processing, the categories of personal data involved, the categories of data subjects concerned, the anticipated recipients of the data, the applicable retention period, and the technical and organizational safeguards. Processing activities shall not commence until these elements have been identified and appropriately documented.

Personal data shall be collected directly from the data subjects whenever practicable and shall be limited to the minimum information necessary to achieve the specified purpose. Personal data shall not subsequently be processed for purposes incompatible with those for which they were originally collected unless such processing is authorized under applicable NATO policies.
Throughout the processing lifecycle, the responsible Organizational Element shall take reasonable measures to ensure that personal data remain accurate, complete, and, where appropriate, up to date. Where inaccuracies are identified, appropriate corrective measures shall be taken without undue delay. Personal data that are no longer required, have become obsolete, or are demonstrated to be inaccurate shall be corrected, archived, or disposed of in accordance with applicable NATO records management and information management policies.
Access to personal data shall be restricted to personnel whose duties require such access and shall be granted in accordance with the principles of need-to-know and responsibility-to-share. Appropriate technical and organizational measures shall be implemented to protect personal data against accidental or destruction, loss, alteration, unauthorized disclosure, or unauthorized access throughout the processing lifecycle. Such measures shall be proportionate to the sensitivity of the personal data, the nature of the processing activity, and the risks associated with that processing.
Personal data shall be retained only for the period necessary to fulfil the purpose for which they were collected. Upon expiry of the applicable retention period, personal data shall be securely archived or disposed of using methods appropriate to the information classification, storage medium, and applicable NATO policies governing records retention and disposition. Disposal activities shall ensure that personal data cannot be reconstructed or recovered by unauthorized persons.
Organizational Elements shall periodically review their processing activities to verify that the continued processing of personal data remains necessary, and consistent with the purposes originally identified. Where processing activities are significantly modified, involve new categories of personal data, introduce new technologies, or are likely to increase risks to the rights or legitimate interests of data subjects, the responsible Organizational Element shall consult the Personal Data Protection Officer to determine whether additional safeguards or a Personal Data Protection Impact Assessment are required before the modified processing activity is implemented.
Where Processing of Personal Data is based on the Consent, the data subject shall give the Consent before Processing of Personal Data commence.
The Consent should be given in an intelligible and easily accessible form, using clear and plain language. The data subject has the right to revoke his or her Consent at any time. The withdrawal of the Consent shall not affect the lawfulness of the Processing of Personal Data based on the Consent given prior to its withdrawal.

8. DOCUMENTATION AND RECORDS

All personal data, both in hardcopy and electronic form, must be handled securely and on a need-to-know basis.
The Centres shall establish and maintain the documentation necessary to demonstrate compliance with the NATO Personal Data Protection Framework Policy and this Directive. Documentation shall support accountability, facilitate management

oversight, enable internal and external audits, and provide evidence that personal data processing activities are conducted in a lawful, transparent and secure manner.
The Personal Data Protection Officer shall establish, maintain, and periodically review the official records supporting the Centres Personal Data Protection Directive. These records shall be maintained in a manner that ensures their integrity, accuracy, availability, and protection against unauthorized access, alteration, disclosure, or destruction. Organizational Elements shall provide the PDPO with complete, accurate, and timely information necessary to establish and maintain these records.
The documentation shall include, as a minimum, the Personal Data Protection Impact Assessment, the Data Subject Request Register, the Personal Data Breach Register, and any additional documentation required to demonstrate compliance with applicable NATO policies or to support the effective administration of the Centres Personal Data Protection Programme.
Each Organizational Element processing personal data shall ensure that information submitted for inclusion in the records maintained by the PDPO accurately reflects the processing activities performed within its area of responsibility. New processing activities, significant modifications to existing processing activities, changes affecting the legal basis, retention periods, recipients, technical safeguards, or any other material aspect of the processing shall be communicated to the PDPO without undue delay to ensure that the official records remain complete and current.
The PDPO shall periodically review the documentation established under this Directive to verify its completeness, accuracy, and relevance. Where deficiencies are identified, the PDPO shall coordinate with the responsible Organizational Elements to ensure that the necessary corrective actions are implemented.

9. DATA PROTECTION AND RISK MANAGEMENT

Organizational Elements shall ensure that personal data protection requirements are considered from the earliest stages of any initiative.
Where a proposed processing activity involves special categories of personal data, introduces new technologies, significantly modifies existing processing arrangements, or is otherwise likely to present a high risk to the rights or legitimate interests of data subjects, the responsible Organizational Element shall conduct a Personal Data Protection Impact Assessment (PDPIA) before the processing activity is authorized.
The Personal Data Protection Officer shall provide advice throughout the preparation of the PDPIA and shall assess whether the proposed processing activity incorporates appropriate technical and organizational safeguards to ensure compliance with this Directive and the NATO Personal Data Protection Framework Policy. Responsibility for implementing the recommended mitigation measures and for accepting any residual risks shall remain with the responsible Organizational Element.
Where operationally feasible, anonymization, pseudonymization, encryption, role-based access controls, and other privacy-enhancing measures shall be considered to reduce risks to data subjects and to strengthen the overall protection of personal data.

10. SHARING AND TRANSFER OF PERSONAL DATA

Personal data shall be shared only where such sharing is necessary to support the execution of the Centres' mission and activities and where it is consistent with the purpose for which the personal data were originally collected. Before personal data are disclosed, the responsible Organizational Element shall ensure that the recipient has a legitimate need to know, that the sharing is authorized under applicable NATO policies, and that appropriate safeguards are in place to protect the personal data throughout the sharing process.

The sharing of personal data within the Centres or with other NATO bodies shall be limited to the minimum information necessary to achieve the intended purpose and shall be carried out in accordance with the principles of need-to-know, responsibility-to-share, and data minimization. Organizational Elements shall ensure that recipients understand and respect any limitations or conditions governing the further use, disclosure, retention, or disposal of the personal data received.

Transfers of personal data to external organizations, nations, contractors, academic institutions, or other entities outside the NATO organizational framework shall take place only where such transfers are necessary to support authorized activities and where appropriate legal, contractual, administrative, technical, and organizational safeguards have been established. The responsible Organizational Element shall consult the Personal Data Protection Officer before initiating any transfer that presents elevated risks or involves special categories of personal data.

Where personal data are shared with external service providers or other organizations processing personal data on behalf of the Centres, the responsible Organizational Element shall ensure that appropriate contractual or administrative arrangements clearly define the purpose of the processing, the respective responsibilities of the parties, the applicable security requirements, the conditions governing the use and retention of personal data, and the procedures for reporting and managing personal data breaches.

Personal data shall not be shared or transferred where the proposed disclosure is incompatible with the purpose for which the data were collected, is not supported by an appropriate legal basis, or cannot be protected through adequate technical, organizational, contractual, or administrative safeguards.

The Personal Data will not normally be releasable to non-NATO entities, unless there is a proven operational justification approved respectively by the NSPCOE and NSFACOE Director and the following rules are adhered to:

- The Recipient applies the same or higher Personal Data protection standards as prescribed by this Policy;
- The amount of the Personal Data to be transferred must be limited to the Recipient's specific purpose and intended Processing;
- The Data Subject should be informed about the transfer;

- The transfer should not be incompatible with the reasonable expectations of the Data Subject.

11. DATA SUBJECT RIGHTS

Requests concerning the processing of personal data shall be handled fairly, consistently, and without undue delay.
Requests relating to access, rectification, erasure, restriction of processing, objection, or any other right established under the NATO Personal Data Protection Framework Policy shall be submitted to the Personal Data Protection Officer.
Before responding to any request, the PDPO shall ensure that the identity of the requester has been verified by appropriate means. Where additional information is required to confirm the identity of the requester or to clarify the scope of the request, the PDPO may seek further information before processing the request.
Upon receipt of a valid request, the PDPO shall determine its nature, identify the Organizational Elements responsible for the relevant processing activities, and coordinate the preparation of the Centres' response. Organizational Elements shall cooperate fully with the PDPO and provide all relevant information necessary to enable the request to be assessed and resolved.
Where a request cannot be fully satisfied because disclosure would prejudice security, ongoing judicial, administrative or disciplinary proceedings, the rights of other individuals, or any other limitation established by applicable NATO policies, the PDPO shall prepare an appropriate recommendation for decision. The Director shall decide cases involving significant restrictions or where the application of an exemption requires management consideration.
Complaints shall be examined by the PDPO in consultation with the responsible Organizational Elements with the objective of resolving the matter at the lowest appropriate level. Where a complaint cannot be resolved, the matter shall be referred to the Director for decision.
The PDPO shall maintain a Data Subject Request Register recording all requests, complaints, appeals, decisions, and associated actions taken under this Directive. The register shall support accountability, demonstrate compliance, facilitate management oversight, and provide evidence for audit and inspection activities. Information contained in the register shall be protected.

12. PERSONAL DATA BREACHES

a. Reporting.

Every member of the Centres has a responsibility to protect personal data and to report, without undue delay, any actual or suspected personal data breach. A personal data breach shall include any event resulting in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or

unauthorized access to personal data, irrespective of whether the breach results from human error, technical failure, malicious activity, or any other cause.

Upon becoming aware of an actual or suspected personal data breach, the individual discovering the incident shall immediately notify the responsible Organizational Element and shall take all reasonable measures, consistent with operational and security requirements, to contain the incident and prevent further compromise of personal data.

b. Assessment.

The responsible Organizational Element shall conduct an initial assessment of the incident to determine the nature and scope of the breach, the categories of personal data involved, the number and categories of affected data subjects, the systems or services concerned, the likely consequences of the breach, and any immediate containment measures required. The Personal Data Protection Officer shall be informed without undue delay and shall be consulted throughout the assessment process.

c. Incident evaluation.

The PDPO shall evaluate the incident to determine whether it constitutes a personal data breach within the meaning of the NATO Personal Data Protection Framework Policy, assess the potential impact on the rights and legitimate interests of data subjects, advise on the need for additional mitigation measures, and recommend whether notification of affected individuals.

Where a personal data breach involves Communication and Information Systems (CIS), cybersecurity incidents, or physical security matters, the PDPO shall coordinate, as appropriate, with the responsible information security, cybersecurity, physical security, legal, and other competent authorities to ensure that the incident is managed in a coordinated manner and that the respective responsibilities of all stakeholders are fulfilled.

d. Record.

Every personal data breach shall be documented in the Personal Data Breach Register maintained by the PDPO. The record shall include, as a minimum, the date of the incident, a description of the breach, the categories of personal data affected, the results of the assessment, the containment and mitigation measures implemented, any notifications made, the corrective actions adopted, and the date on which the incident was formally closed.

e. Preventive measures.

Following the resolution of a personal data breach, the responsible Organizational Element shall review the circumstances that gave rise to the incident and, in consultation with the PDPO, identify and implement appropriate corrective and preventive measures to reduce the likelihood of recurrence.

The PDPO shall periodically analyse personal data breaches and related trends in order to identify recurring issues, evaluate the effectiveness of existing

safeguards, and recommend improvements. Significant findings shall be included in the annual management review submitted to the Director.

13. COMPLIANCE, MONITORING AND REVIEW

a. Compliance.

Compliance with this Directive shall be monitored continuously as an integral part of the Centres' governance and internal control framework. The objective of compliance monitoring is to verify that personal data are processed in accordance with the NATO Personal Data Protection Framework Policy, this Directive, and other applicable NATO policies, and that appropriate technical, organizational, and administrative measures remain effective throughout the lifecycle of personal data processing activities.

b. Monitoring.

The Personal Data Protection Officer shall monitor the implementation of this Directive by reviewing processing activities, advising Organizational Elements, examining the records, assessing the effectiveness of implemented safeguards, and identifying opportunities for continual improvement. Organizational Elements shall cooperate fully with the PDPO and provide access to the information and documentation necessary to perform these activities.

c. Review.

The Centres shall promote a culture of personal data protection through appropriate awareness, education, and training activities. Personnel whose official duties involve the processing of personal data shall maintain an appropriate level of awareness regarding applicable NATO policies, security requirements, and the obligations established by this Directive. Organizational Elements shall ensure that newly assigned personnel receive appropriate awareness before being granted access to personal data.

An annual management review of the Centres' Personal Data Protection Directive/Programme shall be conducted. The review shall consider the results of compliance monitoring activities, the status of processing activities documented in the Record of Processing Activities, completed Personal Data Protection Impact Assessments, personal data breaches, requests submitted by data subjects, corrective actions, training activities, and any other matters affecting the effective implementation of this Directive. Following completion of the review, the Director shall determine any actions necessary to strengthen the Centres' Personal Data Protection Directive and ensure its continued effectiveness.

Where deficiencies or non-compliance are identified, the responsible Organizational Element shall implement appropriate corrective actions. The PDPO shall monitor the implementation of such actions and verify their

effectiveness. Significant deficiencies, recurring issues, or systemic weaknesses shall be reported to the Director together with recommendations for corrective and preventive measures.

15. FINAL PROVISIONS

The Directors shall ensure the implementation of this Directive and shall provide the organizational, administrative, technical, and financial resources necessary to support the effective operation of the Centres' Personal Data Protection Programme.

All Organizational Elements and personnel of the Centres shall comply with the provisions of this Directive and shall ensure that local procedures, working practices, and operational activities are consistent with its requirements.

The Personal Data Protection Officer (PDPO) shall review this Directive periodically and shall recommend amendments where necessary to reflect changes in applicable NATO policies, the Centres' mission, organizational structure, information systems, operational activities, or lessons identified through compliance monitoring, audits, personal data breaches, and management reviews.

Any amendment affecting the provisions of this Directive or the responsibilities established herein shall be submitted to the NSPCOE and NSFACOE Directors for approval.

The Centres are to be responsible to provide training concerning privacy, data protection and security to its personnel having permanent or regular access to the Personal Data.

Place and date 27TH OCTOBER 2016

Colonel Luigi BRAMATI
Director of the NATO Stability Policing Centre of Excellence

Colonel Massimo MONCADA
Director of the NATO Security Force Assistance Centre of Excellence