NATO PERSONAL DATA PROTECTION FRAMEWORK POLICY

Table of Contents

REFERENCES

A. C-M(2007)0118, The NATO Information Management Policy, 11 December 2007
B. C-M(2002)49-REV1, Security Within the North Atlantic Treaty Organization (NATO), 20 November 2020
C. C-M(2002)60, The Management of Non-Classified NATO Information, 11 July 2002
D. AC/35-D/2020 (INV), Directive on the Protection of Communication and Information Systems (CIS) Handling Non-Classified NATO Information, 6 November 2019
E. C-M(2015)0041-REV2 Annex 13, Data Management Policy, 14 December 2018
F. PO(2021)0360, Data Exploitation Framework Policy, 12 October 2021
G. C-M(2011)0043, The NATO Records Policy, 28 June 2011
H. C-M(2008)0116-REV1 (INV), Public Disclosure of NATO Information, 13 February 2017
I. C-M(2009)0021, Policy on Retention and Disposition of NATO Information, 6 February 2009

INTRODUCTION AND OBJECTIVES

1. NATO is committed to protecting the *personal data*[1] *processed* by the organization to achieve its mission. The NATO Personal Data Protection Framework Policy (the Policy) details the measures required to protect *personal data*. This Policy takes a risk-based and balanced approach, as the application of these measures protects *personal data* while enabling its use for the mission of NATO.

2. The Policy provides an overarching framework policy that promotes a coherent approach within NATO civil and military bodies (*NATO bodies*) and that regulates the *sharing* of *personal data* among *NATO bodies*. Each *NATO body* shall develop and maintain a subordinate directive, tailored to their organizational requirements, to implement the Policy.

3. The Policy and its implementation regulates the *transfer* of *personal data* to *3rd Parties*, with the assurance *personal data* will be protected.

4. The Policy supports the NATO Information Management Policy (reference A), and complements, while maintaining the integrity of, the following policies: the Security within NATO Policy (reference B) for *personal data* within classified documents, the Management of Non-Classified NATO Information Policy (reference C), and Directive on the Protection of CIS Handling Non-Classified NATO Information (reference D) for

[1] Terms that are in Italics have a precise meaning for this Policy. The definitions of the terms may be found in the glossary.

personal data within non-classified documents. The Policy complements the Data Management Policy (reference E) and Data Exploitation Framework Policy (reference F) for *processing* a subset of data - *personal data*.

SCOPE and RESTRICTIONS

5. The Policy shall apply to all *NATO bodies*.
6. This Policy shall apply to all *personal data processed* by *NATO bodies*, or on behalf of *NATO bodies*. This is regardless of the format or location of the *personal data.* This includes *personal data* within *metadata* and Information and Communications Technology (ICT) system logs, and *personal data* that has been *pseudonymized*.
7. *Personal data processed* for the purposes of intelligence or counter-intelligence operations shall be out of scope of the Policy.
8. *Data subjects'* rights, and the application of the principle of transparency, may be limited, partially or fully, based on the requirements of applicable NATO policy, such as the use of administrative markings (reference C), or for duly justified and documented reasons. Possible reasons for restriction include:

    i. *Personal data processed* during the course of an personnel inquiry, investigation or disciplinary proceeding[2];

    ii. Personal data processed during the provision of legal advice and litigation;

    iii. Personal data processed during *deliberative proceedings*.

GENERAL POLICY STATEMENTS

9. *NATO bodies* shall develop, implement and maintain a supporting *personal data* protection directive aligned with this framework policy. In their supporting directives, *NATO bodies* should adopt the terminology used in this Policy to foster coherence across NATO.
10. *NATO bodies* shall take a risk-based and balanced approach to *processing personal data*.

[2] Also out of scope are national inquiries, investigations or disciplinary proceedings as they fall under national law or regulations.

a. *NATO bodies* shall assess and track the risk of *processing* a particular set of *personal data* and take measures adapted to the specific risks of the *processing*.

b. The protection of *personal data* shall be balanced with the necessity to accomplish the mission of the organization. In their directives, *NATO bodies* shall not include measures that unreasonably inhibit effective and efficient NATO management and operations, including the normal *sharing* of *personal data* within and between *NATO bodies.*

11. *Personal data* shall be *processed* by *NATO bodies* in compliance with the NATO Information Management Policy (reference A), the Security within NATO Policy (reference B) for *personal data* within classified information, the Management of Non-Classified NATO Information Policy (reference C), and Directive on the Protection of CIS Handling Non-Classified NATO Information (reference D) for *personal data* within non-classified documents.

12. *NATO bodies* shall have *personal data* protection programmes that:

a. Document what *personal data* sets they *process*, the purpose of *processing*, and the means of *processing* (i.e. document the what, why and how of *processing)*;

b. Identify individuals or entities that fulfil the roles of *personal data controllers* and *personal data processors* for all *personal data* sets they *process**;***

c. Ensure *personal data processors process personal data* as per the direction of the *data controller. 3rd party personal data processors process personal data in accordance with specific requirements for personal data processing* agreed with the *data controller;*

d. Create and assign the function of *Personal Data Protection Officer (PDPO). NATO bodies* shall consult the *PDPO* on all *personal data protection* matters. See paragraph 55c for the responsibilities of the *PDPO*;

e. Ensure staff *processing personal data* are appropriately trained and awareness is maintained.

13. *NATO Records,* which may include *personal data,* are the property of NATO and shall be subject to the provisions of Articles VI and VII of the Ottawa Agreement or of Article XIII of the Paris Protocol as per reference G.

14. In the case of a significant *personal data breach* that poses high risk to *data subjects*, *NATO bodies* shall provide appropriate information on the specific *personal data* compromised to the *data subject* in a responsible and timely manner after the confirmation of the breach. The *Personal Data Protection Officer* (*PDPO*) shall be

consulted to assess whether an incident is a significant *personal data breach* that poses high risk.

15. *NATO Bodies* shall determine whether they are required to perform a *Personal Data Protection Impact Assessment* (*PDPIA*) for *processing* a particular set of *personal data:*

    a. A *PDPIA* shall be performed for the *processing* of *special categories of personal data.*

    b. A *PDPIA* shall be performed for the *processing* of *personal data* that may lead to high risk to *data subjects.*

    c. A *PDPIA* may be performed to clarify the risk level of *processing* a set of *personal data*.

PERSONAL DATA PROTECTION BY DESIGN AND BY DEFAULT

16. *NATO bodies* shall consider *personal data* protection when designing any *processing* operations, rather than as an afterthought, and throughout the entire *personal data* lifecycle.

17. *NATO bodies* shall ensure the implementation of appropriate technical and organizational measures for ensuring that, by default, only the *personal data* that is necessary for each specific purpose of the *processing* is *processed*.

18. When performing data analysis, *NATO bodies* shall *anonymize* or *pseudonymize personal data* if the *processing* purpose still may be achieved by the use of these techniques.

    a. If both *anonymization* and *pseudonymization* are suitable techniques, *NATO bodies* shall use *anonymization*.

    b. *Personal data* that has been *anonymized* shall be no longer considered *personal data,* as there is no possibility to link the *anonymized* data back to a *data subject.*

    c. When *pseudonymization* is used, the additional data that can be used to identify *data subjects* shall be kept separately and shall be subject to technical and organizational measures to ensure non-attribution to an identified or identifiable *data subject*.

PERSONAL DATA PROTECTION PRINCIPLES

19. *Processing* of *personal data* shall follow the below principles.

Purpose Specification

20. *Personal data* shall be *processed* only for specific purposes.

21. *Personal data processed* for a specific purpose may be used for another purpose if a compatibility assessment determines the new purpose is closely related to the original purpose. The *PDPO* shall be involved in the compatibility assessment. Additionally, the compatibility assessment shall consider, inter alia:

    a. The context in which the *personal data* was collected;

    b. The nature of the *personal data,* in particular if it is *special categories of personal data*;

    c. The possible consequences to the *data subjects* of *processing* for a new purpose;

    d. The existence of protection security measures, such as encryption, *anonymization* or *pseudonymization*.

Legitimate Basis for Processing

22. *Personal data* shall only be *processed* by *NATO bodies* if the *processing* for a specific purpose is necessary for one of the following reasons:

    a. Pursuant to the NATO mandate;

    b. Compliance with a treaty, legal obligation or contract, or in the course of pre-contractual activities;

    c. Protecting the vital interest of the individual or of another natural person (e.g. for a medical emergency);

    d. The accomplishment of a public interest task;

    e. The legitimate interests of NATO.

        i. *NATO bodies* shall consider the reasonable expectations of *data subjects* based on their relationship with the *NATO body*. *Personal data* shall not be *processed* with this reason if it would override the rights of *data subjects*.

        ii. The use of this basis of *processing* shall not be used for *special categories of personal data*.

23. If none of the legitimate basis to *process* in paragraph 22 apply, a *NATO body* shall seek *consent* of the *data subject* to *process personal data*. The *NATO body* shall be

able to demonstrate in an audit that *consent* has been received to *process personal data. Consent* may be provided on behalf of a person who falls under the legal responsibility of the *data subject* (e.g. minors, elderly people, legally incompetent).

Transparency

24. The purpose of *personal data processing* shall be transparent for the *data subject*. Information about the *processing* shall be made available to the *data subject* by appropriate means and in plain language, for example by notice on a website or on personnel in-processing forms.

Minimization and Access

25. The *processing* of *personal data* shall be limited to the minimal amount necessary to achieve the specified purpose.

26. Access to personal data shall be balanced between the responsibility-to-share and the need-to-know principles (reference A). The access to *special categories of personal data* and *personal data* that may lead to high risk[3] to *data subjects* shall be limited to the community of interest(s) with the need-to-know. When used, administrative markings (reference C) indicate the need for limited access to *personal data*.

Retention

27. *Personal data* shall be retained only until the fulfilment of the specific purpose.

28. *NATO bodies* shall consult the Policy on the Retention and Disposition of NATO Information (reference I) and supporting retention and disposition schedules, to determine retention periods.

29. *Personal data* in NATO information of permanent value, for example names of individuals acting in an official capacity or as public figures, is kept indefinitely in accordance with procedures outlined in reference I.

Accuracy

30. *Personal data* shall be kept accurate, with measures in place for keeping it up to date to the extent reasonable and appropriate given the specific circumstances in which they are *processed*.

[3] High risk depends on the context of use, however, in general it is *personal data* whose release would reasonably be expected to be highly detrimental to the *data subject*. High risk *personal data* includes but is not limited to national identity numbers (e.g. national insurance, military service); financial information (e.g. bank accounts, credit cards, payroll information); personal phone numbers; residential addresses; dates of birth; information on children and spouses; workplace performance.

Accountability

31. *NATO bodies* shall know what *personal data* they *process*, for what purpose and by what means.

32. *NATO bodies* shall document, and be able to demonstrate upon request, the implementation of this policy and its effectiveness in protecting *personal data*.

Security of Processing: Confidentiality, Integrity and Availability

33. *NATO bodies* shall ensure appropriate security of *personal data* that protects its confidentiality and integrity against unauthorized or unlawful *processing*, and against theft, accidental loss, destruction or damage. *NATO bodies* shall take measures to ensure *personal data* is available when needed for NATO activity. The nature of *special categories of personal data* and high risk personal *data* shall be taken into consideration when prescribing enhanced security measures.

34. The security measures taken shall be in line with reference B for *personal data* contained in classified information, and references C and D for *personal data* contained in non-classified information, and their supporting policies and directives.

SHARING, TRANSFERRING AND DISCLOSING PERSONAL DATA

35. *Personal data* may be *shared* without additional restrictions, beyond those detailed in this Policy, between:

    a. *NATO bodies* subject to the provisions of this Policy. If requested, *NATO bodies* shall *share* the original and proposed legitimate basis and specific purpose of *processing*;

    b. Allies when the *personal data* is part of the proceedings of Allied bodies such as Councils, Committees, Boards and Working Groups.

36. *Personal data* may be *transferred* to *3rd parties*, entities which are not *NATO bodies.*

    a. If the *3rd party* is subject to laws, regulations or enforceable rules that provide at least substantively equivalent protections to those provided by this Policy;

    b. Or if the *3rd party* formally agrees to follow this Policy;

    c. Or if a *transfer* agreement is signed before *personal data transfer* takes place to a *3rd Party*.

37. The names of action officers, public figures, and anyone acting in an official capacity as reflected in the decision making process of a *NATO record* may be publicly disclosed along with the rest of the information if approved through the Public Disclosure *process* (reference H).

RIGHTS OF DATA SUBJECTS

38. *Data subjects* have rights regarding their *personal data*. *NATO bodies* shall have procedures supporting the exercise of these rights.

39. The rights of *data subjects* may be limited or restricted in certain circumstances. See paragraph 8.

Right to Information about NATO Personal Data Processing

40. *Data subjects* shall have the right to obtain confirmation from a *NATO body* as to whether it *processes* their *personal data*.

41. Information about the *processing* of *personal data* shall be made available to the *data subject* upon request, in accordance with the principle of transparency.

Right to Access and Portability

42. *Data subjects* shall have the right to access their *personal data* when it is *processed* by a *NATO body*, subject to the caveats of paragraphs 44 and 45.

43. *Data subjects* have the right of portability when the legitimate basis of *processing* is *consent* or a legal contract and the *processing* is carried out by automated means. They have the right to request their *personal data* in a digital format, subject to the caveats of paragraphs 44 and 45.

44. Access and portability shall not be provided when to do so would adversely affect the rights of others, violate NATO policies on the release of classified or non-classified information, or in cases noted in the paragraphs 7 and 8.

45. *Personal data* shall not be made available if to do so would involve disproportionate resources on the part of the *NATO body* concerned, or would be impossible. In such cases, the *NATO body* shall provide access to the extent reasonable.

Right to Rectification and Erasure

46. *Data subjects* shall have the right to rectify inaccurate or incomplete *personal data,* upon request.

47. *Data subjects* shall have the right to request erasure their *personal data* in the following circumstances:

    a. Their *personal data* is no longer necessary for the purpose[4] for which it was initially collected.

[4] Including a compatible purpose as per paragraph 21.

b. Their *personal data* was *processed* in a manner contradictory to the specific purpose.

48. *NATO bodies* shall not erase the names of any *data subject* acting in an official capacity from NATO information of permanent value (reference I).

Right to Object

49. *Data subjects* shall have the right to object to the *processing* of their *personal data*, when they suspect there is not a legitimate basis for *processing* (as identified in paragraph 22).

Right to Appeal

50. *Data subjects* shall have the right to a complaints and appeals procedure. See paragraphs 52 and 52.

REQUEST AND DISPUTE RESOLUTION

51. *NATO bodies* shall have a procedure for handling, within a reasonable timeline, requests that assert *data subject* rights.

52. *NATO bodies* shall have a procedure for handling dispute resolution that has no less than three levels.

a. Level One – Dispute Mediation: The *PDPO* is responsible for coordinating the resolution of disputes with the responsible party making the decision on the matter.

b. Level Two - Complaints Procedure: Any dispute arising from a decision from Level One may referred to the Head of *NATO body*, or delegated authority, for adjudication.

c. Level Three – Appeals Process: Decisions made at Level Two may be appealed to a superordinate authority, whose decisions shall be final and binding.

GOVERNANCE AND ROLES

53. *NATO bodies* are responsible for protecting the *personal data* they *process* and shall:

a. Develop and implement directives to ensure *personal data* is protected in line with this Policy;

b. Develop and maintain *personal data* protection programmes;

c. Consult their *PDPO* on all *personal data* protection matters.

54. The NATO Office of the CIO (OCIO) shall be responsible for the coordination and oversight of *personal data* protection for the NATO Enterprise.

    a. The OCIO shall assist *NATO bodies* in the development, maintenance and operations of their *personal data* protection policies and programmes, and support the collaboration amongst the *NATO bodies* in the application thereof.

    b. The OCIO shall be the staff element responsible for the oversight of the NATO *personal data* protection programme and the application of this Policy by the *NATO bodies*, and responsible for reporting the status of the programme.

55. The *PDPO* provides advice to *personal data controllers* on the *processing* of *personal data* and monitors compliance with this Policy and the *NATO body*'s supporting personal data protection directive.

    a. The *PDPO* shall:

        i. Have the required training and competence to fulfil the *PDPO* tasks;

        ii. Be able to function impartially, without undue influence, and with no conflicts of interest.

    b. The *PDPO* may:

        i. Be a dedicated post;

        ii. Be an additional duty. Other tasks and duties may be performed as long as 56.a.ii is respected;

        iii. Be performed by someone outside of the *NATO body* on the basis of a service contract.

    c. Responsibilities of the *PDPO* should include but are not limited to:

        i. Inform and advise the *NATO body* about obligations detailed in this Policy;

        ii. Monitor compliance with this Policy and developments in data protection law;

        iii. Develop the *process* for the *NATO body* to track the means and purposes of *personal data processing*;

        iv. Train staff on *personal data* protection, and raise awareness on *personal data* protection issues;

        v. Provide advice with regard to the nature, scope, context, purposes and risks of the *processing*;

vi. Provide advice on the risk to *personal data* in the event of a *personal data breach*;

vii. Provide advice, monitor, and if required, support *PDPIAs*;

viii. Be the first point of contact for requests, objections and complaints from *data subjects*;

ix. Lead the dispute mediation (level 1) *process*.

GLOSSARY

1. **3rd Party:** Entities which are not *NATO bodies*, such as the Allies and non-NATO entities other than the public (e.g. Partners, other International Organizations, Non-Governmental Organizations, or businesses).
2. **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*.
3. **Consent:** *Consent* is the freely given, informed and explicit approval by a *data subject* for the *processing* of their *personal data*, or the *personal data* of someone who falls under their legal responsibility. *Consent* can be withdrawn at any time without any negative effect or prejudice to the *data subject*.
4. **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.
5. **Deliberative proceedings**: Information exchanges and critical examinations of an issue leading to decision, such as during the complaints process, recruitment process, and so on.
6. **Metadata:** Structured data that describes, explains, locates, and otherwise makes it easier to retrieve, use and understand an information resource. *Metadata* facilitates the association of records within the context of broader business activities and functions.
7. **Minimization**: Collecting the minimal amount of *personal data* required to achieve the specified purpose of *processing*.
8. **NATO body:** A civilian or military headquarters, or agency or other organizational unit established pursuant to Article 9 of the North Atlantic Treaty, including *NATO bodies* established in support of Alliance Operations and Missions (AOM).
9. **NATO records:** Information created, received, and/or maintained as evidence and information by NATO, in pursuance of legal obligations, NATO missions or in the transaction of business. *NATO records* officially document the actions and decisions of the Organization, verbatim from reference G.
10. **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. This is a subset of “Information” as defined in reference A.

11. **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*.

12. **Personal data controller:** The *personal data controller* defines the purpose and means of *personal data processing*. This role is held by the head of *NATO body* and the responsibility may be delegated. This term roughly corresponds to "Information Owner" in reference A.

13. **Personal data processor:** An element external to a *NATO body*, such as another *NATO body* or a *3rd party* that *processes personal data* on behalf of the *personal data controller*. The corresponding term in reference A is "Information Custodian," however an Information Custodian performs only a subset of *processing* – "makes it visible" and "safe-keeping."

14. **Personal Data Protection Impact Assessment (PDPIA):** Identifies, evaluates and addresses the risks to *personal data* arising from a certain *processing* activity.

15. **Personal Data Protection Officer (PDPO):** A role responsible for providing advice on and overseeing a *NATO body*'s *personal data* protection programme. The *Personal Data Protection Officer* shall be independent from the *personal data controller.*

16. **Processing (of *personal data*):** any operation, or set of operations, that is performed upon *personal data* such as collecting, recording, organizing, storing, adapting, altering, combining, retrieving, consulting, using, disclosing, transmitting, disseminating, blocking, erasing or destroying. Within reference A, the term "handling" is used. *Processing* may be done manually or through automation.

17. **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*.

18. **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.

19. **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.

20. **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.