Allied Command Transformation

Norfolk, Virginia | USA

ACT DIR 040-13
DATED 20 APR 22
TT - 3324

ACT PERSONAL INFORMATION AND PRIVACY PROTECTION DIRECTIVE

REFERENCE: See Annex A.

1. **Status.** This is a new Allied Command Transformation (ACT) directive.

2. **Purpose.** The purpose of this directive is to define personal data protection rules within ACT.

3. **Applicability**. This directive is applicable to all ACT Headquarters and subordinate commands. JJJ commanders may issue local directives or procedures that augment but do not counteract ACT directives to meet the requirements of their specific mission or locality.

4. **Policy Scope**. ACT use and protection of personal information and privacy is an essential activity included in the lifecycle of NATO documents and records described in References A and B. This directive may apply to all NATO records (whether of permanent or temporary value) created, received and/or maintained as evidence and information by ACT in pursuance of legal obligations, NATO missions, or in the transaction of business. As such, this may apply to all ACT official activities, including projects, programmes, contracts, and other related tasks such as Morale Welfare Activities (MWA). The implementation of this Directive will be progressive. Further revisions to this policy will reflect lessons identified and learned with an HQ SACT Chief of Staff agreed implementation plan, including processes, tools, governance instructions and any associated resource requirements.

5. **Publication Updates**. Updates are authorized when approved by signature authorities in accordance with Annex A to ACT Directive 30-1, preparation of Bi-SC, ACT, and HQ SACT Directives and Standard Operating Procedures (SOPs). This Directive will be reviewed annually and updated as required.

6. **Sponsor**. The Sponsor for this ACT directive is Branch Head, Chief Information Office.

FOR THE SUPREME ALLIED COMMANDER TRANSFORMATION:

Guy Robinson OBE
Vice Admiral, GBR N
Chief of Staff

DISTRIBUTION:

Internal:

Action:

Lists I - VI

TABLE OF CONTENTS

CHAPTER 1 - INTRODUCTION

1-1. This directive is to address the protection of personal information and privacy while conducting ACT's mission. The current NATO policies and directives related to information management and security, which have been approved by consensus of the Member Nations of NATO, provide a framework based on the handling of NATO records to accomplish this goal while also accomplishing the purpose of ACT.

1-2. A NATO record is 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. All NATO records, regardless of form, medium or classification level, are the property of NATO (Reference A[1]). They can be of a temporary or permanent value.

1-3. NATO information management polices require the information to be protected at a given level of confidence with respect to confidentiality, integrity, availability, non-repudiation and authentication (Reference B[2]). While the security classification of an information item indicates the minimum level of protection required (Reference C[3]), administrative markings require an additional layer of protection for personal information. For the purposes of this directive, personal information or personal data are any sensitive information, which can be used to distinguish or trace the identity of a natural person.

1-4. NATO information is managed with an emphasis on the responsibility to share balanced by the security principle of need-to-know and managed to facilitate access, optimize information sharing and re-use, and reduce duplication, all in accordance with security, legal, and privacy obligations. NATO records may be shared, if necessary, in accordance with NATO policies, directives, and legitimate purposes including national security.

1-5. Headquarters Supreme Allied Commander Transformation (HQ SACT) and subordinate commands are granted the privilege of the inviolability of their records and archives (Reference G[4]). A responsibility of this privilege is ensuring through professional competence and due care (Reference H)[5], the safeguarding of the personal information contained in the records and the privacy of the records whether created, received and processed by ACT (Reference H[6]). Moreover, as an international organization formed under the Paris Protocol, HQ SACT enjoys immunity from the enforcement of national or supranational data privacy statutes or regulations.

---

[1] C-M(2011)0043 NATO Records Policy, p.1-1, Introduction, paragraph 1 and p.1-2, paragraph 11. Ownership and custodianship (a).
[2] C-M(2007)0118 NATO Information Management Policy, paragraph 10, Information Assurance p.1-2.
[3] C-M(2002)49-REV1 Security Within The North Atlantic Treaty Organization (NATO), Enclosure E, paragraph 7, p. E-2
[4] Protocol on the Status of International Military Headquarters (Paris Protocol) 1952, Article XIII.
[5] ACT Directive 40-0(2019) ACT Policy Statements: Code of Conduct and Core Values, paragraph 13, p.3.
[6] ACT Directive 40-0(2019) ACT Policy Statements: Code of Conduct and Core Values

1-6. The processing, collection, maintenance and disposal of personal information present a risk to privacy that requires management within ACT (References I[7] and J[8]). This directive implements measures to mitigate this risk.

1-7. Issues regarding the interpretation, applicability or enforcement of the requirements, standards and tasks set forth in this directive shall be referred to the Chief Information Office, who will coordinate with relevant stakeholders.

[7] ACT Directive 20-3.2(2020) ACT Risk Management Directive
[8] ACT Directive 25-2 (2015) ACT Records Management Directive

CHAPTER 2 - ACT ORGANIZATION ROLES AND RESPONSIBILITIES

2-1. **PERSONAL DATA OWNER.** The responsibilities of the Heads of NATO civil and military bodies (Reference K[9]) require the Supreme Allied Commander Transformation and the Commanders of the Joint Warfare Command (JWC), the Joint Force Training Centre (JFTC), and the Joint Analysis Lessons Learned Centre (JALLC) to each be the personal data owner (PDO) within their organizations. SACT is the PDO for both HQ SACT and Allied Command Transformation (ACT), and each subordinate commander is the PDO for his or her respective subordinate command.

2-2. **PERSONAL DATA OWNER RESPONSIBILITIES**. PDOs have specific responsibilities under this directive:

a. PDOs shall protect personal information by using the minimum necessary to achieve organizational outputs while managing it throughout the NATO Information lifecycle.

b. PDOs are accountable for the risks to ACT's outputs associated with the use by the ACT NATO bodies of personal information. This includes risks to ACT's reputation and public trust.

c. SACT is supported in this responsibility by the ACT Personal Data Controller and the Commanders of JWC, JFTC, and the JALLC who are responsible to ensure that personal information and privacy are managed.

d. All ACT Commanders are supported by a Personal Data Protection Officer and one or more Personal Data Custodians who they appoint to perform the duties described below.

2-3. **ACT PERSONAL DATA CONTROLLER.** The ACT Personal Data Controller (PDC) for HQ SACT, JWC, JFTC and JALLC is HQ SACT Chief of Staff who is appointed by SACT as the senior ACT official responsible for information management (Reference K[10]). Further delegation of this role is permitted. The PDC determines the purposes and means for collecting personal data, processing personal data and controlling the use of personal data.

2.4 **ACT PERSONAL DATA CONTROLLER RESPONSIBILITIES.** The ACT PDC is responsible for:

a. Supporting SACT and subordinate Commanders in appointing the Personal Data Protection Officers and Personal Data Custodians within ACT and coordinating, training, and ensuring uniformity in the information assurance measures to protect personal information and privacy within ACT.

b. Managing risks to personal information ACT collects, receives, and processes.

---

[9] C-M(2007)0118 NATO Information Management Policy, p. 1-2, paragraph 12, c. and e
[10] C-M (2007)0119 NATO Information Management Policy, p. 1-2 and 1-3, par 12.e.(6)

c. Ensuring that ACT keeps an inventory of personal information processed recording:

1. The nature of the information;
2. The legitimate purpose for which it is processed;
3. Whether it may be transmitted outside of ACT and, if so, where and to whom;
4. That it is securely stored at a level appropriate to its sensitivity;
5. The expected disposition of personal information; and
6. The procedure for handling requests for amendment or deletion by the person whose personal information has been collected or processed by ACT.

d. Coordinate risk assessment recommendations and advice to the ACT Personal Data Owners, Personal Data Protection Officers, Personal Data Custodians, with support of the Branch Head Chief Information Office.

e. Coordinating with Personal Data Protection Officers, Personal Data Custodians, the ACT Security Officer and the Personal Data Owner in the event of a data breach that puts at risk personal information protected by ACT.

f. Ensuring that whenever information is solicited or transmitted by ACT that it is kept to the minimum necessary and is appropriately protected.

g. Ensuring that a Privacy Impact Assessment is carried out for all systems and projects managed and implemented by the organization.

h. Coordinating with ACT Commanders and the ACT Financial Controller to ensure that all contracts entered into by ACT that may involve the collecting and processing of personal information are subject to legal review to ensure that personal information and privacy are protected while respecting the privileges and immunities of ACT.

2-5. **PERSONAL DATA PROTECTION OFFICER.** Appointed by the Head of NATO body of their ACT command or organization. In each ACT command or organization, the number and rank/grade range may vary depending on the role and size of the organization. The Personal Data Protection Officer oversees the implementation of the personal information protection policy.

2-6. **PERSONAL DATA PROTECTION OFFICER RESPONSIBILITIES**. The Personal Data Protection Officer at each ACT body is responsible for:

a. Coordinating with the ACT PDC to ensure the actions they are undertaking to protect personal information and privacy are consistent with ACT best practices and risk mitigation.

b. Completing the ACT Privacy Impact Assessment (PIA) Template.

c. Acting as the initial point of contact within the command for issues and inquiries concerning the handling of personal information.

d. Working with and supervising the command Personal Data Custodian(s) to ensure all personal information obtained or processed is protected in accordance with NATO and ACT policies.

e. Ensuring the command Personal Data Custodian(s) keeps an inventory of personal information processed, recording:

1. The nature of the information;
2. The legitimate purpose for which it is processed;
3. Whether it may be transmitted outside of ACT and, if so, where and to whom;
4. That it is securely stored at a level appropriate to its sensitivity;
5. The expected disposition of personal information; and
6. The procedure for handling requests for amendment or deletion by the person whose personal information has been collected or processed by ACT.

f. In conjunction with the ACT Security Accreditation Authority, conducting an on-going risk assessment of the actions necessary to protect NATO and ACT records containing personal information.

g. Providing regular reports to the ACT Personal Data Controller on the number of NATO and ACT records containing personal information held within the command along with a description of how the personal information is processed, stored, and protected.

h. Ensuring all Personal Data Custodians and other personnel in information handling and processing responsibilities are appropriately trained to fulfil their duties.

i. Ensuring that all new personnel, including contractors, vendors or any other person who must provide their personal information to enter ACT commands or organizations receive an initial awareness about how and why ACT protects and stores personal information.

j. Addressing and resolving Individual Information Request (IIRs), as defined in Annex E, or other requests for personal information.

k. Coordinating with the ACT PDC, the ACT Security Accreditation Authority, the Communication and Information System Operational Authority and the command Personal Data Custodian(s) in the event of an information breach to mitigate the impact of the breach.

l. Developing command procedures and SOPs to detect personal data breaches (breach detection) and to be executed promptly upon the detection of a personal data breach (breach mitigation) including notification procedures to individuals whose personal information may have been the subject of the breach.

2-7. **PERSONAL DATA CUSTODIAN.** The Personal Data Custodian is appointed by the Head of NATO Body. In each ACT command or organization, the number and rank/grade range of Personal Data Custodians may vary, depending on the role and size of the organization. The following mandatory actions of Personal Data Custodians are directed by the guidance of the ACT Personal Data Controller and specifically approved by the Personal Data Protection Officer of each ACT body: HQ SACT, JWC, JFTC, and JALLC.

2-8. **PERSONAL DATA CUSTODIAN RESPONSIBILITIES**. The Personal Data Custodian is responsible for:

a. Granting access to personal information as presented in Reference E.

b. Being the nominated key holder for collections of hard-copy information materials stored in cabinets or a locked room.

c. Ensuring that personal information is obtained, processed, stored and protected in accordance with applicable policies.

d. Keeping an inventory of personal information processed, recording:

1. The nature of the information;
2. The legitimate purpose for which it is processed;
3. Whether it may be transmitted outside of ACT and, if so, where and to whom;
4. That it is securely stored at a level appropriate to its sensitivity;
5. The expected disposition of personal information; and,
6. The procedure for handling requests for amendment or deletion by the person whose personal information has been collected or processed by ACT.

e. Completing Privacy Impact Assessments (Annex B).

f. Executing in close coordination with AOS risk assessments and recommendations. Risk assessments shall be carried out annually or sooner if any of the following occurs:

1. Significant changes to the content and/or volume of records stored;
2. The personal information is no longer required and has been deleted or archived;
3. The purpose of the personal information has changed;
4. Arrangements for obtaining, processing or storing the personal information have changed or,
5. The personal data custodian has changed.

g. Coordinating with the command Personal Data Protection Officer, the Security Accreditation authority, the Communication and Information System Operational Authority and the ACT PDC in the event of an information breach to mitigate the impact of the breach and to reassess policies to ensure improved performance of information protection and privacy policies.

CHAPTER 3 - PRINCIPLES OF PERSONAL INFORMATION AND PRIVACY PROTECTION

3-1. ACT principles regarding personal data protection and privacy.

a. **Consent**. Consent must be freely given, specific, informed and explicit. Requests for consent must be clearly distinguishable from the other matters and presented in clear and plain language. Information subjects can withdraw previously given consent whenever they want, with prospective effect. Children under 18 years old can only give consent with permission from their parent. ACT need to keep documentary evidence of consent. If a consent cannot be obtained, a restriction in the ability of the individual to interact with ACT may occur (e.g. access).
Sample language follows:

1. Individuals providing personal information for ACT authorized purposes or activities do so consensually.
2. Individuals consent to the use, transfer and processing of this consensually-provided personal information in accordance with the standards set forth in this directive.
3. Individuals may withdraw their consent to the use, transfer and processing of this information at any time, with prospective effect.

b. **Transparency.** ACT shall have a functional necessity and legitimate purpose for obtaining, processing or storing personal information. Notice is to be provided upon request to the individuals who provide their personal information to ACT as to the purposes for which their information is being obtained, processed, or stored.

c. **Accessibility.** ACT shall provide individuals the opportunity to access any personal information that is held on them and to have it corrected, subject to security restrictions.

d. **Purpose Limitation.** All personal information must be collected and held for a specific purpose. The collector must be able to articulate the specific purpose for which information is being collected, and that purpose must be no broader than strictly necessary to accomplish the purpose(s).

e. **Information Minimization.** ACT shall obtain process or store the minimum amount of personal information necessary to inform decisions or actions to serve the purpose for which such information was required.

f. **Accuracy.** ACT personal information protection and privacy processes shall ensure that the personal information is accurate and there is a procedure in place for keeping personal information up to date.

g. **Third Party Platforms**. Non-governmental or commercial Third party platforms used by ACT for the purpose of conducting surveys, registering participants, aggregating personal information, and similar functions shall be evaluated by the IPO,

supported by the appropriate stakeholder, for compliance with these standards, at a minimum.

h. **Storage Limitation.** ACT information protection and privacy processes shall ensure that procedures are in place for disposing of personal information promptly in the lifecycle of NATO information when deemed not to have permanent value.

i. **Processing Protections.** Within ACT, personal information shall be protected and handled by trained personnel. Personal information may only be disclosed when it is necessary or with permission of the individual whose personal information has been shared. Non-disclosure agreement will be executed where warranted.

j. **Security.** ACT shall ensure appropriate security of Personal Data, including protection against unauthorized or unlawful processing, and against accidental loss, destruction or damage. The measures to be taken for protection shall be in line with appropriate NATO policies at a minimum. The level of security provided assessment shall take into account the special nature of Sensitive Personal Data.

k. **Training.** ACT Personal information protection and privacy processes shall include training of personnel to ensure proper and consistent handling of personal information throughout the information's lifecycle.

l. **Transacting, Collaborating and Interacting with Outside Entities**.

1. External persons or organizations (not internal to NATO or ACT) shall be advised in writing of the contents of this directive and that it supplies the sole and exclusive set of standards and procedures for receiving, processing, handling and storing personal information.

2. This principle applies to all contracts, collaboration arrangements, MOUs, agreements, and other formal and informal arrangements with non-NATO entities, including but not limited to other international organizations, governments, companies, conference centers, common carriers, non-profit organizations, laboratories, research centers, and universities.

3. The advisory notice shall state: "Allied Command Transformation and its subordinate commands apply ACT Directive 40-13 as the sole and exclusive set of standards and procedures for receiving, processing, handling and storing personal information, in lieu of national and international data protection standards. ACT Dir 40-13 is available at (corresponding URL). This directive shall be available on a public facing website, and the corresponding URL shall be furnished to individuals and organizations with which ACT has commercial, formal, collaborative or informal relationships.

CHAPTER 4 - INDIVIDUAL REVIEW OF ACT PROCESSED PERSONAL INFORMATION

4-1. **Individual Review.** Individuals shall have the opportunity to review their personal information. This opportunity will normally be exercised by examining the personal information for accuracy at the time of input and annually. Individuals may also review their personal information whenever changes need to be made, or at any time, that it becomes apparent to the individuals that the information held on them is inaccurate.

4-2. Their review includes notice of:

a. The existence of a NATO record containing their personal information;

b. Its legitimate purpose and whether the individual's personal information is being shared with the host nation, subject to the security exclusions contained in chapter 7.

c. The opportunity to obtain from the ACT command processing the information:

1. A copy of their personal information; and
2. Correction or erasure of inaccurate personal information.

d. The opportunity to file a complaint regarding the handling of their personal information following existing complaints procedures.

CHAPTER 5 - STORAGE AND HANDLING OF PERSONAL INFORMATION

5-1. All access to records containing personal information shall be subject to a reliable identification and authentication mechanism. All records containing personal information shall be sufficiently protected.

5-2. Care shall be taken when naming electronic files containing personal information so that personal information is not revealed by the file name.

5-3. The processing of personal information shall be conducted with appropriate measures in order to safeguard the interests of the personal information subject, and shall be proportionate to the aim pursued. In accordance with Reference K, in individual cases some personal information provided it is at a level no higher than NATO UNCLASSIFIED and with the handling marking "releasable to Public", may be sent over the internet to the individual if the individual has provided informed written consent for this to happen.

5-4. Personal information shall not be viewed, either electronically or in paper form, in a public place (for example, in an airport or on a train) unless appropriate precautions have been taken, to avoid unauthorised disclosure.

5-5. Special Categories of Personal Information. Personal information related to racial or ethnic origin, sexual orientation, political, philosophical, religious opinions or activities, as well as genetic, biometric data and information concerning health should not be processed, unless some of the following applies:

a. The information subject has given explicit consent to the processing of personal information for one or more specific purposes.

b. The processing is necessary for the protection of the vital interests of the information subject or of another person.

c. The processing is necessary for the observance of NATO security policy and counter intelligence, and also the execution of obligations, the exercising of rights in the field of employment and social security.

d. The processing is necessary for the exercise or defence of legal claims.

e. The processing is necessary for archiving purposes in the public interest, scientific, historical and statistical purposes.

f. The processing is necessary for reasons of public interest in the area of public health, the assessment of the working capacity of the employee, medical diagnosis and the provision of health or social care.

CHAPTER 6 - TRAINING

6-1. **Training.** Education and training are necessary to ensure staff compliance with NATO and ACT Personal information protection and privacy policies.

a. All ACT military and civilian staff members and other personnel including contractors and vendors shall undergo initial training on the policies to protect NATO personal information and privacy during the individual's in processing and security training.

b. All ACT military and civilian staff members and other personnel including contractors shall complete annual training on NATO and ACT information protection and privacy policies and principles, in conjunction with their annual security training.

c. The content of this training will be created and its content relevance maintained by personal data protection subject matter experts. There will be applicable training created for the various levels of custodianship of personal data.

CHAPTER 7—SECURITY EXCLUSIONS

7-1. **Security Exclusions.** Personal Information relating to a security, intelligence, or law-enforcement issues will be excluded from release in the individual review of ACT processed personal information described in CHAPTER 4, and Annex C.

7-2. **Cyber Incident Response**. Where protected personal information is disclosed as a result of a cyber-incident, the NATO Cyber Incident Response Plan will take precedence over the ACT Personal Information Breach Response Plan at ANNEX E.

ANNEX A TO ACT DIR 040-13
DATED 20 APR 22

ANNEX A—REFERENCES

A. C-M(2011)0043 NATO Records Policy.
B. C-M(2007)0118 NATO Information Management Policy.
C. C-M(2002)49-REV1 Security within the North Atlantic Treaty Organization (NATO).
D. AC/322-N(2011) Guidance on the Markings of NATO Information.
E. C-M (2002)60 The Management of Non-Classified NATO Information.
F. Protocol on the Status of International Military Headquarters (Paris Protocol) 1952.
G. ACT Dir 40-0 (2019) ACT Policy Statement: Code of Conduct and Core Values ACT.
H. ACT Dir 20-3.2 (2020) ACT Risk Management Directive.
I. C-M(2009)0021 (INV), Policy on the Retention and Disposition of NATO Information
J. ACT Dir 25-2 (2015) ACT Records Management Directive.
K. Bi-Strategic command interim directive 25-001 (2019) on Information and Knowledge Management.

ANNEX B TO ACT DIR 040-13
DATED 20 APR 22

ACT PRIVACY IMPACT ASSESSMENT

The ACT Privacy Impact Statement is designed as a tool to prompt data users to consider the impacts of data collection, retention and storage, and to document compliance.

ACT Privacy Impact Template

1. Identify the need for a PIA: explain why personal data needs to be collected, processed, and stored _____

2. Whose information are you collecting and storing, and how will you collect, use, store and delete personal information? _____

3. Describe minimization procedures and document a specific and relevant need for each element of personal data collected. If a specific and relevant need for an element of information cannot be articulated, that element of information should not be collected (i.e. consider birthdays, which are rarely relevant to NATO purposes outside Human Resources purposes)._____

4. Disclose this completed PIA form to the ACT IPO for concurrence and retention and document the form of disclosure here (email, hand carry, upload to Sharepoint, etc.) _____

ANNEX C TO ACT DIR 040-13
DATED 20 APR 22

ANNEX C - ACT PRIVACY NOTICE

This ACT Privacy Notice is provided to ensure the persons whose personal information is being processed by (name of ACT Command)

Date: xx/xx/xxxx

ACT Personal Information Privacy Policy

(Name of ACT Command) contact details

Name: *[name of ACT Command]* Information Protection Officer

Address:

Phone Number:
E-mail:

The type of personal information ACT collects:

ACT currently collects and processes the following necessary information:

- Personal identifiers including names, nationality, and characteristics (civilian, military, if necessary, age, gender, and contact details)
- *[Add to this list as appropriate]*

How we get the personal information and why we have it.

Most of the personal information ACT processes is provided to us directly by you for one of the following reasons:

- In order to permit you to have access to (ACT command) and perform the duties and responsibilities of your position.

ACT also receives personal information from the following sources:

- Your nation.
- Your employer if you are working at (ACT command) as a contractor or commercial service provider.

- Other *[provide name of source].*

ACT uses the information that you have given us in order to:

1) provide you access to (ACT command)
2) provide notice to (host nation) of your assignment to (ACT command)
3) Other *[describe other use, with the exception of the security exclusions contained in Chapter 7].*

ACT may share this information with *[enter organizations or individuals].*

The basis ACT relies on for processing this information is/are: [delete as appropriate]

(a) Your consent. If you wish to remove your consent at any time, you can do this by contacting *[name of ACT command contact details]*

(b) We have a contractual obligation.

(c) We have a legal obligation.

(d) We have a vital security interest.

(e) We need it to perform a NATO task.

(f) We have a legitimate interest.

How ACT stores your personal information:
Your information is securely stored at *[name of ACT Command].*

ACT keeps *[type of personal information]* for *[time period].* ACT will then dispose of your information by *[explain how you will delete personal information of temporary value or retain personal information of permanent value].*

You and your access to your NATO records containing your personal information:
You may undertake the following actions concerning your personal information (or on behalf of certain family members such as young children) including:

Access to your personal information - You may ask (name of ACT Command) for copies of your personal information.

Correction of your personal information - You may ask (name of ACT Command) to correct personal information you think is inaccurate. You may also ask (name of ACT Command) to complete information you think is incomplete.

Restriction of processing - You may ask (name of ACT Command) to restrict the processing of your personal information in certain circumstances.

Please contact us *at [name of ACT Command email address, phone number and or postal address]* if you wish to make a request.

How to complain

Complaints will follow existing complaints procedures.

ANNEX D TO ACT DIR 040-13
DATED 20 APR 22

ANNEX D - ACT NON-DISCLOSURE DECLARATION

I _____ certify that I have been fully briefed on, and understand, the NATO and ACT policies and principles pertaining to information protection, personal information and privacy, and I agree to abide by those policies and principles. I am aware of and understand my responsibilities for safeguarding such information and that if I, intentionally or through negligence, allow unauthorized access to, or divulge such information to unauthorized parties, I may be subject to consequences determined by law or administrative authorities.

_____ _____
ACT Staff Member or Contractor Date

_____ _____
Instructor/Trainer Date

ANNEX E TO ACT DIR 040-13
DATED **20** APR 22

ANNEX E - ACT Information Breach Response Plan

Information Breach/suspected Information Breach

- Discovery by an ACT staff member, contractor or otherwise brought to the attention of ACT

ACT staff member or contractor aware or concerned shall:

- Immediately notify the Command Personal Data Protection Officer
- Record and advise the Personal Data Protection Officerof: 1) the time and date the ACT staff member became aware or concerned regarding the Information Breach/suspected Information Breach; 2) the type of personal Information involved; 3) the known or suspected cause and extent of the Information Breach/suspected Information Breach; and 4) the purpose of the impacted personal information.

The ACT Command Information Protection Officer shall:

- Determine whether or not an Information Breach has occurred, and, if so, the severity of the Information Breach
- Initiate the ACT Information Breach Response Plan in coordination with the Personal Data Custodian and notify the ACT Personal Data Controller
- Stop the breach

The ACT Information Breach Response Plan shall include measures to:

- Assess the type and amount of personal information exposed
- Coordinate within ACT and other NATO bodies to determine the source of the Information Breach
- Promptly notify information protection agencies of the affected nationals (NLRs)
- Promptly notify the affected individuals
- Mitigate the risk and harm caused by the Information Breach

Post-Breach Actions:

- Assessment of the failure and vulnerabilities of the system that permitted the Information Breach to occur
- Reassessment of exisitng information protection and privacy policies and best practices to ensure adequacy in the face of threats

ANNEX F TO ACT DIR 040-13
DATED 20 APR 22

ANNEX F - GLOSSARY

ACT Personal Data Controller (ACT PDC). The ACT staff member designated by the ACT Chief of Staff who determines the purposes and processing and controls personal information.

Personal Data Custodian (PDC). Manages the day-to-day use of specific sets of personal information.

Personal Data Protection Officer (PDPO). The ACT staff member appointed by the Head of NATO Body of their ACT command to oversee the implementation of this directive. The IPO works in close coordination with the ACT Personal Information Controller (APIC) and supervises the work of their command's Information Custodian(s).

Personal Information. Any information, which can be used to distinguish or trace the identity of a natural person.

Sensitive Personal Information. Any fact or opinion about an individual's workplace performance, discipline, physical or mental health, financial affairs, or private life, the release of which could reasonably be expected to put the person in physical danger, or harm their career or reputation. (from AC/324-D(2014)0010-REV2, Directive on the Public Disclosure of NATO Information).

Privacy Impact Assessment (PIA). Prior to processing, an assessment of the impact of the planned processing operation on the protection of personal information is conducted. A single assessment may address similar processing operations that share similar risks.