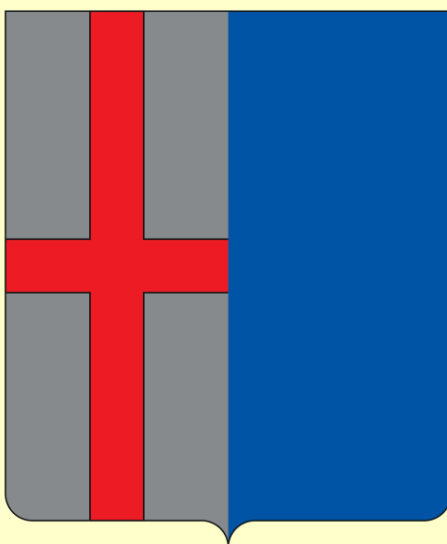
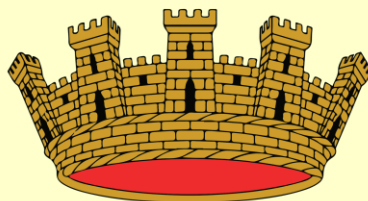




## **33° REGGIMENTO SUPPORTO TATTICO E LOGISTICO "AMBROSIANO"**



## **MANUALE DI GESTIONE DEL SISTEMA DI PROTOCOLLO INFORMATICO E GESTIONE DOCUMENTALE**



**2024**

PAGINA INTEZIONALMENTE BIANCA

## AVVERTENZE

---

La presente pubblicazione è stata approntata secondo quanto previsto dalla Circ. 1001 Modalità per l'approntamento delle pubblicazioni dell'Esercito, Ed. 2016 di SME.

Fatte salve le esigenze di servizio, ufficio o istituto, nessuna parte di questa pubblicazione può essere riprodotta in qualsiasi forma a stampa, fotocopia, microfilm, scansione digitalizzata o altri sistemi, senza l'autorizzazione scritta dell'originatore. Per proporre motivate varianti alle prescrizioni contenute si potrà inviare comunicazione:

UFFICIO MAGGIORITÀ E PERSONALE

Cap. Fabio ZAPPIA

Mail - [aiutmagg@rgtstl33.esercito.difesa.it](mailto:aiutmagg@rgtstl33.esercito.difesa.it)

Sotrin - 1176417

La presente pubblicazione è diramata con lettera in Annesso I.

PAGINA INTEZIONALMENTE BIANCA

## ATTO DI APPROVAZIONE

---

Approvo il presente *Manuale per la gestione interna del sistema di protocollo informatico e gestione documentale ADHOC*.

Il documento definisce, in ossequio alle vigenti disposizioni legislative, comunitarie, nazionali e di F.A. le attività di gestione e trattamento dei documenti gestiti dal sistema di protocollo informatico al fine di garantire il più possibile la corretta gestione e la riservatezza nella visualizzazione e accesso ai dati sensibili ovvero alle informazioni/documenti in genere nel pieno rispetto delle norme a tutela della privacy.

Solbiate Olona (VA), li 7 novembre 2024

**IL COMANDANTE DI REGGIMENTO**  
**(Col. f. (par.) t.ISSMI Amos VIRGONA)**

# INDICE

## PRIMA PARTE - MISURE TECNICHE

|                                                                            |    |
|----------------------------------------------------------------------------|----|
| 1. GENERALITA'.....                                                        | 3  |
| 2. RIFERIMENTI NORMATIVI.....                                              | 5  |
| 3. AMBIENTE DI RIFERIMENTO.....                                            | 7  |
| 3.1. GENERALITA'.....                                                      | 7  |
| 3.2. DEFINIZIONI.....                                                      | 7  |
| 3.3. IDENTIFICAZIONE E NOMINA DELLE FIGURE CHIAVE.....                     | 11 |
| 4. GESTIONE DEL SISTEMA DI PROTOCOLLO INFORMATICO @D <sup>33</sup> OC..... | 11 |
| 4.1. RUBRICA.....                                                          | 12 |
| 4.2. ASSISTENZA E CREZIONE/VARIAZIONE RUOLI.....                           | 12 |
| 4.3. DELEGHE.....                                                          | 12 |
| 4.4. GENERAZIONE E ANNULLAMENTO DI UN PROTOCOLLO.....                      | 12 |
| 4.5. PROTOCOLLAZIONE IN REGIME DI EMERGENZA.....                           | 13 |
| 4.6. RILASCIO DI COPIA INFORMATICA - "GLIFO".....                          | 13 |

## SECONDA PARTE - MISURE PROTEZIONE

|                                                              |    |
|--------------------------------------------------------------|----|
| 5. TRATTAMENTO DEI DATI PERSONALI IN AMBITO F.A.....         | 17 |
| 5.1. GENERALITA'.....                                        | 17 |
| 5.2. TEMPI DI CONSERVAZIONE ( <i>DATA RETENTION</i> ).....   | 17 |
| 5.3. ORGANIZZAZIONE AOO - 33° Reggimento AMBROSIANO.....     | 19 |
| 5.4. COMPITI E RESPONSABILITA'.....                          | 20 |
| 5.5. TRATTAMENTO DEI DATI PERSONALI.....                     | 21 |
| 5.6. INFORMATIVA.....                                        | 22 |
| 5.6.1 PARTICOLARI ADEMPIMENTI.....                           | 25 |
| 5.6.2 RESTRIZIONI NELLA CONSULTAZIONE - CONO VISIBILITÀ..... | 26 |
| 5.7. VIOLAZIONE DATI PERSONALI.....                          | 27 |
| 5.8. BUONE PRASSI.....                                       | 28 |

## TERZA PARTE - MISURE ORGANIZZATIVE

|                                                               |    |
|---------------------------------------------------------------|----|
| 6. TITOLARIO E CLASSIFICAZIONE D'ARCHIVIO.....                | 31 |
| 6.1. GENERALITA'.....                                         | 31 |
| 6.2. METODOLOGIA DI RIFERIMENTO.....                          | 31 |
| 6.3. FASCICOLAZIONE E ARCHIVIAZIONE.....                      | 32 |
| 7. GESTIONE DOCUMENTI IN ENTRATA.....                         | 35 |
| 7.1. DOCUMENTI ANALOGICI.....                                 | 35 |
| 7.2. TIPOLOGIA DI DOCUMENTI ANALOGICI.....                    | 35 |
| 7.3. CONTROLLI DI SICUREZZA.....                              | 36 |
| 7.4. DOC. ORDINARI/RACCOMANDATA/ASSICURATA/PACCHI.....        | 36 |
| 7.5. PLICO CON DOPPIA BUSTA CONTENENTE DOC. CLASSIFICATI..... | 37 |
| 7.6. CORRISPONDENZA DANNEGGIATA.....                          | 37 |
| 7.7. TELEGRAMMI/SPEDIZIONI CORRISPONDENZA ANALOGICA.....      | 37 |
| 7.8. DOCUMENTO IN ENTRATA SU PEI.....                         | 37 |
| 7.9. DOCUMENTO IN ENTRATA SU PEC.....                         | 38 |

|                                                                           |    |
|---------------------------------------------------------------------------|----|
| 7.10. DOCUMENTO IN ENTRATA SU XOMAIL.....                                 | 38 |
| 8. GESTIONE DOCUMENTI IN USCITA.....                                      | 39 |
| 8.1. DOCUMENTO IN USCITA CARTACEO.....                                    | 39 |
| 8.2. DOCUMENTO IN USCITA SU PEI.....                                      | 39 |
| 8.3. DOCUMENTO IN USCITA SU XOMAIL.....                                   | 40 |
| 8.4. DOCUMENTO IN USCITA PEC.....                                         | 40 |
| 8.5. PREDISPOSIZIONE.....                                                 | 41 |
| 8.6. OGGETTO DEL DOCUMENTO IN PREDISPOSIZIONE.....                        | 41 |
| 8.7. INDICAZIONE DEL FASCICOLO DI DESTINAZIONE DEL DOCUMENTO.....         | 42 |
| 8.8. INDICAZIONE DELLE AOO DESTINATARIE, ESTERNE E/O INTERNE ALL'AOO..... | 42 |
| 8.9. EVENTUALI NOTE E FILE ACCESSORI.....                                 | 42 |
| 8.10. DOCUMENTO PRINCIPALE E ALLEGATI (ANNESSI/ALLEGATI).....             | 43 |
| 8.11. RIFERIMENTI E SEGUITI AL DOCUMENTO PRINCIPALE.....                  | 43 |
| 8.12. INDICAZIONE DI "DATI SENSIBILI".....                                | 44 |
| 8.13. SELEZIONE RIGUARDO EVENTUALI DATI ANALOGICI.....                    | 44 |
| 8.14. INDICAZIONE DI PRIORITÀ.....                                        | 44 |
| 8.15. REVISIONE.....                                                      | 44 |
| 8.16. FIRMA-PROTOCOLLAZIONE E INVIO DOCUMENTO.....                        | 45 |

## **ALLEGATI**

- A. ABBREVIAZIONI IN USO
- B. INFORMATIVA DI BASE AGLI INTERESSATI
- C. ATTO DI NOMINA – AUTORIZZAZIONE AL TRATTAMENTO DEI DATI
- D. GESTIONE VIOLAZIONI DATI PERSONALI
- E. SCHEDA E MODALITÀ PER IL CORRETTO TRATTAMENTO DEI DATI PERSONALI  
"PARTICOLARI"
- F. DENOMINAZIONE DEL CAMPO "OGGETTO" NEL SISTEMA ADHOC PER LA PREDISPOSIZIONE  
DELLA CORRISPONDENZA ESTERNA/INTERNA
- G. MODULO DI CREAZIONE/VARIAZIONE/CANCELLAZIONE RUOLO
- H. MODULO ANNULLAMENTO DI UN PROTOCOLLO

## **ANNESSI**

- I. LETTERA DI DIRAMAZIONE

**PRIMA PARTE**

**MISURE TECNICHE**

PAGINA INTENZIONALMENTE BIANCA

# 1. GENERALITÀ

Il presente manuale è finalizzato a disciplinare la gestione interna del sistema di protocollo informatico, la gestione documentale, i relativi flussi e a disciplinare il trattamento dei dati personali raccolti e utilizzati dalle Unità organizzative in seno all'AOO - 33° Reggimento Supporto Tattico e Logistico "AMBROSIANO", denominata in seguito 33° AMBROSIANO, fornendo un insieme di regole della per un corretto ed efficace funzionamento del Servizio, è rivolto a tutti gli utenti, ponendosi come strumento di lavoro per la gestione dei documenti, degli affari e dei procedimenti amministrativi che sono chiamati a trattare nell'esercizio delle proprie funzioni/mansioni. In quanto tale gestione che determina la formazione/generazione, lo scambio e la conservazione nell'ambito dei procedimenti amministrativi e l'asse portante dell'AOO. Il funzionamento si basa su:

- le attività di gestione dei documenti, finalizzate alla:
  - registrazione di protocollo, che certifica la provenienza e la data certa di acquisizione del documento, la sua identificazione univoca nell'ambito di una sequenza numerica collegata con l'indicazione (marca) temporale;
  - classificazione, organizzazione, assegnazione, reperimento e conservazione dei documenti amministrativi, formati o acquisiti dalle Amministrazioni nell'ambito del sistema di classificazione d'archivio adottato
- gli archivi (c.d. fascicoli), cioè il luogo in cui si conservano i documenti nelle diverse fasi di gestione, corrente e di deposito, ma anche il "sistema" all'interno del quale i documenti sono organizzati e reciprocamente collegati;
- i flussi documentali, relativi alle attività che supportano la produzione dei documenti e che sostengono i processi primari dell'AOO.

Il Sistema di protocollo si riferisce, quindi, non solo all'insieme dei documenti - con firma digitale e l'impiego della casella di PEC ([rgtstal@postacert.difesa.it](mailto:rgtstal@postacert.difesa.it)) - prodotti o acquisiti da un soggetto produttore nell'esercizio delle sue funzioni ma include anche il sistema per la gestione, cioè l'insieme delle regole, delle procedure e delle risorse per la loro formazione, organizzazione, reperimento, utilizzo e conservazione. Quindi le finalità di questa piattaforma possono essere riassunte nei seguenti punti:

- fornire ad ogni struttura il necessario supporto documentario per lo svolgimento efficiente delle proprie attività e per la testimonianza giuridicamente valida delle stesse;
- garantire la conservazione e la fruizione dei documenti sia ai fini interni che di trasparenza amministrativa e di memoria storica.

In particolare, presente manuale è articolato in questi termini:

- riferimenti normativi e regolamentari in materia;
- ambiente di riferimento;
- gestione del sistema di protocollo informatico @DhOC;
- trattamento dati personali in ambito F.A.;
- titolario e classificazione d'archivio;
- gestione dei documenti in entrata;
- gestione dei documenti in uscita;
- gestione dei documenti interni all'AOO - 33° Reggimento AMBROSIANO.

PAGINA INTENZIONALMENTE BIANCA

## 2. RIFERIMENTI NORMATIVI

- Direttiva 2002/58/CE (trattamento dati personali e tutela della vita privata nel settore delle comunicazioni).
- Reg. UE 2016/679 General Data Protection Regulation (GDPR).
- D. Lgs. 196/2003 (Codice in materia di protezione dei dati personali), modificato e integrato, in particolare dal D. Lgs. 101/2018.
- D. Lgs. 7 marzo 2005, n. 82, Codice dell'Amministrazione Digitale (CAD).
- D. Lgs. 66/2010 Codice dell'Ordinamento Militare (COM).
- DPR 90/2010 Testo Unico Regolamentare in materia di Ordinamento Militare (TUOM).
- D. Lgs. 69/2012 - Modifiche al D. Lgs. 196/03 in attuazione delle Direttive 2009/136/CE, 2009/140/CE e Reg. (UE) 2006/2004.
- Provvedimento n. 467 dell'11 ottobre 2018 del Garante Protezione dei Dati Personali.
- Elenco delle tipologie di trattamento soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ex art. 35, comma 4, del Regolamento (UE) n. 2016/679".
- Circolare n. 2 del 18 aprile 2017 dell'Agenzia per l'Italia digitale (AgID) e relative Linee guida 2020.
- SME, Ordine del giorno all'Esercito n. 8/2024.
- SME, Circ. 1038 Misure di sicurezza tecniche e organizzative, analisi del rischio e valutazione d'impatto sul trattamento dei dati personali, Ed. 2023.
- SME – Circolare 1001, Modalità per l'approntamento delle pubblicazioni dell'Esercito Italiano, Ed. 2016.
- SME – Circolare 1007, Identità visiva dell'Esercito Italiano, Ed. 2016.
- SME – Titolario di archivio dell'Esercito Italiano, Ed. 2006.
- SME - 5867 Abbreviazioni e Sigle di uso autorizzato nell'Esercito, Ed. 2000.
- SME - 5895 Nomenclatore Militare, Ed. 1998.

PAGINA INTENZIONALMENTE BIANCA

## 3. AMBIENTE DI RIFERIMENTO

### 3.1 GENERALITA'

Il giorno 15 settembre 2017, presso l'allora Reggimento Supporto Tattico e Logistico al (HQ) NRDC-ITA, è stato avviato il sistema di protocollo informatico ADHOC con codice SISME E25169. In data 1° giugno 2022, l'Ente ha subito una ridenominazione in 33° Reggimento Supporto Tattico e Logistico AMBROSIANO, mantenendo invariato il Codice Interno AOO - E25169 e il Codice Univoco AOO - AAB71B3, acquisendo il Codice impiego per l'Area Personale 47050, mentre per la parte TRAMAT, Parchi e Commissariato il codice è 25169. Le disposizioni raccolte in questo manuale hanno lo scopo di organizzare e disciplinare l'utilizzo del sistema di protocollo informatico ADHOC, per la gestione del servizio e dei flussi documentali dell'AOO - 33° Reggimento Supporto Tattico e Logistico AMBROSIANO, di seguito denominata 33° AMBROSIANO. In termini generali l'ambiente di riferimento è quello di una P.A., segnatamente un Ente di F.A. (Esercito Italiano) inquadrato nell'ambito del Ministero della Difesa, amministrativamente autonomo ma gerarchicamente subordinato per livelli sia interni, che esterni.

### 3.2 DEFINIZIONI

**Trattamento dei dati personali:** qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione. Ogni utente abilitato all'utilizzo del Sistema Adhoc dovrà avere la piena conoscenza e totale ottemperanza a tutte le norme in materia di protezione dati personali, ai provvedimenti del Garante per la Protezione Dati Personali e alle disposizioni impartite dallo Stato Maggiore Esercito (in qualità di Titolare del trattamento), i soggetti autorizzati al trattamento di dati personali, per designazione del Titolare, devono conoscere, ottemperare e applicare:

- l'ordine di servizio/provvedimento ordinativo che disciplina il trattamento dei dati personali nell'ambito della struttura di appartenenza (Titolare del trattamento);
- le prescrizioni contenute nel registro delle attività di trattamento;
- le misure di sicurezza organizzative e tecniche adottate dal Titolare del trattamento;
- effettuare i trattamenti di dati personali, esclusivamente, con gli strumenti di servizio assegnati, nei luoghi di lavoro designati, durante l'orario di servizio e con le sole procedure autorizzate/previste;
- non effettuare trattamenti non previsti dalle norme o eccedenti l'attività/predisposizioni di servizio;
- effettuare solo trattamenti leciti, secondo le indicazioni e gli ordini derivanti dallo stato giuridico e dal ruolo/incarico rivestito;
- rispettare tutti i principi del trattamento, previsti dalle norme, con particolare riguardo al criterio della "pertinenza" e della "non eccedenza" del trattamento in relazione alla finalità;

- trattare sia i documenti cartacei, sia quelli digitali relativi a trattamento di dati personali, attenendosi strettamente alle misure tecniche, organizzative e di sicurezza stabilite dalla F.A.;
- protezione a mezzo password o, eventualmente, se disposto, di criptazione delle informazioni;
- non trattare dati personali su supporti non autorizzati (e.g.: hardware privato come PC, smartphone, chiavette USB, hd portatili, ecc.) e non trattare dati personali mediante servizi di posta (non solo elettronica) o di clouding non istituzionali;
- rendere l’informativa all’interessato nei casi previsti e acquisire il consenso al trattamento se richiesto, secondo le disposizioni del Titolare;
- procedere prontamente all’aggiornamento e alla cancellazione dei dati secondo la loro natura e finalità, nel rispetto della tempistica stabilita dal registro delle attività di trattamento. Ove tale tempo non fosse definito, il termine di conservazione deve intendersi “fino al soddisfacimento delle esigenze per le quali i dati sono raccolti”;
- assicurarsi che i dati trattati nello svolgimento della propria funzione non siano accessibili/visibili ad altri non autorizzati o non aventi titolo (e.g.: cartelle di lavoro chiuse, monitor non rivolti verso porte o finestre);
- assicurarsi di non lasciare a vista, non esporre, non dimenticare documenti contenenti dati personali nelle proprie aree di lavoro (e.g.: nella stampa, su stampante condivisa, ritirare tempestivamente i documenti stampati per evitare l’accesso a soggetti non abilitati al trattamento);
- nell’uso di strumenti di lavoro condivisi (e.g.: locali/aree di lavoro, hardware come PC e stampante, fax, telefono, posta elettronica, ecc.), accertarsi sempre della non accessibilità dei dati personali in trattazione da parte di personale non autorizzato o non avente titolo (e.g.: effettuare procedure di log out);
- i locali contenenti dati personali (come gli archivi) non devono essere mai di libero accesso e devono sempre avere una regolamentazione/limitazione d’ingresso. Essi, inoltre, non vanno lasciati incustoditi e devono essere sempre chiusi a chiave quando non in uso;
- fermo restando le disposizioni relative all’utilizzo dei servizi informatici di rete, scambio dati, posta elettronica vigenti nella propria organizzazione, accertarsi di non porre in condivisione e/o inviare dati personali a persone non autorizzate o non aventi titolo;
- assicurarsi, anche durante l’eventuale trasporto, di non lasciare incustoditi documenti contenenti dati personali, che devono essere comunque non visibili (fogli piegati o in cartelle/buste chiuse). Stessa precauzione deve essere tenuta per il trasporto di dati su PC o memorie di massa da proteggere sempre con opportune password;
- non produrre/conservare copie non autorizzate dei documenti contenenti dati personali o raccolte a carattere privato, come database, fogli di lavoro, elenchi, fotocopie, ecc.;
- apporre, nella corrispondenza/documentazione concernente dati personali, la dicitura “contiene dati personali da trattare ai sensi del Regolamento (UE) 2016/679 e del D. Lgs. n. 196/2003”;
- quando non indispensabili, omettere o oscurare informazioni (o parti di esse) che

possano essere dati personali o tali da consentire l'identificazione, anche indiretta, dell'individuo;

- porre particolare attenzione alla trattazione di categorie particolari di dati, quali origine razziale, opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale, dati relativi alla salute, vita sessuale/orientamento sessuale, dati genetici/biometrici/giudiziari;
- usare quando possibile e quando disposto, su istruzioni di volta in volta fornite, tecniche di pseudonimizzazione o anonimizzazione per il trattamento dei dati personali;
- riportare al diretto Superiore eventuali casi dubbi o che presentino elementi di novità.

**Protezione:** l'attività atta a garantire adeguata sicurezza, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali ("integrità e riservatezza").

**Dato personale:** qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, , genetica, psichica, del suo stato di salute, delle sue abitudini, lo stile di vita, le relazioni personali e/o la situazione economica.

- Dati comuni: che permettono l'identificazione diretta della persona (es. nome, cognome, immagine) o indiretta (es. codice fiscale, numero telefono, indirizzo IP, numero di targa).
- Dati personali particolari, cd "sensibili" secondo una vecchia denominazione: che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona e religiosi.
- Dati personali relativi alla salute: sono un sottoinsieme della più ampia categoria dei dati soggetti a trattamento speciale (art. 9 GDPR), in grado di rivelare dettagli estremamente privati della persona e, per questo, sottoposti a tutela ulteriormente rafforzata. Tali tipologie di dati sono ampiamente trattati in F.A., non solo dalle articolazioni propriamente sanitarie (infermerie di Corpo). In merito, fermo restando il necessario rispetto di tutte le prescrizioni normative/regolamentari e, in particolare, dell'art. 5 GDPR relativo ai principi del trattamento, si rammenta a titolo di evidenza (non esaustiva delle casistiche possibili) che i dati relativi alla salute, per le finalità previste dal GDPR di cui:
  - all'art. 9, co.2, let "g" (motivi di interesse pubblico rilevante sulla base del diritto) possono essere trattati dai Comandanti di Corpo, secondo le condizioni di liceità di cui all'art. 6, co.1, let "c" (obbligo legale);
  - all'art. 9, co.2, let "i" (motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero) possono essere trattati per obbligo legale dei Comandanti, come per l'emergenza sanitaria in corso da COVID-19;

- all'art. 9, co.2, let "h" (medicina preventiva/del lavoro, valutazione capacità lavorativa del dipendente, diagnosi, assistenza, ecc.), possono essere trattati solo da specifiche categorie di soggetti, stabilite con L. 24/2017 e norme collegate (personale sanitario).
- Dati giudiziari: relativi a condanne penali, reati che possono rivelare la qualità di indagato e/o imputato o connesse misure di sicurezza personali o patrimoniali, obbligo di soggiorno, misure alternative alla detenzione e condanne. La loro trattazione in ambito F.A. deve essere limitata esclusivamente a pochissimi soggetti Autorizzati, esclusivamente in ragione di espresse previsioni di legge. In particolare, attesi i potenziali effetti della non conforme trattazione di tale tipologia di dati su diritti e libertà degli interessati, devono essere adottate le massime precauzioni possibili per garantire un corretto ed essenziale trattamento.

**Interessati**: le persone fisiche cui si riferiscono i dati personali oggetto di trattamento, identificate o identificabili, in modo diretto o indiretto, facendo riferimento ad informazioni come il nome, un numero d'identificazione, dati riguardanti l'ubicazione, un identificativo on-line, oppure uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

**Privacy**: tutti quegli interventi in materia di protezione dei dati personali diretti a minimizzare l'uso dei dati, limitare le finalità e controllarne la diffusione al fine di tutelare la vita privata dei cittadini.

**Titolare del trattamento**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e le modalità di trattamento dei dati personali conformemente al GDPR.

**Autorizzato al trattamento**: Secondo quanto previsto dall'art. 4.10 del GDPR, sono le persone fisiche che effettuano materialmente le operazioni di trattamento sui dati personali. Per queste figure, il Regolamento europeo non prevede l'obbligo di nomina o designazione espressa, per cui la stessa può avvenire con unico atto per più persone e non necessita di firma per accettazione (sebbene sia utile acquisire una firma per presa visione, quale prova della conoscenza dell'incarico e delle istruzioni fornite). Gli Autorizzati devono attenersi strettamente alle istruzioni ricevute e non devono avere alcuna autonomia (altrimenti assumerebbero il ruolo di Responsabili) ma è fondamentale fornire loro, preventivamente, le necessarie istruzioni operative (art. 29 GDPR), informandoli sugli obblighi inerenti alle misure di sicurezza e, più in generale, provvedere alla loro formazione generale in tema privacy e specifica sul trattamento dati inerente alla propria mansione.

**Informativa**: l'atto con il quale il titolare rende edotti gli interessati circa la raccolta, l'utilizzo e la consultazione dei loro dati personali, precisando on che misura essi saranno trattati.

**Consenso**: la manifestazione di libera volontà, specifica, informata dell'interessato, con la quale esprime il proprio assenso, mediante dichiarazione o azione positiva inequivocabile al trattamento dei dati personali che lo riguardano ed è sempre revocabile.

**Rischio**: ogni condizione o situazione che può concorrere alla compromissione della riservatezza, integrità o disponibilità dei dati personali.

### 3.3 IDENTIFICAZIONE E NOMINA DELLE FIGURE CHIAVE

Le figure chiave per la gestione e l'utilizzo del Sistema, con i relativi compiti, sono:

#### **RESPONSABILE DEL SERVIZIO (RDS):**

- garantisce lo svolgimento ed il buon funzionamento degli strumenti dell'organizzazione delle attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali, nel rispetto delle normative vigenti;
- è funzionalmente individuato nell'ambito dell'Ufficio Maggiorità e Personale e si identifica con il Capo Ufficio Maggiorità e Personale/Ufficiale addetto, viene nominato con atto formale del Comandante dell'Ente di appartenenza e registrato secondo norma (Ordine del Giorno e Atto dispositivo,);
- predispone il Manuale, ai fini della gestione dei documenti informatici e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi e provvede alla pubblicazione dello stesso a livello reggimentale;
- attribuisce il profilo agli utenti in base al ruolo rivestito e alle autorizzazioni concesse dal Comandante dell'Ente (trattamento dati personali, giudiziari e sanitari) per l'accesso alle funzioni del sistema di protocollo informatico e di gestione documentale ivi comprese le autori, sulla base delle autorizzazioni ;
- autorizza le operazioni di annullamento delle registrazioni di protocollo di cui all'articolo 54 del DPR 445/2000;
- autorizza l'apertura del registro d'emergenza dopo aver accertato l'indisponibilità del sistema e, dopo aver verificato il ripristino del suo corretto funzionamento, ne dispone la chiusura;
- garantisce che le operazioni di Registrazione di protocollo e di Segnatura di protocollo si svolgano nel rispetto delle disposizioni del DPR;
- garantisce la corretta produzione e la conservazione del Registro giornaliero di protocollo, anche con sistema automatico di firma;
- garantisce il buon funzionamento degli strumenti e dell'organizzazione dell'attività di Registrazione di protocollo, incluse le funzionalità di accesso;
- vigila sull'osservanza delle disposizioni del DPR da parte del personale autorizzato o incaricato.

**VICARIO RDS/AMMINISTRATORE** : È nominato dal Comandante, può accedere ai profili di configurazione di base del sistema, sotto il diretto controllo del RDS;

**OPERATORE DI PROTOCOLLO:** Riceve il ruolo dal RDS e svolge i seguenti compiti

- protocolla in entrata i documenti informatici in arrivo sulla casella di posta PEC, PEIN, sulla postazione E-MESSAGE e XOMAIL;
- scansiona e registra i documenti cartacei in arrivo al Reggimento.

### 4. GESTIONE DEL SISTEMA DI PROTOCOLLO INFORMATICO

Il flusso della corrispondenza (posta elettronica certificata) in entrata è gestito dal Nucleo Maggiorità con le modalità riportate nei successivi paragrafi.

## 4.1 RUBRICA

Il sistema "ADHOC" utilizza una rubrica che contiene gli indirizzi di tutte le UO ed AOO, per individuare sia il mittente che i destinatari dei singoli documenti. La rubrica è già popolata da un numero consistente di indirizzi dell'area della Difesa e della Pubblica Amministrazione (IPA). Cionondimeno, l'elenco non può essere esaustivo di tutti i possibili destinatari della corrispondenza prodotta e dunque risulta necessario disciplinarne la gestione (inserimento, cancellazione e modifica degli indirizzi). Le UO che hanno necessità di scambiare corrispondenza con Enti o privati non presenti in rubrica, devono chiedere l'inserimento al **RDS**. La richiesta deve pervenire tramite e-mail all'indirizzo [ceemessage@rgtstl33.esercito.difesa.it](mailto:ceemessage@rgtstl33.esercito.difesa.it), contenente, oltre alla e-mail del destinatario, più informazioni possibili (in particolare città, indirizzo, ecc.).

## 4.2 ASSISTENZA E CREAZIONE E VARIAZIONE DEI RUOLI

Le richieste di assistenza dovranno pervenire attraverso l'inoltro di un ticket, tramite



il sito del Reggimento ([33° Ambrosiano - NU.GE.SI.INF.](#) ADHOC) con la descrizione particolareggiata della problematica ed eventuali *screen shoot* qualora il sistema evidenziasse dei "codici errore" o "maschere di avviso". La Creazione/Variazione di ruoli e di dati anagrafici si rendono necessarie in tutti quei casi che comportano una modifica della struttura AOO (aggiunta, modifica, soppressione di UO, ecc.) o delle singole UO (ridenominazione, trasferimento di personale in entrata o in uscita, ecc.) nelle quali essa si articola. La richiesta di creazione/variazione dei ruoli da parte del **Responsabile della UO** si concretizzerà attraverso l'inoltro del ticket di cui sopra, avendo cura di allegare il modulo in Allegato G, ove ne ricorrano le condizioni e previa autorizzazione del **RDS** si procederà ad evadere la richiesta. Dopodiché il personale titolare del ruolo, sarà convocato presso il nucleo maggioranza per la compilazione dell'anagrafica e per la presa visione dell'assunzione di responsabilità relativamente alle norme in vigore per il trattamento dei dati personali.

## 4.3 DELEGHE

Le deleghe si rendono necessarie ogni volta che il titolare di un ruolo si assenti e debba essere sostituito, in quel ruolo, da personale appositamente designato (ad esempio, il Capo Ufficio dall'Ufficiale Addetto/Capo Sezione/SU designato, ecc.).

**L'utilizzo delle deleghe risulta di primaria importanza per assicurare la continuità e correttezza dei flussi documentali.** La gestione delle stesse è un'opzione PRIORITARIA ESERCITABILE DIRETTAMENTE dai singoli **Responsabili delle UO**, che, prima di assentarsi attivano la funzione, qualora per qualsivoglia motivo il Responsabile dell'UO attraverso l'utilizzo della VPN voglia mantenere a se funzioni. Solo in casi di emergenza, quale lo stato di malattia dell'interessato o improvvise assenze non preventivate, la delega può essere attivata dal **RDS**.

#### **4.4 GENERAZIONE E ANNULLAMENTO DI UN PROTOCOLLO**

Il Sistema Adhoc garantisce la non modificabilità delle RDP (Registrazione di protocollo) in quanto:

- il Servizio prevede l'obbligatorietà di compilazione e la non modificabilità dei campi Oggetto, Segnatura Mittente e la UO assegnataria per competenza/conoscenza;
- il Sistema, con carattere di automaticità ed in maniera non modificabile, registra la data della RDP ed il numero progressivo di protocollo sulla AOO-AAB71B3 (cod. univoco);
- il Sistema non consente di effettuare una RDP (Registrazione di protocollo) da parte di un Operatore se prima lo stesso non abbia portato a compimento la RDP precedente con la relativa SDP (Segnatura Di Protocollo).

In nessun caso il Sistema consente di modificare le informazioni relative alla RDP di un documento in entrata una volta che l'Operatore ne ha eseguito la Protocollazione i dati inseriti nella maschera di Predisposizione dei documenti in uscita possono essere modificati prima della Protocollazione e in fase di Revisione. Il Sistema mantiene, nel tempo, traccia di tutte le informazioni legate all'Operatore, alla data e all'ora in cui sono effettuate le operazioni di modifica.

Nel caso in cui ci sia la necessità di annullare un protocollo, il **Responsabile della UO** interessata, dovrà inoltrare un ticket, dal portale del Reggimento, come indicato al para. 4.2 avendo cura di allegare il modulo in Allegato H, dopodiché ove ne ricorrano le condizioni e previa autorizzazione del **RDS** si procederà all'annullamento.

#### **4.5 PROTOCOLLAZIONE IN REGIME DI "EMERGENZA"**

Qualora ci fossero interruzioni gravi e prolungate nel tempo del Sistema "Adhoc", sarà cura dell'RDS o del suo Vicario avviare la procedura di "Emergenza" comunicandolo alle UO, agli EDRC dipendenti e alle S.A. Al determinarsi di una interruzione del Sistema "Adhoc", l'**RDS/Vicario/Amministratore di Sistema** sentiti gli Amministratori del Server Centrale in Roma e valutata la gravità e non veloce ripresa del Servizio, si procederà ad attivare il protocollo di emergenza seguendo le indicazioni fornite dal Nucleo Centrale di Amministrazione e le indicazioni di Download e Setup alla voce - GESTIONE PROTOCOLLO EMERGENZA E PARTICOLARE del manuale di amministrazione del programma.

#### **4.6 RILASCIO DI COPIA INFORMATICA - "GLIFO"**

Il sistema Adhoc consente il supporto alla gestione del **"GLIFO"** (contrassegno generato elettronicamente) sui documenti prodotti dal sistema di protocollo

informatico e gestione documentale, nell'ambito delle disposizioni dell'art. 23ter comma 5 del Codice dell'Amministrazione Digitale e della Circolare dell'Agenzia per l'Italia Digitale n. 62 del 30 aprile 2013 "Linee guida per il contrassegno generato elettronicamente". Si tratta di un **QR-Code** riportato sulla prima pagina del documento il quale consente, attraverso un apposito "**KIT**" di controllo (disponibile alla pagina <http://www.difesa.it/Protocollo/Pagine/Glifo.aspx> o attraverso un lettore **QR-Code** puntando direttamente sul Glifo sopra indicato), di verificare la conformità e titolarità per la richiesta di una copia informatica. E' necessario disporre della copia cartacea del documento sul quale è stato apposto il contrassegno elettronico; in questo caso, sarà segnalato anche l'indirizzo del presente sito. Quindi occorre effettuare la scansione della prima pagina del documento (quella contenente il contrassegno). La scansione va effettuata in **toni di grigio**, con risoluzione di **300 dpi** e deve produrre un file **in formato PDF**. Il file così ottenuto va inviato all'indirizzo segnalato sul documento cartaceo con il contrassegno, utilizzando una casella di posta elettronica certificata. Non verranno esaminate richieste pervenute da canali diversi dalla posta elettronica certificata. Il messaggio inviato deve avere come oggetto: **Richiesta Documento** e in allegato il file PDF prodotto dalla scansione. Dopo aver trasmesso la richiesta alla casella di posta elettronica certificata indicata nel documento cartaceo, l'Ente interessato procederà alla lavorazione della medesima. A seconda della lavorazione intrapresa, potrà essere trasmesso l'originale informatico del documento richiesto, ovvero un messaggio contenente le informazioni ritenute pertinenti. **Attenzione:** Non è possibile allegare più di una scansione per messaggio, pertanto se si volessero richiedere due documenti occorrerà inviare due diverse mail di richiesta.

## **SECONDA PARTE**

### **MISURE DI PROTEZIONE**

PAGINA INTENZIONALMENTE BIANCA

## 5. TRATTAMENTO DEI DATI PERSONALI IN AMBITO F.A.

### 5.1 GENERALITÀ

La F.A., nell'ambito delle competenze attribuite dal D. Lgs. 66/2010 "Codice dell'Ordinamento Militare" e dal DPR 15 marzo 2010, n. 90, recante "Testo Unico delle disposizioni regolamentari in materia di ordinamento militare", cura le attività giuridiche, amministrative e gestionali relative al proprio personale militare e civile delle varie categorie, con adozione dei correlati provvedimenti in materia di reclutamento, di stato giuridico, di avanzamento, di impiego, di disciplina, di matricola e documentazione caratteristica, di trattamento economico, di assistenza morale e materiale, nonché di ogni aspetto connesso alle esigenze logistiche del personale, con particolare riferimento al trattamento sanitario, fino al momento del collocamento in congedo (massimo periodo di *data retention*). Il trattamento dei dati personali<sup>14</sup> effettuato nella struttura del Titolare per il trattamento dati avviene, normalmente, nello svolgimento di rapporti di impiego in regime di diritto pubblico (art. 3, comma 1, del D. Lgs. 30 marzo 2001, n. 165), rimanendo, pertanto, escluso l'obbligo sul consenso in quanto il trattamento è effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti (art. 6, paragrafo 1, lett. e del GDPR). Inoltre, il Titolare di F.A. può trattare, in via residuale e nel rispetto delle norme, i dati personali di soggetti civili o militari non in rapporto di dipendenza con il Titolare stesso. Il trattamento è lecito solo nella misura in cui ricorre almeno una delle condizioni esplicitate dall'art. 6, paragrafo 1 del Regolamento e, in particolare, quella della lett. e, che esprime la liceità quando il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento (nel caso di specie, lo SME).

### 5.2 TEMPI DI CONSERVAZIONE - "DATA RETENTION"

Il tempo di conservazione dei dati personali (personal *data retention*) non può essere indeterminato/indefinito. L'art. 13 del Reg. UE 2016/679 (GDPR) prevede che il titolare del trattamento informi gli interessati circa il periodo di conservazione dei dati personali, oppure, se ciò non è possibile, individui i "criteri utilizzati per determinare tale periodo" (comma 2, lett. a).

Inoltre, l'art. 5 lett. e del GDPR stabilisce che i dati:

- debbano essere conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati;
- possano essere conservati per periodi più lunghi, a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse (il GDPR però non specifica cosa si intende per "pubblico interesse" né in quali ambiti si applica il concetto), di ricerca scientifica, storica o a fini statistici, conformemente all'art. 89, paragrafo 1 e fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal GDPR a tutela dei diritti e delle libertà dell'interessato (c.d. limitazione della conservazione). Il Garante ha emanato alcuni provvedimenti per supportare il titolare nella fissazione dei termini di conservazione dei dati, posto che, alla

scadenza del termine di conservazione, il dato deve essere cancellato (da tutti i supporti, compreso i backup), oppure anonimizzato. Pertanto, a carattere generale, è necessario procedere prontamente all'aggiornamento e alla cancellazione dei dati secondo la loro natura e finalità, nel rispetto dei tempi stabiliti dal Titolare. Ove tale tempo non fosse definito, il termine di conservazione deve intendersi "il più breve possibile" o "fino al soddisfacimento delle esigenze per le quali i dati sono raccolti". L'art. 17 GDPR (recante diritto alla cancellazione, diritto all'oblio) offre alcune linee guida per la cancellazione dei dati personali, che dovrà essere effettuata quando:

- gli stessi non sono più necessari per le finalità per le quali sono stati raccolti/trattati ovvero quando siano stati trattati illegalmente;
- l'interessato revoca il proprio consenso;
- l'interessato si oppone al trattamento e non vi sono motivi legittimi per il trattamento;
- in ottemperanza ad un obbligo legale, ai sensi del diritto dell'Unione o nazionale, a cui è soggetto il responsabile del trattamento.

L'obbligo di cancellazione non si applica se i dati personali sono (ancora) necessari per:

- esercitare il diritto alla libertà di espressione e di informazione;
- adempiere a un obbligo legale richiesto dal diritto dell'Unione o degli Stati membri a cui è soggetto il responsabile del trattamento, o svolgere un compito di interesse pubblico o nell'esercizio di un'autorità pubblica delegata al responsabile del trattamento;
- motivi di interesse pubblico nel campo della sanità pubblica;
- fini di archiviazione di interesse pubblico, fini di ricerca scientifica o storica o fini statistici;
- far valere, esercitare o difendere azioni legali.

L'art. 18 GDPR (diritto di limitazione del trattamento) istituisce invece la facoltà dell'interessato, al verificarsi di determinate condizioni, di chiedere al responsabile del trattamento di limitare il trattamento dei dati, di fatto chiedendone la cancellazione. Ciò premesso, in ambito Forza Armata **non devono essere raccolti e conservati i dati personali, a qualunque titolo trattati, per i quali non si abbia necessità di trattamento concreta e attuale**. A tal riguardo, fatte salve le ulteriori specifiche disposizioni del Titolare, in via generale, i dati relativi al:

- personale dipendente, saranno conservati fino al termine del rapporto di servizio del dipendente con l'Ente;
- personale non dipendente, saranno conservati fino al cessare dell'esigenza per cui i dati sono stati trattati.

I dati personali trattati da ogni Ente, devono essere sottoposti a periodica revisione, almeno con frequenza annuale, provvedendo ad avviare a cancellazione/distruzione quelli non più necessari, in coerenza con quanto indicato dal Titolare o previsto dal piano di conservazione e nei massimali di scarto. Nelle more della definizione di uno standard tecnico specifico, relativamente alle modalità di cancellazione/distruzione per i dati personali (sia digitali che analogici) comunque trattati dall'Ente, trovano

applicazione gli strumenti e le procedure già in uso in F.A. Al riguardo, si osserva che, secondo il GDPR, il Titolare del trattamento può optare per la cancellazione/distruzione fisica (da prediligere come scelta di F.A.) o, in alternativa, procedere all'anonimizzazione dei dati (annullare il legame tra l'interessato ed i dati allo stesso associato).

### 5.3

#### **ORGANIZZAZIONE AOO - 33° AMBROSIANO**

Indirizzo: Via per Busto, 20 - 21058 Solbiate Olona (VA)

Ente di Appartenenza: Brigata di Supporto al (HQ) NRDC-ITA

Codice Interno dell'AOO: E25169

Codice Univoco dell'AOO: AAB71B3

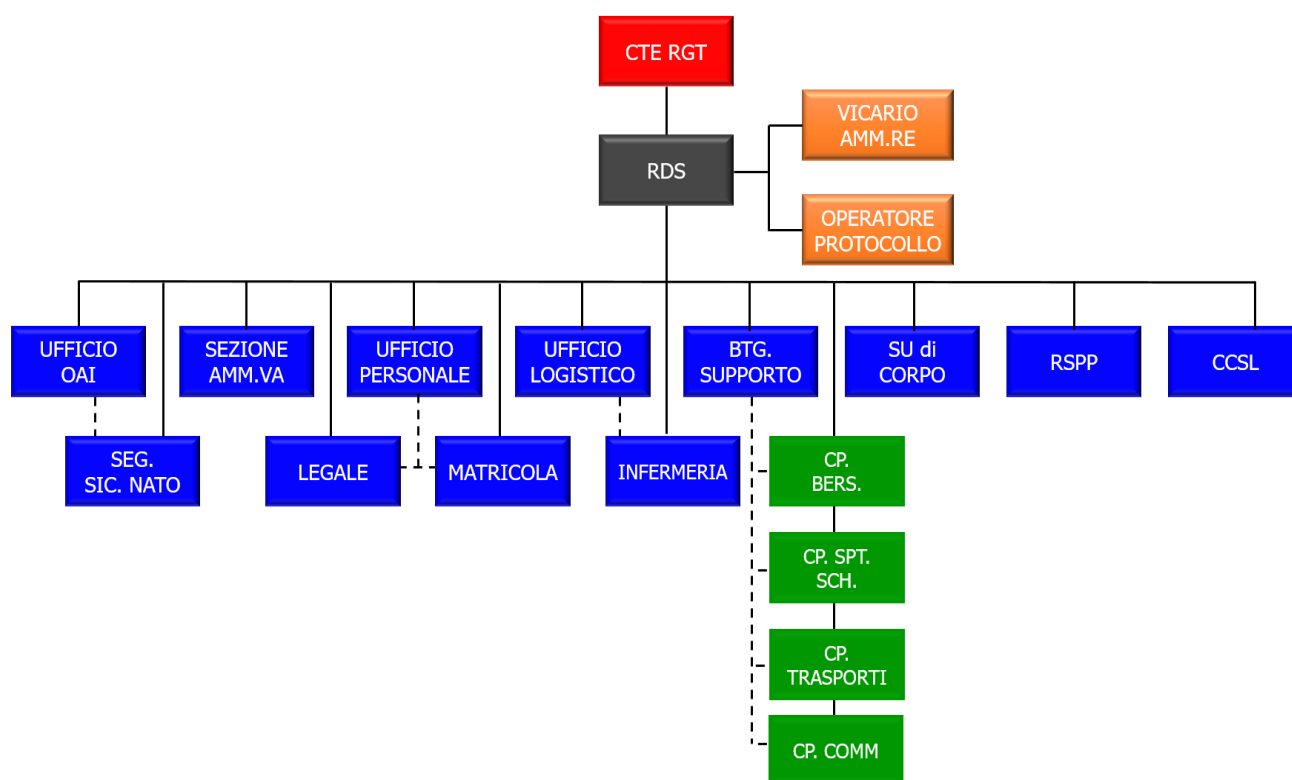
Responsabile del Servizio: Capitano Fabio Zappia

Telefono: 0331-346410

Fax: 0331-323497

E-mail istituzionale: rgtstl33@esercito.difesa.it

E-mail di Posta Certificata: rgtstal@postacert.difesa.it



## 5.4 COMPTITI E RESPONSABILITÀ

Sebbene per ordine del Sig. Capo di SME tutti i soggetti effettivi alla F.A. sono potenzialmente Autorizzati al trattamento dati personali, nell'ambito della specifica organizzazione di F.A. i compiti e le responsabilità sono adeguatamente ripartiti, al fine di garantire la correttezza formale e sostanziale del trattamento. A tal riguardo, in via generale e fatte salve le ulteriori specifiche disposizioni:

- il Titolare del trattamento dei dati personali è lo Stato Maggiore dell'Esercito come persona giuridica nella sua interezza;
- pertanto, alle sue articolazioni, come precedentemente indicato, competono le decisioni in ordine alle finalità, alle modalità del trattamento dei dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;
- analogamente, qualunque azione di un'articolazione dello SME produce effetti in materia di trattamento dati personali, anche quando non coordinata o emanata dal I RRAGEP quale referente del Titolare.

Ai Comandanti di Corpo di tutti gli EDRC di F.A., compete garantire gli aspetti di natura "esecutiva" del trattamento dei dati, nello svolgimento delle attività della propria competenza funzionale. In dettaglio, ai Comandanti di Corpo sono assegnati i seguenti compiti:

- rispettare e far rispettare il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio relativo alla protezione delle persone fisiche, con riguardo al trattamento dei dati personali, che troverà applicazione dal 25 maggio 2018;
- rispettare e far rispettare il D. Lgs. 196/2003, recante "Codice in materia di protezione dei dati personali" e successive modifiche e integrazioni;
- rispettare e far rispettare le disposizioni dell'art. 4 del Decreto Legislativo 14 marzo 2013, n. 33, citato nelle premesse, con particolare riferimento agli obblighi di rendere non intelligibili i dati personali che non siano pertinenti e quelli sensibili/giudiziari che non siano indispensabili, rispetto alle specifiche finalità di trasparenza sancite dal decreto legislativo medesimo;
- accertare che i dati personali siano trattati esclusivamente per il perseguimento delle finalità istituzionali dell'Esercito Italiano e nel rispetto delle prescrizioni di cui agli artt. da 1053 a 1075 del DPR 15 marzo 2010, n. 90, recante "Testo Unico delle disposizioni regolamentari in materia di Ordinamento Militare";
- assicurarsi che i dati personali siano conservati in una forma che consenta l'identificazione dell'interessato, per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati e, comunque, non eccedente il periodo di conservazione previsto;
- rispettare e far rispettare i provvedimenti resi dall'Autorità Garante, in materia di tutela delle persone rispetto al trattamento di dati, con specifico riferimento a quelli particolari di cui all'articolo 9 del Regolamento, attese le rilevanti finalità di interesse pubblico perseguite;
- rendere edotto il personale direttamente dipendente, in merito alla inutilizzabilità dei dati personali trattati in violazione della disciplina normativa e regolamentare vigente in materia.

## 5.5 TRATTAMENTO DEI DATI PERSONALI

Come espressamente indicato dal GDPR si definiscono dati personali (art. 4, n.1) le informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona fisica (interessato) e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, ecc. Per trattamento dei dati personali (GDPR art. 4, n.2) si intende qualsiasi operazione o insieme di operazioni applicate a dati personali o insieme di dati personali. Esse consistono nella raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento, modifica, estrazione, raffronto/interconnessione, consultazione, uso, comunicazione/trasmissione, diffusione, limitazione/cancellazione, distruzione. Ogni utente abilitato all'utilizzo del Sistema Adhoc dovrà avere la piena conoscenza e totale ottemperanza a tutte le norme in materia di protezione dati personali, ai provvedimenti del Garante per la Protezione Dati Personali e alle disposizioni impartite dallo Stato Maggiore Esercito (in qualità di Titolare del trattamento), i soggetti autorizzati al trattamento di dati personali, per designazione del Titolare, devono conoscere, ottemperare e applicare:

- l'ordine di servizio/provvedimento ordinativo che disciplina il trattamento dei dati personali nell'ambito della struttura di appartenenza (Titolare del trattamento);
- le prescrizioni contenute nel registro delle attività di trattamento;
- le misure di sicurezza organizzative e tecniche adottate dal Titolare del trattamento;
- effettuare i trattamenti di dati personali, esclusivamente, con gli strumenti di servizio assegnati, nei luoghi di lavoro designati, durante l'orario di servizio e con le sole procedure autorizzate/previste;
- non effettuare trattamenti non previsti dalle norme o eccedenti l'attività/predisposizioni di servizio;
- effettuare solo trattamenti leciti, secondo le indicazioni e gli ordini derivanti dallo stato giuridico e dal ruolo/incarico rivestito;
- rispettare tutti i principi del trattamento, previsti dalle norme, con particolare riguardo al criterio della "pertinenza" e della "non eccedenza" del trattamento in relazione alla finalità;
- trattare sia i documenti cartacei, sia quelli digitali relativi a trattamento di dati personali, attenendosi strettamente alle misure tecniche, organizzative e di sicurezza stabilite dalla F.A.;
- protezione a mezzo password o, eventualmente, se disposto, di criptazione delle informazioni;
- non trattare dati personali su supporti non autorizzati (e.g.: hardware privato come PC, smartphone, chiavette USB, hd portatili, ecc.) e non trattare dati personali mediante servizi di posta (non solo elettronica) o di clouding non istituzionali;
- rendere l'informativa all'interessato nei casi previsti e acquisire il consenso al trattamento se richiesto, secondo le disposizioni del Titolare;
- procedere prontamente all'aggiornamento e alla cancellazione dei dati secondo la loro natura e finalità, nel rispetto della tempistica stabilita dal registro delle attività di trattamento. Ove tale tempo non fosse definito, il termine di conservazione deve intendersi "fino al soddisfacimento delle esigenze per le quali i dati sono raccolti";
- assicurarsi che i dati trattati nello svolgimento della propria funzione non siano accessibili/visibili ad altri non autorizzati o non aventi titolo (e.g.: cartelle di lavoro chiuse, monitor non rivolti verso porte o finestre);

- assicurarsi di non lasciare a vista, non esporre, non dimenticare documenti contenenti dati personali nelle proprie aree di lavoro (e.g.: nella stampa, su stampante condivisa, ritirare tempestivamente i documenti stampati per evitare l'accesso a soggetti non abilitati al trattamento);
- nell'uso di strumenti di lavoro condivisi (e.g.: locali/aree di lavoro, hardware come PC e stampante, fax, telefono, posta elettronica, ecc.), accertarsi sempre della non accessibilità dei dati personali in trattazione da parte di personale non autorizzato o non avente titolo (e.g.: effettuare procedure di logout);
- i locali contenenti dati personali (come gli archivi) non devono essere mai di libero accesso e devono sempre avere una regolamentazione/limitazione d'ingresso. Essi, inoltre, non vanno lasciati incustoditi e devono essere sempre chiusi a chiave quando non in uso;
- fermo restando le disposizioni relative all'utilizzo dei servizi informatici di rete, scambio dati, posta elettronica vigenti nella propria organizzazione, accertarsi di non porre in condivisione e/o inviare dati personali a persone non autorizzate o non aventi titolo;
- assicurarsi, anche durante l'eventuale trasporto, di non lasciare incustoditi documenti contenenti dati personali, che devono essere comunque non visibili (fogli piegati o in cartelle/buste chiuse). Stessa precauzione deve essere tenuta per il trasporto di dati su PC o memorie di massa da proteggere sempre con opportune password;
- non produrre/conservare copie non autorizzate dei documenti contenenti dati personali o raccolte a carattere privato, come database, fogli di lavoro, elenchi, fotocopie, ecc.;
- apporre, nella corrispondenza/documentazione concernente dati personali, la dicitura "contiene dati personali da trattare ai sensi del Regolamento (UE) 2016/679 e del D. Lgs. n. 196/2003";
- quando non indispensabili, omettere o oscurare informazioni (o parti di esse) che possano essere dati personali o tali da consentire l'identificazione, anche indiretta, dell'individuo;
- porre particolare attenzione alla trattazione di categorie particolari di dati, quali origine razziale, opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale, dati relativi alla salute, vita sessuale/orientamento sessuale, dati genetici/biometrici/giudiziari;
- usare quando possibile e quando disposto, su istruzioni di volta in volta fornite, tecniche di pseudonimizzazione o anonimizzazione per il trattamento dei dati personali;
- riportare al diretto Superiore eventuali casi dubbi o che presentino elementi di novità.

## 5.6 INFORMATIVA - PARTICOLARI ADEMPIMENTI

|                                                                                     |                                                                                                                                                                                                                                                        |
|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <b>Informativa di base agli interessati, ai sensi degli artt. 13 e 14 del Reg. (UE) 2016/679 (GDPR), per il personale in rapporto di dipendenza di servizio o impiego con il Titolare del trattamento dati personali della F.A. - vers. giu. 2021.</b> |
|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

1. Ai sensi degli articoli 13 e 14 del Reg. UE 679/2016 (GDPR), si informano gli interessati che il trattamento dei dati personali da loro forniti o, comunque, acquisiti nel corso dello svolgimento dell'attività amministrativa, è finalizzato esclusivamente all'espletamento delle attività istituzionali del Titolare, in particolare per la gestione del rapporto di impiego e servizio. Il trattamento dei dati personali, particolari e giudiziari avverrà a cura del personale a ciò

appositamente autorizzato, secondo le disposizioni tecniche e di sicurezza impartite dal Titolare, con l'utilizzo di procedure parzialmente informatizzate e con l'ausilio di banche-dati automatizzate, nei modi e nei limiti necessari per il perseguimento delle finalità per cui i dati personali e particolari sono raccolti e/o successivamente trattati; ciò anche nel caso si renda necessaria la comunicazione a terzi, ai sensi delle norme vigenti.

2. Il conferimento di tali dati è obbligatorio e indispensabile ai fini delle attività istruttorie connesse con i procedimenti amministrativi di competenza del Titolare, per garantire gli adempimenti connessi dal rapporto di lavoro/servizio, per adempiere a obblighi legali del Titolare, per l'esecuzione di compiti di interesse pubblico o connesso con l'esercizio di pubblici poteri di cui è investito il Titolare. Per questo motivo, i trattamenti suesposti hanno condizione di liceità che prescinde dal consenso dell'interessato.
3. Per quanto precede, si comunica che:
  - a. il Titolare del trattamento è lo Stato Maggiore dell'Esercito, con sede in Roma 00187, via XX Settembre, 123/A. Il Titolare può essere contattato a mezzo *e-mail* ai seguenti indirizzi:
    - b. posta elettronica ordinaria: *statesercito@esercito.difesa.it*
    - c. posta elettronica certificata: *statesercito@postacert.difesa.it*
  - d. il **Referente del Responsabile della Protezione dei Dati personali è il Capo del I Reparto dello SME, con sede in Roma 00187 in via XX Settembre 123/A e può essere contattato via *e-mail* all'indirizzo: *smelegale@esercito.difesa.it***
  - e. il Responsabile per la Protezione dei Dati personali, come reso noto sul sito istituzionale *www.difesa.it*, può essere contattato a mezzo *e-mail* ai seguenti indirizzi:
    - i. posta elettronica ordinaria: *rpd@difesa.it*
    - ii. posta elettronica certificata: *rpd@postacert.difesa.it*
  - f. la base giuridica del trattamento dei dati personali effettuato dal Titolare è costituita, principalmente, dal D.Lgs. 66/2010 Codice dell'Ordinamento Militare (COM) e nel DPR 90/2010 Testo Unico dell'Ordinamento Militare (TUOM) (e, più in particolare, agli artt. da 1053 a 1075 TUOM) e norme collegate. Il trattamento dati in esame è pertanto conforme alle previsioni del GDPR alle fattispecie di cui:
    - i. all'art. 6, co.1, let. b), c), d), e), f) per i dati comuni;
    - ii. all'art. 9, co. 2, let b), c), f), g), h), i) per le categorie particolari di dati;
    - iii. all'art. 10, relativamente a condanne penali e reati o connesse misure di sicurezza;
  - g. le finalità del trattamento sono direttamente collegate alla gestione del rapporto di impiego e servizio, per finalità connesse e/o strumentali allo svolgimento delle attività istituzionali del Titolare, normativamente previste o nell'interesse del Titolare stesso;
  - h. nel rispetto delle finalità, le tipologie di dati oggetto del trattamento sono:

- i. "dati comuni", ai sensi dell'art. 4 GDPR, in particolare quelli anagrafici, familiari, fiscali, amministrativi, d'impiego, curriculari, disciplinari;
  - ii. "categorie particolari di dati", ai sensi art. 9 GDPR, in particolare dati relativi alla salute, quali dati clinici, medico-legali, vaccinali, psicologici, psico-attitudinali e biometrici;
  - iii. "dati giudiziari", ai sensi art. 10 GDPR, solo nel caso eventuali condanne penali e connesse misure di sicurezza;
- i. i dati personali saranno trattati solo dal personale con competenze tecniche adeguate, all'uopo appositamente formato e specificatamente autorizzato, osservando scrupolosamente le misure di sicurezza disposte per garantire integrità, riservatezza e disponibilità dei dati personali;
- j. non vengono effettuati trattamenti di dati personali mediante l'ausilio di processi decisionali automatizzati, compresa la profilazione, ai sensi dell'art. 4, n. 4 del GDPR;
- k. i dati personali potranno essere comunicati da soggetti operanti in qualità di Titolari e Contitolari del trattamento (quali, a solo titolo esemplificativo e non esaustivo, altri Ministeri, Autorità Giudiziaria, altre Forze Armate e/o di Polizia, strutture Sanitarie, INPS, INAIL, Agenzia dell'Entrate ed ogni altro soggetto pubblico legittimato a trattare i dati), conformemente alle norme vigenti e/o agli eventuali accordi legali. Non è prevista la diffusione di dati personali;
- l. i dati potranno essere trasferiti in paesi Terzi solo se i medesimi hanno aderito alle clausole contrattuali tipo ai sensi dell'art. 46, par. 2, lett. c) e d), o alle norme vincolanti per l'impresa di cui all'art. 47 del GDPR o nel rispetto delle misure derogatorie di cui all'art. 49 del GDPR, laddove consentito ai sensi degli articoli da 1053 a 1075 del D.P.R. n. 90/2010;
- m. nel rispetto delle finalità pubbliche per le quali i relativi dati sono trattati, ivi compresa la tutela degli interessi dell'Amministrazione della Difesa presso le competenti sedi giudiziarie, i dati personali saranno conservati per il tempo strettamente necessario decorso il quale gli stessi saranno distrutti, cancellati o resi anonimi, con le procedure tecniche determinate dal Titolare;
- n. ai sensi del GDPR, sulla base delle condizioni di legittimazione e delle modalità con la quale viene posto in essere il trattamento dati personali, qualora ne ricorrano i presupposti, l'interessato potrà esercitare i diritti riconosciuti dalla legge e, in particolare, il diritto di:
  - i. ottenere l'accesso ai suoi dati personali;
  - ii. chiedere la rettifica o la cancellazione ovvero la limitazione del trattamento;
  - iii. opporsi al trattamento;
  - iv. chiedere la portabilità dei propri dati personali;
  - v. revocare, l'eventuale consenso, quando sia stato richiesto, sebbene tale revoca non pregiudichi i trattamenti precedenti.

La relativa istanza dovrà essere formulata al Referente del Titolare, ai recapiti di cui al punto 3;

- o. gli interessati che ritengano che il trattamento dei dati personali a loro riferiti venga effettuato in violazione delle disposizioni di cui al Reg. UE 679/16 potranno presentare l'eventuale reclamo all'Autorità Garante per la protezione dei dati personali, in qualità di Autorità di controllo, con sede in Piazza Venezia n. 11, Scala B – 00187 Roma, o agli indirizzi *e-mail*: [garante@gpdp.it](mailto:garante@gpdp.it); [protocollo@pec.gpdp.it](mailto:protocollo@pec.gpdp.it).
- p. Ulteriori informazioni e dettagli sono reperibili sul sito *intranet* di F.A. alla sezione dedicata alla "Protezione dati personali", all'indirizzo: [https://intranet.esercito.difesa.it/it/prot\\_dati.page](https://intranet.esercito.difesa.it/it/prot_dati.page).

---

PER PRESA VISIONE

GRADO \_\_\_\_\_ COGNOME \_\_\_\_\_ NOME \_\_\_\_\_

LUOGO \_\_\_\_\_ DATA \_\_\_\_\_ FIRMA \_\_\_\_\_

#### 5.6.1 PARTICOLARI ADEMPIMENTI

Con riferimento alla nomina degli "autorizzati" al trattamento dati personali in ambito F.A., in relazione ad ogni EDCR i Comandanti sono competenti alla cd. nomina.

Pertanto:

- il personale "autorizzato" deve essere preventivamente istruito allo scopo (All. B);
- è indispensabile che ogni soggetto sia autorizzato solo alla specifica attività di trattamento dati assegnata e alla categoria di dati trattati, in considerazione delle relative finalità;
- ciascun soggetto può essere autorizzato per differenti attività di trattamento (All. C);
- sono possibili nomine di più soggetti contemporaneamente nello stesso atto, sia per lo stesso tipo di trattamento, che per trattamenti di natura diversa.

Nella gestione della corrispondenza tramite sistema *Adhoc* è stato rilevato che, talvolta, nel cosiddetto "cono d'ombra" dell'operatore, soggetti non aventi causa possano, con una semplice ricerca, ancorché non raggiungere il testo di un documento non destinato a loro, leggerne l'oggetto, che potrebbe riportare informazioni di soggetti terzi, eccedenti le finalità del trattamento. In tale quadro, occorre rammentare che, le norme in materia di *privacy* impongono il rispetto del principio di adeguatezza, pertinenza e limitazione, rispetto alla necessità (la cosiddetta "minimizzazione") dei dati trattati, di cui l'art. 5 del Reg. UE 679/2016 GDPR. Ciò premesso, si sottolinea, a carattere generale, l'importanza della corretta/opportuna denominazione degli atti (analogici/digitali), atteso il successivo trattamento (anche informatizzato), avendo a riferimento sia la necessità di proteggere le informazioni personali degli interessati, sia i meccanismi di funzionamento dei relativi strumenti, anche informatici, di trattamento. Inoltre, più in

dettaglio, è opportuno che gli operatori *Adhoc*, nella predisposizione dei documenti sul citato sistema provvedano:

- alla spunta “dati sensibili”, in tutti i casi previsti;
- alla corretta compilazione del campo oggetto, inserendo solo gli elementi assolutamente essenziali dell’atto, evitando la contemporanea presenza di dati personali e notizie “sensibili” o non minimizzate rispetto alla finalità dell’atto (All. F).

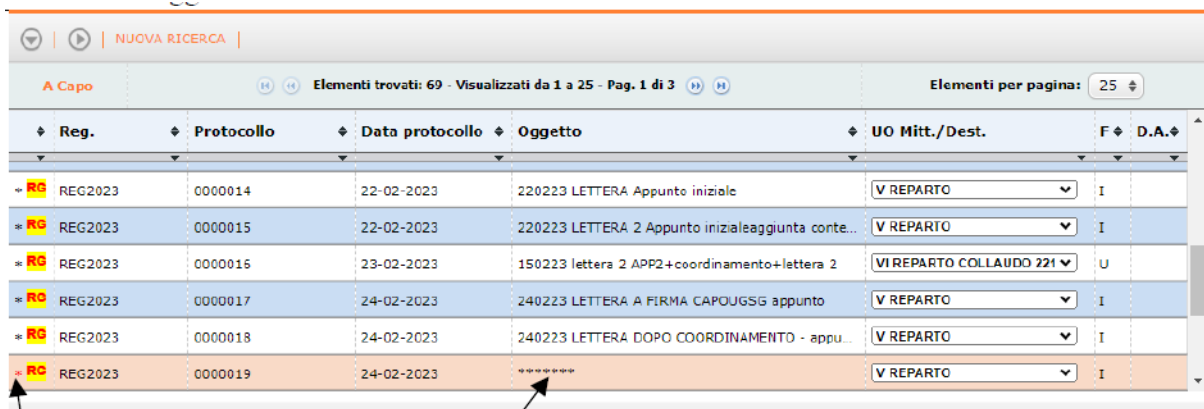
### **5.6.2 RESTRIZIONI NELLA CONSULTAZIONE - CONO VISIBILITÀ**

Senza ripercorrere il percorso normativo intervenuto nel tempo, sembra utile sottolineare come, è stato inizialmente progettato *Adhoc*, quando il D.Lsg.101/2018 e il Regolamento UE 2016/679 Regolamento Generale sulla Protezione dei Dati, i due atti, uno nazionale e l’altro europeo, che normano la materia, non erano ancora disponibili, essendo, all’epoca, tutto ricompreso nel D.lgs. 196/2003. Nel tempo è stato effettuato un percorso di rinnovo di alcune funzioni volte a ricondurre il sistema a criteri più vicini a quelli previsti dalle succitate norme, *in primis* con la gestione dell’archivio, realizzato in armonia con le norme succitate. La funzione di consultazione, una delle prime ad essere stata sviluppata, nasce dal presupposto di accedere al registro generale di protocollo, atto pubblico per definizione. Su tale base, considerando che l’accesso al registro di protocollo può essere richiesto anche da un comune cittadino (salvaguardando comunque eventuali informazioni da non divulgare) l’accesso alle singole registrazioni di protocollo è sempre stato consentito agli utenti, con alcune distinzioni:

- l’accesso alle singole registrazioni, dichiarate contenenti dati sensibili, ai sensi della vigente normativa, sono comunque disponibili solo agli utenti abilitati alla consultazione di tali dati;
- l’accesso ai documenti è comunque soggetto al cono di visibilità di ciascun utente che, pertanto, può venire a conoscenza dell’esistenza di un documento ma può accedervi solo se si trova nell’ambito del predetto cono di visibilità gerarchico.

La necessità di garantire il più possibile la riservatezza delle informazioni, alla luce di quanto previsto dai già citati atti normativi, l’attribuzione della facoltà di visualizzare dati contenenti dati sensibili ad una platea di utenti sempre più vasta, la mancata accortezza da parte della stragrande maggioranza degli addetti che inserisce negli Oggetti degli atti prodotti dati che non dovrebbero essere presenti in quella posizione, hanno creato una situazione che rende necessario implementare qualche strumento in più per fornire, ove necessario e ove ritenuto, maggiori garanzie sull’accesso alle informazioni gestite nel registro di protocollo. La prima implementazione consiste nella neutralizzazione delle informazioni di dettaglio della singola registrazione, che non vengono più rese disponibili nel caso in cui si stia accedendo ad una registrazione di protocollo contenente dati sensibili e l’utente non sia abilitato alla visualizzazione di tali dati.

Le informazioni di cui trattasi si trovano nella porzione sinistra dello schermo.



| Reg.         | Protocollo | Data protocollo | Oggetto                                            | UO Mitt./Dest.          | F | D.A. |
|--------------|------------|-----------------|----------------------------------------------------|-------------------------|---|------|
| * RG REG2023 | 0000014    | 22-02-2023      | 220223 LETTERA Appunto iniziale                    | V REPARTO               | I |      |
| * RG REG2023 | 0000015    | 22-02-2023      | 220223 LETTERA 2 Appunto inizialeaggiunta conte... | V REPARTO               | I |      |
| * RG REG2023 | 0000016    | 23-02-2023      | 150223 lettera 2 APP2+coordinamento+lettera 2      | VI REPARTO COLLAUDO 221 | U |      |
| * RG REG2023 | 0000017    | 24-02-2023      | 240223 LETTERA A FIRMA CAPOUGSG appunto            | V REPARTO               | I |      |
| * RG REG2023 | 0000018    | 24-02-2023      | 240223 LETTERA DOPO COORDINAMENTO - appu...        | V REPARTO               | I |      |
| * RG REG2023 | 0000019    | 24-02-2023      | 240223 LETTERA DOPO COORDINAMENTO - appu...        | V REPARTO               | I |      |

La videata soprastante riproduce la visualizzazione realizzata tramite la funzione di consultazione effettuata da un utente che NON ha accesso ai documenti contenenti dati sensibili. Secondo la regola generale, viene mostrata la riga della registrazione di protocollo che, tuttavia, qualora contenente dati sensibili, NON mostra l'oggetto (asterischi in sua vece) e, sia nella porzione destra, che in basso a sinistra non viene visualizzata nessuna informazione aggiuntiva. Rammentiamo che, a sinistra dell'icona identificante la tipologia documentale di appartenenza del documento, appare un asterisco che può essere nero, o **rosso** (nel caso in cui il documento contenga dati sensibili). La seconda implementazione è molto più rilevante e riguarda la qualità delle informazioni visualizzate anche a livello di registrazione di protocollo. In pratica, nelle UO è attivata la visualizzazione delle registrazioni di protocollo limitata al cono di visibilità dell'utente e dei fascicoli e documenti da essi trattati. Per le modalità di ricerca documenti vds. All. I.

## 5.7 VIOLAZIONE DATI PERSONALI (*PERSONAL DATA BREACH*)

Sono *personal data breach* tutte le violazioni afferenti all'integrità, alla riservatezza e alla disponibilità dei dati personali, siano essi in forma analogica, che digitale. Al riguardo, è estremamente importante riconoscere una violazione ai dati personali per consentire con la massima celerità (non oltre le 72 ore dalla scoperta della violazione) le eventuali comunicazioni formali alle Autorità e l'adozione di interventi per eliminare/mitigare l'insorgenza dell'eventuale rischio per i diritti e le libertà dell'interessato. In merito si precisa che l'atto di dichiarazione di avvenuto *personal data breach* è di esclusiva competenza del Titolare del trattamento o della competente Autorità giudiziaria mentre agli Enti compete l'individuazione e la relativa segnalazione direttamente a I RRAGEP degli elementi essenziali per consentire i successivi adempimenti normativi (comunicazioni al Garante e agli interessati). Pertanto, si precisa che, vanno tenute debitamente distinte le presunte ed asserite violazioni, basate sulle mere dichiarazioni/affermazioni degli interessati, rispetto a quelle effettive e ben definite/accertate dal Titolare o delle Autorità all'uopo preposte, unici soggetti muniti di competenza in merito. Le eventuali comunicazioni al Garante (ex art. 33 GDPR) e agli interessati (ex art. 34 GDPR), sono di competenza di SME - I RRAGEP, in quanto "Referente" del Titolare per il trattamento dei dati di F.A., mentre rimangono competenze degli Enti le eventuali segnalazioni

alle Autorità Giudiziarie, ove necessarie/previste. Per la gestione delle violazioni (al trattamento) di dati personali vigono le specifiche disposizioni in uso in ambito F.A., già diramate ad ogni livello organizzativo, oggetto di periodica revisione e aggiornamento. Al riguardo, deve essere immediatamente allertato il Referente in tutti i casi, sebbene si tratti ancora di una presunta violazione e la valutazione dei fatti con le successive eventuali azioni spetti ai preposti organi di staff, operanti nell'organizzazione del Titolare. A tal riguardo, in dettaglio, in caso di sospetta violazione dei dati personali (All. D) (ovvero presunto danno a riservatezza, integrità, disponibilità di tali dati), gli Enti invieranno al Referente una comunicazione che deve:

- essere effettuata senza ingiustificato ritardo dal momento in cui si rileva il fatto;
- descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati coinvolti nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- comunicare il nome e i dati di contatto del Responsabile della Protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- illustrare le probabili conseguenze della violazione dei dati personali;
- indicare le misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti.

## **5.8 BUONE PRASSI**

Istruzione e formazione non possono essere intesi come sinonimi, giacché la seconda è più approfondita e, pur non essendo riservata ad un ristretto numero di autorizzati, è spesso utilizzata a favore figure particolari, con deleghe specifiche o preposte alla trattazione di dati la cui peculiarità necessita di conoscenze più ampie o di tipo tecnico (vds. Dati Particolari All. E) Inoltre, la formazione deve essere continua e i destinatari devono essere periodicamente aggiornati per restare aderenti alle evoluzioni sia normative che tecnologiche. Pertanto a titolo esemplificativo e sicuramente non esaustivo si elencano alcune indicazioni cd "Buone Prassi", sia per i documenti analogici, sia per i documenti digitali, da porre in essere da parte degli utenti:

- non fare copie di lavoro private dei documenti e distruggere quelle in eccesso;
- è vietato comunicare con persone non autorizzate i dati personali di qualunque genere (giudiziari, sanitari o altri);
- tenere le porte degli uffici chiuse e le scrivanie libere da pratiche non in trattazione;
- al termine dell'attività lavorativa riporre i documenti/file in cartelle e armadi chiusi impedendo che terzi non autorizzati possano prenderne visione;
- per i dati particolari o giudiziari, utilizzare archivi controllati; per quelli sanitari trattarli utilizzando buste ed armadi chiusi;
- attenzione all'utilizzo delle stampanti, specie se condivise; utilizzare password e non lasciare documenti in giacenza;
- utilizzare solo strumenti dell'A.D.;

- non utilizzare cartelle condivise visibili a terzi;
- attenersi a compiti, procedure e vincoli di legge;
- i documenti nativi digitali non vanno stampati;
- definire per ogni U.O. i «con di visibilità»;
- il nome utente e la password sono esclusivamente personali;
- la password deve essere sicura e modificata spesso;
- non utilizzare caselle di posta personali;
- non utilizzare la casella di posta istituzionale per fini privati;
- in caso di non utilizzo o assenza temporanea, bloccare la postazione di lavoro tramite blocco manuale salvaschermo;
- non utilizzare piattaforme di condivisione sociale (e.g. Whatapp, Telegram, etc. etc.) per inoltrare ai colleghi dati personali o per trasmettere documenti contenenti dati personali.

## **TERZA PARTE**

### **MISURE ORGANIZZATIVE**

## 6. TITOLARIO E CLASSIFICAZIONE DI ARCHIVIO

### 6.1 GENERALITÀ

Il **"Titolario di archivio" dell'Esercito Italiano**, utilizzato da tutti gli EDR della F.A. dal 1° gennaio 2005, è il risultato di una iniziativa volta alla razionalizzazione ed alla unificazione delle metodologie, delle tecniche e delle modalità di archiviazione dei documenti e di gestione degli archivi presso tutte le Aree Organizzative Omogenee dell'Esercito.

### 6.2 METODOLOGIA DI RIFERIMENTO

La classificazione, obbligatoria per legge (DPR 445/2000), si presenta come uno schema generale di voci logiche, articolate in modo tendenzialmente gerarchico e stabilite in modo uniforme, che identificano le funzioni e le attività di ciascuna amministrazione. Tali voci non si identificano con la struttura organizzativa in quanto quest'ultima può essere soggetta a trasformazioni. La struttura portante è costituita dalle seguenti 12 voci che costituiscono il 1° livello di classifica denominato TITOLO:

1. ORGANIZZAZIONE;
2. PIANIFICAZIONE;
3. PROGRAMMAZIONE;
4. STUDI, RICERCHE E SVILUPPO PROGETTI;
5. GESTIONE RISORSE UMANE;
6. GESTIONE RISORSE FINANZIARIE;
7. GESTIONE RISORSE LOGISTICHE;
8. FORMAZIONE, ADDESTRAMENTO E AGGIORNAMENTO;
9. IMPIEGO DELLO STRUMENTO OPERATIVO;
10. IMPIEGO DELLO STRUMENTO LOGISTICO;
11. CONTROLLO;
12. PUBBLICA INFORMAZIONE, COMUNICAZIONE E STAMPA.

Il Titolario (consultabile sulla rete EINET) consta di circa 1400 voci per la successiva associazione, a ciascuna delle suddette funzioni di 1° livello (TITOLO), delle rispettive sotto funzioni e/o attività e/o materie di pertinenza costituenti le voci di 2°, 3° e 4° livello.

Il 2° livello (CLASSE) e il 3° livello (SOTTOCLASSE) del Titolario corrispondono alle successive articolazioni, mediante l'associazione alle suddette funzioni di 1° livello, delle rispettive sotto-funzioni e/o attività e/o materie di pertinenza, individuate mediante una preventiva analisi di studio da attaching al EDCR di riferimento. Tutti i documenti ricevuti e prodotti, indipendentemente dal supporto sul quale sono formati, sono classificati in base al Titolario d'archivio. Durante la classificazione del documento si assegnano, altro al codice completo dell'indice di classificazione (TITOLO, CLASSE e SOTTOCLASSE) anche il numero del fascicolo ed eventualmente il sotto-fascicolo.

### 6.3 ARCHIVIAZIONE E FASCICOLAZIONE

Tutti i documenti, indipendentemente dalla forma originale, qualora presi in carico a protocollo assumono a tutti gli effetti di legge valore legale. Rimane altresì facoltà della Autorità Giudiziaria la eventuale "verificazione" della Firma Autografa. All'atto dell'assunzione a protocollo i documenti protocollati, informatici o derivanti da dematerializzazione, devono essere:

- CLASSIFICATI, secondo il Titolario d'Archivio di F.A.;
- FASCICOLATI, secondo un Piano di Classificazione a cura della competente UO;
- ARCHIVIATI e CONSERVATI, in formato digitale non modificabile all'interno del sistema Adhoc (server centralizzato Adhoc).

A seconda della natura "originale" il documento è suddiviso nelle seguenti tipologie:

- documento informatico firmato digitalmente dal dirigente, è un "originale" ed è conservato nella sua forma digitale;
- documento analogico con firma autografa, de-materializzato viene firmato/validato digitalmente da un Pubblico Ufficiale (Attività Certificativa Militare) che ne certifica la "copia autentica";
- documento analogico con firma autografa, de-materializzato all'atto dell'assunzione a protocollo e conservato in forma digitale nel Sistema Adhoc.

Il **FASCICOLO** è lo strumento di base per gestire la classificazione, che subordinatamente alla sottoclasse, costituisce l'insieme ordinato di documenti che fa riferimento a uno "stesso affare" ovvero a una "stessa materia", ovvero a una stessa "tipologia documentaria". E' possibile registrare documenti in fascicoli e sotto-fascicoli già aperti fino alla conclusione degli argomenti trattati e chiusura degli stessi o a seconda delle pratiche procedere alla chiusura annuale per poi proseguire con un rinnovo cadenzato ad ogni anno. Il Sistema "Adhoc" prevede la creazione di fascicoli a livello di UO rendendo così visibile ciascuno di essi a tutti gli utenti inseriti in detta UO, con conseguente possibilità di raccogliere in essi i documenti prodotti nell'ambito dell'UO cui gli utenti appartengono, fermo restando il principio secondo il quale ciascun utente continua a mantenere la visibilità sui soli documenti per i quali è autorizzato secondo c.d. principio del "**cono d'ombra**". Il meccanismo del "**cono d'ombra**" è necessario, sia dal punto di vista formale che dal punto di vista normativo al fine di garantire il principio del "need to know" ovvero la necessità dell'utente di avere accesso al documento per esigenze lavorative e/o d'istituto. Per garantire la razionalizzazione delle operazioni di fascicolazione è importante assicurare che p e r ciascun fascicolo sia prevista una "durata", possa cioè essere chiuso quando il procedimento cui si riferisce sia definitivamente concluso (o la pratica, se si è scelto un differente criterio di archiviazione, lo richieda). Pertanto, si ritiene opportuno porre dei limiti all'utilizzazione dei fascicoli e dettare regole univoche per la loro denominazione a cura dei Responsabili di UO (proprietari).

- **Livello del fascicolo**, il fascicolo dovrà essere creato al livello delle UO, i componenti delle quali saranno i soli autorizzati ad inserire documenti in essi.
- **Denominazione del fascicolo**, per essere univocamente identificato, ogni fascicolo deve avere:

- i. titolo, classe e sottoclasse, che rappresentano la classificazione secondo il Titolario d'archivio (sarà sufficiente scegliere le voci desiderate dagli appositi menu a scorrimento);
- ii. Codice numerico e identificativo del fascicolo con testo descrittivo, che deve essere sintetico ed esprimere significativamente il contenuto del fascicolo. Il sotto-fascicolo verrà eventualmente creato secondo necessità avendo cura di assicurarne la denominazione secondo i medesimi criteri di concisione e chiarezza, senza produrre in generale ambiguità gestionale.

PAGINA INTENZIONALMENTE BIANCA

## 7. GESTIONE DOCUMENTI IN ENTRATA

### 7.1 DOCUMENTI ANALOGICI

Il flusso della corrispondenza in entrata è gestito dal Nucleo Adhoc inquadrata nell'ufficio Maggiorità e Personale con le modalità di seguito riportate. La corrispondenza cartacea deve essere considerata come residuale rispetto alla gestione de-materializzata dei documenti dell'AOO. A cura degli operatori preposti, la corrispondenza cartacea (ordinaria e raccomandata) ricevuta esclusivamente tramite Servizio Postale di Poste Italiane o Servizio Corriere, verrà de-materializzata e trasformata in formato PDF, protocollata ed inoltrata Capo Ufficio Maggiorità e Personale che provvederà allo smistamento ai responsabili delle UO interessate. Ai fini della Conservazione Sostitutiva, come previsto dal D.lgs. 82/2005 (CAD), art. 22 e s.m.i., il documento informatico contenente la copia derivante da un originale analogico lo sostituisce "ex lege" con piena efficacia se ad esso è apposto o associato, da parte di colui che lo spedisce o rilascia, una Firma Digitale e una dichiarazione di autenticità. Il documento cartaceo, sarà archiviato, per la conservazione, presso il Nucleo Adhoc.

### 7.2 TIPOLOGIA DI DOC. ANALOGICI

Per corrispondenza analogica si intende l'insieme dei plichi (buste, pacchi, ecc.) all'interno dei quali viaggiano i documenti analogici oggetto della presente trattazione. Essa si riferisce alla corrispondenza contemplata dalle "Condizioni generali di servizio per l'espletamento del servizio universale postale di Poste Italiane", indirizzate all'AOO-33° AMBROSIANO, ovvero a UO interne, esclusivamente per l'espletamento delle rispettive attività di carattere istituzionale, escludendo, quindi.

In particolare, è possibile distinguere la corrispondenza analogica in:

- ordinaria: non presenta, generalmente, la possibilità di verificare lo stato di lavorazione e la percorrenza, anche in corso, dell'invio e la sua consegna non è subordinata a ricevuta di ricezione. Invece, per quella spedita mediante "Posta celere" è possibile risalire, tramite le Poste Italiane, alla traccia dello stato di lavorazione e percorrenza, ferma restando l'assenza di una ricevuta di consegna;
- raccomandata: fornisce al mittente la ricevuta a riprova dell'avvenuta spedizione e consente di verificare lo stato di lavorazione e la percorrenza, anche in corso, dell'invio. Su richiesta è previsto l'Avviso di Ricevimento che, compilato dal mittente all'atto della spedizione e firmato dal destinatario all'atto della consegna, è recapitato al mittente come notifica dell'avvenuta consegna;
- assicurata: presenta le stesse modalità della Raccomandata con l'ulteriore possibilità di stabilire i limiti di valore assicurabili, a favore del mittente, contro lo smarrimento, il furto e il danneggiamento, previo pagamento di un corrispettivo proporzionale al valore dichiarato;
- atti giudiziari: è un servizio di posta Raccomandata attinente alle notificazioni di atti e di comunicazioni a mezzo posta, connesse con la notificazione di atti giudiziari di cui alla legge 20 novembre 1982, n. 890 e successive modifiche.

### 7.3 CONTROLLI DI SICUREZZA

Tutta la corrispondenza in entrata (ufficio postale o diretta alla CSI) è sottoposta alle attività di controllo, sia del personale addetto al ritiro sia dal personale di servizio all'ingresso della Caserma, secondo le modalità previste dalle procedure di sicurezza (Piano Difesa e Regolamento Interno di Sicurezza).

### 7.4 DOC. ORDINARI/RACCOMANDATA/ASSICURATA/PACCHI

Dopo l'apertura della corrispondenza pervenuta o ritirata, l'Operatore di protocollo verificherà preventivamente che non sia già presente in Adhoc il documento cartaceo pervenuto e, in tal caso, acquisisce/scansiona il documento annotandone gli estremi sul Registro. Il documento è, quindi, reso disponibile al personale autorizzato della UO destinataria che, al momento del ritiro, appone la propria firma "*Per ricevuta*" sul medesimo Registro. I documenti analogici sono così sottoposti, qualora ne sia prevista la protocollazione, al processo di dematerializzazione, a meno di eventuali allegati per i quali non è possibile procedere alla dematerializzazione (libri, CD/DVD, supporti magnetici, documentazione caratteristica, documentazione voluminosa, ecc.).

L'Operatore di Protocollo non procederà all'apertura di buste e/o plichi che riportino una delle seguenti diciture riferite al destinatario:

- Grado Nome Cognome;
- ESCLUSIVO PER IL TITOLARE;
- ESCLUSIVO PER (Grado) Nome Cognome;
- PERSONALE PER (Grado) Nome Cognome.

Ma le renderà disponibili al ritiro da parte del personale, sarà cura del destinatario valutare l'opportunità della successiva assunzione a protocollo. In tal caso, l'originale sarà consegnato al Nucleo posta per le operazioni di protocollazione e la successiva custodia.

L'Assicurata è la forma tipica di trasmissione della documentazione di bassa classifica di sicurezza. Pertanto, le Assicurate saranno trattate nelle modalità descritte dal Regolamento Interno di Sicurezza, qualora non si trattasse di documentazione classificata il documento viene restituito all'Operatore di protocollo per le azioni previste.

I pacchi, qualora riportino una lettera di trasmissione esterna allo stesso, sono considerati alla stregua degli "Allegati per i quali non è possibile procedere alla dematerializzazione" e pertanto sono sottoposti alla procedura per la corrispondenza ordinaria. Nel caso, invece, non si rinvienga all'esterno la lettera di accompagnamento, il personale addetto al Servizio provvede alla registrazione degli estremi del pacco e lo rende disponibile per la consegna al personale autorizzato della UO destinataria che, al momento del ritiro, appone la propria firma "*Per ricevuta*" sul medesimo Registro. Qualora la UO destinataria dovesse rinvenire all'interno del pacco la lettera di trasmissione, ne dovrà disporre la consegna all'Operatore di protocollo per le successive azioni di competenza.

## 7.5 PLICO CON DOPPIA BUSTA CONTENENTE DOC. CLASSIFICATI

Qualora all'interno di plico si rilevasse la presenza di una busta ovvero di documenti classificati, bisognerà contattare tempestivamente il personale della Segreteria di Sicurezza.

## 7.6 CORRISPONDENZA DANNEGGIATA

In tale ipotesi, il personale addetto al ritiro (Nucleo posta/Op. di Protocollo) rilevato il danneggiamento/parziale, provvede ad avvisare il Capo Ufficio Maggiorità e Personale che in base alla sua valutazione provvede a comunicare le circostanze al mittente ovvero restituisce la corrispondenza danneggiata/parzialmente aperta.

## 7.7 TELEGRAMMI/SPEDIZIONE DOC. ANALOGICO

Il personale del Nucleo posta provvede all'invio, presso le Poste Italiane, dei telegrammi per le esigenze istituzionali secondo quanto previsto dalle norme in vigore. La spedizione della corrispondenza analogica ordinaria, raccomandata e/o assicurata, pacchi, ecc. da parte delle UO dell'AOO 33° AMBROSIANO, è a cura del Nucleo posta. Il personale del Nucleo posta provvede alla consegna o alla spedizione della corrispondenza analogica in uscita:

- presso lo scambio posta del Cdo Brigata, per la corrispondenza diretta a enti militari della Caserma Ugo MARA;
- con affrancatura postale, nelle altre ipotesi, presso l'Ufficio Postale di zona. In tale ipotesi, le UO originatrici avranno cura di consegnare al Nucleo posta la corrispondenza, già incartata e pronta alla spedizione (indirizzo destinatario).

## 7.8 DOCUMENTO IN ENTRATA SU PEI

La casella di Posta Elettronica Istituzionale (PEI) è associata al sistema Adhoc, ciò permette al AOO 33° AMBROSIANO lo scambio automatico della corrispondenza in formato elettronico. La casella PEI è la casella di posta elettronica NON CERTIFICATA, ma rende comunque disponibili al Sistema Adhoc tutti i messaggi di posta elettronica pervenuti 24 ore su 24 e senza l'intervento dell'Operatore di protocollo. I documenti giunti via e-mail, completi di eventuali allegati, destinati alle UO sono prese automaticamente in carico dal sistema Adhoc. In particolare le e-mail sono:

- assunte a protocollo a cura del personale predisposto;
- inoltrate tramite Adhoc per conoscenza al Cte di Reggimento e per competenza al Capo Ufficio Maggiorità e Personale che provvede smistarle alla UO destinataria, per la trattazione o per conoscenza, tra quelle in indirizzo. L'invio sarà effettuato al livello "**Responsabile di UO**". Una volta ricevuti i documenti in formato elettronico sulle rispettive scrivanie virtuali, il personale delle singole UO procederà alla loro gestione mediante le funzioni del sistema Adhoc (assegnazione, classificazione, fascicolazione, ecc.) e trattamento della pratica.

## 7.9 DOCUMENTO IN ENTRATA SU PEC

La Posta Elettronica Certificata (PEC) è il sistema che consente di inviare e-mail con valore legale equiparato a una raccomandata con ricevuta di ritorno. La casella di PEC [rgtstal@postacert.difesa.it](mailto:rgtstal@postacert.difesa.it) è associata al sistema Adhoc. Ciò permette l'inoltro e la ricezione automatica della corrispondenza "certificata". La casella PEC è la casella di posta elettronica a cui inviare i documenti informatici indirizzati all' AOO 33° AMBROSIANO, rende disponibili al Sistema Adhoc tutti i messaggi di posta elettronica pervenuti 24 ore su 24 e senza l'intervento dell'Operatore di protocollo. Il Sistema rende disponibili agli Operatori i documenti pervenuti secondo l'ordine di ricezione, non modificabile ai fini della registrazione di protocollo.

Le PEC, complete di eventuali allegati, sono prese automaticamente in carico dal sistema Adhoc e successivamente rese disponibili alle UO destinataria per competenza o conoscenza tra quelle in indirizzo. In particolare le PEC sono:

- assunte a protocollo;
- inoltrate tramite Adhoc per conoscenza al Cte di Reggimento e per competenza al Capo Ufficio Maggiorità e Personale che provvede smistarle alla UO destinataria, per la trattazione o per conoscenza, tra quelle in indirizzo. L'invio sarà effettuato al livello "**Responsabile di UO**". Una volta ricevuti i documenti in formato elettronico sulle rispettive scrivanie virtuali, il personale delle singole UO procederà alla loro gestione mediante le funzioni del sistema Adhoc (assegnazione, classificazione, fascicolazione, ecc.) e trattamento della pratica.

## 7.10 DOCUMENTO IN ENTRATA SU XOMAIL

I messaggi telegrafici vengono ricevuti sulla postazione "XOMAIL" dedicata presso in Nucleo Maggiorità. Il personale provvederà a:

- esportare il messaggio ricevuto in formato PDF;
- eseguire l'acquisizione del file PDF così ottenuto in Adhoc;
- protocollare il messaggio;
- inoltrate tramite Adhoc per conoscenza al Cte di Reggimento e per competenza al Capo Ufficio Maggiorità e Personale che provvede smistarle alla UO destinataria, per la trattazione o per conoscenza, tra quelle in indirizzo. L'invio sarà effettuato al livello "**Responsabile di UO**". Una volta ricevuti i documenti in formato elettronico sulle rispettive scrivanie virtuali, il personale delle singole UO procederà alla loro gestione mediante le funzioni del sistema Adhoc (assegnazione, classificazione, fascicolazione, ecc.) e trattamento della pratica.

## 8. GESTIONE DOCUMENTI IN USCITA

### 8.1 DOCUMENTO IN USCITA CARTACEO

**Documenti analogici non trasmissibili per via informatica.** Per gli atti che devono essere inviati esclusivamente in formato cartaceo (p.es.: fogli di viaggio, atti giudiziari, documentazione caratteristica, ecc.), dovrà essere:

- attuato il processo di materializzazione (stampa ed apposizione della firma olografa) del documento protocollato;
- effettuata la spedizione del documento e degli eventuali allegati, per via posta ordinaria o nelle modalità previste per la tipologia di documentazione.

**Documenti informatici non trasmissibili per via informatica.** Per gli atti che non possono essere inviati per via informatica in quanto il destinatario non ha capacità di riceverli (p.es. corrispondenza con un privato) si dovrà procedere alla “**materializzazione**” dei documenti informatici. Il documento cartaceo frutto del processo di materializzazione, il cui originale in formato digitale è conservato all’interno del sistema Adhoc, deve recare, sul retro ovvero apposita lettera di trasmissione, l’attestazione di conformità all’originale elettronico. Tale dichiarazione, che può essere apposta anche mediante l’uso di timbri e deve essere redatta secondo il seguente schema:

|                                                                                                                                                                |                            |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| Si attesta che il presente documento è copia integrale del documento informatico originale firmato digitalmente, composto complessivamente da n. _____ pagine. |                            |
| Località , _____                                                                                                                                               | IL CAPO UFFICIO/COMANDANTE |
|                                                                                                                                                                | (Grado. Xxxxx XXXXXX)*     |
| (*) l’attestazione del documento deve essere firmata esclusivamente dal responsabile dell’ UO autorizzato alla spedizione.                                     |                            |

Successivamente si provvederà alla spedizione del documento analogico tramite il Servizio Postale / corriere abilitato. L’Operatore di protocollo riceve dalle UO la corrispondenza precedentemente predisposta per la spedizione e ne controlla la corretta marcatura (indirizzi, protocollo, integrità del pacco/busta, indicazione tipologia prodotto postale, ecc.), registra su apposita distinta da conservare agli atti tutti i prodotti postali da inviare e ne effettua la spedizione tramite il nucleo Poste.

### 8.2 DOCUMENTO IN USCITA SU PEI

La casella di Posta Elettronica Istituzionale [rgtstl33@esercito.difesa.it](mailto:rgtstl33@esercito.difesa.it) è impiegata dal sistema Adhoc per ricevere e inviare i documenti informatici. La documentazione prodotta dalle UO è inviata dal sistema anche tramite questo canale alle AOO nel caso in cui il destinatario non sia in possesso di casella di Posta Certificata che rimane il metodo di trasmissione impostato come principale nel sistema.

**Compiti delle UO.** L’Utente accreditato per l’ UO provvederà nell’ordine a:

- predisporre i documenti e gli eventuali allegati in formato digitale (o direttamente in formato informatico attraverso la “**dematerializzazione**” dell’analogico);
- procedere alla gestione documentale tramite le funzioni di Classificazione, Fascicolazione e predisposizione degli indirizzi destinatari tramite il sistema

AdHoc; inoltrare gli atti informatici predisposti, fino al livello **Responsabile della UO**, per la visione e l'approvazione;

- Il Responsabile di UO validerà il documento e provvederà all'inoltro dello stesso ovvero al Comandante di RGT per il seguito di competenza;
- Il Comandante di RGT provvederà ad approvare i documenti, mediante apposizione della Firma Digitale (in qualità di Responsabile della AOO 33° AMBROSIANO), contestualmente il sistema effettuerà la registrazione del protocollo; Il sistema "AdHoc" procederà automaticamente a trasmettere la documentazione informatica ai rispettivi destinatari precedentemente predisposti.

### 8.3 DOCUMENTO IN USCITA SU XOMAIL

Il sistema di messaggistica XOMAIL dovrà essere limitato a comunicazioni brevi ed urgenti (es. messaggi di segnalazione eventi, "messaggistica operativa"), per l'invio di documenti/avvisi/ordini di particolare urgenza e immediata trattazione o a Liste di Distribuzione PEC molto lunghe e per le quali il Sistema rimanda un errore peso Eccessivo. La postazione XOMAIL dedicata è ubicata all'interno del Nucleo Maggiorità, stanza n. 43 della palazzina C2. Tale sistema è usato principalmente dal Graduato di servizio al Comando di Reggimento per l'inoltro di eventuale messaggistica inerente eventi/incidenti o di quella a carattere operativo in particolari circostanze su disposizioni delle SS.AA. L'Operatore/Graduato di Servizio provvederà a:

- assegnare la qualifica di competenza/conoscenza dei destinatari indicata nel modulo per messaggio;
- inserire nel testo del messaggio il numero di protocollo attribuito dal sistema Adhoc;
- trasmettere il documento tramite sistema XOMAIL;
- inoltrare una copia del messaggio trasmesso alla UO che ha generato il documento.

### 8.4 DOCUMENTO IN USCITA SU PEC

La casella di Posta Elettronica Certificata [rgtstal@postacert.difesa.it](mailto:rgtstal@postacert.difesa.it) è associata al sistema Adhoc. Ciò permette alle UO dipendenti, per il tramite del Codice Univoco AOO - AAB71B3 l'inoltro e la ricezione automatica di corrispondenza in formato elettronico con **valore legale di raccomandata con ricevuta di ritorno**. L'utilizzo di tale casella è prioritario rispetto alla posta elettronica istituzionale.

**Compiti delle UO.** Gli Operatori accreditati presso le UO del 33° AMBROSIANO provvederanno nell'ordine a:

- predisporre i documenti e gli eventuali allegati in formato digitale (o direttamente in formato informatico o attraverso la "dematerializzazione" dell'analogico); procedere alla gestione documentale tramite le funzioni di Classificazione, Fascicolazione e predisposizione degli indirizzi destinatari tramite il sistema Adhoc;
- inoltrare gli atti informatici predisposti al rispettivo Responsabile di UO, per la visione e l'approvazione;

- Il Responsabile di UO revisionerà/validerà il documento e provvederà all’inoltro direttamente, se a firma “d’ordine” secondo quanto disposto dall’Atto Dispositivo n.1 (A.D. n.1), ovvero al Comandante di Reggimento;
- Il Comandante di RGT, in qualità di Responsabile dell’AOO 33 AMBROSIANO, provvederà ad approvare i documenti apponendovi la Firma Digitale, contestualmente il sistema effettuerà la registrazione del protocollo;
- Il sistema Adhoc procederà automaticamente a trasmettere la documentazione informatica ai rispettivi destinatari precedentemente predisposti.

## **8.5 PREDISPOSIZIONE**

La “Predisposizione” dei documenti è finalizzata all’approntamento, a cura del personale addetto delle UO, della documentazione da sottoporre alla “Firma” del Responsabile UO delegato alla firma d’ordine (vds. A.D. n. 1) ovvero dal Comandante di Reggimento, previa attività di revisione da parte del Responsabile UO. La funzionalità del Sistema consente di predisporre la documentazione da sottoporre a Revisione e successiva Firma, completa di:

- oggetto del documento con misure di pseudonomizzazione o anonimizzazione (vds. All. F);
- indicazione del fascicolo di destinazione del documento;
- indicazione delle AOO destinatarie, esterne (per competenza/conoscenza) all’AOO 33° AMBROSIANO;
- indicazione delle UO destinatarie interne (per competenza/conoscenza) all’AOO 33° AMBROSIANO;
- eventuali “Note” esplicative per il Responsabile UO/AOO;
- eventuali “File Accessori”;
- documento principale e documenti allegati (annessi/allegati);
- riferimenti e seguiti al documento principale;
- eventuale indicazione della presenza di “Dati Sensibili” contenuti nella documentazione;
- selezione riguardo eventuali “Dati Analogici”;
- eventuale indicazione di “Urgente”;
- selezione della “Tipologia Documentale” (e.g. Generale, OdG, OdS, ecc. ecc.).

## **8.6 OGGETTO DEL DOCUMENTO IN PREDISPOSIZIONE**

L’Oggetto del documento deve permettere l’identificazione della tipologia del documento ma non del contenuto o parti di esso. Non sono ammessi caratteri speciali, è necessario non solo, ai fini della tutela della privacy/dati personali, evitare di indicare nel campo Oggetto del sistema, nominativi di personale con associazioni di fatti eventi, procedimenti e/o procedure, ma anche per uniformare la denominazione dei documenti formati dalle singole UO. Pertanto in Allegato F è riportato un elenco per tipologia documentale, che non racchiude tutte le tipologie di documenti prodotti ma individua in modo chiaro le linee guida e i criteri per la denominazione dei file.

## **8.7 INDICAZIONE DEL FASCICOLO DI DESTINAZIONE DEL DOCUMENTO**

Quando il documento sarà sottoposto a "Firma", il Sistema provvederà, tra le altre funzioni alla Fascicolazione del documento secondo quanto indicato in questa fase. Essendo il fascicolo per definizione il "contenitore" (l'unità archivistica di aggregazione) dei documenti relativi allo stesso procedimento o materia, ne discende che l'attività di Fascicolazione di un documento si traduce nell'indicazione del Fascicolo di pertinenza in cui il Sistema dovrà inserirlo all'atto della sua Firma. In tal modo, il Sistema assegnerà al documento il medesimo Indice di classificazione del fascicolo in cui è stato inserito, comune a tutti gli altri documenti in esso contenuti, composto da:

- anno di riferimento del fascicolo (e.g. 2024);
- classifica attribuita al fascicolo all'atto della sua istruzione (es. 5/9/5);
- nome del fascicolo (es. 00226), con il formato: 2024 – 5/9/5.00226.

## **8.8 INDICAZIONE DELLE AOO DESTINATARIE, ESTERNE E/O INTERNE ALL'AOO**

In questa sezione, devono essere indicate le AOO esterne e/o interne all'AOO 33° AMBROSIANO a cui il documento deve essere inviato, traendole dalla "Rubrica Indirizzi". Nel caso in cui l'indirizzo di una o più AOO non dovesse essere presente nella Rubrica Indirizzi, il suo inserimento può essere chiesto al Vicario Amministratore, previa autorizzazione del RDS. La scelta nella Rubrica Indirizzi deve essere effettuata tenendo presente che non esiste una corrispondenza univoca tra il numero/nome dei destinatari del documento indicati nel "corpo lettera" e le AOO riportate nella "Rubrica indirizzi". Infatti, più destinatari posso far parte della stessa AOO di destinazione, anche se apparentemente non legati da reciproca dipendenza gerarchica o funzionale. Inoltre, in questa sezione, si ha la possibilità di scegliere se il documento deve essere inviato alla rispettiva PEC del destinatario (come predisposto automaticamente dal Sistema) ovvero sulla casella di PEI, il tutto scegliendo infine l'invio per competenza e/o conoscenza.

## **8.9 EVENTUALI NOTE E FILE ACCESSORI**

La disponibilità da parte del "Revisore delle Note" apposte dall'estensore della Predisposizione, hanno la stessa valenza di ausilio dei noti "cavallucci" che accompagnano le lettere in visione in modalità analogica. Le "Note" non faranno parte della documentazione che sarà inviata all'atto della "Firma". "File Accessori" eventualmente riportati nella predisposizione (foto, testi, specchi, ecc.), hanno la stessa funzione di ausilio al "Revisore" delle precedenti "Note" e anch'essi non saranno inviati con il documento firmato.

## **8.10 DOCUMENTO PRINCIPALE E ALLEGATI (ANNESI/ALLEGATI)**

L'avvio dell'attività presuppone la disponibilità di tutti i documenti che comporranno la documentazione da sottoporre alla "Revisione" e successiva "Firma" e cioè:

- del documento principale, che conterrà il testo oggetto della decretazione finale e la firma;

- degli annessi/allegati.

I predetti documenti sono stati approntati dal personale addetto utilizzando i programmi di videoscrittura, fogli di calcolo, presentazioni, ecc. in dotazione alla Difesa, a seconda della valenza e della finalità del documento stesso.

In particolare, è **necessario attenersi** alle seguenti prescrizioni:

- il documento principale deve essere prodotto esclusivamente con un programma di videoscrittura e salvato come file con una delle estensioni previste;
- è **proscritto** il ricorso a documenti principali il cui file abbia estensione “.pdf” quando prodotti con la scansione di documenti precedentemente sottoposti a firma autografa. Al riguardo è opportuno sottolineare come il quadro legislativo in vigore consegna alla sola Firma digitale l’unica valenza legale alla sottoscrizione di un documento, di cui la firma autografa è assolutamente priva, per le AOO iscritte all’Indice delle Pubbliche Amministrazioni che hanno adottato un Sistema di protocollo informatico e gestione documentale;
- i documenti allegati a quello principale (annessi, allegati), prodotti o meno con programmi di videoscrittura, ecc. in dotazione, possono essere file con qualsiasi estensione tenendo ben presente che:
  - i. salvo diversa configurazione da parte del Responsabile UO, la successiva Firma digitale sarà apposta, sia al documento principale, sia agli allegati, tranne che sui file dei fogli di calcolo, rendendoli così modificabili ai destinatari;
  - ii. i file .pdf o comunque i file contenenti già una Firma digitale, tipo Kit Firma Difesa, e gli allegati che si vogliono rendere modificabili da parte dei destinatari (presentazioni, testi, ecc.), devono essere sottratti alla Firma digitale;
  - iii. i file con estensione diversa da quella dei comuni programmi del pacchetto di videoscrittura, ecc. (es “.jpeg”), potrebbero richiedere una installazione necessaria per la loro visione;
  - iv. escludere caratteri speciali per la denominazione dei file, evitando denominazioni lunghe con informazioni già contenute nel corpo della lettera di trasmissione.

### 8.11 RIFERIMENTI E SEGUITI AL DOCUMENTO PRINCIPALE

In questa sezione è necessario associare alla predisposizione i documenti in Riferimento e/o a Seguito, menzionati nel documento principale. L’associazione può avvenire soltanto se il documento in riferimento o a seguito è presente nell’archivio della AOO 33° AMBROSIANO. In caso contrario, una sua copia può essere inserita nella precedente sezione dei “File Accessori”. La scelta del documento da associare quale Riferimento e/o Seguito, avviene mediante la sua ricerca in “archivio”.

### 8.12 INDICAZIONE DI “DATI SENSIBILI”

La presenza di questa indicazione farà sì che il documento, una volta firmato e inviato, sarà accessibile in lettura, all’interno della AOO 33° AMBROSIANO, ai soli “Utenti” abilitati alla:

- trattazione dei “Dati sensibili”, predisposti dal RdS su indicazione del Responsabile AOO (Cte Rgt.);
- abilitazione dell’Utente all’accesso ai documenti dello specifico fascicolo, attribuita dal Responsabile UO di appartenenza.

### **8.13 SELEZIONE RIGUARDO EVENTUALI DATI ANALOGICI**

Se è presente l’indicazione di “Dati Analogici”, una volta firmato il documento il Sistema provvede a:

- non recapitarlo agli indirizzi di PEI/PEC indicati per i destinatari per competenza;
- inserire il documento nella “Lista documenti da materializzare”, ai fini della sua successiva stampa da parte dell’Utente;
- a recapitare, alle PEI/PEC dei soli destinatari per conoscenza, il documento privo degli “Allegati”.

Al riguardo si evidenzia che:

- per destinatari per competenza/conoscenza, si intendono le AOO indicate in tal modo al momento della selezione dei “Destinatari Esterni”;
- i “Destinatari Interni” riceveranno comunque anche gli “Allegati”;
- qualora non si volessero inviare gli allegati di un documento con “Dati Analogici” ad un Destinatario Esterno”, bisogna indicarlo come destinatario per competenza e non per conoscenza.

### **8.14 INDICAZIONE DI PRIORITÀ**

L’indicazione di Priorità: Normale, Urgente e Urgentissimo ad un documento in “Predisposizione” ne consente l’immediata visibilità lungo la catena di “Revisione e Firma, ma non riporta alcuna indicazione per i destinatari.

### **8.15 REVISIONE**

Terminata la fase di Predisposizione del documento, questo può essere inoltrato al Responsabile della UO di appartenenza ai fini della sua Revisione. Il Responsabile può esercitare due tipi di controllo sulla Predisposizione ricevuta:

- sul documento e sui relativi allegati, in merito ai contenuti ed agli aspetti formali;
- sull’impianto della predisposizione stessa, riguardo alla esattezza e completezza di quanto predisposto in ciascun settore, avendo facoltà di poter:
  - i. effettuare egli stesso le eventuali correzioni, agendo sugli strumenti di correzione del sistema di videoscrittura ovvero modificando la Predisposizione del documento;
  - ii. inoltrare la Predisposizione al Responsabile/Addetto dal quale è stata ricevuta, indicando nelle Note i correttivi da apportare per la successiva firma d’ordine (vds. A.V. n. 1) ovvero l’inoltro al Responsabile dell’AOO A (Cte rgt.)

### **8.16 FIRMA-PROTOCOLLAZIONE E INVIO DOCUMENTO**

L’apposizione della Firma digitale da parte del Responsabile UO/AOO, può essere effettuata sul singolo documento o su più documenti previa loro selezione e prevede:

- la preventiva presa visione del documento/i da firmare, quale ultimo livello dell’attività di Revisione di cui al precedente sottopara. 8.15;

- l'utilizzo della propria Carta Multiservizi della Difesa (mod. ATe) e di entrambi i Codici carta e Codice firma personali.

Al completamento di questa operazione, il Sistema:

- firma il documento/i, associando la firma digitale corrispondente ai Certificati di firma presenti sulla predetta Carta e apponendola al documento/i principale di ciascuna Predisposizione e a tutti gli Allegati per i quali è stata prevista;
- protocolla ciascun documento appena firmato, associandogli la rispettiva Segnatura di protocollo composta da:
- Codice IPA dell'Amministrazione (Ministero della Difesa: M\_D);
- identificativo univoco della AOO che ha assunto in carico il documento in entrata (AAB71B3);
- il Registro di protocollo di riferimento (e.g. REG2024);
- numero di protocollo (e.g. 0000055);
- la data di protocollazione (es. 01-01-2022),

con il formato: M\_D AAB71B3 REG2024 0000055 24-04-2024.

Invia il documento/i ai Destinatari esterni/interni, secondo quanto indicato in fase di Predisposizione, alle rispettive Caselle di PEI o di PEC, dalle Caselle di PEI o PEC della AOO/UO interessate. Qualora in fase di Predisposizione sia stata selezionata l'opzione Dati Analogici, l'Utente deve provvedere alla stampa del documento presente nella Lista documenti da materializzare, avendo cura che il documento analogico così ottenuto sia provvisto del relativo "Glifo".

In conclusione è opportuno evidenziare quanto segue:

- la Firma digitale apposta sul documento, conferisce a questo piena **validità legale** ai sensi di quanto sancito dalla normativa vigente e unitamente alla contestuale Segnatura di protocollo ne fanno, di fatto, un documento **amministrativo** e un **Atto dello Stato**, il Sistema riporta, sul documento firmato, il nominativo, la data e l'ora del Responsabile Titolare del procedimento che ha apposto la Firma. Tale nominativo **deve corrispondere** a quello riportato nel Gruppo Firma del documento principale ovvero a quello relativo al Delegato indicato nello stesso.
- il nominativo relativo alla Firma del Delegato, **deve corrispondere** al nominativo Delegato nel Sistema da parte del Titolare.
- la non rispondenza dei requisiti indicati nei precedenti due alinea rende di fatto il documento intrinsecamente incoerente, rendendolo soggetto a contestazione da parte di terzi e comunque alla libera valutazione in caso di opponibilità dello stesso in giudizio.

# ALLEGATI

## ABBREVIAZIONI/ACRONIMI IN USO

|                     |                                                                                |
|---------------------|--------------------------------------------------------------------------------|
| <b>AC</b>           | ALTO COMANDO                                                                   |
| <b>A.D.</b>         | AMMINISTRAZIONE DIFESA                                                         |
| <b>AgID</b>         | AGENZIA PER L'ITALIA DIGITALE (EX DIGITPA, EX CNIPA, EX AIPA)                  |
| <b>All.</b>         | ALLEGATO                                                                       |
| <b>Ann.</b>         | ANNESSO                                                                        |
| <b>Apt.</b>         | APPUNTO                                                                        |
| <b>AOO</b>          | AREA ORGANIZZATIVA OMOGENEA                                                    |
| <b>a.p.s.</b>       | ASSENTE PER SERVIZIO                                                           |
| <b>ARQ</b>          | ASPETTATIVA PER RIDUZIONE QUADRI                                               |
| <b>ASL</b>          | AZIENDA SANITARIA LOCALE                                                       |
| <b>B.</b>           | BRIGATA                                                                        |
| <b>btg.</b>         | BATTAGLIONE                                                                    |
| <b>CAD</b>          | DLGS. 7 MARZO 2005, N.82: "CODICE DELL'AMMINISTRAZIONE DIGITALE"               |
| <b>C.A.</b>         | CORPO D'ARMATA                                                                 |
| <b>CASD</b>         | CENTRO ALTI STUDI DIFESA                                                       |
| <b>Cdo</b>          | COMANDO                                                                        |
| <b>COINT</b>        | COMANDO INTERMEDIO                                                             |
| <b>CLS</b>          | CLASSIFICA DI SEGRETEZZA                                                       |
| <b>CMO</b>          | COMMISSIONI MEDICHE OSPEDALIERE                                                |
| <b>Co.</b>          | CORPO (E.G. SANITARIO, COMMISSARIATO, GUARDIA DI FINANZA)                      |
| <b>COM</b>          | "CODICE DELL'ORDINAMENTO MILITARE"<br>DECRETO LEGISLATIVO 15 MARZO 2010, N. 66 |
| <b>COMTA</b>        | COMANDO TRUPPE ALPINE                                                          |
| <b>NRDC-ITA</b>     | NATO RAPID DEPLOYABLE CORP-ITALY                                               |
| <b>COMLOG</b>       | COMANDO LOGISTICO                                                              |
| <b>COMFORDOT</b>    | COMANDO FORMAZIONE SPECIALIZZAZIONE DOTTRINA                                   |
| <b>COMFOTER</b>     | COMANDO FORZE OPERATIVE TERRESTRI                                              |
| <b>COMFOP NORD</b>  | COMANDO FORZE OPERATIVE NORD                                                   |
| <b>COMFOP SUD</b>   | COMANDO FORZE OPERATIVE SUD                                                    |
| <b>COMFOTER SPT</b> | COMANDO FORZE OPERATIVE TERRESTRI DI SUPPORTO                                  |
| <b>Cte</b>          | COMANDANTE                                                                     |
| <b>DDI</b>          | DIREZIONE DI INTENDENZA                                                        |
| <b>D.G.</b>         | DIREZIONE GENERALE                                                             |
| <b>DGUE</b>         | DIREZIONE GENERALE DEGLI UFFICIALI DELL'ESERCITO                               |
| <b>DIPE</b>         | DIPARTIMENTO IMPIEGO DEL PERSONALE                                             |
| <b>D.Lgvo.</b>      | DECRETO LEGISLATIVO                                                            |
| <b>D.M.</b>         | DECRETO MINISTERIALE                                                           |
| <b>DMML</b>         | DIPARTIMENTO MILITARE DI MEDICINA LEGALE                                       |
| <b>DPCM</b>         | DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI                              |
| <b>D.P.R.</b>       | DECRETO DEL PRESIDENTE DELLA REPUBBLICA                                        |
| <b>D.S.S.</b>       | DIRIGENTE DEL SERVIZIO SANITARIO                                               |
| <b>DUM</b>          | DOCUMENTO UNICO MTRICOLARE                                                     |
| <b>EdO</b>          | ELEMENTO DI ORGANIZZAZIONE                                                     |
| <b>EDRC</b>         | ENTE/DISTACCAMENTO/REPARTO/COMANDO                                             |

|                     |                                                               |
|---------------------|---------------------------------------------------------------|
| <b>EI</b>           | ESERCITO ITALIANO                                             |
| <b>MM</b>           | MARINA MILITARE                                               |
| <b>AM</b>           | AERONAUTICA MILITARE                                          |
| <b>CC</b>           | CORPO DEI CARABINIERI                                         |
| <b>EI-NET</b>       | RETE INTRANET DELL'ESERCITO ITALIANO                          |
| <b>EPC</b>          | ESERCITAZIONE POSTI COMANDO                                   |
| <b>f.n.</b>         | FOGLIO NUMERO                                                 |
| <b>F.A.</b>         | FORZA ARMATA                                                  |
| <b>f.f.</b>         | FACENTE FUNZIONI                                              |
| <b>GDO</b>          | GRUPPO DATA-ORARIO                                            |
| <b>GEPA</b>         | GESTIONE PROCEDURE AVANZAMENTO                                |
| <b>Gr.</b>          | GRUPPO                                                        |
| <b>Grd.</b>         | GRADUATI                                                      |
| <b>G.U.</b>         | GRANDE UNITA'                                                 |
| <b>IPA</b>          | INDICE DELLA PUBBLICA AMMINISTRAZIONE                         |
| <b>ISPE</b>         | ISPETTORATO                                                   |
| <b>ISSMI</b>        | ISTITUTO SUPERIORE DI STATO MAGGIORE INTERFORZE               |
| <b>IT SNR</b>       | ITALIAN SENIOR NATIONAL REPRESENTATIVE                        |
| <b>L.</b>           | LEGGE                                                         |
| <b>let.</b>         | LETTERA                                                       |
| <b>MdG</b>          | MANUALE DI GESTIONE                                           |
| <b>Mod.</b>         | MODELLO                                                       |
| <b>MS</b>           | MEMORIE STORICHE                                              |
| <b>MSG.</b>         | MESSAGGIO                                                     |
| <b>NOS</b>          | NULLA-OSTA DI SICUREZZA                                       |
| <b>O.</b>           | ORDINE                                                        |
| <b>O.C.</b>         | ORGANI CENTRALI                                               |
| <b>ord.</b>         | ORDINARIO                                                     |
| <b>Ordn.</b>        | ORDINAMENTO                                                   |
| <b>OF</b>           | ORGANIZZAZIONE DELLE FORZE                                    |
| <b>O.I.</b>         | ORGANISMI INTERNAZIONALI                                      |
| <b>Op. Mil.</b>     | OPERAZIONE MILITARE                                           |
| <b>ORBAT</b>        | ORDINE DI BATTAGLIA                                           |
| <b>O. mov.</b>      | ORDINE DI MOVIMENTO                                           |
| <b>O. mov. v.o.</b> | ORDINE DI MOVIMENTO PER VIA ORDINARIA                         |
| <b>OLA</b>          | ORDINE LOGISTICO AMMINISTRATIVO                               |
| <b>O. Op.</b>       | ORDINE DI OPERAZIONE                                          |
| <b>O. perm.</b>     | ORDINE PERMANENTE                                             |
| <b>Org. L.</b>      | ORGANIZZAZIONE LOGISTICA                                      |
| <b>or.</b>          | ORGANO                                                        |
| <b>Or. imp.</b>     | ORIENTAMENTO IMPIEGO                                          |
| <b>P.A.</b>         | PUBBLICA AMMINISTRAZIONE                                      |
| <b>PAQ/PAR</b>      | PIANI ANNUALI DELLE QUALIFICAZIONI/RIQUALIFICAZIONI ORDINARIE |
| <b>PEC</b>          | POSTA ELETTRONICA CERTIFICATA                                 |
| <b>PEI</b>          | POSTA ELETTRONICA ISTITUZIONALE                               |
| <b>PEIN</b>         | POSTA ELETTRONICA ISTITUZIONALE NOMINATIVA                    |

|                  |                                                                                                                                                                               |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>PEIF</b>      | POSTA ELETTRONICA ISTITUZIONALE FUNZIONALE                                                                                                                                    |
| <b>PERSOMIL</b>  | DIREZIONE GENERALE PER IL PERSONALE MILITARE                                                                                                                                  |
| <b>PREVIMIL</b>  | DIREZIONE GENERALE DELLA PREVIDENZA MILITARE E DELLA LEVA                                                                                                                     |
| <b>PI</b>        | PUBBLICA INFORMAZIONE                                                                                                                                                         |
| <b>p.o.</b>      | POSIZIONI ORGANICHE                                                                                                                                                           |
| <b>pol. ti.</b>  | POLIGONO DI TIRO                                                                                                                                                              |
| <b>PTZ</b>       | PRONTEZZA                                                                                                                                                                     |
| <b>PC</b>        | POSTO COMANDO                                                                                                                                                                 |
| <b>Q.P.</b>      | QUADRO PERMANENTE                                                                                                                                                             |
| <b>QP</b>        | QUALIFICA DI PRECEDENZA                                                                                                                                                       |
| <b>I RRAGEP</b>  | I REPARTO AFFARI GIURIDICI ED ECONOMICI DEL PERSONALE                                                                                                                         |
| <b>RDP</b>       | REGISTRAZIONE DI PROTOCOLLO                                                                                                                                                   |
| <b>RdS</b>       | RESPONSABILE DEL SERVIZIO                                                                                                                                                     |
| <b>rgpt.</b>     | RAGGRUPPAMENTO                                                                                                                                                                |
| <b>rgt.</b>      | REGGIMENTO                                                                                                                                                                    |
| <b>Rep.</b>      | REPARTO                                                                                                                                                                       |
| <b>ric.</b>      | RICOGNIZIONE                                                                                                                                                                  |
| <b>RM</b>        | REGIONE MILITARE                                                                                                                                                              |
| <b>RPG</b>       | REPARTO PIANIFICAZIONE GENERALE                                                                                                                                               |
| <b>RN</b>        | RUOLO NORMALE                                                                                                                                                                 |
| <b>R.O.</b>      | RUOLO D'ONORE                                                                                                                                                                 |
| <b>RS</b>        | RUOLO SPECIALE                                                                                                                                                                |
| <b>SA</b>        | SEZIONE AMMINISTRATIVA                                                                                                                                                        |
| <b>SDP</b>       | SEGNATURA DI PROTOCOLLO                                                                                                                                                       |
| <b>SIEFIN</b>    | SISTEMA INFORMATIVO FINANZIARIO DELL'ESERCITO                                                                                                                                 |
| <b>SIGE</b>      | SISTEMA INFORMATIVO GESTIONALE DELL'ESERCITO                                                                                                                                  |
| <b>SIGE-PERS</b> | SISTEMA INFORMATIVO GESTIONALE DELL'ESERCITO- SOTTOSISTEMA PERSONALE                                                                                                          |
| <b>SIVE</b>      | SISTEMA INFORMATIVO VESTIARIO EQUIPAGGIAMENTO                                                                                                                                 |
| <b>S.I. COM.</b> | SISTEMA INFORMATIVO DI COMMISSARIATO                                                                                                                                          |
| <b>SISE</b>      | SISTEMA INFORMATIVO SICUREZZA ESERCITO                                                                                                                                        |
| <b>SM</b>        | STATO MAGGIORE                                                                                                                                                                |
| <b>SMD</b>       | STATO MAGGIORE DELLA DIFESA                                                                                                                                                   |
| <b>SME</b>       | STATO MAGGIORE DELL'ESERCITO                                                                                                                                                  |
| <b>s.m.i.</b>    | SERVIZIO MILITARE INCONDIZIONATO                                                                                                                                              |
| <b>s.p.</b>      | SERVIZIO PERMANENTE                                                                                                                                                           |
| <b>s.SM</b>      | SERVIZIO DI STATO MAGGIORE                                                                                                                                                    |
| <b>SU.</b>       | SOTTUFFICIALI                                                                                                                                                                 |
| <b>t.a.</b>      | TEMPORANEA ASSEGNAZIONE                                                                                                                                                       |
| <b>t.a.</b>      | TEMPORANEA ASSENZA (NEL GRUPPO FIRMA)                                                                                                                                         |
| <b>T.O.</b>      | TABELLE ORGANICHE                                                                                                                                                             |
| <b>Te. Op.</b>   | TEATRO OPERATIVO                                                                                                                                                              |
| <b>Tr.</b>       | TRUPPA                                                                                                                                                                        |
| <b>TRAMAT</b>    | TRASPORTI E MATERIALI                                                                                                                                                         |
| <b>TUOM</b>      | "TESTO UNICO DELLE DISPOSIZIONI REGOLAMENTARI IN MATERIA DI ORDINAMENTO MILITARE, A NORMA DELL'ARTICOLO 14 DELLA LEGGE 28 NOVEMBRE 2005, N. 246" DECRETO DEL PRESIDENTE DELLA |

|                 |                                             |
|-----------------|---------------------------------------------|
|                 | REPUBBLICA 15 MARZO 2010, N. 90             |
| <b>U.</b>       | UFFICIALI                                   |
| <b>Uf. Imp.</b> | UFFICIO IMPIEGO                             |
| <b>U.F.P.</b>   | UFFICIALI IN FERMA PREFISSATA               |
| <b>UGPF</b>     | UFFICIO GENERALE PIANIFICAZIONE FINANZIARIA |
| <b>un.</b>      | UNITA'                                      |
| <b>UO</b>       | UNITÀ ORGANIZZATIVA                         |
| <b>v.A.</b>     | VARIE ARMI                                  |
| <b>VA</b>       | VERTICE D'AREA                              |
| <b>VFP1</b>     | VOLONTARI IN FERMA PREFISSATA DI 1 ANNO     |
| <b>VFP4</b>     | VOLONTARI IN FERMA PREFISSATA DI 4 ANNI     |
| <b>VFI</b>      | VOLONTARIO IN FERMA INIZIALE                |
| <b>VFT</b>      | VOLONTARIO IN FERMA TRIENNALE               |
| <b>VPN</b>      | VIRTUAL PRIVATE NETWORK                     |
| <b>VSP</b>      | VOLONTARI IN SERVIZIO PERMANENTE            |

|                                                                                   |                                                                                                                                                                                                                                                        |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <b>Informativa di base agli interessati, ai sensi degli artt. 13 e 14 del Reg. (UE) 2016/679 (GDPR), per il personale in rapporto di dipendenza di servizio o impiego con il Titolare del trattamento dati personali della F.A. - vers. giu. 2021.</b> |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

1. Ai sensi degli articoli 13 e 14 del Reg. UE 679/2016 (GDPR), si informano gli interessati che il trattamento dei dati personali da loro forniti o, comunque, acquisiti nel corso dello svolgimento dell'attività amministrativa, è finalizzato esclusivamente all'espletamento delle attività istituzionali del Titolare, in particolare per la gestione del rapporto di impiego e servizio. Il trattamento dei dati personali, particolari e giudiziari avverrà a cura del personale a ciò appositamente autorizzato, secondo le disposizioni tecniche e di sicurezza impartite dal Titolare, con l'utilizzo di procedure parzialmente informatizzate e con l'ausilio di banche-dati automatizzate, nei modi e nei limiti necessari per il perseguimento delle finalità per cui i dati personali e particolari sono raccolti e/o successivamente trattati; ciò anche nel caso si renda necessaria la comunicazione a terzi, ai sensi delle norme vigenti.
2. Il conferimento di tali dati è obbligatorio e indispensabile ai fini delle attività istruttorie connesse con i procedimenti amministrativi di competenza del Titolare, per garantire gli adempimenti connessi dal rapporto di lavoro/servizio, per adempiere a obblighi legali del Titolare, per l'esecuzione di compiti di interesse pubblico o connesso con l'esercizio di pubblici poteri di cui è investito il Titolare. Per questo motivo, i trattamenti suesposti hanno condizione di liceità che prescinde dal consenso dell'interessato.
3. Per quanto precede, si comunica che:
  - a) il Titolare del trattamento è lo Stato Maggiore dell'Esercito, con sede in Roma 00187, via XX Settembre, 123/A. Il Titolare può essere contattato a mezzo *e-mail* ai seguenti indirizzi:
    - posta elettronica ordinaria: [statesercito@esercito.difesa.it](mailto:statesercito@esercito.difesa.it)
    - posta elettronica certificata: [statesercito@postacert.difesa.it](mailto:statesercito@postacert.difesa.it)
  - b) il **Referente del Responsabile della Protezione dei Dati personali è il Capo del I Reparto dello SME, con sede in Roma 00187 in via XX Settembre 123/A e può essere contattato via *e-mail* all'indirizzo: [smelegale@esercito.difesa.it](mailto:smelegale@esercito.difesa.it)**
  - c) il Responsabile per la Protezione dei Dati personali, come reso noto sul sito istituzionale [www.difesa.it](http://www.difesa.it), può essere contattato a mezzo *e-mail* ai seguenti indirizzi:
    - posta elettronica ordinaria: [rpd@difesa.it](mailto:rpd@difesa.it)
    - posta elettronica certificata: [rpd@postacert.difesa.it](mailto:rpd@postacert.difesa.it)
  - d) la base giuridica del trattamento dei dati personali effettuato dal Titolare è costituita, principalmente, dal D.Lgs. 66/2010 Codice dell'Ordinamento Militare (COM) e nel DPR 90/2010 Testo Unico dell'Ordinamento Militare (TUOM) (e, più in particolare, agli artt. da 1053 a 1075 TUOM) e norme collegate. Il trattamento dati in esame è pertanto conforme alle previsioni del GDPR alle fattispecie di cui:
    - all'art. 6, co.1, let. b), c), d), e), f) per i dati comuni;
    - all'art. 9, co. 2, let b), c), f), g), h), i) per le categorie particolari di dati;
    - all'art. 10, relativamente a condanne penali e reati o connesse misure di sicurezza;
  - e) le finalità del trattamento sono direttamente collegate alla gestione del rapporto di impiego e servizio, per finalità connesse e/o strumentali allo svolgimento delle attività istituzionali del Titolare, normativamente previste o nell'interesse del Titolare stesso;
  - f) nel rispetto delle finalità, le tipologie di dati oggetto del trattamento sono:
    - “dati comuni”, ai sensi dell'art. 4 GDPR, in particolare quelli anagrafici, familiari, fiscali, amministrativi, d'impiego, curriculari, disciplinari;
    - “categorie particolari di dati”, ai sensi art. 9 GDPR, in particolare dati relativi alla salute, quali dati clinici, medico-legali, vaccinali, psicologici, psico-attitudinali e biometrici;
    - “dati giudiziari”, ai sensi art. 10 GDPR, solo nel caso eventuali condanne penali e connesse misure di sicurezza;
  - g) i dati personali saranno trattati solo dal personale con competenze tecniche adeguate, all'uopo appositamente formato e specificatamente autorizzato, osservando scrupolosamente le misure di sicurezza disposte per garantire integrità, riservatezza e disponibilità dei dati personali;



**Informativa di base agli interessati, ai sensi degli artt. 13 e 14 del Reg. (UE) 2016/679 (GDPR), per il personale in rapporto di dipendenza di servizio o impiego con il Titolare del trattamento dati personali della F.A. - vers. giu. 2021.**

- h) non vengono effettuati trattamenti di dati personali mediante l'ausilio di processi decisionali automatizzati, compresa la profilazione, ai sensi dell'art. 4, n. 4 del GDPR;
- i) i dati personali potranno essere comunicati da soggetti operanti in qualità di Titolari e Contitolari del trattamento (quali, a solo titolo esemplificativo e non esaustivo, altri Ministeri, Autorità Giudiziaria, altre Forze Armate e/o di Polizia, strutture Sanitarie, INPS, INAIL, Agenzia dell'Entrate ed ogni altro soggetto pubblico legittimato a trattare i dati), conformemente alle norme vigenti e/o agli eventuali accordi legali. Non è prevista la diffusione di dati personali;
- j) i dati potranno essere trasferiti in paesi Terzi solo se i medesimi hanno aderito alle clausole contrattuali tipo ai sensi dell'art. 46, par. 2, lett. c) e d), o alle norme vincolanti per l'impresa di cui all'art. 47 del GDPR o nel rispetto delle misure derogatorie di cui all'art. 49 del GDPR, laddove consentito ai sensi degli articoli da 1053 a 1075 del D.P.R. n. 90/2010;
- k) nel rispetto delle finalità pubbliche per le quali i relativi dati sono trattati, ivi compresa la tutela degli interessi dell'Amministrazione della Difesa presso le competenti sedi giudiziarie, i dati personali saranno conservati per il tempo strettamente necessario decorso il quale gli stessi saranno distrutti, cancellati o resi anonimi, con le procedure tecniche determinate dal Titolare;
- l) ai sensi del GDPR, sulla base delle condizioni di legittimazione e delle modalità con la quale viene posto in essere il trattamento dati personali, qualora ne ricorrano i presupposti, l'interessato potrà esercitare i diritti riconosciuti dalla legge e, in particolare, il diritto di:
- ottenere l'accesso ai suoi dati personali;
  - chiedere la rettifica o la cancellazione ovvero la limitazione del trattamento;
  - opporsi al trattamento;
  - chiedere la portabilità dei propri dati personali;
  - revocare, l'eventuale consenso, quando sia stato richiesto, sebbene tale revoca non pregiudichi i trattamenti precedenti.
- La relativa istanza dovrà essere formulata al Referente del Titolare, ai recapiti di cui al punto 3;
- m) gli interessati che ritengano che il trattamento dei dati personali a loro riferiti venga effettuato in violazione delle disposizioni di cui al Reg. UE 679/16 potranno presentare l'eventuale reclamo all'Autorità Garante per la protezione dei dati personali, in qualità di Autorità di controllo, con sede in Piazza Venezia n. 11, Scala B – 00187 Roma, o agli indirizzi e-mail: [garante@gpdp.it](mailto:garante@gpdp.it); [protocollo@pec.gpdp.it](mailto:protocollo@pec.gpdp.it).
4. Ulteriori informazioni e dettagli sono reperibili sul sito *intranet* di F.A. alla sezione dedicata alla "Protezione dati personali", all'indirizzo: [https://intranet.esercito.difesa.it/it/prot\\_dati.page](https://intranet.esercito.difesa.it/it/prot_dati.page)

---

PER PRESA VISIONE

GRADO \_\_\_\_\_ COGNOME \_\_\_\_\_ NOME \_\_\_\_\_

LUOGO \_\_\_\_\_ DATA \_\_\_\_\_ FIRMA \_\_\_\_\_



# DENOMINAZIONE ENTE

## AUTORIZZAZIONE AL TRATTAMENTO DEI DATI PERSONALI PER LE ATTIVITÀ DI XXXXXXXX

Il sottoscritto (*GRADO, CONOME, NOME*), in qualità di Comandante del (*Ente che fornisce il servizio*),

- VISTO** il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (di seguito denominato Regolamento/GDPR), con particolare riferimento all'art. 29, il quale prevede che il personale agente sotto l'autorità o il controllo di altro soggetto, come individuato dai rispettivi ordinamenti di Forza Armata in funzione dell'incarico ricoperto, non possa trattare i dati personali se non istruito in tal senso ed a tale scopo;
- VISTO** il Decreto Legislativo 30 giugno 2003, n. 196, recante "Codice in materia di protezione dei dati personali" e successive modifiche e integrazioni (di seguito denominato Codice privacy);
- VISTO** il Decreto Legislativo 15 marzo 2010, n. 66, concernente "Codice dell'Ordinamento Militare" e successive modifiche e integrazioni;
- VISTO** il Decreto del Presidente della Repubblica 15 marzo 2010, n. 90, recante "Testo Unico delle disposizioni regolamentari in materia di Ordinamento Militare" e successive modifiche e integrazioni e, in particolare, gli articoli da 1053 a 1075, concernenti l'identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate dall'Amministrazione della Difesa;
- VISTO** il Codice di comportamento dei dipendenti del ministero della Difesa, di cui al D.M. del 23 marzo 2018, ed in particolare l'art.12, comma 5, laddove è prescritto che "*il dipendente osserva il segreto d'ufficio e la normativa in materia di tutela e trattamento dei dati personali...*";
- VISTO** il Decreto Ministeriale del 18 novembre 2020 con il quale, fra l'altro, sono individuati i soggetti mediante i quali il Ministero della Difesa esercita le funzioni di Titolare;
- VISTO** l'atto dirigenziale, Ordine del Giorno n. 05 del 17 marzo 2021 del Capo di Stato Maggiore dell'Esercito il quale, in qualità di Titolare nell'ambito della Forza Armata Esercito Italiano, ha definito ed attribuito i compiti e le funzioni a soggetti fisici e/o giuridici espressamente designati ed a chiunque agisca sotto la sua Autorità ed ha, al contempo, fornito modalità, obblighi e limiti utili a rendere efficaci ed aderenti alla normativa privacy i trattamenti effettuati nella macro-area del Titolare medesimo verso le unità organizzative di livello dirigenziale anche se periferiche;
- VISTE** tutte le disposizioni vigenti dello "SME", quale Titolare per trattamento dati di F.A. e, in particolare, quelle relative a nomina degli autorizzati, indottrinamento/istruzione degli autorizzati, gestione delle violazioni ai dati personali, tempi di conservazione, misure tecniche organizzative e di sicurezza per il trattamento dati personali;

**VISTA** la circolare n.1033 dello Stato Maggiore dell'Esercito "Gestione della protezione e del trattamento dei dati personali", edizione 2020 che contiene, fra l'altro, specifiche procedure organizzative della F.A. per attagliare le disposizioni normative in materia di "privacy" al contesto lavorativo in cui agiscono gli Enti dell'Esercito Italiano;

**VISTA** la Direttiva del Responsabile della Protezione dei dati personali (RPD/DPO) del Ministero Difesa, prot. n. M\_D GRPD REG2021 0000020 del 20 gennaio 2021;

**VISTO** *(inserire altri documenti specifici riferiti all'attività di trattamento/procedimento amministrativo)*

### **AUTORIZZA**

il *(GRADO, COGNOME, NOME)* nato a \_\_\_\_\_, il \_\_\_\_\_, in qualità di *(indicare incarico/mansione)*, al "trattamento dei dati personali per:  
– *(Indicare/elencare le attività di trattamento da effettuare oggetto del presente atto di nomina)*

Si dà atto, altresì, di aver istruito il predetto, compatibilmente con la funzione da assolvere, in merito a:

1. le previsioni normative generali e particolari riguardanti il trattamento dati personali, incluse ma solo, le norme richiamate nella premessa;
2. i principi generali del trattamento di cui all'art 5 GDPR e, in particolare, in merito alla "minimizzazione" dei dati trattati;
3. i contenuti delle "misure tecniche organizzative e di sicurezza" e sul "Registro delle Attività di trattamento";
4. il riconoscimento e la gestione delle violazioni ai dati personali;
5. ...(eventuali altre prescrizioni)

Roma, li \_\_\_\_\_

Firma del Comandante \_\_\_\_\_

Firma del dell'autorizzato \_\_\_\_\_ \\\



**STATO MAGGIORE DELL'ESERCITO**  
**I Reparto RAGEP**  
**Ufficio Giuridico Legale e Contenzioso**

OGGETTO: Gestione delle violazioni ai  
dati personali (*Personal Data Breach*).

**SCHEDA**

**1. SCOPO**

Istruire e sensibilizzare gli Enti al riconoscimento e alla corretta gestione dei *personal data breach*.

**2. INDICAZIONI GENERALI**

- a. Ai sensi dell'art. 4 del GDPR per violazione dei dati personali (*personal data breach*) si intende la violazione di sicurezza che comporta accidentalmente o dolosamente la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati e comunque trattati.
- b. Ai sensi del combinato disposto dell'art. 33 e del considerando 85 del GDPR, in caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente (Garante per la Protezione Dati Personali) senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.
- c. Ai sensi dell'art. 34 GDPR, quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.
- d. Ai sensi del considerando 86 GDPR, il Titolare del trattamento dovrebbe comunicare all'interessato la violazione dei dati personali senza indebito ritardo, qualora questa violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà della persona fisica, al fine di consentirgli di prendere le precauzioni necessarie. La comunicazione dovrebbe descrivere la natura della violazione dei dati personali e formulare raccomandazioni per la persona fisica interessata intese ad attenuare i potenziali effetti negativi. Tali comunicazioni agli interessati dovrebbero essere effettuate non appena ragionevolmente possibile e in stretta collaborazione con l'autorità di controllo e nel rispetto degli orientamenti impartiti da questa o da altre autorità competenti quali le autorità incaricate dell'applicazione della legge. Ad esempio, la necessità di attenuare un rischio immediato di danno richiederebbe che la comunicazione agli interessati fosse tempestiva, ma la necessità di attuare opportune misure per contrastare violazioni di dati personali ripetute o analoghe potrebbe giustificare tempi più lunghi per la comunicazione.
- e. In caso di presunto *personal data breach* riferito ad un trattamento compiuto con mezzi digitali, l'Ente coinvolto, dovrà effettuare anche la segnalazione dell'evento/incidente informatico secondo quanto stabilito dalla Direttiva 6006 "La Gestione degli Incidenti Informatici in ambito Esercito, Ed. 2020, dello SME".

**3. PRESCIZIONI SPECIFICHE**

- a. Occorre preliminarmente considerare che **la violazione ai dati personali può occorrere sia in caso di evento doloso** (ad esempio: attacco informatico) **che di evento accidentale** (ad esempio: accesso abusivo ad un data base, perdita di un supporto rimovibile come una chiavetta *usb*, *hard disk*, ecc.). Pertanto, prima ancora di ricostruire le cause di una violazione è indispensabile verificare l'effettiva violazione.
- b. Ai fini della determinazione del verificarsi di un *personal data breach* è necessario tenere presente che **i dati personali possono essere estremamente vari**, atteso che si tratta di

qualunque informazione che anche indirettamente consente l'identificazione di una persona fisica. È importante, pertanto, come impostazione *by design and default* che siano preventivamente identificati i dati necessari per ciascun trattamento.

- c. Il riconoscimento immediato di una violazione si ottiene in sintesi mediante:
  - istruzione costante e ripetuta degli autorizzati al trattamento;
  - processi lavorativi consolidati e standardizzati;
  - procedure di verifica cicliche e controlli accurati.
- d. Tenendo conto del rischio per i diritti e le libertà dell'interessato che la violazione dei dati personali è in grado di generare è estremamente importante riconoscerla tempestivamente per consentire, con la massima celerità (non oltre le 72 ore dalla scoperta della violazione) le comunicazioni formali, nonché l'adozione degli interventi opportuni per eliminare/mitigare l'eventuale rischio generato dal suddetto evento.
- e. L'Ente che venga a conoscenza di un *personal data breach* deve con immediatezza riferire direttamente a I RRAGEP (al momento a mezzo *e-mail*, preferibilmente anticipando la comunicazione con una telefonata) gli elementi descrittivi essenziali del fatto.
- f. L'eventuale Responsabile operante per conto del Titolare di F.A., ove sia oggetto di una violazione ai dati personali, dovrà immediatamente comunicarla all'Ente per il quale effettua il trattamento, onde consentire le successive comunicazioni al Titolare.
- g. Solo I RRAGEP è competente ad effettuare le eventuali notifiche al Garante, mentre rimangono competenze degli Enti le eventuali segnalazioni alle Autorità Giudiziarie, ove necessarie/previste.
- h. È opportuno rammentare che ai sensi dell'art. 34 GDPR, **il Titolare del trattamento può non comunicare la violazione all'interessato quando “ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure vengono applicate ai dati personali”**.

#### **4. ESEMPI DI PERSONAL DATA BREACH**

Al fine di supportare gli Enti nell'identificazione di un *personal data breach*, si riportano di seguito alcuni casi esemplificativi:

- *ransomware* senza un *backup* adeguato;
- *ransomware* con *backup* adeguato che permette però a soggetti non autorizzati l'esfiltrazione dei dati personali;
- il *firmware*, il sistema operativo e il *software* applicativo sui *server*, sui *computer client* componenti di rete e qualsiasi altra macchina sulla stessa *LAN* (compresi i dispositivi *Wi-Fi*) non aggiornati;
- l'assenza della crittografia forte e autenticazione a più fattori, in particolare per l'accesso amministrativo ai sistemi IT;
- gestione inadeguata di chiavi e *password*;
- assenza di un *Computer Security Incident Response Team (CSIRT)* o *Computer Emergency Response Team (CERT)* all'interno dell'organizzazione;
- non vengono regolarmente testati i *Recovery Plan* e una *Business Continuity Plan*;
- i dipendenti adibiti alla gestione della documentazione contenente i dati personali non sono stati formati/sensibilizzati sui metodi per riconoscere e prevenire gli attacchi informatici;
- furto o perdita di un supporto (*cd/dvd/cassetta*) o *pc* contenente un *backup* non criptato e contenente dati personali;
- perdita o distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità;
- impossibilità, in particolare, di accedere ai dati per cause accidentali o per attacchi esterni, *virus*, *malware*;
- trasmissione/invio per errore di dati personali altamente riservati;
- divulgazione non autorizzata dei dati personali;

- smarrimento della documentazione cartacea contenente i dati personali, ivi compresi, in particolar modo, dati sanitari e/o giudiziari. In merito si evidenzia che è sufficiente anche lo smarrimento del plico in fase di spedizione dello stesso;
- la deliberata alterazione di dati personali.

Inoltre, **la perdita della disponibilità “temporanea” dei dati personali (ad esempio un *data base* non funzionante per un lasso prolungato di tempo), può rilevare come *personal data breach*, ex art. 32 del GDPR, in quanto la mancanza di accesso a tali dati può avere un impatto significativo sui diritti e sulle libertà delle persone fisiche.**

## **5. CIRCOSTANZE POTENZIALMENTE FACILITANTI *PERSONAL DATA BREACH***

A titolo esemplificativo e non esaustivo, si riportano di seguito alcuni fattori abilitanti che facilitano il verificarsi di violazioni ai dati personali:

- scarsa formazione/sensibilizzazione del personale autorizzato al trattamento;
- salvataggio delle informazioni in cartelle/condivise;
- creazione di archivi di lavoro temporanei, non previsti;
- utilizzo di strumenti informatici (*hardware/software*) di elaborazione dati non censiti/autorizzati dal Titolare;
- mancato rispetto delle prescrizioni lavorative, con particolare riguardo ai limiti delle specifiche competenze;
- copie/stampe di documenti non necessari, specie se nativi digitali;
- accessi indiscriminati in aree deputate al trattamento dati personali (stanze archivio, uffici personale, segreterie/furerie).

## **6. ELEMENTI ESSENZIALI PER COMUNICARE UN *DATA BREACH***

Nel relazionare a I RRAGEP le circostanze di una presunta violazione ai dati personali, per gli eventuali adempimenti legali, occorre inderogabilmente comunicare i seguenti elementi essenziali:

- tipo di violazione (violazione della riservatezza, dell’integrità e della disponibilità);
- natura, sensibilità e volume dei dati personali;
- misure tecniche predisposte volte a mitigare/eliminare la sottrazione/compromissione dei dati personali;
- *report* contenente l’analisi di rischio, di competenza del reparto *IT*, volto a descrivere l’adeguatezza tecnica delle medesime alla tutela dei dati personali;
- facilità nella identificazione degli interessati;
- gravità delle conseguenze per gli interessati;
- particolarità degli interessati (es. minori);
- particolarità dei responsabili del trattamento (es. personale sanitario);
- numero degli interessati;
- eventuali azioni intraprese sia dall’Ente che dall’interessato coinvolto nella violazione.



**STATO MAGGIORE DELL'ESERCITO**  
**I Reparto Affari Giuridici ed Economici del Personale**  
 Ufficio Giuridico Legale e Contenzioso

Sensibilizzazione al corretto trattamento dei dati personali “particolari” (art. 9 GDPR).

## **1. SCOPO**

Sintetizzare il quadro normativo e organizzativo di F.A. relativamente al trattamento e alla protezione dei dati personali particolari (ex. art. 9 GDPR).

## **2. DATI PERSONALI PARTICOLARI**

- a. I **dati personali “particolari”**, ai sensi dell’art. 9 del Reg. UE 2016/679 GDPR sono dati cosiddetti “sensibili”, perché rivelano l’origine razziale od etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l’appartenenza sindacale, le informazioni relative alla salute o alla vita sessuale; sono altresì inclusi i dati genetici, i dati biometrici e quelli relativi all’orientamento sessuale. In generale, **salvo i casi specifici, espressamente elencati dalle norme, è vietato trattare tali tipologie di dati personali**. In merito, il **Garante** per la protezione dei dati personali, con **provvedimento n. 146 del 2019** chiarisce meglio ambiti, limiti e modalità dei relativi trattamenti dati.
- b. Tali tipologie di dati, con l’eccezione di quelli relativi alla salute, sono **raramente trattati in F.A.**, nell’ambito delle ordinarie attività di gestione del rapporto di lavoro/servizio.

## **3. DATI PERSONALI RELATIVI ALLA SALUTE**

- a. I **dati personali relativi alla salute** sono un sottoinsieme della più ampia categoria dei dati soggetti a trattamento speciale (art. 9 GDPR), in grado di rivelare dettagli estremamente privati della persona e, per questo, sottoposti a tutela ulteriormente rafforzata. A tal riguardo, il **provvedimento del Garante n. 55 del 2019** fornisce ulteriori chiarimenti sull’applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario, stabilendo, in particolare, **l’essenzialità del consenso**, per i dati sanitari trattati con Fascicolo Sanitario Elettronico, *app* mediche o per l’invio via *e-mail*.
- b. **Tali tipologie di dati sono ampiamente trattati in F.A.**, non solo dagli Enti propriamente sanitari. In merito, fermo restando il necessario rispetto di tutte le prescrizioni normative/regolamentari e, in particolare, dell’art. 5 GDPR relativo ai principi del trattamento, si rammenta a titolo di evidenza (non esaustiva delle casistiche possibili) che i dati relativi alla salute, per le finalità previste dal GDPR di cui:
  - all’art. 9, co.2, let “g” (**motivi di interesse pubblico** rilevante sulla base del diritto) possono essere trattati dai **Comandanti di Corpo**, secondo le condizioni di liceità di cui all’art. 6, co.1, let “c” (**obbligo legale**);
  - all’art. 9, co.2, let “i” (motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero) possono essere trattati per obbligo legale dei Comandanti, come per l’emergenza sanitaria in corso da COVID-19;
  - all’art. 9, co.2, let “h” (medicina preventiva/del lavoro, valutazione capacità lavorativa del dipendente, diagnosi, assistenza, ecc.), possono essere trattati solo da specifiche categorie di soggetti, stabilite con L. 24/2017 e norme collegate (personale sanitario).

## **4. PRESCRIZIONI GENERALI SUL TRATTAMENTO**

Le caratteristiche del dato, le operazioni eseguibili, le circostanze e le limitazioni da parte dell’Amministrazione della Difesa nello svolgimento delle proprie funzioni istituzionali, sono riportate nel TUOM negli artt. da 1053 a 1075, mentre i **soggetti responsabili** sono individuati, in generale dalla legge e, più in particolare, dall’**ordinamento militare**.

## **DENOMINAZIONE FILE E DEL CAMPO "OGGETTO" IN FASE DI PREDISPOSIZIONE**

- Annullamento rva n.
- Attività extraprofessionale\_ U\_SU\_GRD\_TRP (*indicare la categoria d'interesse*)
- Avvio\_procedimento disciplinare\_ U\_SU\_GRD\_TRP
- CdV Richiesta\_ U\_SU\_GRD\_TRP
- CdV Richiesta\_Movimenti Collettivi
- Certificato Medico \_ U\_SU\_GRD\_TRP
- CMD\_Richiesta\_ U\_SU\_GRD\_TRP
- Comandata\_Evento/Attività\_EDRC\_Luogo
- Conclusione procedimento\_disciplinare U\_SU\_GRD\_TRP
- Congedo di maternità
- Congedo di paternità
- Congedo parentale
- Congedo parentale in deroga
- Comunicazione/Conclusione Infortunio\_ U\_SU\_GRD\_TRP
- Documenti Causa di Servizio\_ U\_SU\_GRD\_TRP
- Documentazione Sanitaria\_Mod. GL\_ U\_SU\_GRD\_TRP
- Documentazione Caratteristica\_ U\_SU\_GRD\_TRP
- Dichiarazione di pronto impiego
- Esercizio Diritto allo studio\_PERMESSO\_LICENZA PER ESAMI
- Esercizio Diritto allo studio\_GIUSTIFICATIVO
- Forza presente mensile (indicare mese di riferimento)
- Idoneità sanitaria=IS\_U\_SU\_GRD\_TRP
- Indennità accessorie\_CFG
- Indennità accessorie\_CFI

- Indennità festivi\_s\_festivi\_mese di riferimento
- Indennità marcia
- Intervento assistenziale\_U\_SU\_GRD\_TRP
- Invio Infermeria Presidiaria\_U\_SU\_GRD\_TRP
- Istanza\_accesso atti
- Istanza art. 1369\_Cancellazione Sanzioni Disciplinari
- Istanza\_conferimento
- Licenza
- Licenza GMF
- Licenza matrimoniale
- Licenza straordinaria di trasferimento
- Licenza straordinaria donazione sangue
- Licenza straordinaria legge 104\_permessi
- Licenza straordinaria permesso elettorale
- Licenza straordinaria permesso elettorale\_GIUSTIFICATIVO
- Malattia del figlio
- Ordine del giorno n.
- Ordine di servizio n.
- Ordine Operazione EAME2024 - si indicano le prime due iniziali del nome completo EAME2024 (Eagle Meteor\_2024) – (*esempio*)
- Ordine Logistico EAME2024 - si indicano le prime due iniziali del nome completo EAME2024 (Eagle Meteor\_2024) – (*esempio*)
- Ordine Movimento EAME2024 - si indicano le prime due iniziali del nome completo EAME2024 (Eagle Meteor\_2024) – (*esempio*)
- Permesso per esami\_accertamenti clinici\_medico specialistici
- Permesso per esercizio cariche amministrative
- Permesso per esercizio cariche amministrative\_GIUSTIFICATIVO

- Permesso Sindacale
- Provvedimento Medico Legale U - (PML\_U)
- Provvedimento Medico Legale SU - (PML\_SU)
- Provvedimento Medico Legale Grd - (PML\_Grd)
- Provvedimento Medico Legale Tr - (PML\_Tr)
- Rettifica rva n.
- Riposo per allattamento
- Richiesta\_Visita\_Medica Specialistica
- Trasmissione CdV\_Annullamento
- Trasmissione CdV\_Chiusura
- Trasmissione CdV\_Restituzione
- Trasmissione\_atti\_U\_SU\_GRD\_TR
- Trasmissione\_denuncia\_querela
- Trasmissione\_relazione di servizio
- Variazioni\_ODG
- Verbali PEFO



## 33° REGGIMENTO SUPPORTO TATTICO E LOGISTICO "AMBROSIANO"

(Ufficio/Btg/Compagnia)

Caserma "Ugo Mara" via per Busto, 20-21058 Solbiate Olona (VA)  
Indirizzo di Posta elettronica certificata: [rgtstal@postacert.difesa.it](mailto:rgtstal@postacert.difesa.it)

### MODULO DI RICHIESTA Attivazione/Variazione/Cancellazione RUOLO AdHoc (da stampare in pdf e inviare)

Il sottoscritto \_\_\_\_\_, nato a \_\_\_\_\_ il \_\_\_\_\_,  
Grado Nome COGNOME localit  GG/MM/AAAA

email funzionale \_\_\_\_\_@[rgtstl33.esercito.difesa.it](mailto:rgtstl33.esercito.difesa.it), tel. 117 \_\_\_\_\_

#### CHIEDE

|                              |  |
|------------------------------|--|
| nuova attivazione ruolo      |  |
| variazione/spostamento ruolo |  |
| cancellazione ruolo          |  |

Solbiate Olona (VA), li \_\_\_\_\_

Responsabile UO

#### SI AUTORIZZA

Responsabile Servizio Adhoc



## 33° REGGIMENTO SUPPORTO TATTICO E LOGISTICO "AMBROSIANO"

\_\_\_\_\_  
(Ufficio/Btg/Compagnia)

*Caserma "Ugo Mara" via per Busto, 20-21058 Solbiate Olona (VA)  
Indirizzo di Posta elettronica certificata: [rgtstal@postacert.difesa.it](mailto:rgtstal@postacert.difesa.it)*

### MODULO DI RICHIESTA ANNULLAMENTO REGISTRAZIONE PROTOCOLLO AdHoc (da stampare in pdf e inviare)

Il sottoscritto \_\_\_\_\_, nato a \_\_\_\_\_ il \_\_\_\_\_,  
Grado Nome COGNOME localit  GG/MM/AAAA

email funzionale \_\_\_\_\_@[rgtstl33.esercito.difesa.it](mailto:rgtstl33.esercito.difesa.it), tel. 117 \_\_\_\_\_

Responsabile U.O. \_\_\_\_\_, chiede l'annullamento della  
(Ufficio/Btg/Compagnia)

Registrazione del protocollo n  \_\_\_\_\_ in data \_\_\_\_\_  
GG/MM/AAAA

Per il seguente motivo:

\_\_\_\_\_  
\_\_\_\_\_

Con la presente si dichiara inoltre che il protocollo in questione   privo di classificazione e fascicolazione.

Solbiate Olona (VA), li \_\_\_\_\_

\_\_\_\_\_  
Responsabile UO

**SI AUTORIZZA**

\_\_\_\_\_  
Responsabile Servizio Adhoc



## **33° REGGIMENTO SUPPORTO TATTICO E LOGISTICO AMBROSIANO** **COMANDO**

*Caserma "Ugo Mara" via per Busto, 20 - 21058 Solbiate Olona (VA)*  
*Indirizzo di PEC: [rgtstal@postacert.difesa.it](mailto:rgtstal@postacert.difesa.it)*



Allegati: 1  
Annessi: 1

(vds segnatura @dhoc)  
Cap. ZAPPIA F. 1176417  
[aiutmagg@rgtstl33.esercito.difesa.it](mailto:aiutmagg@rgtstl33.esercito.difesa.it)

**OGGETTO:** Manuale di gestione del sistema di protocollo informatico e gestione documentale - @DhOC, Edizione 2024.

A ELENCO INDIRIZZI IN ALLEGATO A

^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^

1. Questo Comando ha approvato il Manuale di gestione in oggetto (in annesso) per la scrupolosa osservanza da parte del personale che a vario titolo utilizza il sistema di protocollo informatico denominato @DhOC.
2. Il Manuale in parola definisce, in ossequio alle vigenti disposizioni, le attività di gestione e trattamento dei documenti gestiti dal sistema di protocollo informatico, al fine di garantire il più possibile la corretta gestione e la riservatezza necessaria, nel pieno rispetto delle norme a tutela della privacy.
3. Per quanto precede, vogliano codesti reparti diramare il presente manuale a tutto il personale avente titolo. La presente lettera costituisce parte integrante del documento che, ove stampato, dovrà includerla in Annesso "I".

**IL COMANDANTE**  
**(Col. f. (par.) t.ISSMI Amos VIRGONA)**

## ELENCO INDIRIZZI

|                   |                                                |             |
|-------------------|------------------------------------------------|-------------|
| A                 | UFFICIO PERSONALE                              | <u>SEDE</u> |
|                   | UFFICIO LOGISTICO                              | <u>SEDE</u> |
|                   | UFFICIO OAI                                    | <u>SEDE</u> |
|                   | SEZIONE AMMINISTRATIVA                         | <u>SEDE</u> |
|                   | BATTAGLIONE SUPPORTO                           | <u>SEDE</u> |
|                   | COMPAGNIA COMANDO E SUPPORTO LOGISTICO         | <u>SEDE</u> |
|                   | SOTTUFFICIALE DI CORPO                         | <u>SEDE</u> |
|                   | RESPONSABILE SERVIZIO PREVENZIONE E PROTEZIONE | <u>SEDE</u> |
|                   | COMPAGNIA BERSAGLIERI                          | <u>SEDE</u> |
|                   | COMPAGNIA SUPPORTO ALLO SCHIERAMENTO           | <u>SEDE</u> |
|                   | COMPAGNIA TRASPORTI                            | <u>SEDE</u> |
|                   | COMPAGNIA COMMISSARIATO                        | <u>SEDE</u> |
| e per conoscenza: |                                                |             |
|                   | BRIGATA DI SUPPORTO AL (HQ) NRDC-ITA           | <u>SEDE</u> |
|                   | SM - Ufficio Personale e Segreteria            |             |