IL MODELLO ORGANIZZATIVO *PRIVACY* DELL'ARMA DEI CARABINIERI

IL MODELLO ORGANIZZATIVO *PRIVACY* DELL'ARMA DEI CARABINIERI

1. FINALITA' E AMBITO DI APPLICAZIONE

a. Finalità

Il presente documento:

- definisce la politica interna all'Arma dei Carabinieri volta a proteggere le persone fisiche e a garantire i loro diritti e le loro libertà fondamentali attraverso l'accoglimento dei principi della protezione dei dati personali nei processi organizzativi, in modo da assicurarne un livello di protezione adeguato ai rischi connessi ai trattamenti;

Considerando 78 e art. 24 GDPR

- scaturisce dalla integrazione e aggiornamento delle misure tecniche ed organizzative fissate in ambito istituzionale con la circolare dell'Ufficio:
  - Operazioni del Comando Generale n.1128/28-126-6-1997 datata 2 luglio 2019 in forza della quale sono state adottate le misure organizzative per regolare i trattamenti di dati personali eseguiti per finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali;
  - Relazioni con il Pubblico n. 123/26-1-2018 del 10 gennaio 2020, finalizzata ad individuare le misure organizzative per regolare i trattamenti di dati personali eseguiti per finalità diverse da quelle di polizia.

Con il presente documento vengono stabiliti in particolare:

- ruoli e responsabilità;
- le regole da seguire per svolgere determinate operazioni;
- le sequenze di attività e gli eventi che innescano una certa attività o decisione.

b. Ambito di applicazione

Il documento è vincolante per tutto il personale dipendente dell'Arma dei Carabinieri che esegue trattamenti di dati personali.

c. Riferimenti normativi

L'Arma dei Carabinieri, in qualità di ***"titolare del trattamento"*** deve applicare:

- la Direttiva UE 2016/680, recepita nell'Ordinamento Italiano con il D.Lgs. 51/2018 per i trattamenti eseguiti per finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali (di seguito indicate come *"finalità di polizia"*);
- il D.P.R. 15/2018 recante l'individuazione delle modalità di attuazione dei principi del Codice in materia di protezione dei dati personali relativamente al trattamento dei dati effettuato, per le finalità di polizia, da organi, uffici e comandi di polizia;
- il D.M. Interno 24.05.2017 recante l'individuazione dei trattamenti di dati personali effettuati dal Centro elaborazione dati del Dipartimento della pubblica sicurezza o da Forze di polizia sui dati destinati a confluirvi, ovvero da organi di pubblica sicurezza o altri soggetti pubblici nell'esercizio delle attribuzioni conferite da disposizioni legislative o regolamentari - effettuati con strumenti elettronici e i relativi titolari;
- il Regolamento (UE) 2016/678 (c.d. **GDPR: General Data Protection Regulation**) in relazione ai trattamenti di dati personali che esegue *per altre diverse finalità* (ad esempio, gestione del personale, dei concorsi per l'arruolamento e del sito web);

- il D.Lgs. 196/2003, c.d. "Codice Privacy novellato" che reca disposizioni per l'adeguamento dell'ordinamento nazionale al GDPR;
- le linee guida, le raccomandazioni e le migliori prassi (c.d *"Soft Law"*) pubblicate dal Garante per la Protezione dei Dati Personali e dal Comitato Europeo per la Protezione dei Dati (c.d. ***EDPB: European Data Protection Regulation*** – già denominato - sotto la vigenza dell'abrogata Direttiva UE 95/46/CE - ***WP29: Working Party 29***) al fine di promuovere l'applicazione coerente del GDPR.

Art.2 D.Lgs. 196/2003

Art. 154 bis, D.Lgs.196/2003 e Art.70, paragrafo 1, lett. e) GDPR

Segnale di attenzione

I Regolamenti (UE) sono fonti del diritto che si applicano automaticamente e in modo uniforme a tutti i paesi dell'UE non appena entrano in vigore e, senza bisogno di essere recepiti nell'Ordinamento nazionale, sono vincolanti in tutti i loro elementi.
Nell'Ordinamento Italiano sono fonti "Super-primarie" (vds. art. 117, 1° comma Costituzione) ponendosi, nella gerarchia delle fonti, ***al di sopra le fonti primarie***: Leggi Ordinarie, Decreti legge e Decreti Legislativi.
I Regolamenti (UE) comprendono *"Considerando"* che motivano in modo conciso le norme essenziali e gli *"Articoli"*. I commi degli articoli sono denominati *"Paragrafi"* (l'uso del termine "comma"- che in inglese significa "virgola" - può ingenerare confusione).

d. Oggetto di tutela

L'oggetto di tutela dell'intera normativa, seppure continui ad essere qualificato atecnicamente, per convenzione, come *"privacy"*, è la **protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché la tutela dei loro diritti e delle loro libertà fondamentali, con particolare riguardo al diritto alla protezione dei dati personali**.

Art. 1 D.Lgs.51/2019 e art. 1 GDPR

La rilevanza dell'oggetto di tutela postula la necessità di definire ed attuare misure tecniche e organizzative volte a garantire un livello di protezione e sicurezza dei dati personali, trattati in ambito istituzionale, adeguato ai connessi rischi per i diritti e le libertà fondamentali.
A tal fine il presente documento è volto a disegnare una *cornice di salvaguardia dei processi organizzativi* che possa garantire un *livello base di protezione dei dati personali* da elevare, di volta in volta, in occasione del rimodellamento dei diversi processi organizzativi.

Considerando 75 e 85 GDPR

2. DEFINIZIONI

- ***"Dato personale"***: qualsiasi informazione riguardante una persona fisica identificata o identificabile (***interessato***);
- ***"Trattamento"***: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati, 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, la diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

Art.2 D.Lgs.51/2018 e art. 4 GDPR

- ***"Archivio"***: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
- "***Titolare del trattamento e Autorità competente":*** l'Arma dei Carabinieri che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali;
- ***"Contitolare del trattamento"***. la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, quale titolare del trattamento, determina, congiuntamente all'Arma dei Carabinieri, le finalità e i mezzi di un trattamento di dati personali;
- ***"Esercente le funzioni di titolare"***: il dirigente dell'Arma dei Carabinieri al quale è attribuito il potere decisionale circa le finalità e i mezzi del trattamento di dati personali;
- ***"Designato"***: Il Dirigente/Comandante/Capo Ufficio compreso nell'elenco in **Allegato 1**, al quale, in applicazione dell'art. 2 quaterdecies del D.Lgs. 196/2003, sono attribuiti specifiche competenze e funzioni connesse al trattamento di dati personali;
- ***"Autorizzato"***: il dipendente dell'Arma dei Carabinieri specificamente autorizzato, previa istruzione, a trattare dati personali;
- ***"Responsabile del trattamento"***: i fornitori, persone fisiche o giuridiche, che trattano dati personali per conto dell'Arma dei Carabinieri.
- ***"Destinatario":*** la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali dall'Arma dei Carabinieri;
- ***"Terzo":*** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
- ***"Consenso dell'interessato":*** qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento
- ***"Violazione dei dati personali (c.d. data breach)"***: la violazione della sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
- ***"Categorie particolari di dati personali":*** dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché 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.
- ***"Dati genetici"***: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica, che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione.
- ***"Dati biometrici":*** i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
- ***"Dati relativi alla salute":*** i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.

- ***"File di log":*** registro degli accessi e delle operazioni.

3. L'ORGANIGRAMMA PRIVACY: RUOLI E RESPONSABILITÀ DEL PERSONALE

a. *Premessa*

Il fondamentale principio costituzionale secono cui gli appartenenti all'Arma devono svolgere il loro servizio con disciplina ed onore, assume maggiore rilevanza nel momento in cui si sviluppano le attività istituzionali che comportano l'esecuzione di trattamenti di dati personali, poiché l'oggetto di tutela della normativa di settore è costituito dai diritti e dalle libertà fondamentali delle persone fisiche riconosciuti e garantiti dall'art. 2 della Costituzione e dalla Carta dei Diritti Fondamentali dell'Unione Europea (c.d. "Carta di Nizza").

Art. 97 Cost.

A tale scopo, viene quindi delineato il modello organizzativo dell'Arma attraverso l'attribuzione di ruoli e responsabilità a tutti i soggetti dell'Istituzione in linea con la normativa di settore.

b. *Figure previste dal D.Lgs. 51/2018 e dal GDPR*

L'"organigramma privacy" disegnato dal D.Lgs.51/2018 e dal GDPR prevede cinque figure coinvolte nel trattamento di dati personali:

- il *Titolare*;
- il *Contitolare*;
- il *Responsabile della protezione dei dati*;
- il *Responsabile del trattamento*;
- l'*Autorizzato al trattamento*.

Art. 2 D.Lgs. 51/2018 e Art. 4, par. 1, n 10) e art. 37 GDPR

c. *Cosa prevede il D.Lgs. 196/2003 (Codice Privacy Novellato)*

Ad integrazione di quanto previsto dal GDPR, il "Codice Privacy novellato", al fine di garantire nelle organizzazioni complesse un'effettiva governance del sistema di protezione dei dati, sancisce che il titolare del trattamento:

- può attribuire *specifici compiti e funzioni connessi al trattamento di dati personali a persone fisiche che operano sotto la sua autorità espressamente designate*;
- individua *le modalità più opportune per autorizzare* al trattamento dei dati personali le persone che operano sotto la propria autorità diretta.

Art.2 quaterdecies D.Lgs. 196/2003

d. *Modalità di attribuzione di compiti e funzioni in ambito istituzionale*

In tale quadro normativo, l'"Organigramma privacy dell'Arma" comprende:

- le figure espressamente previste dal D.Lgs. 51/2019 e dal GDPR;
- quattro specifici nuovi ruoli:
  - il *Manager Privacy;*
  - gli *Esercenti le funzioni di Titolare;*
  - i *Referenti Privacy;*
  - i *Designati*.

Questi nuovi ruoli sono stati formalizzati in applicazione del citato art. 2 quaterdecies del Codice Privacy Novellato, attraverso il riconoscimento che le competenze gestionali e organizzative necessarie a garantire la protezione dei dati personali sono già contenute "*in*

nuce" nei compiti di comando, direzione e controllo attribuiti dal Codice dell'Ordinamento Militare e dai documenti ordinativi ad alcune categorie di dipendenti dell'Arma.

Quindi, salvo per la figura tecnica del *Manager Privacy*, più che attraverso una vera e propria delega di compiti e funzioni, i nuovi ruoli nel modello organizzativo sono stati istituiti applicando il *"principio di effettività",* cioè polarizzando al trattamento dei dati personali i compiti e le funzioni già attribuite dal C.O.M. e dai documenti ordinativi a particolari soggetti.

Ciò premesso, vengono di seguito delineati i vari ruoli privacy in ambito isituzionale, con la correlativa descrizione dei compiti, delle funzioni e delle responsabilità attribuite.

3.1. "RUOLI PRIVACY" PREVISTI DAL D.LGS.51/2018 E DAL GDPR

a. Il Titolare del trattamento

Titolare del trattamento è l'Arma dei Carabinieri che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.

L'Arma, quale titolare ha la responsabilità generale per qualsiasi trattamento di dati personali che effettua direttamente o che altri effettuano per suo conto. Il Comandante Generale, rappresentante dell'Arma, nell'esercizio delle sue specifiche attribuzioni, gestisce tale responsabilità determinando le modalità di funzionamento dei comandi, reparti, unità, istituti ed enti vari nei settori di attività tecnico-operativa, comprendenti anche il settore della protezione dei dati personali.

Considerando 74 GDPR

Art.164 C.O.M.

b. Il Contitolare del trattamento

Contitolare del trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, quale titolare del trattamento, determina congiuntamente all'Arma dei Carabinieri le finalità e i mezzi di un trattamento di dati personali. Può sussistere una situazione di contitolarità nel caso di accordi e protocolli di collaborazione stipulati dall'Istituzione con altre amministrazioni pubbliche o Enti privati, che comportano un trattamento di dati personali le cui finalità e modalità siano determinate congiuntamente.

Art. 17 D.Lgs. 51/2018 e Art. 26 GDPR

Nei casi di contitolarità, l'Arma e i Contitolari del trattamento determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal D.Lgs. 51/2018 e dal GDPR, con particolare riguardo all'esercizio dei diritti degli interessati, e le rispettive funzioni di comunicazione delle informazioni.

Con l'accordo di contitolarità deve essere sempre designato il punto di contatto per gli interessati. Indipendentemente dalle disposizioni di tale accordo, gli interessati possono esercitare i loro diritti nei confronti di ciascun titolare del trattamento.

c. Il Responsabile della Protezione dei Dati

Il Responsabile della Protezione dei Dati svolge le funzioni di consulente dell'Arma dei Carabinieri e punto di contatto del Garante della Protezione dei dati personali. In particolare il D.Lgs. 51/2018 ed il GDPR gli attribuiscono i compiti di:

Artt.28-30 D.Lgs.51/2018 e Artt. 37-39 GDPR

- informare e fornire consulenza a tutto il personale dell'Arma in merito agli obblighi da adempiere nel settore della protezione dei dati;
- sorvegliare l'osservanza del GDPR nonché delle politiche definite in ambito istituzionale, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;

- fungere da punto di contatto con il Garante per la Protezione dei Dati Personali.

Il Responsabile della Protezione dei Dati deve essere tempestivamente ed adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.

d. Il Responsabile (e il sub responsabile) del trattamento

Art.18 D.Lgs.51/2018 e Art. 28 GDPR

Allorchè l'Arma, per esigenze organizzative, ha la necessità di *esternalizzare una attività* che comporta un trattamento di dati personali affidandola ad un fornitore, sussiste l'obbligo posto dal D.Lgs. 51/2018 e dal GDPR di ricorrere unicamente ad un responsabile del trattamento che presenti *garanzie sufficienti*, per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti degli interessati.

Art. 28 GDPR, par. 3, GDPR

Il fornitore, come responsabile del trattamento deve essere vincolato all'Arma dei Carabinieri, per conto della quale tratta i dati personali, attraverso ***un contratto o altro atto giuridico*** che fissi *precise istruzioni* e *pertinenti condizioni di garanzia*.

E' quindi necessario che ogni contratto di fornitura venga ***corredato con un altro contratto*** che regoli il rapporto tra l'Arma ed il fornitore nel suo ruolo di *Responsabile del trattamento*. *Tale contratto deve prevedere l'oggetto, la durata, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento*. Lo stesso contratto deve prevedere anche che il responsabile del trattamento:

- agisca soltanto su istruzione documentata dell'Arma dei Carabinieri;
- garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
- adotti tutte le misure di sicurezza richieste;
- ricorra ad un sub-responsabile solo previa autorizzazione dell'Arma dei Carabinieri;
- assista l'Arma dei Carabinieri con ogni mezzo adeguato per garantire il rispetto delle disposizioni relative ai diritti dell'interessato e agli adempimenti da porre in essere in occasione di eventuali violazioni di sicurezza;
- su scelta dell'Arma dei Carabinieri cancelli o restituisca tutti i dati personali una volta terminata la prestazione dei servizi di trattamento di dati e cancelli le copie esistenti, salvo che il diritto dell'Unione europea o la legge preveda la conservazione dei dati;
- metta a disposizione dell'Arma le informazioni necessarie a dimostrare il rispetto delle condizioni prescritte dalla normativa *privacy*, contribuendo alle attività di *audit*.

Segnale di attenzione

*Per la predisposizione del contratto con il Responsabile del trattamento è possibile anche fare riferimento ai nuovi modelli di "Clausole Contrattuali Tipo" che la Commissione UE ha adottato con la Decisione di Esecuzione 2021/915 del 4 giugno 2021 (in **Allegato 2**).*

e. Gli Autorizzati

Artt. 29 e 32, paragrafo 4 GDPR

Tutto il personale dipendente dell'Arma dei Carabinieri che ha accesso ai dati personali non può trattare tali dati se non è specificamente autorizzato ed istruito.

Questa prescrizione costituisce anche una fondamentale misura di sicurezza dei trattamenti.

Come misura organizzativa strutturale di carattere generale, con provvedimento in **Allegato 3**, a firma del *Manager Privacy*, è autorizzato al trattamento dei dati personali tutto il personale in servizio presso l'Arma dei Carabinieri che tratta dati personali in relazione alle competenze della unità organizzativa (Reparto, Comando, Ufficio) alla quale è stato assegnato, salvo diverse determinazioni adottate, in applicazione dell'art. 2 quaterdecies del Codice privacy novellato, per attribuire specifici compiti e funzioni finalizzate a garantire la protezione dei dati personali.

I ***Comandanti/Capi Ufficio*** che rivestono il ruolo di DESIGNATI (vds. Elenco in **Allegato 1**) ***devono integrare la nomina*** di carattere generale attribuendo, con lettera formale - come da modulo in **Allegato 4** - una specifica nomina di autorizzato a tutto il personale dipendente che ***svolge le funzioni di tecnico informatico*** e/o ***esegua il trattamento di***:

Punto 12.1 UNI PdR 43.1:2018

- ***categorie particolari di dati personali*** (*cioè dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché 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*);
- ***dati personali relativi a condanne penali o reati***.

Segnale di attenzione

Il personale autorizzato al trattamento che agisca *al di fuori del perimetro delineato dall'autorizzazione* e dalle istruzioni *esegue un trattamento non autorizzato.*
Casi emblematici di trattamenti non autorizzati ed illeciti sono la diffusione tramite servizi personali di messaggeria istantanea (tipo whatsapp o telegram) o social media (facebook, instagram etc) di video, foto o informazioni raccolte da militari nel corso del servizio per finalità istituzionali.
*In tali casi, il militare, di fatto perde la qualifica di "**autorizzato**" ed assume la qualifica giuridica di "**terzo**", indicato all'art.4, par,1 n. 10 GDPR e come tale può essere corresponsabile o responsabile unico di eventuali danni cagionati agli interessati ed all'erario in violazione della normativa privacy.*

Punto 19, Linee Guida EDPB 7/2020

3.2 RUOLI PRIVACY ATTRIBUITI DALL'ARMA DEI CARABINIERI IN APPLICAZIONE DELL'ART. 2 QUATERDECIES DEL D.LGS.196/2013

a. Il Manager Privacy

Il *Manager Privacy*, previsto dalla standard nazionale UNI 11697:2017, è una figura di garanzia, che assiste il Comandante Generale nelle attività di coordinamento di tutti i soggetti coinvolti nel trattamento di dati personali all'interno dell'Arma, assicurando il rispetto delle norme e il mantenimento di un adeguato livello di misure organizzative, di sicurezza e di protezione dei dati.
A tale figura sono attribuiti i seguenti compiti:

- assicurare il rispetto e l'applicazione delle norme in materia di protezione dei dati personali nei processi sviluppati da tutte le unità organizzative dell'Arma;

- svolgere attività di assistenza al Comandante Generale, quale Autorità *Titolare del trattamento*, nella definizione e nella gestione del sistema di protezione dei dati personali dell'Istituzione comprendente le politiche, le procedure e i processi per gestire e monitorare i requisiti (organizzativi, legali e relativi ai rischi connessi al trattamento) e nel coordinamento di tutti i soggetti coinvolti nel trattamento.

Il *Manager Privacy* in particolare:

- definisce e implementa le politiche e le procedure del modello organizzativo *privacy* istituzionale, fornendo, ai soggetti decentrati/delegati all'esercizio delle funzioni di titolare del trattamento dei dati personali, le linee di azione per lo svolgimento dei relativi compiti;
- concorre alla definizione e garantisce l'adozione di misure tecniche e organizzative adeguate per garantire che tutti i trattamenti di dati personali eseguiti in ambito istituzionale siano conformi alla normativa di settore;
- coordina le figure delegate dal titolare del trattamento dei dati personali, indirizzandole nell'adozione e nell'applicazione delle misure tecniche e organizzative adeguate per garantire la conformità dei trattamenti dei dati personali eseguiti in ambito istituzionale con la normativa di settore;
- governa, avvalendosi rispettivamente dell'Ufficio Operazioni e dell'Ufficio Relazioni con il Pubblico, i processi organizzativi relativi al trattamento dei dati personali per finalità:
  - di prevenzione, indagine, accertamento e perseguimento dei reati o esecuzione di sanzioni penali;
  - diverse da quelle "di polizia";
- vigila sul raggiungimento nonché sul mantenimento di un livello di protezione dei dati personali adeguato al rischio per i diritti e libertà fondamentali delle persone;
- promuove lo svolgimento di corsi di aggiornamento e formazione tecnico professionale del personale autorizzato al trattamento dei dati;
- analizza e verifica le valutazioni di impatto sulla protezione dei dati personali, consultando in merito il RPD.

b. Gli Esercenti le funzioni di titolare

Artt. 169, 170, 844 C.O.M.

In conformità all'assetto organizzativo dell'Arma dei Carabinieri, in base ai compiti di alta direzione, coordinamento e controllo dei Comandi dipendenti, fissati dal Codice dell'Ordinamento Militare e dai documenti ordinativi, i soggetti individuati per l'esercizio delle funzioni di titolare dei trattamenti dei dati personali, ciascuno nel rispettivo ambito di competenza sono:

- il Vice Comandante Generale dell'Arma dei Carabinieri;
- il Capo di Stato Maggiore del Comando Generale dell'Arma;
- i Comandanti Interregionali;
- il Comandante delle Scuole dell'Arma dei Carabinieri;
- il Comandante del Comando Unità Forestali, Ambientali e Agroalimentari Carabinieri;
- il Comandante del Comando Unità Mobili e Specializzate "Palidoro".

A queste figure sono conferite le seguenti attribuzioni:

- nell'esercitare i compiti di alta direzione, coordinamento e controllo dei Comandi dipendenti garantiscono che tutti i trattamenti di dati personali eseguiti nell'area organizzativa posta sotto la loro responsabilità siano conformi alla normativa di settore e alle politiche interne;

- gestiscono e mantengono aggiornate le Sezioni dei due Registri delle attività di trattamento (quello per finalità di polizia e quello per altre finalità) relative all'area organizzativa posta sotto la loro alta direzione, coordinamento e controllo;
- verificano e si assicurano che tutti i trattamenti di dati personali eseguiti nell'ambito dell'area organizzativa posta sotto loro sfera di responsabilità siano sempre allineati ai principi fondamentali posti dall'art. 3 del D.Lgs. 51/2018 e dall'art. 5 del GDPR;
- in caso di violazione dei dati verificano il rispetto della procedura ed autorizzano l'U.R.P. ad inviare la notifica all'Autorità Garante e, ove necessario, la comunicazione agli interessati.

c. I Referenti Privacy

A ciascun Vice Comandante dei Comandi Interregionali sono attribuite le funzioni di *Referente Privacy*, per le quali è in collegamento funzionale con il *Manager Privacy* nonchè con gli Uffici OAIO e Personale del relativo Comando Interregionale, di cui si avvale per i trattamenti di dati personali, rispettivamente per finalità di polizia e per altre finalità. In tale ambito:

- assicura il rispetto e l'applicazione delle norme in materia di protezione dei dati personali nei processi sviluppati dai Comandie dai reparti dipendenti dal Comando Interregionale;
- coordina i designati del trattamento dei dati personali, indirizzandoli nell'adozione e nell'applicazione delle misure tecniche ed organizzative adeguate a garantire la conformità dei trattamenti dei dati personali con la normativa di settore;
- vigila sul raggiungimento nonché sul mantenimento di un livello di protezione dei dati personali adeguato al rischio per i diritti e le libertà fondamentali delle persone fisiche.

d. I Designati

I *Designati* sono i soggetti che rivestono gli incarichi elencati nell'**Allegato 1**, ai quali il Codice dell'Ordinamento Militare attribuisce funzioni di comando, di direzione, di coordinamento e di controllo dei reparti alle loro dipendenze e che trattano dati personali in relazione alle competenze attribuite o comunque esercitate presso le Unità organizzative cui sono preposti, secondo l'ordinamento dell'Arma.

Artt. 169, 170, 845 e 846 C.O.M.

Essi:

- sono autorizzati al trattamento nel rispetto delle misure e delle istruzioni adottate da chi *esercita le funzioni di titolare del trattamento* dei dati personali;
- sovrintendono alle attività istituzionali in generale ed alle attività di trattamento dei dati personali in particolare, in ragione delle competenze professionali e nei limiti di poteri gerarchici e funzionali adeguati alla natura dell'incarico ad essi conferito;
- garantiscono l'attuazione delle direttive ricevute, controllandone la corretta esecuzione da parte del personale "autorizzato" ad eseguire trattamenti di dati personali ed esercitando un funzionale potere di iniziativa;
- utilizzando il modulo in **Allegato 4**, ***nominano formalmente come Autorizzato il personale posto alle loro dipendenze*** che svolge le funzioni di tecnico informatico e/o che esegue il trattamento di categorie particolari di dati personali o dati relativi a condanne penali e reati;
- ***curano che il personale "autorizzato" al trattamento posto alle loro dipendenze sia sempre adeguatamente istruito*** circa le operazioni di trattamento dei dati personali;

- raccolgono gli elementi necessari a dar corso alle richieste di esercizio dei diritti *privacy* da parte degli interessati;
- consultano tempestivamente il *Responsabile della Protezione dei Dati* per qualsiasi questione significativa riguardante la protezione dei dati personali.

4. FORMAZIONE INIZIALE E CONTINUA

a. *Formazione iniziale o di base*

La formazione, iniziale o di base è riferita al complesso delle attività formative che, essendo svolte al fine dell'immissione o della stabilizzazione in ruolo di ogni militare, indirizzano le risorse umane attraverso la preparazione culturale, etica, morale e tecnico professionale orientata all'acquisizione di competenze che consentono a ciascun appartenente all'Arma di svolgere adeguatamente il proprio ruolo professionale. Pertanto ciascun programma di formazione iniziale dei diversi isituti di formazione dell'Arma *deve prevedere almeno un modulo dedicato alla protezione dei dati personali* che comprenda l'illustrazione dei principi e delle regole di applicazione del D.Lgs. 51/2018 e del GDPR.

Art.715, 1° comma, C.O.M.

b. *Formazione continua e addestramento*

Ciascun appartenente all'Arma mantiene e migliora, aggiornandola, la propria professionalità seguendo un processo di formazione continua e di addestramento, attraverso il quale si sviluppano nei militari, le abilità e le capacità di assolvere specifici compiti e funzioni, in specifici ambienti operativi per il tramite di esercitazioni, collettive e individuali, nonché di attività di abilitazione, qualificazione e specializzazione condotte ai fini dell'assolvimento dei compiti istituzionali, *ivi compresi quelli connessi ai trattamenti di dati personali.*

In tale quadro, ***l'istruzione periodica programmata presso i Reparti dell'Arma*** costituisce uno strumento prezioso per mantenere elevata la soglia di istruzione di tutto il personale in relazione agli adempimenti da porre in essere per garantire la piena conformità dei trattamenti di dati personali alla normativa di settore.

Art.715, 2° comma, C.O.M.

5. I PRINCIPI DELLA PROTEZIONE DEI DATI PERSONALI

a. *Fondamento e vincolo dei trattamenti di dati personali*

Tutte le unità organizzative dell'Arma dei Carabinieri (Reparti, Comandi, Uffici) eseguono trattamenti di dati personali per finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali ("*finalità di polizia*") o per *altre diverse finalità* (ad esempio gestione del personale o dei concorsi per l'arruolamento e del sito web) in applicazione delle rispettive normative: D.Lgs.51/2018 o Regolamento (UE) 2016/679 (c.d. **GDPR: General Data Protection Regulation**).

Artt. 3 e 16 del D.Lgs. 51/2018 e artt. 5 e 25 GDPR

Tutti i trattamenti di dati personali, durate il relativo "ciclo di vita" - cioè dalla progettazione fino alla cessazione delle operazioni - devono essere sempre allineati ai seguenti principi fondamentali fissati dall'art. 3 del D.Lgs. 51/2018 e dall'art. 5 del Reg. (UE) 2016/679:

- principio di *limitazione della finalità*;
- principio di *necessità, proporzionalità e minimizzazione dei dati*;
- principio di *liceità*;
- principio di *correttezza*;

- principio di *trasparenza*;
- principio della *conservazione*;
- principio dell'*esattezza*;
- principio dell'*integrità e riservatezza*.

Una volta avviato il trattamento, l'Arma è tenuta a dare attuazione efficace e costante a detti principi, tenendosi aggiornata sullo stato dell'arte e riesaminando il livello di rischio. Infatti la natura, l'ambito di applicazione e il contesto delle operazioni di trattamento, nonché il livello di rischio possono mutare nel corso del trattamento, richiedendo l'obbligo di valutazioni e riesami periodici dell'efficacia delle misure e garanzie scelte a monte.

Punto 37, Linee Guida EDPB 4/2019

b. Principio della limitazione della finalità

Tutti i trattamenti di dati personali sono necessariamente rivolti al raggiungimento di *finalità determinate, esplicite e legittime* e vanno sviluppati coerentemente ad esse.

Le finalità specifiche dei trattamenti eseguiti in ambito istituzionale devono essere sempre:

- espresse e collegate in modo diretto od indiretto ad una fonte del diritto nazionale o eurounitario che ne qualifichi la legittimità;
- precisate nelle informative sin dal momento della raccolta dei dati personali necessari all'esecuzione del trattamento;
- tenute presenti per determinare quali sono i dati personali necessari per eseguire i relativi trattamenti;
- periodicamente riesaminate per verificare se il trattamento sia ancora necessario per il raggiungimento delle finalità per le quali sono stati raccolti i dati.

Solo un ulteriore trattamento dei dati personali a fini di *archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici* non è considerato incompatibile con le finalità iniziali.

c. Principio di necessità, proporzionalità e minimizzazione dei dati

Solo i dati personali che sono adeguati, pertinenti e limitati a quanto *necessario per la specifica finalità* sono sottoposti a trattamento. La *minimizzazione dei dati* realizza e rende operativo il principio di necessità. In ambito istituzionale allorchè si progetti di avviare un trattamento di dati, si deve sempre:

Punto 73, Linee Guida EDPB 4/2019

- in primo luogo, valutare se via sia bisogno o meno di trattare i dati personali per realizzare le specifiche finalità;
- verificare se sia possibile conseguire le finalità pertinenti trattando una quantità inferiore di dati personali o disponendo di dati personali meno dettagliati o aggregati, oppure senza doverli trattare affatto. Questa verifica dovrebbe essere eseguita prima di qualunque trattamento, ma potrebbe anche aver luogo in qualsiasi momento nel corso del ciclo di vita del trattamento.

d. Principio di liceità

I trattamenti di dati personali devono essere eseguiti in modo lecito.

Il trattamento per ***"finalità di polizia"*** e' lecito se è necessario per l'esecuzione di un compito dell'Arma dei Carabinieri per finalita' di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni. Deve trovare fondamento nel diritto dell'Unione europea o in disposizioni di legge o, nei casi normativamente previsti, di regolamenti che prevedano il trattamento di dati personali e le finalita'.

Art.5 D.Lgs. 51/2018

Il trattamento per le ***"altre diverse finalità"*** ,invece, è lecito solo se e nella misura in cui si basi su una delle sei seguenti condizioni di liceità fissate dall'art. 6 del GDPR: **Art.6 GDPR**

- il consenso dell'interessato;
- la necessità di eseguire un contratto di cui l'interessato è parte o misure precontrattuali adottate su richiesta dello stesso;
- la necessità di adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
- la necessità di salvaguardare gli interessi vitali dell'interessato o di un'altra persona fisica;
- la necessità di eseguire un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
- la necessità di perseguire il legittimo interesse del titolare o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato.

Di queste sei, le basi giuridiche che ***generalmente*** rendono leciti i trattamenti eseguiti dall'Arma dei Carabinieri sono costituite dalla necessità di:

- ***adempiere ad un obbligo giuridico al quale è soggetta l'Arma dei Carabinieri;***
- ***eseguire un compito di interesse pubblico o connesso all'esercizio di pubblici poteri***.

Quando il trattamento è fondato sulla "*necessità di eseguire un compito di interesse pubblico o connesso all'esercizio di pubblici poteri*", va contestualmente applicata la specifica norma integrativa del ***Codice Privacy Novellato*** che stabilisce che: **Art. 2ter , D.Lgs. 196/2003**

- la base giuridica è costituita da una norma di legge o di regolamento o da atti amministrativi generali
- i trattamenti eseguiti dalla Pubbliche Amministrazioni, e quindi anche dall'Arma dei Carabinieri, sono anche consentiti se necessari per l'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri ad esse attribuiti.

Trattamento di particolari categorie di dati.

Quando si eseguono trattamenti di particolari categorie di dati (ad esempio dati sanitari, biometrici o genetici) *oltre alla citata base giuridica è necessario* ***verificare***:

- ***per le finalità di polizia****:* che il trattamento di dati sia strettamente necessario e assistito da garanzie adeguate per i diritti e le libertà dell'interessato e specificamente previsto dal diritto dell'Unione europea o da legge o, nei casi normativamente previsti, da regolamento, ovvero, ferme le garanzie dei diritti e delle liberta', sia necessario per salvaguardare un interesse vitale dell'interessato o di un'altra persona fisica o abbia ad oggetto dati resi manifestamente pubblici dall'interessato; **Art.7, D.Lgs. 51/2018**
- ***per le altre diverse finalità***: che sussista una delle condizioni elencate al paragrafo 2 dell'art. 9 Reg. (UE) 2016/679, la prima è il *consenso esplicito* dell'interessato, le altre sono che il trattamento: **Art.9, paragrafo 2, GDPR**
  - sia necessario all'Arma , come titolare, per assolvere gli obblighi ed esercitare i diritti specifici degli interessati in materia di diritto del lavoro e della sicurezza sociale e protezione sociale;
  - sia necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica;
  - sia effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali;

- riguardi dati personali resi manifestamente pubblici dall'interessato;
- sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giudiziarie esercitino le loro funzioni giurisdizionali;
- sia necessario per ***motivi di interesse pubblico rilevante*** sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;
- sia necessario per finalità di cura cioè di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale;
- sia necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici ovvero gestione dei sistemi e servizi sanitari o sociali;
- sia necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.

e. Principio di correttezza

La correttezza è un principio di natura trasversale, secondo cui i dati personali non devono essere trattati in modo illegittimamente discriminatorio, imprevisto o fuorviante per l'interessato. Un trattamento è corretto quando corrisponde alle aspettative ragionevoli degli interessati.

Punto 69, Linee Guida EDPB 4/2019

f. Principio di trasparenza

Il principio di trasparenza:

- garantisce che gli interessati siano resi edotti delle le modalità con cui sono raccolti, utilizzati, consultati o altrimenti trattati dati personali che li riguardano nonché la misura in cui i dati personali sono o saranno trattati;
- impone che le informazioni e le comunicazioni relative al trattamento di tali dati personali siano facilmente accessibili e comprensibili e che sia sempre utilizzato un linguaggio semplice e chiaro;
- viene attuato attraverso il *rilascio delle informative*.

Art.5, paragrafo1, lett.a) GDPR

g. Principio della conservazione

I dati personali raccolti e trattati dall'Arma devono essere:

- conservati con modalità che consentano l'identificazione degli interessati per il tempo necessario al conseguimento delle finalità per le quali sono trattati;
- sottoposti a esame periodico per verificarne la persistente necessità di conservazione;
- cancellati o anonimizzati una volta decorso tale termine.

Art.3, comma 1, lett. e) D.Lgs.51/2018 e Art.5, paragrafo1, lett.e) GDPR

h. Principio dell'esattezza

I dati personali trattati dall'Arma devono essere esatti e, se necessario, aggiornati. Devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati. I dati inesatti potrebbero costituire un rischio per i diritti e le libertà degli interessati. Quindi i "designati" e gli "autorizzati" devono sempre:

Art.3, comma 1, lett. d) D.Lgs.51/2018 e Art.5, paragrafo1, lett.d) GDPR

- cancellare o rettificare tempestivamente i dati inesatti;
- evitare la propagazione di errori nonché attenuare l'effetto di un errore accumulato nella catena di trattamento.

i. Principi della integrità e riservatezza

I dati personali devono essere trattati in modo da garantire un'adeguata sicurezza e protezione da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali, mediante l'adozione di misure tecniche e organizzative adeguate.

Questo principio viene attuato in ambito istituzionale attraverso l'implementazione delle misure di sicurezza descritte al successivo par.7.

Art.3, comma 1, lett. f) D.Lgs.51/2018 e Art.5, par. 1, lett.f) GDPR

6. REGISTRI DELLE ATTIVITA' DEI TRATTAMENTI ED INFORMATIVE

a. Strumenti operativi di lavoro e documenti probatori di adempimenti

L'Arma dei Carabinieri, in applicazione di quanto prescritto dall'art. 20 del D.Lgs. 51/2018 dall'art. 30 del Reg. (UE) 2016/679 ***deve tenere due registri dei trattamenti*** eseguiti in ambito istituzionale rispettivamente ***per le finalità di polizia e per le altre diverse finalità***.

Entrambi i registri:

- hanno la duplice natura di strumento operativo di lavoro e documento probatorio di adempimenti formali;
- devono contenere tutti i trattamenti eseguiti in ambito istituzionale.

Art.20 D.Lgs.51/2018 e Art.30, GDPR

Segnale di attenzione

Un trattamento in atto che non sia annotato sul registro, non è regolare e non è conforme alla normativa in materia di Protezione dei dati personali .

I due registri sono tenuti in formato elettronico sul Portale Intranet "Leonardo".

Il *"registro delle attività di trattamento per altre **diverse finalità**"* è diviso in ***sei sezioni*** relative alle seguenti aree organizzative:

- l'area organizzativa posta sotto la responsabilità del Vice Comandante Generale dell'Arma dei Carabinieri (*Ufficio del Vice Comandante Generale, Servizio di controllo e validazione, Direzione dei beni storici e documentali e Museo Storico*);
- lo Stato Maggiore del Comando Generale dell'Arma;
- i Comandi Interregionali (*tutti i cinque Comandi Interregionali gestiscono contestualmente un'unica sezione del registro*);
- il Comando delle Scuole dell'Arma dei Carabinieri;
- il Comando Unità Forestali, Ambientali e Agroalimentari Carabinieri;
- il Comando Unita' Mobili e Specializzate "Palidoro".

Il *"registro delle attività di trattamento per **finalità di polizia**"* è diviso in ***quattro sezioni,*** analoghe a quelle precedentemente descritte (*non sono previsti per il Vice Comandante*

Generale ed il Comando delle Scuole che gestiscono solo la Sezione del registro delle attività di trattamento per altre diverse finalità).

Ogni Comandante che riveste il ruolo di *Esercente le funzioni di titolare* ha la responsabilità della gestione e dell'aggiornamento della sezione di ciascun registro relativa all'area organizzativa posta sotto la sua azione di Alta direzione, Comando e Controllo. Le operazioni di gestione e aggiornamento dei registri sono attribuite rispettivamente:

- per la tenuta del registro delle attività di trattamento per finalità di polizia: all'Ufficio Operazioni dello SM del Comando Generale ed agli Ufficio O.A.I.O. dei Comandi di Vertice;
- per la gestione del registro delle attività di trattamento per altre finalità: all'U.R.P. del Comando Generale, al Capo Ufficio del Vice Comandante Generale ed agli Uffici Personale dei Comandi di Vertice.

b. Il registro delle attività di trattamento per altre diverse finalità

Il registro delle attività di trattamento per altre diverse finalità è suddiviso in **sei sezioni.** Ciascuna sezione contiene le seguenti informazioni:

- l'indicazione dell'Arma dei Carabinieri quale titolare e i punti di contatto dell'U.R.P.;
- le finalità del trattamento;
- una descrizione delle categorie di interessati e delle categorie di dati personali;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

c. Il registro delle attività di trattamento per finalità di polizia

Il registro delle attività di trattamento per finalità di polizia è suddiviso **in *quattro sezioni***. Ciascuna sezione contiene le seguenti informazioni:

- l'indicazione dell'Arma dei Carabinieri quale titolare e i punti di contatto dell'U.R.P.;
- se previsti, il nome e i dati di contatto di ogni contitolare del trattamento nonché del responsabile della protezione dei dati;
- le finalità del trattamento;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi o presso organizzazioni internazionali;
- una descrizione delle categorie di interessati e delle categorie di dati personali;
- se previsto, il ricorso alla profilazione;
- se previste, le categorie di trasferimenti di dati personali verso un Paese terzo o verso organizzazioni internazionali;
- un'indicazione del titolo giuridico del trattamento cui sono destinati i dati personali, anche in caso di trasferimento;

- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati personali;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative;

d. Le informative

Art.10 D.Lgs.51/2018 e Artt.13 e 14, GDPR

Le informazioni relative ai trattamenti di dati personali annotati sui due predetti registri devono essere fornite agli interessati in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice, chiaro, e comprensibile.

Tali informazioni devono essere fornite attraverso canali e mezzi di comunicazione diversi, non solo quelli testuali, per aumentare la probabilità che raggiungano efficacemente l'interessato. Quindi ogni *Esercente le funzioni di titolare* dovrà verificare quale sia la modalità adeguata a fornire effettive informazioni.

In relazione a ciascun trattamento, agli interessati devono essere fornite le seguenti informazioni:

- l'indicazione dell'Arma dei Carabinieri quale titolare e i punti di contatto dell'U.R.P.;
- i dati di contatto del responsabile della protezione dei dati;
- le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
- gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
- l'intenzione dell'Arma dei Carabinieri, ove applicabile, di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, paragrafo 1, secondo comma, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali garanzie o il luogo dove sono state rese disponibili;
- il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- l'esistenza del diritto dell'interessato di chiedere all'Arma dei Carabinieri l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
- l'esistenza, qualora il trattamento sia basato sul consenso, del diritto di revocarlo in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
- il diritto di proporre reclamo a un'autorità di controllo;
- l'eventualità che la comunicazione di dati personali sia un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, o che l'interessato abbia l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

L'informativa **può essere omessa** nel caso in cui le citate informazioni siano già in possesso dell'interessato e – nel caso in cui i dati personali oggetto del trattamento non siano stati ottenuti presso l'interessato – quando:

- comunicare tali informazioni risulta impossibile o implicherebbe uno sforzo sproporzionato;
- l'ottenimento o la comunicazione dei dati personali sono espressamente previsti dal diritto italiano o comunitario e che prevede misure appropriate per tutelare gli interessi legittimi dell'interessato;
- i dati personali debbano rimanere riservati conformemente a un obbligo di segreto professionale disciplinato dal diritto dell'Unione o degli Stati membri, compreso un obbligo di segretezza previsto per legge.

Segnale di attenzione

Tutte le situazioni che giustificano l'omissione dell'informativa agli interessati vanno adeguatamente documentate.

E' possibile strutturare i contenuti in modalità ***multi strato (c.d.multi-layer)*** ponendo i contenuti in blocchi informativi che l'utente può visionare utilizzando diversi canali. Per esempio tramite un QR Code o un numero telefonico, posti su un cartello che riporta le informazioni di carattere generale, è possibile far rinvio a ulteriori contenuti dettagliati dell'informativa, che l'interessato può conoscere, consultando un sito internet o ascoltando un messaggio telefonico pre-registrato.

7. SICUREZZA DEI TRATTAMENTI

a. Sicurezza dei trattamenti eseguiti per altre diverse finalità

Art.32, GDPR

Per mantenere la sicurezza e prevenire trattamenti in violazione alla normativa di settore bisogna sempre valutare i rischi inerenti al trattamento e attuare misure per limitarli.

Nella valutazione del rischio per la sicurezza dei dati è opportuno tenere in considerazione i rischi presentati dal trattamento dei dati personali, come la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati, che potrebbero cagionare in particolare un danno fisico, materiale o immateriale.

Gli *Esercenti le funzioni di titolare* ed i *Designati,* ai sensi dell'art. 32 del GDPR, quando sviluppano un trattamento di dati personali, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio per i diritti e le libertà delle persone fisiche, *devono mettere in atto misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio*, che comprendono, tra le altre, se del caso:

- la pseudonimizzazione e la cifratura dei dati personali;
- la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;
- una adeguata formazione ed informazione del personale "autorizzato" al trattamento dei dati.

b. Sicurezza dei trattamenti eseguiti per finalità di polizia

Art.25 D.Lgs.51/2018

Gli *Esercenti le funzioni di titolare* ed i *Designati*, tenuto conto delle cognizioni tecniche disponibili, dei costi di attuazione, della natura, dell'oggetto, del contesto e delle finalità del trattamento, nonché del grado di rischio per i diritti e le libertà delle persone fisiche, nel disporre qualsiasi servizio che comporti un trattamento di dati personali devono, come dettagliatamente previsto dll'art. 25 del D.Lgs. 51/2018 garantire un livello di sicurezza **adeguato ai rischi connessi allo stesso trattamento**, applicando in fase di pianificazione, organizzazione ed esecuzione del servizio le seguenti misure di ***controllo***:

- ***dell'accesso alle attrezzature*** che deve essere *interdetto alle persone non autorizzate*. La documentazione contenente dati personali deve essere custodita in un locale idoneo, appositamente individuato, che presenti un perimetro chiaramente delimitato e sia dotato di misure di protezione minime tali da consentire l'accesso alle sole persone autorizzate, ovvero in *armadi di sicurezza con procedura di tracciamento delle chiavi in uso*;
- ***dei supporti di dati*** per impedire che supporti di dati possano essere letti, copiati, modificati o asportati da persone non autorizzate;
- ***sulla conservazione*** per evitare che i dati personali siano inseriti senza autorizzazione e che siano visionati, modificati o cancellati senza autorizzazione;
- ***dell'utente*** per impedire che persone non autorizzate utilizzino sistemi di trattamento automatizzato mediante attrezzature per la trasmissione di dati. Occorre quindi che vengano garantite:
  - l'identificazione degli utenti e la gestione delle identità digitali;
  - la determinazione dei privilegi di accesso alle risorse da associare agli "autorizzati". L'accesso alle informazioni deve essere consentito, previa autenticazione, sulla base del principio della ***"necessità di conoscere"*** per cui ciascun appartenente all'Arma ***deve conoscere solo le informazioni necessarie a svolgere le sue mansioni***;
- ***della trasmissione*** per garantire la possibilità di individuare i soggetti ai quali siano stati trasmessi o resi disponibili i dati personali;
- ***dell'introduzione*** per consentire la possibilità di accertare a posteriori quali dati personali sono stati introdotti nei sistemi di trattamento automatizzato, il momento della loro introduzione e la persona che l'ha effettuata;
- ***del trasporto*** per impedire che i dati personali possano essere letti, copiati, modificati o cancellati in modo non autorizzato durante i trasferimenti di dati o il trasporto di supporti di dati.

Bisogna infine garantire che, in caso di interruzione, i sistemi utilizzati possano essere ripristinati e che i dati personali conservati non possano essere falsati da un errore di funzionamento del sistema.

c. Valutazione d'impatto sulla protezione dei dati (c.d. DPIA)

La valutazione d'impatto sulla protezione dei dati (la c.d. *DPIA: Data Protection Impact Assessment*) è un ***processo inteso a garantire e dimostrare la conformità alla normativa privacy*** delle attività di trattamento eseguite in ambito istituzionale e rientra nel contesto dell'obbligo generale di gestire adeguatamente i rischi presentati dai trattamenti di dati personali.

Per cui, quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, l'*Esercente le funzioni di titolare* deve effettuare, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali.

L'Esercente le funzioni di titolare, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il Responsabile della Protezione dei Dati.

d. In quali casi deve essere eseguita una valutazione di impatto sulla protezione dei dati

La valutazione d'impatto sulla protezione dei dati *va sempre eseguita* prima di avviare un trattamento che rientri in una delle seguenti **tipologie di trattamenti**:

Elenco in allegato Provv. GPDP n. 467

- valutativi o di *scoring* su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche *on-line* o attraverso *app*, relativi ad aspetti riguardanti il *rendimento professionale*, la *situazione economica*, la *salute*, le preferenze o gli *interessi personali*, l'*affidabilità* o il *comportamento*, l'*ubicazione* o gli spostamenti dell'*interessato*;
- automatizzati finalizzati ad assumere decisioni che producono *effetti giuridici* oppure che incidono *in modo analogo significativamente* sull'interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio;
- che prevedono un utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche *on-line* o attraverso *app*;
- su larga scala di dati aventi *carattere estremamente personale*: si fa riferimento, fra gli altri, ai dati connessi alla vita familiare o privata, o che incidono sull'esercizio di un diritto fondamentale oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell'interessato;
- effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici anche con riguardo ai sistemi di *videosorveglianza* e di *geolocalizzazione*, dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti;
- non occasionali di dati relativi a *soggetti vulnerabili*;
- effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo;
- che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche;
- di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento;

- di categorie particolari di dati ai sensi dell'art. 9 GDPR oppure di dati relativi a condanne penali e a reati di cui all'art. 10 GDPR interconnessi con altri dati personali raccolti per finalità diverse;
- sistematici di dati biometrici e genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.

e. Criteri per una valutazione d'impatto sulla protezione dei dati accettabile

L'*Esercente la funzione di titolare* per stabilire se sia richiesta una valutazione d'impatto sulla protezione dei dati o meno, oppure se una metodologia per lo svolgimento di una tale valutazione sia sufficientemente completa, deve procedere a:

Allegato 2 alle Linee Guida WP 248 rev. 01

- una *descrizione sistematica dei trattamenti* previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
- una valutazione della *necessità e proporzionalità dei trattamenti* in relazione alle finalità;
- una *valutazione dei rischi* per i diritti e le libertà degli interessati

Art.35, GDPR

f. Coinvolgimento del Responsabile della Protezione dei Dati

Il *Responsabile della protezione dei dati* deve essere tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.

Pertanto ogni situazione in cui sussistano dubbi circa l'applicazione della normativa in materia di protezione dei dati personali va segnalata nel più breve tempo possibile al RPD ai punti di contatto presenti in tutte l informative.

8. PROCEDURA PER L'ESERCIZIO DEI DIRITTI *PRIVACY*

a. Finalità e ambito di responsabilità

Per adempiere agli obblighi imposti dalla normativa di settore all'Arma dei Carabinieri, è necessario fissare una *procedura* per gestire le istanze presentate dagli *interessati* (cioè il personale militare e civile dipendente e i cittadini a cui si riferiscono i dati personali trattati in ambito istituzionale) per esercitare i diritti previsti dagli artt. 15-22 del Reg. (UE) 2016/679. e dagli artt. 11 e 12 del D.Lgs 51/2018.

I ruoli coinvolti nella procedura sono: l'U.R.P. del Comando Generale, i Designati, il RPD ed il Manager Privacy.

Tutto il personale dipendente dell'Arma dei Carabinieri che esegue trattamenti di dati personali, concorre, comunque, al regolare sviluppo del processo di gestione delle richieste di esercizio dei diritti *privacy*.

b. I diritti esercitabili

In relazione al trattamento dei dati personali da parte dell'Arma dei Carabinieri per **finalità di polizia** gli interessati possono esercitare i seguenti diritti:

- **diritto di accesso dell'interessato**, per ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali alle informazioni basilari;

Art.11 del D.Lgs. 51/2018

- **diritto di rettifica o cancellazione di dati personali e limitazione di trattamento**, volto a ottenere dal titolare del trattamento, senza ingiustificato ritardo, la rettifica dei dati personali inesatti che lo riguardano.

Art.12 del D.Lgs. 51/2018

Quando sussistono specifiche condizioni, il titolare del trattamento cancella senza

ingiustificato ritardo i dati personali, quando il trattamento si pone in contrasto con le disposizioni di cui agli articoli 3, 5 o 7 del D.Lgs. 51/2018 e in ogni altro caso previsto dalla legge.

In luogo della cancellazione, il titolare del trattamento limita il trattamento quando l'esattezza dei dati, contestata dall'interessato, non può essere accertata o se i dati devono essere conservati a fini probatori.

In relazione al trattamento dei dati personali da parte dell'Arma dei Carabinieri per **finalità diverse da quelle di polizia** gli interessati possono esercitare i seguenti diritti:

- **diritto di accesso dell'interessato**, per ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e avere l'accesso ai dati personali e alle informazioni basilari riguardo allo stesso trattamento; **Art.15, GDPR**
- **diritto di rettifica**, affinché il titolare del trattamento proceda, senza giustificato ritardo, alla rettifica dei dati personali inesatti che lo riguardano; **Art.16, GDPR**
- **diritto alla cancellazione**, volto ad ottenere dal titolare del trattamento, per particolari motivi, la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali; **Art.17, GDPR**
- **diritto di limitazione di trattamento**, per ottenere dal titolare del trattamento, quando ricorrono particolari ipotesi, la limitazione del trattamento; **Art.18, GDPR**
- **diritto di opposizione**, con il quale l'interessato può di opporsi in qualsiasi momento, per motivi connessi con la sua situazione particolare, al trattamento dei dati personali che lo riguardano quando le basi giuridiche sono l'esecuzione di un compito di interesse pubblico o connesso con l'esercizio di pubblici poteri nonché il legittimo interesse; **Art.21, GDPR**
- **diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato**, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida significativamente sulla sua persona. **Art.22, GDPR**

c. Processo di gestione. Ruoli e Responsabilità

Il processo di gestione delle richieste di esercizio dei diritti in materia di protezione dei dati personali è volto a realizzare **due obiettivi:**

- *soddisfare le richieste degli interessati* di esercitare i diritti a loro riconosciuti dal D.Lgs. 51/2018 e dal Reg. (UE) 2016/679, accrescendo contestualmente anche la capacità di soddisfare i loro bisogni e le loro aspettative, attraverso una migliore conoscenza e controllo dell'Istituzione;
- *correggere contestualmente eventuali non conformità alla normativa privacy* individuate nel corso della gestione delle richieste stesse, contribuendo a migliorare le prestazioni e l'efficacia dei processi interni. **§ 10.1 Norma ISO 9001:2015**

Nel processo di gestione delle istanze intervengono sempre:

- il ***Capo Ufficio Relazioni con il Pubblico***, in tutte le fasi in cui è necessario relazionarsi con l'interessato/richiedente (ricezione dell'istanza, informazioni, comunicazioni e riscontro all'interessato/richiedente);
- il ***Responsabile della Protezione dei Dati*** per il controllo e la consulenza sul corretto sviluppo del processo;
- il ***Comandante*** o il ***Capo Ufficio*** dell'unità organizzativa che esegue il trattamento di dati personali al quale si riferisce l'istanza, per eseguire l'attività istruttoria e per adottare ogni

iniziativa e adempimento necessari per correggere eventuali non conformità alla normativa di settore;
- il ***Manager Privacy,*** per garantire il corretto sviluppo della procedura, attraverso eventuali azioni di coordinamento e di governo del processo di gestione, nonchè per analizzare i risultati delle attività, al fine di valutare l'opportunità o la necessità di definire nuove politiche interne o aggiornare quelle vigenti.

d. Ricezione dell'istanza

L'istanza può essere presentata dall'interessato ***senza formalità.***

Per agevolare la presentazione delle richieste sono sempre, chiaramente evidenziati, i punti di contatto dell'U.R.P. del Comando Generale:
- in tutte le informative rese agli interessati per i trattamenti eseguiti in ambito istituzionale;
- sui registri delle attività di trattamento;
- sul sito *web* istituzionale;
- sul Portale *Intranet* "Leonardo".

Quindi, *normalmente*, l'istanza viene ricevuta dall'U.R.P. che è l'interfaccia relazionale tra l'Arma e gli interessati/richiedenti.

Immediatamente dopo la ricezione, l'**URP** trasmette:
- una ricevuta all'interessato/richiedente utilizzando il modello in **Allegato 5**;
- l'istanza per la trattazione al **Comando/Ufficio** che esegue il relativo trattamento di dati - e per conoscenza al Responsabile della Protezione dei Dati - utilizzando il modello in **Allegato 6.**

Potrebbe avvenire che un interessato/richiedente presenti la richiesta di esercizio dei diritti direttamente ad un Comando o ad un Ufficio. In questo caso, tale unità organizzativa:
- se esegue il trattamento di dati al quale l'istanza si riferisce, trasmette immediatamente una ricevuta all'interessato/richiedente utilizzando il modello in **Allegato 7** e trattiene l'istanza per la trattazione dandone notizia con lettera all'U.R.P. e al Responsabile della Protezione dei Dati;
- se non è coinvolta nel trattamento al quale fa riferimento l'istanza, trasmette immediatamente:
  - una ricevuta all'interessato/richiedente utilizzando il modello in **Allegato 8**;
  - l'istanza per la trattazione al Comando/Ufficio che esegue il relativo trattamento di dati e per conoscenza all'U.R.P. ed al Responsabile della Protezione dei Dati utilizzando il modello in **Allegato 9**.

Qualora si nutrano ragionevoli dubbi circa l'identità della persona fisica che presenta l'istanza è opportuno richiedere le ulteriori informazioni necessarie a confermare l'identità dell'interessato**.** Se ritenuto utile e/o necessario per chiarire i contenuti della richiesta, è anche consigliabile, ove possibile, un contatto telefonico con il richiedente/interessato.

e. Trattazione dell'istanza e riscontro all'interessato

Le informazioni fornite al richiedente ed eventuali comunicazioni e azioni intraprese per agevolare l'esercizio dei diritti *privacy* sono gratuite.

Il riscontro all'interessato/richiedente va dato senza ingiustificato ritardo e, comunque, al più tardi **entro un mese** dal ricevimento della richiesta stessa. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste.

Segnale di attenzione

Questi sono i termini fissati dall'art. 12 del GDPR.

Nondimeno il riscontro alla richiesta di esercizio dei diritti va dato tempestivamente, al fine di attenuare eventuali malumori degli interessati e ingenerare in loro un sentimento di fiducia verso l'Istituzione.

f. Gestione del processo

Il **Comandante /Capo Ufficio** *Designato* competente:

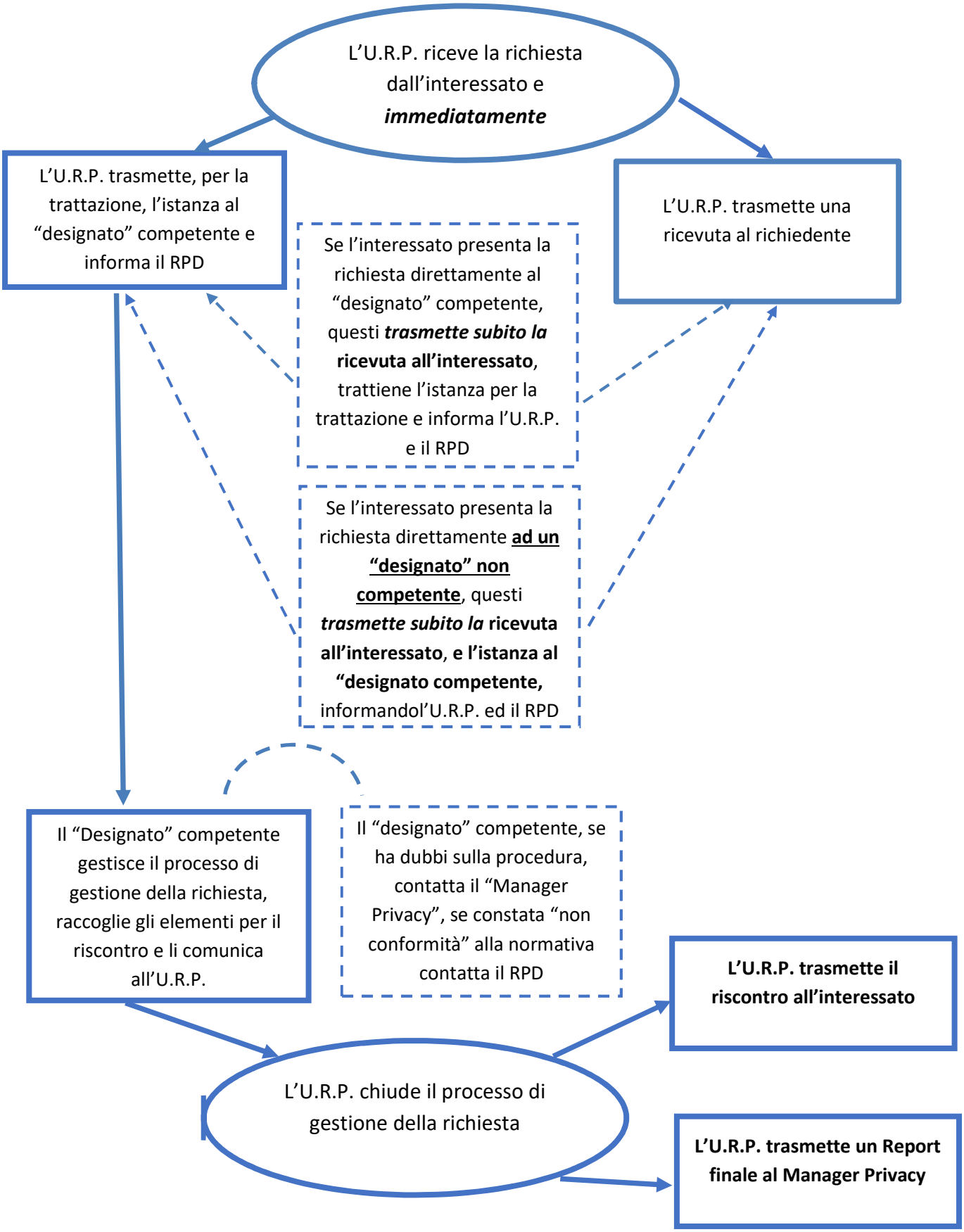
- *analizza attentamente il contenuto della richiesta*. Se questa appare manifestamente infondata o eccessiva, in particolare per il suo carattere ripetitivo documenta gli elementi di fatto che comprovano la particolare situazione e li comunica all'U.R.P. per gli adempimenti conseguenti. In particolare l'U.R.P. potrà valutare se richiedere all'interessato un contributo alle spese tenendo conto dei costi amministrativi sostenuti per svolgere le connesse attività istruttorie, in applicazione delle note regole invalse nel procedimento per l'accesso documentale;
- se il contenuto della richiesta *appare ragionevole*, verifica che il trattamento, a cui fa riferimento la richiesta in esame, viene eseguito in conformità ai principi e alle regole della normativa in materia di protezione dei dati;
- se ha qualche dubbio sulla *competenza* a procedere, contatta direttamente il *Manager Privacy* e segue le sue istruzioni;
- se ha qualche dubbio sulla *conformità* del trattamento alla normativa di settore contatta il *Responsabile della Protezione dei dati Personali* e raccoglie le sue indicazioni;
- individua gli elementi per *soddisfare la richiesta* e li comunica all'U.R.P..

L'**U.R.P. chiude il processo di gestione della richiesta**, trasmettendo:

- il riscontro all'interessato;
- un *report* finale al *Manager Privacy*.

PROCEDURA PER L'ESERCIZIO DEI DIRITTI "PRIVACY"

Diagramma di flusso che illustra gli adempimenti



9. PROCEDURA PER LA GESTIONE DI UNA VIOLAZIONE DI SICUREZZA (*DATA BREACH*)

a. Premessa

Il GDPR impone di mettere in atto misure tecniche e organizzative adeguate per:

- garantire un livello di sicurezza commisurato al rischio cui sono esposti i dati personali trattati;
- stabilire immediatamente se c'è stata violazione dei dati personali. In tale caso scatta per l'Arma dei Carabinieri, quale titolare, l'obbligo di eseguire alcuni specifici adempimenti.

§ I, "B", Linee Guida WP 250 rev. 01

Un aspetto fondamentale di qualsiasi politica di sicurezza dei dati è la capacità, ove possibile, di prevenire una violazione e, laddove essa si verifichi ciò nonostante, di reagire tempestivamente.

Per poter porre rimedio a una violazione occorre innanzitutto che il titolare del trattamento sia in grado di riconoscerla.

L'art.4, punto 12 del GDPR definisce la ***violazione dei dati personali*** come segue:

"la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati".

In particolare le violazioni possono essere classificate in base ai seguenti tre principi ben noti della sicurezza delle informazioni

- *violazione della riservatezza*, in caso di divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali;
- *violazione dell'integrità,* in caso di modifica non autorizzata o accidentale dei dati personali;
- *violazione della disponibilità,* in caso di perdita, accesso o distruzione accidentali o non autorizzati di dati personali.

La conseguenza di una violazione è che il titolare del trattamento non è più in grado di garantire l'osservanza dei principi relativi al trattamento dei dati personali di cui all'articolo 5 del GDPR.

La violazione dei dati può riguardare sia i trattamenti eseguiti senza l'ausilio di strumenti automatizzati, cioè utilizzando i supporti cartacei ed analogici, sia i trattamenti digitalizzati.

b. Procedura interna per la gestione di una violazione di sicurezza (c.d. "Data Breach")

In caso di violazione dei dati personali che presenti un rischio per i diritti e le libertà delle persone fisiche, l'Arma è tenuta a *notificare la violazione al Garante per la Protezione dei Dati Personali, senza ingiustificato ritardo* e, ove possibile, entro 72 ore dal momento in cui se ne è avuta conoscenza.

Si riportano di seguito gli adempimenti da porre in essere per strutturare una risposta rapida, efficace ad un *Data Breach*, in grado di minimizzare le conseguenze dell'evento.

I ruoli coinvolti nella procedura sono: ***l'U.R.P. del Comando Generale, gli Esercenti la funzione di Titolari, i Designati, il RPD ed il Manager Privacy.***

Tutto il personale dipendente dell'Arma dei Carabinieri che esegue trattamenti di dati personali, concorre, comunque, al regolare sviluppo del processo di gestione di una violazione dei dati personali.

c. La notifica al Garante per la Protezione dei Dati Personali

Si ritiene che il personale dell'Arma coinvolto debba considerarsi *a conoscenza della violazione nel momento in cui è ragionevolmente certo* che si sia verificato un incidente di sicurezza che ha portato alla compromissione dei dati personali.

Qualunque appartenente all'Arma dei Carabinieri che, trattando dati personali, venga a conoscenza di una possibile violazione di sicurezza, è tenuto a segnalarlo al proprio superiore che rivesta il ruolo di *Designato* (vds. elenco in **Allegato 1**).

Il Comandante/Capo Ufficio Designato che venga a conoscenza di una *violazione che riguarda un trattamento eseguito con* ***supporti cartacei*** (ad esempio smarrimento, perdita o distruzione di un fascicolo o di una pratica "cartacea"contenente numerosi documenti in cui sia riportato un volume elevato di vari dati personali) deve informare subito direttamente l'*Esercente la funzione di titolare* da cui dipende. Questi, dopo aver effettuato tutte le verifiche invia **A VISTA** un *Report* all' U.R.P. del Comando Generale che curerà la notifica entro 72 ore al Garante per la Protezione dei Dati Personali, previa autorizzazione del *Manager Privacy.*

Il Comandante/Capo Ufficio Designato, che venga a conoscenza di una *violazione di dati trattati con l'ausilio di* ***strumenti automatizzati****,* deve:

- contattare **subito** telefonicamente il *Centro di Sicurezza Telematica* del Comando Generale per verificare che si tratti effettivamente di una violazione di sicurezza;
- adottare le eventuali misure indicate nell'immediatezza dal *Centro Sicurezza Telematica* del Comando Generale;
- allertare il *Responsabile della Protezione dei Dati*;
- raccogliere tutti gli elementi di conoscenza disponibili riguardanti la violazione e comunicarli all'*Esercente la funzione di titolare*. Questi, dopo aver effettuato tutte le verifiche invia **A VISTA** un *Report* all' U.R.P. del Comando Generale che curerà la notifica entro 72 ore al Garante per la Protezione dei Dati Personali, previa autorizzazione del *Manager Privacy*.

Se il ***Centro di Sicurezza Telematica*** acquisisce direttamente conoscenza della violazione, **deve tempestivamente:**

- allertare il *Responsabile della Protezione dei Dati*;
- comunicare i relativi elementi di conoscenza all'U.R.P. che curerà la notifica entro 72 ore al Garante per la Protezione dei Dati Personali, previa autorizzazione del *Manager Privacy*.

Il ***Responsabile Protezione Dati*** deve mantenere i contatti con l'Autorità Garante e svolgere la funzione di "interfaccia" tra la stessa Autorità e le unità organizzative interessate.

L'**URP** deve **notificare la violazione al Garante per la Protezione dei Dati Personali**, senza ingiustificato ritardo e, ove possibile, **entro 72 ore** dal momento in cui se ne è avuta conoscenza, **esclusivamente** mediante la procedura telematica disponibile all'indirizzo https://servizi.gpdp.it/databreach/s/, che costituisce l'unica e ordinaria modalità di notifica accettata dal Garante.

Provv. GPDP n. 209 del 27/05/2021

La notifica deve essere effettuata mediante la compilazione *online* del modello (https://servizi.gpdp.it/databreach/resource/1629905132000/DB_Istruzioni) previsto dalla citata procedura, secondo le istruzioni (https://servizi.gpdp.it/databreach/s/istruzioni) rinvenibili al medesimo indirizzo, dove è presente anche uno strumento di autovalutazione (https://servizi.gpdp.it/databreach/s/self-assessment) che consente di individuare le azioni da intraprendere a seguito di una violazione dei dati personali derivante da un incidente di sicurezza.

Segnale di attenzione

Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

d. La comunicazione agli interessati

Quando la violazione dei dati è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche l'Arma dei Carabinieri, oltre alla notifica all'Autorità Garante è tenuta a comunicare la violazione agli interessati senza ingiustificato ritardo.

Art. 34, GDPR

Una violazione può avere potenzialmente numerosi effetti negativi significativi sulle persone fisiche, che possono causare danni fisici, materiali o immateriali, ad esempio la perdita del controllo da parte degli interessati sui loro dati personali, la limitazione dei loro diritti, la discriminazione, il furto o l'usurpazione d'identità, perdite finanziarie, la decifratura non autorizzata della pseudonimizzazione, il pregiudizio alla reputazione e la perdita di riservatezza dei dati personali protetti da segreto professionale, nonché qualsiasi altro danno economico o sociale rilevante per le persone fisiche interessate.

Considerando 75 e 85 GDPR

In questi casi:

- la violazione di sicurezza è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
- l'Arma, oltre alla notifica all'Autorità Garante, è obbligata a comunicare la stessa violazione agli interessati senza ingiustificato ritardo.

La soglia per la comunicazione delle violazioni alle persone fisiche è quindi più elevata rispetto a quella della notifica alle autorità di controllo, di conseguenza non tutte le violazioni dovranno essere comunicate agli interessati.

La comunicazione agli interessati deve essere data dall'U.R.P. del Comando Generale che deve descrivere con un linguaggio semplice e chiaro la natura della violazione dei dati personali e riportare almeno le informazioni contenute nella predetta notifica all'Autorità Garante.

Non è richiesta la comunicazione agli interessati quando:

- l'Arma dei Carabinieri:
  - abbia messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili, quale ad esempio la cifratura;
  - successivamente alla violazione abbia adottato misure per scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
- la stessa comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

Nel caso in cui non venga comunicata la violazione agli interessati, l'Autorità Garante può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che l'Arma vi provveda.

e. Violazione constatata da un Responsabile del trattamento

Se la violazione di sicurezza viene constatata da un responsabile del trattamento (che sta trattando dati personali per conto dell'Arma) questi **deve notificarla all'U.R.P. del Comando Generale *senza ingiustificato ritardo***. Si evidenzia che il Responsabile del trattamento non deve valutare la probabilità di rischio derivante dalla violazione prima di notificarla all'U.R.P.; cui spetta effettuare la valutazione nel momento in cui viene a conoscenza della violazione.

Tale adempimento va sempre riportato in ogni contratto con i fornitori dell'Arma che rivestono il ruolo di *Responsabili del trattamento*.

f. Documentare le violazioni

Indipendentemente dal fatto che una violazione debba o meno essere notificata all'autorità di controllo, **l'U.R.P.** del Comando Generale deve conservare la documentazione di tutte le violazioni di dati personali, comprese le circostanze ad essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.

Segnale di attenzione

Va documentato anche il ragionamento alla base delle decisioni prese in risposta a una violazione. In particolare, se una violazione non viene notificata perché si ritiene che non presenti un rischio per i diritti e le libertà fondamentali, è opportuno ***documentare una giustificazione di tale decisione.*** La giustificazione dovrebbe includere i motivi per cui l'esercente le funzioni di titolare del trattamento ritiene improbabile che la violazione possa presentare un rischio per i diritti e le libertà delle persone fisiche.

Se l'U.R.P. notifica una violazione all'autorità di controllo, ma la notifica avviene in ritardo, *l'Esercente le funzioni di titolare* deve essere in grado di fornire i motivi del ritardo; la documentazione relativa a tale circostanza potrebbe contribuire a dimostrare che il ritardo nella segnalazione è giustificato e non eccessivo.

IL MODELLO ORGANIZZATIVO PRIVACY DELL'ARMA DEI CARABINIERI

ALLEGATI

1. ELENCO DEI "DESIGNATI" AI QUALI SONO ATTRIBUITI SPECIFICI COMPITI CONNESSI AL TRATTAMENTO DI DATI PERSONALI

ORGANIZZAZIONE CENTRALE (COMANDO GENERALE)

- Presidente della CO.VA.;
- Sottocapo di Stato Maggiore;
- Capi Reparto;
- Comandante del Centro Nazionale Amministrativo;
- Direttore del Centro Nazionale di Selezione e Reclutamento;
- Direttori, Capi Ufficio, Capi Centro;
- Comandante del Reparto Autonomo;
- Capo Servizio Amministrativo;
- Dirigente del Servizio Sanitario;
- Comandante, Vicecomandante, Capo di Stato Maggiore, Sottocapo di Stato Maggiore (ACOS)
- per Operazioni / per Piani e Policy / per Logistica / per Intelligence, Capo Ufficio
- Amministrazione/Budget/Finanza (solo se italiani), Capo del Gruppo di Supporto, della Forza di Gendarmeria Europea (EUROGENDFOR).
- Direttore, Capi Sezione Administration, Logistic e Security del Nato SP COE.

==========

ORGANIZZAZIONE TERRITORIALE

COMANDO INTERREGIONALE

- Capo di Stato Maggiore;
- Capi Ufficio OAIO, Personale e Logistico.

COMANDO LEGIONE

- Comandante;
- Vice Comandante;
- Capo di Stato Maggiore;
- Capo Servizio Amministrativo;
- Capi Ufficio Personale, OAIO e Logistico;
- Comandante del Reparto Comando;
- Responsabile del Servizio/Sezione Sanità.

COMANDO PROVINCIALE / GRUPPO / REPARTO TERRITORIALE / COMPAGNIA / TENENZA / STAZIONE

- Comandanti;
- Capo Ufficio Comando.

REPARTO SERVIZI MAGISTRATURA / REPARTO SCORTE E SICUREZZA / REPARTO SERVIZI SICUREZZA ENTI VARI / SQUADRONE CC ELIPORTATO CACCIATORI

- Comandanti.

==========

ORGANIZZAZIONE ADDESTRATIVA

COMANDO DELLE SCUOLE DELL'ARMA DEI CARABINIERI

- Capo di Stato Maggiore;
- Capi Ufficio Personale, Addestramento e Logistico.

CENTRO DI PSICOLOGIA APPLICATA PER LA FORMAZIONE DELL'ARMA DEI CARABINIERI

- Direttore.

CENTRO SPORTIVO CARABINIERI

- Comandante.

SCUOLA UFFICIALI CARABINIERI

- Comandante;
- Capo di Stato Maggiore;
- Capi Ufficio Personale, Addestramento e Studi, Logistico;
- Direttore dell'Istituto di Studi Professionali e Giuridico Militari;
- Comandante del Reparto Corsi;
- Comandante del Reparto Comando;
- Capo del Servizio Amministrativo.
- Capo Sezione Sanità.

SCUOLA MARESCIALLI E BRIGADIERI DEI CARABINIERI

- Comandante;
- Capo di Stato Maggiore;
- Capi Ufficio Personale, Addestramento, Logistico;
- Direttore dell'Istituto di Studi Professionali;
- Comandante del Reparto Comando;
- Capo del Servizio Amministrativo;
- Capo Sezione Sanità;
- Comandanti dei Reggimenti Allievi;
- Capi Ufficio Comando, Capo Servizio Amministrativo e Capo Sezione Sanità dei Reggimenti Allievi.

LEGIONE ALLIEVI CARABINIERI

- Comandante;
- Capo di Stato Maggiore;
- Capi Ufficio Personale, Addestramento, Logistico;

- Comandante del Reparto Comando;
- Comandanti delle Scuole Allievi;
- Capi Ufficio/Nucleo Comando, Comandante Reparto Comando, Capi Sezione Sanità, Capi dei Servizi Amministrativi delle Scuole Allievi.

ISPETTORATO DEGLI ISTITUTI DI SPECIALIZZAZIONE DELL'ARMA DEI CARABINIERI
- Comandante;
- Capo Ufficio Comando.

SCUOLA FORESTALE CARABINIERI
- Comandante;
- Capo di Stato Maggiore;
- Capi Ufficio Personale, Addestramento, Logistico, Divulgazione Naturalistica;
- Comandante del Reparto Comando;
- Capo Sezione Sanità e Capo del Servizio Amministrativo.
- Comandanti dei Centri Addestramento.

CENTRO LINGUE ESTERE DELL'ARMA DEI CARABINIERI
- Comandante;

SCUOLA DI PERFEZIONAMENTO AL TIRO
- Comandante.

ISTITUTO SUPERIORE DI TECNICHE INVESTIGATIVE DELL'ARMA DEI CARABINIERI
- Comandante.

CENTRO CARABINIERI ADDESTRAMENTO ALPINO
- Comandante.

CENTRO CARABINIERI CINOFILI
- Comandante.

CENTRO CARABINIERI SUBACQUEI
- Comandante.

==========

ORGANIZZAZIONE MOBILE E SPECIALE

COMANDO UNITÀ MOBILI E SPECIALIZZATE CARABINIERI

- Capo di Stato Maggiore;
- Capo Servizio Amministrativo,
- Capi Ufficio;
- Comandante del Reparto Comando;
- Capo Sezione Sanità.

COESPU

- Direttore;
- Capo di Stato Maggiore;
- Capi Ufficio Personale e Logistico;
- Capo Sezione Sanità;
- Capo del Servizio Amministrativo;
- Comandante del Reparto Supporti;
- Comandante del Reparto Corsi;
- Capo Dipartimento Studi e Ricerche;
- Capo Ufficio Affari Internazionali;
- Capo Ufficio Studi Valutazione e Formazione;
- Capo Ufficio Ricerche.

DIVISIONE UNITA' MOBILI E DIVISIONE UNITA' SPECIALIZZATE

- Comandanti;
- Capi di Stato Maggiore;
- Capi Ufficio.

RAGGRUPPAMENTO OPERATIVO SPECIALE

- Comandante;
- Capo Ufficio Comando;
- Comandanti di Reparto/Sezione Anticrimine.

1^ BRIGATA MOBILE

- Comandante;
- Capo di Stato Maggiore;
- Capi Ufficio Personale e OAIO;
- Comandante del 4° Reggimento Carabinieri a Cavallo e Capo Ufficio Comando;
- Comandanti, Capi Ufficio Comando, Capi Sezione Sanità dei Reggimenti/Battaglioni.

==========

ORGANIZZAZIONE FORESTALE AMBIENTALE E AGROALIMENTARE

COMANDO UNITÀ FORESTALE AMBIENTALE E AGROALIMENTARE CARABINIERI

- Capo di Stato Maggiore;
- Capo Servizio Amministrativo;
- Capi Ufficio;
- Comandante del Reparto Comando;
- Capo Sezione Sanità.

COMANDO CARABINIERI PER LA TUTELA DELLA BIODIVERSITA' E DEI PARCHI

- Comandante;
- Capi Ufficio.

RAGGRUPPAMENTO CARABINIERI BIODIVERSITA'

- Comandante;
- Capo Ufficio Comando;
- Comandanti di Reparto/Nucleo/Centro Nazionale Carabinieri Biodiversità.

RAGGRUPPAMENTO CARABINIERI PARCHI

- Comandante;
- Capo Ufficio Comando;
- Comandanti di Reparto Carabinieri "Parco Nazionale" /Stazione "Parco".

RAGGRUPPAMENTO CARABINIERI CITES

- Comandante;
- Capo Ufficio Comando.

COMANDO CARABINIERI PER LA TUTELA FORESTALE

- Comandante;
- Capo Ufficio Comando.

COMANDO REGIONE CARABINIERI FORESTALE

- Comandante;
- Capo Ufficio Comando.

COMANDO GRUPPO CARABINIERI FORESTALE / CENTRI ANTICRIMINE NATURA / STAZIONE CARABINIERI FORESTALE

- Comandante.

COMANDO CARABINIERI PER LA TUTELA DELL'AMBIENTE

- Comandante;
- Capo Ufficio Comando;
- Comandanti dei Gruppi Tutela Ambiente, Comandanti dei NOE;

==========

REPARTI CON DIPENDENZA DA ALTRI ENTI

- Comandante del Reggimento Corazzieri, Capo Ufficio Comando, Capi dei Servizi Sanitario e Amministrativo;
- Comandante del Reparto Carabinieri Presidenza della Repubblica;
- Comandante del Comando Carabinieri Senato della Repubblica;
- Comandante del Comando Carabinieri Camera dei Deputati;
- Comandante del Comando Carabinieri Corte Costituzionale;
- Comandante del Comando Carabinieri Corte dei Conti;
- Comandante del Reparto Carabinieri Difesa – Gabinetto;
- Comandante del Comando Carabinieri PM Segredifesa;
- Comandante del Comando Carabinieri PM Stato Maggiore Difesa;
- Comandante e Capo Ufficio Comando del Comando Carabinieri per la Marina, Comandante del Gruppo Carabinieri Marina, Comandanti delle Compagnie Carabinieri Marina, Comandanti delle Stazioni Carabinieri Marina;
- Comandante del Reparto Carabinieri Agenzia Sicurezza S.M.M., Dirigenti delle Agenzie Sicurezza Interregionale Carabinieri;
- Comandante e Capi Ufficio SP e OAIO del Comando Carabinieri per l'Aeronautica Militare,
- Comandanti dei Gruppi Carabinieri AM, Comandanti delle Compagnie Carabinieri AM,
- Comandanti delle Stazioni Carabinieri AM;
- Comandante del Gruppo Carabinieri Sicurezza AM;
- Comandante del Comando Carabinieri PM S.M.E., Comandanti delle Sezioni e dei Nuclei
- Carabinieri P.M.;
- Comandante del Gruppo e delle Compagnie Carabinieri SETAF;
- Comandante del Reparto Sicurezza del Q.G.I. presso JFC SOUTH;
- Comandanti dei Nuclei Sicurezza Industriale Carabinieri;
- Comandante della Compagnia RUD.

==========

PERSONALE ADDETTO A MINISTERI

- Ufficiale Superiore Addetto al Ministero della Giustizia;
- Ufficiale Superiore Addetto al Ministero delle Infrastrutture e Trasporti;
- Ufficiale Superiore Addetto al Ministero dello Sviluppo Economico;
- Ufficiale Superiore Addetto al Ministero della Istruzione, dell'Università e della Ricerca.

2. DECISIONE 2021/915 DELLA COMMISSIONE DELL' UNIONE EUROPEA

DECISIONE DI ESECUZIONE (UE) 2021/915 DELLA COMMISSIONE

del 4 giugno 2021

relativa alle clausole contrattuali tipo tra titolari del trattamento e responsabili del trattamento a norma dell'articolo 28, paragrafo 7, del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio e dell'articolo 29, paragrafo 7, del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio

(Testo rilevante ai fini del SEE)

LA COMMISSIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea,

visto il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), in particolare l'articolo 28, paragrafo 7,

visto il regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n.45/2001 e la decisione n.1247/2002/CE, in particolare l'articolo 29, paragrafo 7,

considerando quanto segue:

(1) I concetti di titolare del trattamento e di responsabile del trattamento hanno un ruolo cruciale nell'applicazione del regolamento (UE) 2016/679 e del regolamento (UE) 2018/1725. Il titolare del trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali. Ai fini del regolamento (UE) 2018/1725, per titolare del trattamento si intende l'istituzione o l'organo dell'Unione, la direzione generale o qualunque altra entità organizzativa che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali. Quando le finalità e i mezzi di tale trattamento sono determinati da un atto specifico dell'Unione, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione. Il responsabile del trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

(2) Al rapporto tra titolari del trattamento e responsabili del trattamento soggetti al regolamento (UE) 2016/679 e tra titolari del trattamento e responsabili del trattamento soggetti al regolamento (UE) 2018/1725 dovrebbe applicarsi lo stesso insieme di clausole contrattuali tipo. Questo perché, per assicurare un approccio coerente alla protezione dei dati personali in tutta l'Unione e la libera circolazione dei dati personali all'interno dell'Unione, le norme sulla protezione dei dati del regolamento (UE) 2016/679, applicabili al settore pubblico negli Stati membri, e le norme sulla protezione dei dati del regolamento (UE) 2018/1725, applicabili alle istituzioni, agli organi e agli organismi dell'Unione, sono state per quanto possibile allineate tra loro.

(3) Per garantire il rispetto delle prescrizioni dei regolamenti (UE) 2016/679 e (UE) 2018/1725, quando affida delle attività di trattamento a un responsabile del trattamento, il titolare del trattamento dovrebbe ricorrere unicamente a responsabili del trattamento che presentino garanzie

sufficienti, in particolare in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto misure tecniche e organizzative che soddisfino i requisiti dei regolamenti (UE) 2016/679 e (UE) 2018/1725, anche per la sicurezza del trattamento.

(4) I trattamenti da parte di un responsabile del trattamento devono essere disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli gli elementi elencati all'articolo 28, paragrafi 3 e 4, del regolamento (UE) 2016/679 o all'articolo 29, paragrafi 3 e 4, del regolamento (UE) 2018/1725. Tale contratto o atto è stipulato in forma scritta, anche in formato elettronico.

(5) A norma dell'articolo 28, paragrafo 6, del regolamento (UE) 2016/679 e dell'articolo 29, paragrafo 6, del regolamento (UE) 2018/1725, il titolare del trattamento e il responsabile del trattamento possono scegliere di negoziare un contratto individuale contenente gli elementi obbligatori di cui, rispettivamente, all'articolo 28, paragrafi 3 e 4, del regolamento (UE) 2016/679 o all'articolo 29, paragrafi 3 e 4, del regolamento (UE) 2018/1725, oppure di utilizzare, in tutto o in parte, le clausole contrattuali tipo adottate dalla Commissione in conformità dell'articolo 28, paragrafo 7, del regolamento (UE) 2016/679 e dell'articolo 29, paragrafo 7, del regolamento (UE) 2018/1725.

(6) Il titolare del trattamento e il responsabile del trattamento dovrebbero essere liberi di includere le clausole contrattuali tipo stabilite nella presente decisione in un contratto più ampio e di aggiungere altre clausole o garanzie supplementari, purché queste non contraddicano, direttamente o indirettamente, le clausole contrattuali tipo o pregiudichino i diritti o le libertà fondamentali degli interessati. L'utilizzo delle clausole contrattuali tipo lascia impregiudicato qualunque obbligo contrattuale del titolare del trattamento e/o del responsabile del trattamento di garantire il rispetto dei privilegi e delle immunità applicabili.

(7) Le clausole contrattuali tipo dovrebbero contenere norme sia sostanziali che procedurali. In linea con l'articolo 28, paragrafo 3, del regolamento (UE) 2016/679 e l'articolo 29, paragrafo 3, del regolamento (UE) 2018/1725, le clausole contrattuali tipo dovrebbero inoltre imporre al titolare del trattamento e al responsabile del trattamento di indicare la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali in questione e le categorie di interessati, nonché gli obblighi e i diritti del titolare del trattamento.

(8) In conformità dell'articolo 28, paragrafo 3, del regolamento (UE) 2016/679 e dell'articolo 29, paragrafo 3, del regolamento (UE) 2018/1725, il responsabile del trattamento deve informare immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione del titolare del trattamento violi il regolamento (UE) 2016/679 o il regolamento (UE) 2018/1725 o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

(9) Quando un responsabile del trattamento ricorre a un altro responsabile del trattamento per l'esecuzione di specifiche attività, si dovrebbero applicare i requisiti specifici di cui all'articolo 28, paragrafi 2 e 4, del regolamento (UE) 2016/679 o all'articolo 29, paragrafi 2 e 4, del regolamento (UE) 2018/1725. In particolare, è necessaria un'autorizzazione preliminare scritta, specifica o generale. A prescindere dal carattere specifico o generale di tale autorizzazione, il primo responsabile del trattamento dovrebbe tenere un elenco aggiornato degli altri responsabili del trattamento.

(10) Per soddisfare i requisiti di cui all'articolo 46, paragrafo 1, del regolamento (UE) 2016/679, la Commissione ha adottato clausole contrattuali tipo in conformità dell'articolo 46, paragrafo 2, lettera c), dello stesso regolamento (UE) 2016/679. Tali clausole soddisfano anche i requisiti di ui all'articolo 28, paragrafi 3 e 4, del regolamento (UE) 2016/679 per i trasferimenti di dati da titolari del trattamento soggetti al regolamento (UE) 2016/679 a responsabili del trattamento che non rientrano nell'ambito di applicazione territoriale di tale regolamento, o da responsabili del trattamento soggetti al regolamento (UE) 2016/679 a sub-responsabili del trattamento che non rientrano nell'ambito di applicazione territoriale di tale regolamento. Le presenti clausole contrattuali tipo non possono essere utilizzate come clausole contrattuali tipo ai fini del capo V

del regolamento (UE) 2016/679.

(11)I terzi dovrebbero poter diventare parti delle clausole contrattuali tipo durante l'intero ciclo di vita del contratto.

(12)Il funzionamento delle clausole contrattuali tipo dovrebbe essere valutato nell'ambito della valutazione periodica del regolamento (UE) 2016/679 di cui all'articolo 97 di tale regolamento.

(13)Il garante europeo della protezione dei dati e il comitato europeo per la protezione dei dati sono stati consultati a norma dell'articolo 42, paragrafi 1 e 2, del regolamento (UE) 2018/1725 e hanno espresso un parere congiunto il 14 gennaio 2021, di cui si è tenuto conto nella preparazione della presente decisione.

(14)Le misure di cui alla presente decisione sono conformi al parere del comitato istituito a norma dell'articolo 93 del regolamento (UE) 2015/679 e dell'articolo 96, paragrafo 2, del regolamento (UE) 2015/1725,

HA ADOTTATO LA PRESENTE DECISIONE:

Articolo 1

Le clausole contrattuali tipo figuranti in allegato soddisfano i requisiti per i contratti tra titolari del trattamento e responsabili del trattamento di cui all'articolo 28, paragrafi 3 e 4, del regolamento (UE) 2016/679 e all'articolo 29, paragrafi 3 e 4, del regolamento (UE) 2018/1725.

Articolo 2

Le clausole contrattuali tipo figuranti in allegato possono essere utilizzate nei contratti tra un titolare del trattamento e un responsabile del trattamento che tratta dati personali per conto del titolare del trattamento.

Articolo 3

La Commissione valuta l'applicazione pratica delle clausole contrattuali tipo figuranti in allegato, sulla base di tutte le informazioni disponibili, nell'ambito della valutazione periodica prevista all'articolo 97 del regolamento (UE) 2016/679.

Articolo 4

La presente decisione entra in vigore il ventesimo giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

Fatto a Bruxelles, il 4 giugno 2021

Per la Commissione

La presidente

Ursula VON DER LEYEN

ALLEGATO

Clausole contrattuali tipo

SEZIONE I

Clausola 1

Scopo e ambito di applicazione

a)Scopo delle presenti clausole contrattuali tipo (di seguito «clausole») è garantire il rispetto dell'articolo 28, paragrafi 3 e 4, del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

b) I titolari del trattamento e i responsabili del trattamento di cui all'allegato I hanno accettato le presenti clausole al fine di garantire il rispetto dell'articolo 28, paragrafi 3 e 4, del regolamento (UE) 2016/679.

c)Le presenti clausole si applicano al trattamento dei dati personali specificato all'allegato II.

d Gli allegati da I a IV costituiscono parte integrante delle clausole.

e) Le presenti clausole lasciano impregiudicati gli obblighi cui è soggetto il titolare del trattamento a norma del regolamento (UE) 2016/679 e/o del regolamento (UE) 2018/1725.

f) Le presenti clausole non garantiscono, di per sé, il rispetto degli obblighi connessi ai trasferimenti internazionali conformemente al capo V del regolamento (UE) 2016/679 o del regolamento (UE) 2018/1725.

Clausola 2

Invariabilità delle clausole

a) Le parti si impegnano a non modificare le clausole se non per aggiungere o aggiornare informazioni negli allegati.

b) Ciò non impedisce alle parti di includere le clausole contrattuali tipo stabilite nelle presenti clausole in un contratto più ampio o di aggiungere altre clausole o garanzie supplementari, purché queste non contraddicano, direttamente o indirettamente, le presenti clausole o ledano i diritti o le libertà fondamentali degli interessati.

Clausola 3

Interpretazione

a) Quando le presenti clausole utilizzano i termini definiti, rispettivamente, nel regolamento (UE) 2016/679 o nel regolamento (UE) 2018/1725, tali termini hanno lo stesso significato di cui al regolamento interessato.

b) Le presenti clausole vanno lette e interpretate alla luce delle disposizioni del regolamento (UE) 2016/679 o del regolamento (UE) 2018/1725, rispettivamente.

c) Le presenti clausole non devono essere interpretate in un senso che non sia conforme ai diritti e agli obblighi previsti dal regolamento (UE) 2016/679 / dal regolamento (UE) 2018/1725, o che pregiudichi i diritti o le libertà fondamentali degli interessati.

Clausola 4

Gerarchia

In caso di contraddizione tra le presenti clausole e le disposizioni di accordi correlati, vigenti tra le parti al momento dell'accettazione delle presenti clausole, o conclusi successivamente, prevalgono le presenti clausole.

Clausola 5 — Facoltativa

Clausola di adesione successiva

a) Qualunque entità che non sia parte delle presenti clausole può, con l'accordo di tutte le parti, aderire alle presenti clausole in qualunque momento, in qualità di titolare del trattamento o di responsabile del trattamento, compilando gli allegati e firmando l'allegato I.

b) Una volta compilati e firmati gli allegati di cui alla lettera a), l'entità aderente è considerata parte delle presenti clausole e ha i diritti e gli obblighi di un titolare del trattamento o di un responsabile del trattamento, conformemente alla sua designazione nell'allegato I.

c) L'entità aderente non ha diritti od obblighi derivanti a norma delle presenti clausole per il periodo precedente all'adesione.

SEZIONE II
OBBLIGHI DELLE PARTI

Clausola 6

Descrizione del trattamento

I dettagli dei trattamenti, in particolare le categorie di dati personali e le finalità del trattamento per le quali i dati personali sono trattati per conto del titolare del trattamento, sono specificati nell'allegato II.

Clausola 7

Obblighi delle parti

7.1. Istruzioni

a) Il responsabile del trattamento tratta i dati personali soltanto su istruzione documentata del titolare del trattamento, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento. In tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto lo vieti per

rilevanti motivi di interesse pubblico. Il titolare del trattamento può anche impartire istruzioni successive per tutta la durata del trattamento dei dati personali. Tali istruzioni sono sempre documentate.

b) Il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, le istruzioni del titolare del trattamento violino il regolamento (UE) 2016/679/ il regolamento (UE) 2018/1725 o le disposizioni applicabili, nazionali o dell'Unione, relative alla protezione dei dati.

7.2. Limitazione delle finalità

Il responsabile del trattamento tratta i dati personali soltanto per le finalità specifiche del trattamento di cui all'allegato II, salvo ulteriori istruzioni del titolare del trattamento.

7.3. Durata del trattamento dei dati personali

Il responsabile del trattamento tratta i dati personali soltanto per la durata specificata nell'allegato II.

7.4. Sicurezza del trattamento

a) Il responsabile del trattamento mette in atto almeno le misure tecniche e organizzative specificate nell'allegato III per garantire la sicurezza dei dati personali. Ciò include la protezione da ogni violazione di sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati (violazione dei dati personali). Nel valutare l'adeguato livello di sicurezza, le parti tengono debitamente conto dello stato dell'arte, dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi per gli interessati.

b) Il responsabile del trattamento concede l'accesso ai dati personali oggetto di trattamento ai membri del suo personale soltanto nella misura strettamente necessaria per l'attuazione, la gestione e il controllo del contratto. Il responsabile del trattamento garantisce che le persone autorizzate al trattamento dei dati personali ricevuti si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza.

7.5.Dati sensibili

Se il trattamento riguarda dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, dati genetici o 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, o dati relativi a condanne penali e a reati («dati sensibili»), il responsabile del trattamento applica limitazioni specifiche e/o garanzie supplementari.

7.6.Documentazione e rispetto

a) Le parti devono essere in grado di dimostrare il rispetto delle presenti clausole.

b) Il responsabile del trattamento risponde prontamente e adeguatamente alle richieste di informazioni del titolare del trattamento relative al trattamento dei dati conformemente alle presenti clausole.

c) Il responsabile del trattamento mette a disposizione del titolare del trattamento tutte le informazioni necessarie a dimostrare il rispetto degli obblighi stabiliti nelle presenti clausole e che derivano direttamente dal regolamento (UE) 2016/679 e/o dal regolamento (UE) 2018/1725. Su richiesta del titolare del trattamento, il responsabile del trattamento consente e contribuisce alle attività di revisione delle attività di trattamento di cui alle presenti clausole, a intervalli ragionevoli o se vi sono indicazioni di inosservanza. Nel decidere in merito a un riesame o a un'attività di revisione, il titolare del trattamento può tenere conto delle pertinenti certificazioni in possesso del responsabile del trattamento.

d) Il titolare del trattamento può scegliere di condurre l'attività di revisione autonomamente o incaricare un revisore indipendente. Le attività di revisione possono comprendere anche ispezioni nei locali o nelle strutture fisiche del responsabile del trattamento e, se del caso, sono effettuate con un preavviso ragionevole.

e) Su richiesta, le parti mettono a disposizione della o delle autorità di controllo competenti le informazioni di cui alla presente clausola, compresi i risultati di eventuali attività di revisione.

7.7. Ricorso a sub-responsabili del trattamento

a) OPZIONE 1: AUTORIZZAZIONE PRELIMINARE SPECIFICA: Il responsabile del trattamento non può subcontrattare a un sub-responsabile del trattamento i trattamenti da effettuare per conto del titolare del trattamento conformemente alle presenti clausole senza la previa autorizzazione specifica scritta del titolare del trattamento. Il responsabile del trattamento presenta la richiesta di autorizzazione specifica almeno [SPECIFICARE IL PERIODO] prima di ricorrere al sub-responsabile del trattamento in questione, unitamente alle informazioni necessarie per consentire al titolare del trattamento di decidere in merito all'autorizzazione. L'elenco dei sub-responsabili del trattamento autorizzati dal titolare del trattamento figura nell'allegato IV. Le parti tengono aggiornato tale allegato.

   OPZIONE 2: AUTORIZZAZIONE SCRITTA GENERALE: Il responsabile del trattamento ha l'autorizzazione generale del titolare del trattamento per ricorrere a sub-responsabili del trattamento sulla base di un elenco concordato. Il responsabile del trattamento informa specificamente per iscritto il titolare del trattamento di eventuali modifiche previste di tale elenco riguardanti l'aggiunta o la sostituzione di sub-responsabili del trattamento con un anticipo di almeno [SPECIFICARE IL PERIODO], dando così al titolare del trattamento tempo sufficiente per poter opporsi a tali modifiche prima del ricorso al o ai sub-responsabili del trattamento in questione. Il responsabile del trattamento fornisce al titolare del trattamento le informazioni necessarie per consentirgli di esercitare il diritto di opposizione.

b) Qualora il responsabile del trattamento ricorra a un sub-responsabile del trattamento per l'esecuzione di specifiche attività di trattamento (per conto del responsabile del trattamento), stipula un contratto che impone al sub-responsabile del trattamento, nella sostanza, gli stessi obblighi in materia di protezione dei dati imposti al responsabile del trattamento conformemente alle presenti clausole. Il responsabile del trattamento si assicura che il sub-responsabile del trattamento rispetti gli obblighi cui il responsabile del trattamento è soggetto a norma delle presenti clausole e del regolamento (UE) 2016/679 e/o del regolamento (UE) 2018/1725.

c) Su richiesta del titolare del trattamento, il responsabile del trattamento gli fornisce copia del contratto stipulato con il sub-responsabile del trattamento e di ogni successiva modifica. Nella misura necessaria a proteggere segreti aziendali o altre informazioni riservate, compresi i dati personali, il responsabile del trattamento può espungere informazioni dal contratto prima di trasmetterne una copia.

d) Il responsabile del trattamento rimane pienamente responsabile nei confronti del titolare del trattamento dell'adempimento degli obblighi del sub-responsabile del trattamento derivanti dal contratto che questi ha stipulato con il responsabile del trattamento. Il responsabile del trattamento notifica al titolare del trattamento qualunque inadempimento, da parte del sub-responsabile del trattamento, degli obblighi contrattuali.

e) Il responsabile del trattamento concorda con il sub-responsabile del trattamento una clausola del terzo beneficiario secondo la quale, qualora il responsabile del trattamento sia scomparso di fatto, abbia giuridicamente cessato di esistere o sia divenuto insolvente, il titolare del trattamento ha diritto di risolvere il contratto con il sub-responsabile del trattamento e di imporre a quest'ultimo di cancellare o restituire i dati personali.

7.8. Trasferimenti internazionali

a) Qualunque trasferimento di dati verso un paese terzo o un'organizzazione internazionale da parte del responsabile del trattamento è effettuato soltanto su istruzione documentata del titolare del trattamento o per adempiere a un requisito specifico a norma del diritto dell'Unione o degli Stati membri cui è soggetto il responsabile del trattamento, e nel rispetto del capo V del regolamento (UE) 2016/679 o del regolamento (UE) 2018/1725.

b) Il titolare del trattamento conviene che, qualora il responsabile del trattamento ricorra a un sub-responsabile del trattamento conformemente alla clausola 7.7 per l'esecuzione di specifiche attività di trattamento (per conto del titolare del trattamento) e tali attività di trattamento comportino il trasferimento di dati personali ai sensi del capo V del regolamento (UE) 2016/679, il responsabile del trattamento e il sub-responsabile del trattamento possono garantire il rispetto

del capo V del regolamento (UE) 2016/679 utilizzando le clausole contrattuali tipo adottate dalla Commissione conformemente all'articolo 46, paragrafo 2, del regolamento (UE) 2016/679, purché le condizioni per l'uso di tali clausole contrattuali tipo siano soddisfatte.

Clausola 8

Assistenza al titolare del trattamento

a) Il responsabile del trattamento notifica prontamente al titolare del trattamento qualunque richiesta ricevuta dall'interessato. Non risponde egli stesso alla richiesta, a meno che sia stato autorizzato in tal senso dal titolare del trattamento.

b) Il responsabile del trattamento assiste il titolare del trattamento nell'adempimento degli obblighi di rispondere alle richieste degli interessati per l'esercizio dei loro diritti, tenuto conto della natura del trattamento. Nell'adempiere agli obblighi di cui alle lettere a) e b), il responsabile del trattamento si attiene alle istruzioni del titolare del trattamento.

c) Oltre all'obbligo di assistere il titolare del trattamento in conformità della clausola 8, lettera b), il responsabile del trattamento assiste il titolare del trattamento anche nel garantire il rispetto dei seguenti obblighi, tenuto conto della natura del trattamento dei dati e delle informazioni a disposizione del responsabile del trattamento:

   1) l'obbligo di effettuare una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali («valutazione d'impatto sulla protezione dei dati») qualora un tipo di trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche;

   2) l'obbligo, prima di procedere al trattamento, di consultare la o le autorità di controllo competenti qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio;

   3) l'obbligo di garantire che i dati personali siano esatti e aggiornati, informando senza indugio il titolare del trattamento qualora il responsabile del trattamento venga a conoscenza del fatto che i dati personali che sta trattando sono inesatti o obsoleti;

   4) gli obblighi di cui all'articolo 32 regolamento (UE) 2016/679.

d) Le parti stabiliscono nell'allegato III le misure tecniche e organizzative adeguate con cui il responsabile del trattamento è tenuto ad assistere il titolare del trattamento nell'applicazione della presente clausola, nonché l'ambito di applicazione e la portata dell'assistenza richiesta.

Clausola 9

Notifica di una violazione dei dati personali

In caso di violazione dei dati personali, il responsabile del trattamento coopera con il titolare del trattamento e lo assiste nell'adempimento degli obblighi che incombono a quest'ultimo a norma degli articoli 33 e 34 del regolamento (UE) 2016/679 o degli articoli 34 e 35 del regolamento (UE) 2018/1725, ove applicabile, tenuto conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento.

9.1. Violazione riguardante dati trattati dal titolare del trattamento

In caso di una violazione dei dati personali trattati dal titolare del trattamento, il responsabile del trattamento assiste il titolare del trattamento:

a) nel notificare la violazione dei dati personali alla o alle autorità di controllo competenti, senza ingiustificato ritardo dopo che il titolare del trattamento ne è venuto a conoscenza, se del caso/(a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche);

b) nell'ottenere le seguenti informazioni che, in conformità dell'articolo 33, paragrafo 3, del regolamento (UE) 2016/679, devono essere indicate nella notifica del titolare del trattamento e includere almeno:

   1) la natura dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

   2) le probabili conseguenze della violazione dei dati personali;

3) le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali, se del caso anche per attenuarne i possibili effetti negativi.

Qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente, la notifica iniziale contiene le informazioni disponibili in quel momento, e le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo.

c) nell'adempiere, in conformità dell'articolo 34 del regolamento (UE) 2016/679, all'obbligo di comunicare senza ingiustificato ritardo la violazione dei dati personali all'interessato, qualora la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

9.2. Violazione riguardante dati trattati dal responsabile del trattamento

In caso di una violazione dei dati personali trattati dal responsabile del trattamento, quest'ultimo ne dà notifica al titolare del trattamento senza ingiustificato ritardo dopo esserne venuto a conoscenza. La notifica contiene almeno:

a) una descrizione della natura della violazione (compresi, ove possibile, le categorie e il numero approssimativo di interessati e di registrazioni dei dati in questione);

b) i recapiti di un punto di contatto presso il quale possono essere ottenute maggiori informazioni sulla violazione dei dati personali;

c) le probabili conseguenze della violazione dei dati personali e le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione, anche per attenuarne i possibili effetti negativi.

Qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente, la notifica iniziale contiene le informazioni disponibili in quel momento, e le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo.

Le parti stabiliscono nell'allegato III tutti gli altri elementi che il responsabile del trattamento è tenuto a fornire quando assiste il titolare del trattamento nell'adempimento degli obblighi che incombono al titolare del trattamento a norma degli articoli 33 e 34 del regolamento (UE) 2016/679.

SEZIONE III
DISPOSIZIONI FINALI

Clausola 10

Inosservanza delle clausole e risoluzione

a) Fatte salve le disposizioni del regolamento (UE) 2016/679 e/o del regolamento (UE) 2018/1725, qualora il responsabile del trattamento violi gli obblighi che gli incombono a norma delle presenti clausole, il titolare del trattamento può dare istruzione al responsabile del trattamento di sospendere il trattamento dei dati personali fino a quando quest'ultimo non rispetti le presenti clausole o non sia risolto il contratto. Il responsabile del trattamento informa prontamente il titolare del trattamento qualora, per qualunque motivo, non sia in grado di rispettare le presenti clausole.

b) Il titolare del trattamento ha diritto di risolvere il contratto per quanto riguarda il trattamento dei dati personali conformemente alle presenti clausole qualora:

1) il trattamento dei dati personali da parte del responsabile del trattamento sia stato sospeso dal titolare del trattamento in conformità della lettera a) e il rispetto delle presenti clausole non sia ripristinato entro un termine ragionevole e in ogni caso entro un mese dalla sospensione;

2) il responsabile del trattamento violi in modo sostanziale o persistente le presenti clausole o gli obblighi che gli incombono a norma del regolamento (UE) 2016/679 e/o del regolamento (UE) 2018/1725;

3) il responsabile del trattamento non rispetti una decisione vincolante di un organo giurisdizionale competente o della o delle autorità di controllo competenti per quanto riguarda i suoi obblighi in conformità delle presenti clausole o del regolamento (UE) 2016/679 e/o del regolamento (UE) 2018/1725.

c) Il responsabile del trattamento ha diritto di risolvere il contratto per quanto riguarda il trattamento

dei dati personali a norma delle presenti clausole qualora, dopo aver informato il titolare del trattamento che le sue istruzioni violano i requisiti giuridici applicabili in conformità della clausola 7.1, lettera b), il titolare del trattamento insista sul rispetto delle istruzioni.

d) Dopo la risoluzione del contratto il responsabile del trattamento, a scelta del titolare del trattamento, cancella tutti i dati personali trattati per conto del titolare del trattamento e certifica a quest'ultimo di averlo fatto, oppure restituisce al titolare del trattamento tutti i dati personali e cancella le copie esistenti, a meno che il diritto dell'Unione o dello Stato membro non richieda la conservazione dei dati personali. Finché i dati non sono cancellati o restituiti, il responsabile del trattamento continua ad assicurare il rispetto delle presenti clausole.

ALLEGATO I
Elenco delle parti

Titolare/i del trattamento: [*Identità e dati di contatto del/dei titolari del trattamento e, ove applicabile, del suo/loro responsabile della protezione dei dati]*

1. Nome: …

Indirizzo: …

Nome, qualifica e dati di contatto del referente: …

Firma e data di adesione: …

.

Responsabile/i del trattamento [*Identità e dati di contatto del/dei responsabili del trattamento e, ove applicabile, del suo/loro responsabile della protezione dei dati]*

1. Nome: …

Indirizzo: …

Nome, qualifica e dati di contatto del referente: …

Firma e data di adesione: …

ALLEGATO II
Descrizione del trattamento

Categorie di interessati i cui dati personali sono trattati

…

Categorie di dati personali trattati

…

Dati sensibili trattati (se del caso) e limitazioni o garanzie applicate che tengono pienamente conto della natura dei dati e dei rischi connessi, ad esempio una rigorosa limitazione delle finalità, limitazioni all'accesso (tra cui accesso solo per il personale che ha seguito una formazione specializzata), tenuta di un registro degli accessi ai dati, limitazioni ai trasferimenti successivi o misure di sicurezza supplementari.

…

Natura del trattamento

…

Finalità per le quali i dati personali sono trattati per conto del titolare del trattamento

…

Durata del trattamento

…

…

Per il trattamento da parte di (sub-)responsabili del trattamento, specificare anche la materia disciplinata, la natura e la durata del trattamento

---

ALLEGATO III

Misure tecniche e organizzative, comprese misure tecniche e organizzative per garantire la sicurezza dei dati

NOTA ESPLICATIVA:

Le misure tecniche e organizzative devono essere descritte in modo concreto e non genericamente.

Descrizione delle misure di sicurezza tecniche e organizzative messe in atto dal o dai responsabili del trattamento (comprese le eventuali certificazioni pertinenti) per garantire un adeguato livello di sicurezza, tenuto conto della natura, dell'ambito di applicazione, del contesto e della finalità del trattamento, nonché dei rischi per i diritti e le libertà delle persone fisiche. Esempi di possibili misure:

misure di pseudonimizzazione e cifratura dei dati personali

misure per assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento

misure per assicurare la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento

misure di identificazione e autorizzazione dell'utente

misure di protezione dei dati durante la trasmissione

misure di protezione dei dati durante la conservazione

misure per garantire la sicurezza fisica dei luoghi in cui i dati personali sono trattati

misure per garantire la registrazione degli eventi

misure per garantire la configurazione del sistema, compresa la configurazione per impostazione predefinita

misure di informatica interna e di gestione e governance della sicurezza informatica

misure di certificazione/garanzia di processi e prodotti

misure per garantire la minimizzazione dei dati

misure per garantire la qualità dei dati

misure per garantire la conservazione limitata dei dati

misure per garantire la responsabilità

misure per consentire la portabilità dei dati e garantire la cancellazione]

Per i trasferimenti a (sub-)responsabili del trattamento, descrivere anche le misure tecniche e organizzative specifiche che il (sub-)responsabile del trattamento deve prendere per essere in grado di fornire assistenza al titolare del trattamento.

Descrizione delle misure tecniche e organizzative specifiche che il responsabile del trattamento deve prendere per essere in grado di fornire assistenza al titolare del trattamento.

ALLEGATO IV

Elenco dei sub-responsabili del trattamento

NOTA ESPLICATIVA:

Il presente allegato deve essere compilato in caso di autorizzazione specifica di sub-responsabili del trattamento [clausola 7.7, lettera a), opzione 1].

Il titolare del trattamento ha autorizzato il ricorso ai seguenti sub-responsabili del trattamento:

1. Nome: …

Indirizzo: …

Nome, qualifica e dati di contatto del referente: …

Descrizione del trattamento (compresa una chiara delimitazione delle responsabilità qualora siano autorizzati più sub-responsabili del trattamento): …

…

3. AUTORIZZAZIONE GENERALE AL TRATTAMENTO

Comando Generale dell'Arma dei Carabinieri

Nr.18/12-2 di prot. Roma, 20 marzo 2022

IL MANAGER PRIVACY

VISTO l'art. 29 e l'art. 32, paragrafo 4 del Regolamento (UE) 2016/679 che stabiliscono che chiunque agisca sotto l'autorità del titolare del trattamento che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento;

VISTO l'art. 2 quaterdecies, comma 2 del D.Lgs. 196/2003 che sancisce che il titolare del trattamento nell'ambito del proprio assetto organizzativo individua le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta;

VISTO l'art. 715 del D.Lgs. 66/2010 rubricato *"Formazione e addestramento"* che, in riferimento agli appartenenti alle Forze Armate, stabilisce che:

- la formazione, iniziale o di base se riferita al complesso delle attività formative svolte al fine dell'immissione o della stabilizzazione in ruolo del militare ovvero successiva o permanente, è il complesso delle attività con cui si educano, si migliorano e si indirizzano le risorse umane attraverso la preparazione culturale, etica, morale e tecnico professionale orientata all'acquisizione di competenze che consentono al singolo militare di svolgere adeguatamente il proprio ruolo professionale. Questo processo si realizza attraverso la maturazione delle caratteristiche personali e la creazione di competenze;
- l''addestramento è il processo attraverso il quale si sviluppano negli individui, organi di staff, Comandi e Unità, le abilità e le capacità di assolvere specifici compiti e funzioni, in specifici ambienti operativi per il tramite di esercitazioni, collettive e individuali, nonché di attività di abilitazione, qualificazione e specializzazione condotte ai fini dell'assolvimento dei compiti istituzionalmente assegnati alle Forze armate e allo sviluppo, mantenimento e miglioramento della prontezza operativa desiderata;

CONSIDERATO che i processi di formazione iniziale e continua e di addestramento garantiscono che tutto il personale dell'Arma dei Carabinieri raggiunga e mantenga uno standard di professionalità adeguato allo svolgimento di tutte le funzioni attribuite dalla legge, ***comprese quelle connesse al trattamento di dati personali***

AUTORIZZA

al trattamento dei dati personali tutto il personale in servizio presso l'Arma dei Carabinieri che tratta dati personali in relazione alle competenze della unità organizzativa (Reparto, Comando, Ufficio) alla quale è stato assegnato, salvo diverse determinazioni adottate, in applicazione dell'art. 2 quaterdecies del Codice privacy novellato, per attribuire specifici compiti e funzioni finalizzate a garantire la protezione dei dati personali.

IL MANAGER PRIVACY
(Gen. D. Massimo MENNITTI)

4. ATTO FORMALE DI NOMINA DI SOGGETTO AUTORIZZATO AL TRATTAMENTO DI DATI PERSONALI CON SPECIFICI COMPITI

INTESTAZIONE DEL COMANDO/UFFICIO

Nr. di prot. Luogo, data

OGGETTO: **Atto formale di nomina di soggetto autorizzato al trattamento di dati personali con specifici compiti**

- Art. 2 quaterdecies D.Lgs. 196/2013 e artt. 29 e 32 Reg. UE 2016/679 -

A grado Nome Cognome

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

Il sottoscritto (*Grado, Cognome e Nome*), Comandante/Capo Ufficio dell'unità organizzativa in intestazione, in qualità di ***"DESIGNATO"*** per lo svolgimento dei compiti e l'assolvimento delle funzioni in materia di trattamento di dati personali come previsto dal "Modello Organizzativo Privacy" dell'Arma dei Carabinieri,

nomina la S.V. "*AUTORIZZATO*" al trattamento dei dati personali

per lo svolgimento delle mansioni connesse all'incarico ricoperto. Tali mansioni dovranno essere eseguite seguendo le istruzioni ed indicazioni che sono contenute nel "Mansionario" di seguito riportato e da considerarsi a titolo esemplificativo e non anche esaustivo.

==========

MANSIONARIO PER "AUTORIZZATO" AL TRATTAMENTO DI DATI PERSONALI

1. ***Definizioni***

a. ***"Dato personale"***: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»);

b. ***"Trattamento"***: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati, 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

Art.2 D.Lgs.51/2018 e art. 4 GDPR

qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

c. ***"Archivio"***: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
d. "***Titolare del trattamento e Autorità competente":*** l'Arma dei Carabinieri che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali;
e. ***"Contitolare del trattamento"***. la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, quale titolare del trattamento, determina congiuntamente all'Arma dei Carabinieri le finalità e i mezzi di un trattamento di dati personali;
f. ***"Esercente le funzioni di titolare"***: il dirigente dell'Arma dei Carabinieri al quale è attribuito il potere decisionale circa le finalità e i mezzi del trattamento di dati personali;
g. ***"Designato"***: Il Dirigente/Comandante/Capo Ufficio di cui all'elenco in **Allegato 1**, del "Modello Organizzativo Privacy" dell'Arma dei Carabinieri cui sono attribuiti specifici compiti e funzioni connessi al trattamento di dati personali;
h. ***"Autorizzato"***: il dipendente dell'Arma dei Carabinieri specificamente autorizzato, previa istruzione, a trattare dati personali;
i. ***"Responsabile del trattamento"***: i fornitori, persone fisiche o giuridiche, che trattano dati personali per conto dell'Arma dei Carabinieri.
j. ***"Destinatario":*** la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali dall'Arma dei Carabinieri;
k. ***"Terzo":*** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
l. ***"Violazione dei dati personali (c.d. data breach)"***: la violazione della sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
m. ***"Categorie particolari di dati personali":*** dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché 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.
n. ***"Dati genetici"***: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica, che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione.
o. ***"Dati biometrici":*** i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
p. ***"Dati relativi alla salute":*** i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.
q. ***"File di log":*** registro degli accessi e delle operazioni.

2. ***Prescrizioni generali***

L'"AUTORIZZATO":

a. ***deve avvisare immediatamente il proprio superiore in ogni caso in cui venga a conoscenza di un'irregolarità, evidente o sospetta, nell'attività di trattamento di dati personali;***

b. ha un **obbligo legale di riservatezza**, in osservanza del quale deve: **Art. 28, par. 3 , lett. b) GDPR**
   - mantenere riservati i dati personali di cui venga in possesso o comunque a conoscenza nell'espletamento del proprio incarico;
   - non divulgarli in alcun modo o in alcuna forma e non farne oggetto di utilizzazione a qualsiasi titolo per scopi diversi da quelli strettamente necessari al raggiungimento delle finalità istituzionali;
   - osservare, quindi, il massimo riserbo in merito ai dati personali che raccoglie e tratta e non dovrà rivelarli ad alcuna persona che non sia coinvolta nel trattamento;

c. quando raccoglie i dati, deve verificarne l'esattezza, la completezza e la pertinenza;

d. **deve utilizzare esclusivamente gli strumenti e gli applicativi forniti dall'Arma dei Carabinieri. Quindi, non può e non deve, quindi, utilizzare propri strumenti personali per eseguire le proprie mansioni;**

3. Misure di sicurezza

L'"AUTORIZZATO":

a. riguardo ai trattamenti eseguiti senza l'ausilio di strumenti elettronici deve:
   - porre la massima diligenza nella gestione e custodia dei documenti cartacei contenenti dati personali. Durante momentanee assenze dal luogo di lavoro deve riporli in luoghi adatti ad evitare che terzi non autorizzati possano accedervi;
   - al termine della prestazione lavorativa giornaliera, riporre i documenti contenenti dati personali nei rispettivi archivi, avendo cura di chiuderli a chiave, limitando così l'accesso alle sole persone autorizzate;
   - custodire con diligenza le chiavi dei locali, degli armadi e/o degli archivi evitando di cederle a terzi e di farne copia e comunicando tempestivamente al proprio superiore diretto lo smarrimento o il furto;

b. riguardo ai trattamenti eseguiti con l'ausilio di strumenti elettronici deve:
   - utilizzare le credenziali di accesso fornite dall'unità organizzativa competente;
   - non cedere ad alcuno le credenziali di accesso;
   - impostare una password con non meno di 8 caratteri alfanumerici, contenenti almeno una lettera maiuscola, un numero un carattere speciale;
   - modificare periodicamente la password;
   - attenersi scrupolosamente alla politica di sicurezza informatica interna all'Arma evitando di aprire e-mail o allegati dall'incerta provenienza anche se non segnalate dall'applicativo antivirus;
   - aggiornare sistematicamente i software e i sistemi operativi;
   - evitare di gestire dati personali attraverso propri dispositivi personali;
   - accedere unicamente alle banche dati collegate alla propria mansione, ed in particolare:

*(specificare le risorse alle quali è autorizzato ad accedere)*_____

La presente lettera di nomina viene redatta in 2 copie, una delle quali è consegnata all'"AUTORIZZATO", previa lettura e commento dei contenuti

IL COMANDANTE/CAPO UFFICIO
(XXXXXXXXXXX)

Per presa visione e ricezione : Luogo, data

L'"AUTORIZZATO" ____(firma)_____

5. RICEVUTA AI SENSI DELL'ART. 18 BIS DELLA LEGGE 241/1990.

Intestazione dell'U.R.P.

Nr. di prot. Località, data

OGGETTO: GRADO/SIG./SIG.RA COGNOME E NOME DELL'INTERESSATO/A.
ESERCIZIO DEI DIRITTI IN MATERIA DI PROTEZIONE DEI DATI PERSONALI.
RICEVUTA AI SENSI DELL'ART. 18 BIS DELLA LEGGE 241/1990.

A GRADO/SIG./SIG.RA COGNOME E NOME DELL'INTERESSATO/A
INDIRIZZO P.E.C. XXXXX@XXXXXX

==========

1. La sua richiesta di esercizio del diritto di (*accesso/rettifica/cancellazione/limitazione del trattamento/opposizione/non sottoposizione a decisione basata unicamente su trattamento automatizzato*):
   - è stata ricevuta e protocollata in data odierna;
   - sarà tempestivamente trasmessa, per la trattazione, al Comando/Ufficio_____ che effettua il relativo trattamento di dati personali.

2. Il riscontro Le sarà fornito senza ingiustificato ritardo e, comunque, al più tardi entro un mese da oggi. Tale termine potrebbe essere prorogato di due mesi, se necessario, tenuto conto della complessità della richiesta. In tal caso sarà nostra cura informarLa di tale proroga, e dei motivi del ritardo, entro un mese da oggi.

IL CAPO UFFICIO
(xxxxxxxxxxxxxxxxxxxxxx)

6. TRASMISSIONE DELL'ISTANZA PER LA TRATTAZIONE AL "DESIGNATO" COMPETENTE.

Intestazione dell'U.R.P.

Nr. di prot. Località, data

OGGETTO: GRADO/SIG./SIG.RA COGNOME E NOME DELL'INTERESSATO/A.
ESERCIZIO DEI DIRITTI IN MATERIA DI PROTEZIONE DEI DATI PERSONALI.
TRASMISSIONE DELL'ISTANZA PER LA TRATTAZIONE AL "DESIGNATO" COMPETENTE.

A COMANDO/UFFICIO
(COMPRESO TRA I "DESIGNATI" NELL'ELENCO IN ALL.1 AL MODELLO ORGANIZZATIVO PRIVACY)

E PER CONOSCENZA:

RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI

==========

1. Per la relativa trattazione, come previsto dal Modello Organizzativo "Privacy" dell'Arma dei Carabinieri, si trasmette la richiesta di esercizio del diritto di (*accesso/rettifica/cancellazione/limitazione del trattamento/opposizione/non sottoposizione a decisione basata unicamente su trattamento automatizzato*) presentata dal nominato/a in oggetto.
2. All'interessato/a è stata data notizia dell'inoltro a Codesto Comando/Ufficio.
3. Per qualsiasi dubbio relativo agli adempimenti da porre in essere è possibile contattare, telefonicamente o via e-mail il Responsabile della Protezione dei Dati che legge per conoscenza.
4. Si resta in attesa degli elementi per il riscontro.

IL CAPO UFFICIO
(XXXXXXXXXXXXXXXXXXXXXX)

7. RICEVUTA ALL'INTERESSATO DA PARTE DELL'UNITÀ ORGANIZZATIVA COMPETENTE

Intestazione del Comando/Ufficio

Nr. di prot. Località, data

OGGETTO: GRADO/SIG./SIG.RA COGNOME E NOME DELL'INTERESSATO/A.
ESERCIZIO DEI DIRITTI IN MATERIA DI PROTEZIONE DEI DATI PERSONALI.
RICEVUTA AI SENSI DELL'ART. 18 BIS DELLA LEGGE 241/1990.

A GRADO/SIG./SIG.RA COGNOME E NOME DELL'INTERESSATO/A
INDIRIZZO P.E.C. XXXXX@XXXXXX

==========

1. La sua richiesta di esercizio del diritto di (*accesso/rettifica/cancellazione/limitazione del trattamento/opposizione/non sottoposizione a decisione basata unicamente su trattamento automatizzato*):
   - è stata ricevuta e protocollata in data odierna;
   - **sarà trattata da questo Comando/Ufficio che effettua il relativo trattamento di dati personali.**

2. Il riscontro Le sarà fornito senza ingiustificato ritardo e, comunque, al più tardi entro un mese da oggi. Tale termine potrebbe essere prorogato di due mesi, se necessario, tenuto conto della complessità della richiesta. In tal caso sarà nostra cura informarLa di tale proroga, e dei motivi del ritardo, entro un mese da oggi.

IL COMANDANTE/CAPO UFFICIO
(xxxxxxxxxxxxxxxxxxxxxxx)

8. RICEVUTA ALL'INTERESSATO DA PARTE DELL'UNITÀ ORGANIZZATIVA NON COMPETENTE

Intestazione del Comando/Ufficio

Nr. di prot. Località, data

OGGETTO: GRADO/SIG./SIG.RA COGNOME E NOME DELL'INTERESSATO/A.
ESERCIZIO DEI DIRITTI IN MATERIA DI PROTEZIONE DEI DATI PERSONALI.
RICEVUTA AI SENSI DELL'ART. 18 BIS DELLA LEGGE 241/1990.

A GRADO/SIG./SIG.RA COGNOME E NOME DELL'INTERESSATO/A
INDIRIZZO P.E.C. XXXXX@XXXXXX

==========

1. La sua richiesta di esercizio del diritto di (*accesso/rettifica/cancellazione/limitazione del trattamento/opposizione/non sottoposizione a decisione basata unicamente su trattamento automatizzato*):
   - è stata ricevuta e protocollata in data odierna;
   - **sarà tempestivamente trasmessa, per la trattazione, al Comando/Ufficio_____ che effettua il relativo trattamento di dati personali.**

2. Il riscontro Le sarà fornito senza ingiustificato ritardo e, comunque, al più tardi entro un mese da oggi. Tale termine potrebbe essere prorogato di due mesi, se necessario, tenuto conto della complessità della richiesta. In tal caso sarà nostra cura informarLa di tale proroga, e dei motivi del ritardo, entro un mese da oggi.

IL COMANDANTE/CAPO UFFICIO
(xxxxxxxxxxxxxxxxxxxxxxx)

9. TRASMISSIONE DELL'ISTANZA PER LA TRATTAZIONE AL "DESIGNATO" COMPETENTE.

Intestazione del Comando/Ufficio

Nr. di prot. Località, data

OGGETTO: GRADO/SIG./SIG.RA COGNOME E NOME DELL'INTERESSATO/A.
ESERCIZIO DEI DIRITTI IN MATERIA DI PROTEZIONE DEI DATI PERSONALI.
TRASMISSIONE DELL'ISTANZA PER LA TRATTAZIONE AL "DESIGNATO" COMPETENTE.

A COMANDO/UFFICIO
(COMPRESO TRA I "DESIGNATI" NELL'ELENCO IN ALL.1 AL MODELLO ORGANIZZATIVO PRIVACY)

E PER CONOSCENZA:

RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI ROMA

UFFICIO RELAZIONI CON IL PUBBLICO ROMA

==========

1. Per la relativa trattazione, come previsto dal Modello Organizzativo "Privacy" dell'Arma dei Carabinieri, si trasmette la richiesta di esercizio del diritto di (*accesso/rettifica/cancellazione/limitazione del trattamento/opposizione/non sottoposizione a decisione basata unicamente su trattamento automatizzato*) presentata dal nominato/a in oggetto.
2. All'interessato/a è stata data notizia dell'inoltro a Codesto Comando/Ufficio.
3. Per qualsiasi dubbio relativo agli adempimenti da porre in essere è possibile contattare, telefonicamente o via e-mail il Responsabile della Protezione dei Dati che legge per conoscenza.
4. Gli elementi per il riscontro dovranno essere comunicati all'U.R.P. che legge per conoscenza.

IL COMANDANTE/CAPO UFFICIO
(xxxxxxxxxxxxxxxxxxxxxxx)