M_D GARM DE12021 0000004 22-02-2021

MINISTERO DELLA DIFESA

SEGRETARIATO GENERALE DELLA DIFESA E DIREZIONE NAZIONALE DEGLI ARMAMENTI

DIREZIONE DEGLI ARMAMENTI AERONAUTICI E PER L'AERONAVIGABILITA'

MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE CON VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI

Documento redatto ai sensi e per gli effetti del
Regolamento (UE) 2016/679 del Parlamento Europeo
e del Consiglio in data 27 aprile 2016

Edizione febbraio 2021

Digitally signed by GIUSEPPE
ANTONIO LUPOLI
Date: 2021.02.22 13:47:36 CET

INDICE

INDICE 2
PREMESSA 4
PARTE I 8
1. DEFINIZIONI E PRINCIPI APPLICABILI al trattamento DEI DATI PERSONALI 8
2. IDENTIFICAZIONE DEI DATI DA TRATTARE 9
3. ORGANIZZAZIONE PREPOSTA AL TRATTAMENTO DEI DATI PERSONALI 10
4. COMPITI E RESPONSABILITA DEL PERSONALE 10
5. PROCEDURE DI TRATTAMENTO DEI DATI PERSONALI 13
a. Trattamento dei dati personali senza strumenti informatici 13
b. Trattamento dei dati effettuato con strumenti informatici 14
6. MISURE DI PROTEZIONE ADOTTATE 15
a) Suddivisione delle misure 15
b) Misure di carattere fisico 16
c) Misure di carattere procedurale 17
d) Misure di carattere elettronico/informatico 17
e) Criteri e modalità di ripristino dei dati 18
7. ANALISI DEI RISCHI 19
a) Metodo adottato per la quantificazione del rischio 20
b) Individuazione delle minacce e valutazione del rischio 23
8. PIANIFICAZIONE DEGLI INTERVENTI FORMATIVI 26
PARTE II 27
1. VALUTAZIONE D'IMPATTO 27
2. PROSPETTIVE E APPROFONDIMENTI 27

ALLEGATO A - Identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate – Estratto del D.P.R. 15 marzo 2010, n. 90 29

ALLEGATO B – TRATTAMENTO EFFETTUATO CON APPLICATIVI ESTERNI ALLA DIREZIONE 64

ALLEGATO C – TRATTAMENTO EFFETTUATO CON APPLICATIVI DELLA DIREZIONE 67

ALLEGATO D – MODULO DI ASSUNZIONE DI RESPONSABILITA' 68

PREMESSA

Il presente documento è redatto conformemente al Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (Regolamento generale sulla protezione dei dati, nel prosieguo indicato come "Regolamento") e alla vigente normativa in materia (d.lgs. 10 agosto 2018, n. 118 che adegua il Codice in materia di protezione dei dati personali - d.lgs. 101 giugno 2003, n. 196, alle disposizioni del succitato Regolamento UE). Il presente documento costituisce parte integrante del Registro delle Attività di trattamento, dando contezza delle misure tecniche e organizzative in atto presso la Direzione degli Armamenti Aeronautici e per l'Aeronavigabilità ivi inclusi gli Uffici Tecnici Territoriali dipendenti (nel prosieguo indicati nel complesso come "Direzione"), per garantire il livello di sicurezza adeguato al rischio, in armonia con il disposto dell'art. 32 del Regolamento (PARTE I). Fornisce, altresì, appropriati elementi sulla valutazione d'impatto dei trattamenti previsti sulla protezione dei dati personali, effettuata dal Titolare ai sensi dell'art. 35 del Regolamento (PARTE II).

Esso costituisce uno dei fattori attraverso cui si manifesta l'elemento della responsabilizzazione (*accountability*) del Titolare (cui concorrono i Responsabili delle UU.OO. elencati nell'Allegato A al D.D. n. 18 dell'8 marzo 2019 "Protezione dei dati personali - Regolamento UE 2016/679"), tenuto a comportamenti proattivi volti a dimostrare la corretta adozione di misure finalizzate ad assicurare l'applicazione del Regolamento (art. 24 del Regolamento), con il compito di decidere le modalità, le garanzie e i limiti del trattamento dei dati personali[1], dovendo, peraltro, fin d'ora osservare come la Direzione si avvale, in concreto, di sistemi informatici la cui gestione è posta in capo al Comando C4 Difesa che assume la veste di "Amministratore di Foresta/Dominio"[2]. Nella Direzione

[1] In altri termini, opera il criterio, riassunto nell'espressione anglosassone "*data protection by default and by design*" (art. 25 del Regolamento), il quale impone che siano previste fin dall'inizio le garanzie indispensabili al fine di soddisfare i requisiti del Regolamento e a tutelare i diritti e le libertà degli interessati.

[2] Cfr. la Pubblicazione SMD-VI Reparto "Procedure per la gestione in sicurezza dell'attuale architettura di sistemi ICT non classificati", ed. marzo 2017. Essa è basata sulla "Foresta" che *rappresenta una soluzione architetturale che definisce un modello organizzativo finalizzato a garantire l'interoperabilità tra le infostrutture e la loro sicurezza tramite una integrazione del coordinamento centrale, ma salvaguardando l'indipendenza e l'autonomia operativa delle varie componenti. La sicurezza dell'attuale Foresta basa la sua efficacia sul rispetto di un dispositivo di regole e prescrizioni stringenti destinate a tutte le componenti organizzative che ne fanno parte, che si prestano a rispettarle,*

l'amministrazione locale dei sistemi è affidata agli Amministratori di Foresta/Dominio coadiuvati dai "Referenti Locali Informatici" di Livello 1 e Livello 2 della Direzione. Tali referenti sono stati designati sulla base delle proprie conoscenze tecnico professionali.

Il testo del presente documento sviluppa, nella PARTE I, argomenti concernenti:

- l'elenco dei trattamenti di dati personali;
- la distribuzione dei compiti nell'ambito delle strutture preposte al trattamento dei dati;
- l'analisi dei rischi che incombono sul trattamento dei dati;
- le misure adottate (ed, eventualmente, quelle ulteriori *in itinere*) per garantire l'integrità (nessuna loro alterazione), la disponibilità dei dati (per evitare la loro distruzione, indisponibilità o perdita) e la riservatezza (divulgazione e accesso[3]);
- i criteri e le modalità di ripristino dei dati in seguito a perdita, deterioramento, modifica, distruzione o danneggiamento;
- la previsione di interventi formativi a favore del personale autorizzato al trattamento;
- le procedure da seguire per il controllo sullo stato della sicurezza;
- le dichiarazioni d'impegno, custodia e distribuzione del documento.

Nella PARTE II, viene fornita una prima valutazione dell'impatto in relazione ai trattamenti previsti presso la Direzione che potrebbero presentare caratteri di rischiosità per i diritti e per le libertà delle persone fisiche, fermo restando che si verte, normalmente, in tema di trattamenti dei dati effettuati in applicazione dall'art. 6, paragrafo 1, lettera e) del Regolamento (il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento), per i quali potrebbe operare il disposto dell'art. 35, paragrafo 10 [4] (si

pur nella propria autonomia gestionale, a vantaggio dell'intera comunità, rafforzando la sicurezza e la protezione del sistema nel suo complesso.

[3] L'applicazione del Regolamento può richiedere in concreto un'attenta azione di equilibrio con le esigenze derivanti dal *Freedom of Information Act* (FOIA), introdotto nella legislazione nazionale dall'art. 7 della legge 7 agosto 2015, n. 124 e dal conseguente d.lgs. 25 maggio 2016, n. 97, che ha modificato il d.lgs. 14 marzo 2013, n. 33, in materia di trasparenza, disciplinando il nuovo istituto dell'accesso civico generalizzato.

[4] "*Qualora il trattamento effettuato ai sensi dell'articolo 6, paragrafo 1, lettere c) o e), trovi nel diritto dell'Unione o nel diritto dello Stato membro cui il titolare del trattamento è soggetto una base giuridica, tale diritto disciplini il trattamento specifico o l'insieme di trattamenti in questione, e sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nell'ambito di una valutazione d'impatto generale nel contesto dell'adozione di tale base giuridica,*

richiamano, al riguardo, gli articoli del Libro VI, Titolo II del DPR n. 90/2010, concernenti l'identificazione dei dati sensibili – adesso costituenti le categorie particolari di dati personali, di cui all'art. 9 del Regolamento, e giudiziari trattati e delle relative operazioni effettuate, su cui vedasi *infra* e nell'Allegato "A"), ovvero potrebbe intervenire una causa escludente ai sensi del paragrafo 5 dello stesso art. 35.

La Direzione, nell'ambito delle competenze attribuite dal D.M. 16 gennaio 2013, concernente "Struttura del Segretariato generale, delle Direzioni generali e degli Uffici centrali del Ministero della difesa", in attuazione dell'articolo 113, comma 4 del decreto del Presidente della Repubblica 15 marzo 2010, n. 90, recante il testo unico delle disposizioni regolamentari in materia di ordinamento militare", con specifico riferimento all'art. 15, provvede: all'ammissione alla navigazione aerea degli aeromobili militari mediante la certificazione di tipo aeromobile e la loro immatricolazione nel Registro degli Aeromobili Militari (RAM), di cui cura la custodia e l'aggiornamento previa verifica della configurazione approvata e dei requisiti di aeronavigabilità; a svolgere e rappresentare negli organismi nazionali e internazionali la funzione esclusiva di Autorità di Aeronavigabilità militare italiana, individuata e definita all'art. 745 del codice della navigazione aerea; all'approvvigionamento degli aeromobili militari e dei mezzi spaziali, delle armi, delle munizioni, degli armamenti, delle apparecchiature e degli equipaggiamenti formanti parte integrante e inscindibile dei sistemi d'arma aeronautici e spaziali, dei materiali di aviolancio e, dove richiesto, dei carbolubrificanti; all'emanazione della normativa tecnica e alla formazione relativa all'aeronavigabilità, all'acquisizione, utilizzo, conservazione e dismissione degli aeromobili militari e di detti sistemi e mezzi; a sovraintendere alle attività di studio, progettazione, sviluppo tecnico, costruzione, produzione, trasformazione, ammodernamento e alle indagini tecniche sui materiali di competenza (si rimanda all'art. 1044 del d.P.R. n. 90/2010, che riguarda i procedimenti di competenza della Direzione).

Ai sensi dell'art. 13 del Regolamento UE 2016/679 si informano i soggetti interessati che il trattamento dei dati personali loro forniti o acquisiti è finalizzato esclusivamente all'espletamento delle relative attività istituzionali. Il trattamento dei dati personali e particolari avverrà a cura dei soggetti a ciò appositamente autorizzati con l'utilizzo di

---

i paragrafi da 1 a 7 non si applicano, salvo che gli Stati membri ritengano necessario effettuare tale valutazione prima di procedere alle attività di trattamento".

procedure anche informatizzate e con l'eventuale ausilio di apposita banca automatizzata, nei modi e nei limiti necessari per il perseguimento della finalità per cui i dati personali e particolari sono raccolti e/o successivamente trattati; ciò anche in caso di eventuale comunicazione a terzi. In relazione al trattamento dei dati sono comunicati: il Titolare del Trattamento, indirizzo, posta elettronica istituzionale e posta elettronica certificata; la finalità del trattamento. Il periodo di conservazione dei dati personali e particolari è stabilito in un arco temporale non superiore al conseguimento delle finalità pubbliche per le quali i dati sono trattati, ivi compresa la tutela degli interessi dell'A.D. presso le giurisdizioni ordinarie, amministrativa e contabile. L'eventuale reclamo potrà essere proposto all'Autorità Garante per la protezione dei dati personali, in qualità di Autorità di controllo.

PARTE I

1. DEFINIZIONI E PRINCIPI APPLICABILI AL TRATTAMENTO DEI DATI PERSONALI

Il presente documento definisce le politiche e gli *standard* di sicurezza in merito al trattamento dei dati personali.

A tale proposito è opportuno precisare che:

1. L'art. 4 del Regolamento fornisce, tra le altre, le seguenti definizioni:

a) "«dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale".

b) "trattamento", termine con cui si intende "qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione".

2. Ai sensi dell'art. 5 del Regolamento, i dati personali sono trattati:

a) in modo lecito, corretto e trasparente nei confronti dell'interessato ("liceità, correttezza e trasparenza")

b) raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo che non sia incompatibile con tali finalità ("limitazione della finalità")

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati "minimizzazione dei dati")

d) esatti e, se necessario, aggiornati ("esattezza")

e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati ("limitazione della conservazione")

f) i dati personali sono trattati in maniera da garantire la loro adeguata sicurezza, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

3. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle condizioni esplicitate dall'art. 6, paragrafo 1 del Regolamento.

Nell'ambito della Direzione trova applicazione, in particolare, quanto previsto dalla lettera e) dell'art. 6 paragrafo 1, che esprime la liceità quando il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

2. IDENTIFICAZIONE DEI DATI DA TRATTARE

Nell'ambito della Direzione i Dati personali da trattare per le esigenze istituzionali sono:

- Dati Anagrafici: relativi al personale militare e civile in servizio presso la Direzione e gli Uffici Tecnici Territoriali dipendenti, nonché del personale delle società con cui vengono definite attività tecnico-amministrative;
- Dati Sanitari: relativi al personale militare e civile in servizio presso la Direzione e gli Uffici Tecnici Territoriali dipendenti;
- Dati Disciplinari: relativi al personale militare e civile in servizio presso la Direzione e gli Uffici Tecnici Territoriali dipendenti;
- Dati Giuridici: relativi al personale militare e civile in servizio presso la Direzione e gli Uffici Tecnici Territoriali dipendenti nonché il personale delle società con cui vengono definite attività tecnico-amministrative.

Tali informazioni sono disponibili in formato cartaceo e/o informatico.

3. ORGANIZZAZIONE PREPOSTA AL TRATTAMENTO DEI DATI PERSONALI

Ai fini del presente documento, ferme restando le specifiche funzioni attribuite al Responsabile unico della protezione dei dati personali (RPD) della Difesa ai sensi degli artt. 37-39 del Regolamento, l'organizzazione della Direzione è articolata come segue:

(1) il "Titolare del Trattamento dei Dati personali" (TTD) è la Direzione;

(2) il "Referente del Responsabile della Protezione dei Dati personali dell'Amministrazione della Difesa" è il Referente della Prevenzione della Corruzione e per la Trasparenza della Direzione;

(3) al personale che svolge o che assume l'incarico di:

- Vice Direttore;
- Capo Reparto;
- Capo Divisione;
- Capo Ufficio;
- Capo Segreteria Particolare del Direttore
- Capo Servizio;
- Direttore di Ufficio Tecnico Territoriale

in aggiunta alle funzioni previste dal vigente Decreto Ministeriale di struttura sono stati assegnati specifici compiti con il citato D.D. n. 18 dell'8 marzo 2019, al fine di assicurare la liceità di trattamento dei dati personali nello svolgimento delle attività di rispettiva competenza;

(4) tutto il personale della Direzione è autorizzato al trattamento dei dati personali, ai sensi dell'articolo 4, n. 10 del Regolamento, limitatamente allo svolgimento delle attività istituzionali di rispettiva competenza connesse con le attribuzioni dell'incarico ricoperto.

4. COMPITI E RESPONSABILITA DEL PERSONALE

I compiti e le responsabilità sono adeguatamente ripartiti, al fine di evitare l'indebita acquisizione di informazioni oggetto del trattamento, come di seguito specificato:

(1) Al **Titolare del Trattamento dei Dati personali** competono le decisioni in ordine alle finalità, alle modalità del trattamento dei dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;

(2) Al **Personale che svolge uno degli incarichi di rilievo** elencati al precedente para 3.a.(3) sono assegnati i seguenti compiti:

- rispettare e far rispettare il Regolamento, con riguardo al trattamento dei dati personali;
- rispettare e far rispettare il Decreto Legislativo 30 giugno 2003, n. 196, recante "Codice in materia di protezione dei dati personali" e successive modifiche e integrazioni;
- rispettare e far rispettare le disposizioni dell'articolo 4 del Decreto Legislativo 14 marzo 2013, n. 33, con particolare riferimento agli obblighi di rendere non intelligibili i dati personali che non siano pertinenti e quelli sensibili/giudiziari che non siano indispensabili, rispetto alle specifiche finalità di trasparenza sancite dal decreto legislativo medesimo;
- rispettare e far rispettare, nello svolgimento delle attività di competenza, le presenti Misure Tecniche e Organizzative, adeguate per garantire il livello di sicurezza rapportato al rischio, ai sensi dell'articolo 32 del Regolamento, approvate nell'ambito Direzione con apposito Ordine del Giorno;
- rispettare e far rispettare, nello svolgimento delle attività di competenza, le prescrizioni contenute nel Registro delle Attività di trattamento, quale parte integrante del citato Decreto Direttoriale di attribuzione dei compiti e delle responsabilità;
- accertare che i dati personali siano trattati esclusivamente per il perseguimento delle finalità istituzionali della Direzione e nel rispetto delle prescrizioni di cui agli articoli da 1053 a 1075 del Decreto del Presidente della Repubblica 15 marzo 2010, n. 90, recante "Testo Unico delle disposizioni regolamentari in materia di Ordinamento Militare", citato nelle premesse;
- assicurarsi che i dati personali siano conservati in una forma che consenta l'identificazione dell'interessato, per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati

e, comunque, non eccedente il periodo di conservazione previsto nel Registro delle Attività sopracitato;

- proporre al Titolare del Trattamento Dati l'adozione dei provvedimenti connessi con l'esercizio dei diritti di accesso, di informazione, nonché quelli di rettifica, integrazione, cancellazione, limitazione e opposizione, riguardanti il trattamento dei dati personali, di cui al Capo III del Regolamento;
- informare il Referente della Direzione, in merito agli aspetti connessi con le prescrizioni del Regolamento che siano stati segnalati dagli interessati, ovvero riguardo a quelli ritenuti utili/opportuni, al fine del corretto espletamento delle attività di competenza;
- rispettare e far rispettare i provvedimenti resi dall'Autorità garante della privacy, in materia di tutela delle persone rispetto al trattamento di dati, con specifico riferimento a quelli particolari di cui all'articolo 9 del Regolamento[5], attese le rilevanti finalità di interesse pubblico perseguite;
- rendere edotto il personale direttamente dipendente, in merito alla inutilizzabilità dei dati personali trattati in violazione della disciplina normativa e regolamentare vigente in materia.

(3) Il **personale civile e militare autorizzato** al trattamento dei dati personali è tenuto, nello svolgimento dei doveri d'ufficio, alla rigorosa osservanza delle seguenti disposizioni:

- trattare i dati personali in modo lecito, corretto e trasparente, esclusivamente per il perseguimento delle finalità istituzionali della Direzione e nell'ambito delle prescrizioni di cui agli articoli da 1053 a 1075 del Decreto del Presidente della Repubblica 15 marzo 2010, n. 90;

---

[5] Articolo 9 del Regolamento: Trattamento di categorie particolari di dati personali. È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare 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.

- rispettare le disposizioni in materia di privacy, dettate dal Codice di Comportamento dei dipendenti dell'Amministrazione della Difesa, approvato in data 23 marzo 2018;
- raccogliere i dati personali per le finalità istituzionali determinate, esplicite e legittime e successivamente trattarli in modo compatibile con tali finalità;
- trattare i dati personali in modo adeguato, pertinente e limitatamente a quanto necessario, rispetto alle finalità istituzionali perseguite;
- verificare l'esattezza dei dati e, se necessario, aggiornarli, provvedendo alla loro cancellazione ovvero alla tempestiva rettifica di quelli inesatti, rispetto alle finalità per le quali sono trattati;
- conservare i dati personali in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore a quello previsto nel Registro delle attività;
- rendere non intelligibili i dati personali che non siano pertinenti e quelli particolari, di cui all'articolo 9 del Regolamento, che non siano indispensabili per le specifiche finalità di trattamento.

5. PROCEDURE DI TRATTAMENTO DEI DATI PERSONALI

a. Trattamento dei dati personali senza strumenti informatici

Il trattamento dei dati personali effettuato senza l'ausilio di strumenti elettronici deve avvenire nel rispetto delle seguenti prescrizioni:

- deve essere effettuato esclusivamente per il perseguimento delle finalità istituzionali della Direzione e nell'ambito delle norme di legge e regolamentari vigenti, operando con la massima riservatezza nell'utilizzo dei dati medesimi;
- deve essere effettuato in modo lecito e secondo correttezza, verificandone l'esattezza e promuovendo le azioni necessarie al loro aggiornamento;
- i dati personali trattati devono essere pertinenti, completi e non eccedenti le finalità per le quali sono stati raccolti o successivamente conservati e devono essere custoditi secondo i criteri della diligenza qualificata, propria dell'incarico ricoperto e nella

scrupolosa osservanza dei doveri di riservatezza e, se necessario, provvedere al loro aggiornamento;

- gli atti ed i documenti contenenti i dati devono essere conservati in archivi con accesso consentito al solo personale dipendente e per lo svolgimento dei doveri d'ufficio;
- devono essere rispettati i provvedimenti resi dall'Autorità garante in materia di trattamento di dati personali, di dati sensibili e di quelli aventi carattere giudiziario;
- deve essere informato il Titolare del trattamento in merito ad eventuali ricorsi all'Autorità garante;
- devono rendersi noti al Titolare del trattamento gli aspetti connessi alle prescrizioni del Regolamento che siano stati segnalati dagli interessati (utenti), ovvero quelli ritenuti utili e/o opportuni al fine del corretto espletamento delle attività di competenza;
- il personale dipendente deve essere reso edotto in merito alla inutilizzabilità dei dati personali, trattati in violazione della disciplina normativa e regolamentare vigente in materia.

b. Trattamento dei dati effettuato con strumenti informatici

Nell'ambito della Direzione i trattamenti dei dati, effettuati con strumenti informatici, sono di seguito elencati:

- trattamenti effettuati con applicativi di carattere generale (i.e. @D[h]OC, etc.), come elencati in Allegato "B", forniti da altri Enti della Difesa attraverso la rete DIFENET. Per l'utilizzo di tali applicativi si rinvia alla relativa documentazione proveniente dall'Ente originatore, tenuto conto che la Direzione utilizza i sistemi di sicurezza e di connettività del Comando C4 Difesa tramite la rete DIFENET;
- trattamenti effettuati con applicativi specifici acquisiti dalla Direzione, descritti in Allegato "C" e dislocati presso il Centro Elaborazione Dati (CED) del Segretariato Generale/DNA, sito in Via Marsala, la cui sicurezza e *privacy* sono di competenza del Comando C4 Difesa;
- trattamenti effettuati sui *personal computer* individuali della Direzione. Il personale è autorizzato a trattare sul proprio ***personal computer*** **i dati personali**

esclusivamente per lo svolgimento dei compiti istituzionali per il tempo strettamente necessario, secondo la vigente normativa e le disposizioni in merito alla sicurezza dei dati e dei sistemi EAD.

6. MISURE DI PROTEZIONE ADOTTATE

a) **Suddivisione delle misure**

Avuto riguardo a quanto emerge anche da atti e tutorial provenienti dal Garante per la Protezione dei dati personali, le misure per la gestione del rischio possono sommariamente riepilogarsi come di seguito riportato:

- misure organizzative: ruoli, *governance*, procedure, *audit*, strumenti di controllo per interessati, contatti, istruzioni e formazione; ad eccezione delle ultime due misure per le quali è direttamente responsabile la Direzione tramite il rilascio di istruzioni per l'uso dei *software* interni e la raccolta dei Moduli di assunzione di responsabilità individuali per la navigazione *web* (in Allegato "E"), le restanti misure risalgono alla competenza dello SMD VI Reparto/Comando C4 Difesa[6];

- misure tecnologiche: impostazione di *policy* di sicurezza logiche e fisiche, rilascio di aggiornamenti servizi e *software*, *test*, controllo accessi e tracciamento delle operazioni, anch'esse sostanzialmente riferibili alla competenza dello SMD VI Reparto/Comando C4 Difesa;

- minimizzazione: principio di base per il quale i dati devono essere sempre adeguati, pertinenti e limitati a quanto necessario per il perseguimento delle finalità per cui sono raccolti e trattati (c.d. criterio di pertinenza e di non eccedenza, rinvenibile anche nel Codice dell'Amministrazione Digitale – CAD, di cui al d.lgs. 7 marzo 205, n. 82): in

[6] Cfr. le <<Linee guida per l'implementazione delle "misure minime di sicurezza *ICT*" in ambito A.D. (Circolare n. 2 del 18 aprile 2017 – Agenzia per l'Italia Digitale)>>, approvate dal Capo Reparto del VI Rep. e D.G.Re.S.I.A.D. in data 21 dicembre 2017, significando, in merito, che, ai sensi del DM 8 novembre 2011, il Capo di SMD VI Reparto svolge le funzioni di Dirigente Generale Responsabile dei Sistemi Informativi Automatizzati dell'A.D.. La circolare AgID è richiamata in precedenza, al para 3.e.(2).

sostanza il Titolare deve trattare solo i dati di cui ha realmente bisogno per raggiungere le finalità del trattamento;

- anonimizzazione dei dati: si configura come un trattamento che ha lo scopo di impedire l'identificazione dell'interessato; i dati resi anonimi non rientrano così nell'ambito di applicazione della legislazione in materia di protezione dei dati[7];

- conservazione adeguata: impone di garantire che i dati personali siano conservati in modo da consentire l'identificazione degli interessati per un tempo non superiore a quello necessario al conseguimento della finalità del trattamento; una volta soddisfatta la finalità del trattamento i dati devono essere cancellati;

- cifratura: strumento volto a mitigare i rischi connessi al trattamento, diverso dall'anonimizzazione Se infatti l'anonimizzazione consente la cancellazione, in modo irreversibile, di ogni elemento dal dato personale che consente l'identificazione dell'interessato, la cifratura continua a permettere un'identificazione dell'individuo, anche se in via indiretta;

- qualità dei dati: è il concetto per cui il trattamento dei dati personali deve avvenire rispettando determinati requisiti, in particolare in relazione alla pertinenza rispetto alla finalità del trattamento e alla esattezza dei dati stessi.

b) **Misure di carattere fisico**

Le misure di carattere fisico applicate sono di seguito elencate:

- le apparecchiature informatiche critiche (*server* di rete, *computer* e apparecchiature di telecomunicazione) e gli archivi cartacei contenenti dati personali o sensibili/giudiziari devono essere situati in locali ad accesso controllato;

[7] Nell'ambito della Direzione non dovrebbe trovare diretta applicazione la c.d. pseudonimizzazione, ovvero il principio per cui le informazioni di profilazione devono essere conservate in una forma che impedisca l'identificazione dell'utente, in quanto non vengono effettuate attività di profilazione.

- i server che custodiscono gli archivi informatici si trovano presso il CED di SGD, in ambienti protetti e controllati rispondenti alle precauzioni sopra indicate; il controllo di tali server è sotto la responsabilità di SGD;
- gli archivi cartacei sono custoditi negli uffici della Direzione, all'interno di armadi chiusi a chiave; le chiavi degli armadi sono custodite dal personale preposto (una copia delle chiavi degli armadi è conservata in busta chiusa nella cassaforte del Capo dell'Ufficio del Direttore o presso il Direttore/Capo Distaccamento/Capo Nucleo degli Uffici Tecnici Territoriali); nei locali interessati è autorizzato ad accedere solo il personale preposto; tali locali, quando non sono presidiati, vengono chiusi;
- l'ingresso ai locali ad accesso controllato è possibile solo dall'interno dell'area;
- i locali devono essere dotati di sistemi di condizionamento e di apparecchiature di continuità elettrica e di rilevazione fumi/spegnimento incendio.

c) **Misure di carattere procedurale**

Le misure di carattere procedurale adottate sono elencate come segue:

- l'ingresso nei locali ad accesso controllato è consentito solo alle persone autorizzate;
- il Responsabile dell'area ad accesso controllato deve mantenere un effettivo controllo sull'area di sua responsabilità;
- i visitatori occasionali delle aree ad accesso controllato sono accompagnati da un incaricato e non possono rimanere da soli in detti locali;
- per l'ingresso ai locali ad accesso controllato è necessaria la preventiva autorizzazione da parte del personale preposto;
- l'ingresso in locali ad accesso controllato da parte di dipendenti o estranei per operazioni di pulizia o di manutenzione avviene solo se i contenitori dei dati sono protetti e non accessibili e i *computer* non sono utilizzabili.

d) **Misure di carattere elettronico/informatico**

Le misure di carattere elettronico/informatico sono emanate a cura del Comando C4 Difesa.
Il personale della Direzione, nell'utilizzo giornaliero dei sistemi, dovrà, comunque:

- Rispettare e far rispettare le disposizioni fornite dal Comando C4 Difesa

- Rispettare e far rispettare le disposizioni fornite dai referenti informatici della Direzione;
- Prestare particolare attenzione all'utilizzo della lan/intranet/internet;;
- Prestare particolare attenzione al rischio di contaminazione di *virus* e *malware* in genere, veicolati per mezzo di posta elettronica o *usb key*
- Gestire con estrema oculatezza le credenziali di accesso ai sistemi informatici, rispettando le policy richieste dai gestori.
- Salvare i dati nelle cartelle di rete per le quali è assicurato dal C4D il controllo degli accessi e il backup periodico.
- Utilizzare il computer individuale solo per accedere agli applicativi o per predisporre i documenti; eventuali copie locali dei documenti contenenti dati personali dovranno essere tenuti solo per il tempo strettamente necessario alla lavorazione del documento.
- Non utilizzare i servizi di posta elettronica privata per l'invio dei documenti contenenti dati personali.
- Non utilizzare computer privati per trattare dati personali per esigenze di servizio.

e) Criteri e modalità di ripristino dei dati

(1) Generalità

La procedura di salvataggio degli archivi elettronici oggetto del trattamento dati (*backup*) contribuisce a garantire l'integrità del dato, permettendo di ripristinarlo in caso di cancellazione o distruzione, totale o parziale, intenzionale o accidentale nell'ambito della banca dati e/o sistema informatico di riferimento.

Per quanto concerne i sistemi informatici e gli applicativi utilizzati dalla Direzione il servizio di *backup* è a cura del CED del Segretariato Generale /DNA secondo indicazioni che sono state fornite dalla Direzione.

Per quanto concerne i sistemi informatici e gli applicativi forniti dalla Difesa il servizio di *backup* è sempre a cura del CED del Segretariato Generale /DNA, secondo le indicazioni fornite dal C4Difesa.

(2) Periodicità dei salvataggi

Nell'ambito della Direzione, le attività di salvaguardia degli archivi, di cui al precedente comma a., vengono svolte adottando le procedure di seguito descritte:

- Utilizzo del "*file server*" è un servizio reso disponibile dal Servizio Informatica, per mezzo del CED del Segretariato Generale/DNA, che ne cura anche il *backup*, progettato per mettere a disposizione del personale della Direzione uno spazio su disco da condividere tra gli appartenenti a una stessa unità organizzativa, nel quale è possibile salvare, leggere, modificare e creare *file* in aderenza alle politiche di sicurezza riportate nel presente documento. A tale scopo le banche dati da salvaguardare dovranno essere contenute all'interno del "*file server*" in argomento;
- adozione di procedure proprie il Responsabile di ciascuna Unità organizzativa dovrà, nell'ambito dei processi lavorativi, identificare quelli che generano e alimentano banche dati di particolare interesse e/o ritenute sensibili a vario livello, emanando le procedure che faranno parte di un disciplinare interno all'Unità organizzativa di che trattasi;
- ripristino dei dati danneggiati a seguito di eventi accidentali e/o volontari, può essere necessario dover ripristinare, in tutto o in parte, il *software* impiegato per il trattamento di dati personali e/o le basi dati oggetto del trattamento. Tale operazione deve svolgersi in condizioni di sicurezza a cura del Servizio Informatica della Direzione Generale.

7. ANALISI DEI RISCHI

Per "rischio" si intende uno scenario descrittivo di un evento e delle relative conseguenze, che sono stimate in termini di gravità e di probabilità di avere impatto sui diritti e sulle libertà degli interessati[8]. La sua valutazione è, pertanto, riferita non solo a preservare la sicurezza dei dati durante il loro trattamento ma deve riferirsi anche agli effetti complessivi derivanti

[8] Definizione tratta dalle Linee guida del Gruppo di lavoro Articolo 29 WP248 rev.1. Il Gruppo di lavoro è stato istituito in virtù dell'art. 29 della Direttiva 95/46/CE ed è l'organo consultivo indipendente dell'UE per la protezione dei dati personali e della vita privata.

dalla malaugurata compromissione di quelli trattati presso la Direzione[9], garantendo la loro disponibilità, integrità e riservatezza.

L'analisi dei rischi si basa su:

- Ricognizione del patrimonio informativo da proteggere, di cui al precedente paragrafo 2.
- Organizzazione preposta al trattamento dei dati, esaminata al precedente paragrafo 3.
- Compiti specifici assegnati al personale preposto al trattamento dei dati, trattati al precedente paragrafo 4.
- Procedure definite per il trattamento dei dati, indicate al precedente paragrafo 5.
- Misure di protezione dei dati adottate nella Direzione, esaminate al precedente paragrafo 6.

La presente analisi si prefigge lo scopo di valutare il rischio residuo, che si verifichino eventi di perdita o danneggiamento dei dati o divulgazione dei dati, nonostante le precauzioni adottate.

a) Metodo adottato per la quantificazione del rischio

Lo specifico contesto in esame non consente una misura diretta ed inequivocabile dei parametri che determinano il rischio. Sono state utilizzate pertanto delle stime di tipo probabilistico mediante l'utilizzo di scale semi-quantitative dei parametri in gioco.

In sostanza, è stato considerato il Rischio come prodotto della Probabilità che si verifichi un evento per la Magnitudo (gravità del Danno atteso), ovvero:

$$R = P \times D$$

dove:

R = Rischio;

P = Probabilità che l'evento accada;

D = magnitudo o gravità del Danno atteso.

[9] Con specifico riferimento alla perdita di controllo dei dati e all'impossibilità di esercitare diritti, servizi o altre opportunità, oltre a possibili svantaggi economici o sociali e danni per la reputazione.

La **scala delle Probabilità** fa riferimento all'esistenza di una correlazione più o meno diretta tra la carenza riscontrata ed il danno ipotizzato ed all'esistenza di analisi statistiche di inconvenienti verificatisi in passato. Tale Probabilità ha quattro ordini di grandezza:

VALORE	LIVELLO DI PROBABILITA'	DEFINIZIONI/CRITERI
4	MOLTO PROBABILE	Sono noti episodi in cui il l'evento si è verificato provocando un danno e/o l'evento può provocare un danno con una correlazione diretta. Il verificarsi del danno conseguente alla mancanza rilevata non susciterebbe alcuno stupore.
3	PROBABILE	È noto qualche episodio in cui l'evento ha causato danno e/o l'evento può provocare il danno anche se non in modo automatico. Il verificarsi del danno ipotizzato susciterebbe sorpresa.
2	POSSIBILE	Sono noti rari episodi già verificati, e/o l'evento può verificarsi solo in circostanze particolari. Il verificarsi del danno ipotizzato susciterebbe sorpresa.
1	IMPROBABILE	Non sono noti episodi già verificati e/o il danno si può verificare solo per una concatenazione di eventi improbabili e tra loro indipendenti. Il verificarsi del danno ipotizzato susciterebbe grande sorpresa ed incredulità.

La **scala della Magnitudo,** ovvero la scala della gravità del danno ipotizzato "D" ipotizzando le conseguenze della perdita di controllo dei dati e dell'impossibilità di esercitare diritti, servizi o altre opportunità, oltre a possibili svantaggi economici o sociali e danni per la reputazione. La scala della Magnitudo ha anch'essa quattro ordini di grandezza:

VALORE	LIVELLO DI GRAVITA'	DEFINIZIONI/CRITERI
4	GRAVISSIMO	Danno molto grave irreversibile.

		Ingenti conseguenze economiche
3	GRAVE	Danno con impatto notevole che comporta conseguenze prolungate nel tempo. Significative conseguenze economiche
2	MODESTO	Danno con impatto contenuto e limitato nel tempo. Conseguenze economiche molto limitate o nulle
1	LIEVE	Danno con basso impatto temporalmente circoscritto. Conseguenze economiche nulle.

Definiti il Danno atteso e la Probabilità che tale danno si verifichi, il Rischio viene automaticamente graduato mediante la formula **R = P x D** ed è raffigurabile con la seguente rappresentazione grafico – matriciale avente in ordinata la gravità del Danno ed in ascisse la probabilità del suo verificarsi:

MATRICE DI VALUTAZIONE						
DANNO GRAVISSIMO	MAGNITUDO	4	4	8	12	16
DANNO GRAVE		3	3	6	9	12
DANNO MODESTO		2	2	4	6	8
DANNO LIEVE		1	1	2	3	4
			1	2	3	4
			PROBABILITA'			
Rischio basso			IMPROBABILE	POCO PROBABILE	PROBABILE	MOLTO PROBABILE
Rischio medio						
Rischio elevato						

In tale matrice, i rischi maggiori occupano le caselle di destra in alto (danno molto grave, probabilità elevata), quelli minori le posizioni in basso a sinistra (danno lieve, probabilità trascurabile), con tutta una serie di posizioni intermedie.

La valutazione numerica del livello di rischio permette di identificare i settori in cui è necessario adottare maggiori misure di protezione ovvero è necessario approfondire l'analisi d'impatto. A tal fine viene adottata la seguente scala di valutazione:

R	RISCHIO
$1 \leq R \leq 4$	BASSO
$5 \leq R \leq 9$	MEDIO
$10 \leq R \leq 16$	ELEVATO

Il metodo utilizzato è un valido aiuto per cercare di rendere il più oggettivo possibile il giudizio sui vari rischi presenti in quanto scompone la decisione di priorità in una serie di scelte successive più semplici.

L'inevitabile soggettività sulle scelte delle scale di Probabilità e di gravità del Danno sarà attenuata dal confronto continuo con il personale che esegue il trattamento dei dati.

b) Individuazione delle minacce e valutazione del rischio

MINACCIA	MISURA DI PROTEZIONE	PROBABILITA'	DANNO	RISCHIO	
Accesso agli archivi cartacei contenenti le informazioni anagrafiche o disciplinari da	Gli archivi cartacei sono custoditi in armadi chiusi a chiave in un locale in cui è autorizzato ad	2	2	4	BASSO

parte di personale non autorizzato	accedere solo il personale preposto				
Accesso non autorizzato agli archivi cartacei contenenti le informazioni sanitarie o giudiziarie	Gli archivi sono custoditi in armadi chiusi a chiave in un locale in cui è autorizzato ad accedere solo il personale preposto. Le informazioni sanitarie sono chiuse in busta chiusa. Le informazioni giudiziarie sono custodite separatamente.	2	3	6	MEDIO
Modifica accidentale dei dati in archivio	I dati vengono periodicamente controllati dagli interessati. Eventuali errori verrebbero quindi rilevati e corretti	1	3	3	BASSO
Divulgazione dei dati da parte del personale preposto per errore procedurale o per slealtà	Il personale preposto è selezionato, formato e frequentemente richiamato al rispetto delle regole.	2	3	6	MEDIO
Accesso non autorizzato ai dati informatici a seguito di sottrazione delle credenziali al personale preposto	Le policy di sicurezza definite da SMD VI Reparto – C4I prevedono il cambio periodico della password con frequenza almeno mensile	1	3	3	BASSO
Attacco software dall'esterno che comporta la violazione o l'alterazione o la cancellazione o l'indisponibilità dei dati (malware, web based attack, web application attack, Denial of service, botnet, data breach, data leakage)	SMD - VI Reparto Sistemi C4I e Trasformazione, aderendo a quanto prescritto dall'AgID con la Circolare n. 2 del 18 aprile 2017 recante le "Misure minime di sicurezza *ICT* per le Pubbliche Amministrazioni", nell'ottica della realizzazione di una cornice di protezione di base all'intera struttura *ICT* della Difesa, ha implementato una serie di	1	3	3	BASSO

		misure di sicurezza finalizzate a prevenire e contrastare le minacce cibernetiche più comuni e frequenti cui sono sottoposti i propri sistemi informativi.				
	Indisponibilità temporanea dei dati a causa di guasti (blackout elettrico, malfunzionamento rete, …).	I sistemi del CED di SGD e la rete elettrica di Palazzo Guidoni sono alimentati in emergenza tramite generatori elettrici locali. La architettura di rete dei sistemi informatici prevede una adeguata ridondanza.	1	2	2	BASSO
	Perdita dei dati a causa di guasti ai sistemi informatici (danneggiamento unità di archiviazione, terremoto, incendio, allagamento dei locali dove sono custoditi i sistemi informatici sensibili).	Le strutture dove sono custoditi i sistemi informatici sono dotate delle protezioni di sicurezza previste per legge. Vengono effettuate copie di backup in accordo a policy fissate da SMD-C4I per i sistemi della Difesa e dalla Direzione per i sistemi acquisiti localmente. Tali policy prevedono il backup almeno giornaliero. La eventuale perdita di dati è quindi molto contenuta.	1	2	2	BASSO

In relazione a quanto sopra rappresentato, lo SMD - VI Reparto Sistemi C4I e Trasformazione, aderendo a quanto prescritto dall'AgID con la Circolare n. 2 del 18 aprile 2017 recante le "Misure minime di sicurezza *ICT* per le Pubbliche Amministrazioni", nell'ottica della realizzazione di una cornice di protezione di base all'intera struttura *ICT* della Difesa, ha implementato una serie di misure di sicurezza finalizzate a prevenire e contrastare le minacce cibernetiche più comuni e frequenti cui sono sottoposti i propri sistemi informativi.

8. PIANIFICAZIONE DEGLI INTERVENTI FORMATIVI

La formazione alla privacy può essere definita come "l'insieme delle attività e degli interventi in materia di trattamento di dati personali e sicurezza delle informazioni, predisposti da un determinato Titolare, finalizzati ad aumentare le competenze cognitive, operative e comportamentali di Responsabili e incaricati ed in grado di incidere in maniera significativa sull'etica e le metodologie di lavoro pubblico."

Nel concetto di formazione alla *privacy* sono compresi tutti quegli interventi in materia di protezione di dati personali diretti a modificare abitudini comportamentali scorrette, a riconoscere pericoli e condizioni potenziali che potrebbero determinare eventi indesiderati, a prevenire i rischi e a fronteggiare eventuali emergenze.

Nell'ambito della Direzione la responsabilità di organizzare tali attività, secondo una programmazione annuale e con il maggiore possibile coinvolgimento del personale, fa capo all'Ufficio del Direttore. I dirigenti che svolgono i compiti elencati al paragrafo 3.a.(3) dovranno destinare il personale alle dirette dipendenze alla frequenza dei corsi affinché possa ricevere la prevista formazione.

Al fine di informare gli *"Autorizzati al trattamento dati*" sulle tematiche richiamate, è, altresì, compito del personale che svolge gli incarichi elencati al paragrafo 3.a.(3) svolgere una costante azione di sensibilizzazione e di istruzione sulle norme generali in materia di *privacy*, sulle disposizioni innovative recate dal Regolamento e sugli aspetti peculiari dei trattamenti effettuati:

- all'ingresso in servizio;
- in occasione dell'introduzione di nuovi strumenti e/o programmi informatici;
- in occasione di cambiamenti di mansione;
- sulle pratiche di utilizzo sicuro della rete;
- sulle azioni da intraprendere allorquando vengono riscontrate eventuali anomalie di funzionamento dei sistemi (*hardware* e *software*) correlate a problemi di sicurezza.

Ferme restanti le attività formative che saranno definite dal Responsabile della Protezione dei Dati personali della Difesa, sono previsti, come accennato in precedenza, seminari informativi e di aggiornamento, con cadenza periodica, cui gli "*Autorizzati al trattamento dati*" (in particolare, Personale delle Segreterie, Capi Sezione ed eventuali altri soggetti in relazione a specifiche attività) sono tenuti a partecipare.

PARTE II

1. VALUTAZIONE D'IMPATTO

La Valutazione d'Impatto sulla Protezione dei Dati (DPIA *Data Protection Impact Assessment*) è obbligatoria qualora un trattamento "possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (art. 35, paragrafo 1 del Regolamento e Linee guida del Gruppo di lavoro Articolo 29). Il rischio, infatti, si deve riferire al soggetto interessato e viene valutato in termini di gravità e di probabilità.

All'esito dell'analisi del rischio effettuata nell'ambito della Direzione risulta che l'impatto del trattamento sui dati personali, anche particolari ai sensi dell'articolo 9 del Regolamento, si presenta **BASSO**, eccezione fatta per le conseguenze derivanti dall'accesso non autorizzato ai dati giudiziari e dai comportamenti sleali o fraudolenti del personale il cui impatto è ritenuto **MEDIO**. Ciò, in quanto i trattamenti della Direzione sono svolti in "ambiente altamente protetto" ed i sistemi informativi sono amministrati dal Comando C4 Difesa per l'intero Dicastero.

Pertanto, in sede di prima applicazione del sopravvenuto Regolamento, non appare indispensabile procedere a ulteriori valutazioni di impatto.

Il trattamento dati svolto presso la Direzione non prevede, tra l'altro, l'uso di nuove tecnologie (art. 35, paragrafo 1 e considerando 89 e 91 del Regolamento) e non appare suscettibile di determinare significativi scostamenti nel livello di rischio, avuto riguardo alla natura, all'oggetto, al contesto e alle finalità pubbliche del trattamento stesso.

2. PROSPETTIVE E APPROFONDIMENTI

Si deve, peraltro, osservare come la Direzione tratti anche le categorie particolari di dati personali di cui all'art. 9 del Regolamento, con particolare riferimento a quelli relativi alla salute, alla disciplina e di carattere giudiziario. Si aggiunge, comunque, che molti di questi dati sono, altresì, trattati da diverse Articolazioni della Difesa (in particolare, le Direzioni Generali per il Personale Militare e Civile, gli Organi sanitari e medico-legali unitamente alla Direzione Generale della Previdenza Militare e della Leva).

In tale situazione, stante il disposto dell'art. 35, paragrafo 1, ultimo periodo ("una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi") e paragrafo 2 ("il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno"), si fa riserva di condurre, ulteriori approfondimenti congiunti, coinvolgendo anche le Componenti C4 delle Forze Armate e della Difesa, oltre al Reparto V del Segretariato Generale/DNA. E ciò anche nella prospettiva di un *risk based approach* coerente con i concetti di protezione dei dati fin dalla progettazione e di protezione per impostazione predefinita di cui all'art. 25 del Regolamento, ponendo l'interessato al centro del sistema di protezione dei dati personali, con garanzia di una tutela effettiva da un punto di vista sostanziale.

ALLEGATO A - IDENTIFICAZIONE DEI DATI SENSIBILI E GIUDIZIARI TRATTATI E DELLE RELATIVE OPERAZIONI EFFETTUATE – ESTRATTO DEL D.P.R. 15 MARZO 2010, N. 90

Testo Unico delle disposizioni regolamentari in materia di Ordinamento Militare

(Pubblicato nella Gazzetta Ufficiale del 18 giugno 2010, n. 140, S.O.)

Titolo II

Identificazione dei dati sensibili e giudiziari trattati

e delle relative operazioni effettuate

Capo I Disposizioni generali

Art. 1053 Oggetto

1. Il presente titolo identifica, in attuazione del decreto legislativo 30 giugno 2003, n. 196, di seguito denominato «decreto n. 196», i tipi di dati sensibili e giudiziari e le operazioni eseguibili da parte dell'Amministrazione della difesa nello svolgimento delle proprie funzioni istituzionali.

Art. 1054 Individuazione dei tipi di dati trattati e delle operazioni eseguibili

1. Nel capo II sono identificati i tipi di dati sensibili e giudiziari per cui è consentito il relativo trattamento, nonché le operazioni eseguibili in riferimento alle specifiche finalità di rilevante interesse pubblico di cui agli articoli 65, 66, 67, 68, 69, 71, 85, 98 e 112 del decreto n. 196.
2. I dati sensibili e giudiziari individuati dal presente titolo sono trattati previa verifica della loro pertinenza, completezza e indispensabilità rispetto alle finalità perseguite nei singoli casi, in particolare nell'ipotesi in cui la raccolta non avvenga presso l'interessato.
3. Le operazioni eseguibili mediante comunicazione e trasferimento all'estero, individuate nel presente titolo, sono ammesse soltanto se indispensabili all'adempimento degli obblighi o allo svolgimento dei compiti di volta in volta indicati per il perseguimento delle specifiche finalità di rilevante interesse pubblico e nel rispetto delle disposizioni in materia di protezione dei dati personali, nonché degli altri limiti stabiliti dalla legge e dai regolamenti.
4. Sono inutilizzabili i dati trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali.

Capo II Trattamento dei dati sensibili e giudiziari

Art. 1055 Reclutamento e formazione del personale militare e assunzione del personale civile

1. In relazione alla rilevante finalità di interesse pubblico dell'instaurazione del rapporto di impiego o di servizio, ai sensi dell'art. 112 del decreto n. 196, il trattamento dei dati sensibili e giudiziari in materia di reclutamento e formazione del personale militare avviene nell'ambito dei seguenti procedimenti e attività:
   a) concorsi allievi dei licei militari;
   b) concorsi allievi accademie;
   c) concorsi allievi ufficiali in ferma prefissata;
   d) concorsi allievi ufficiali piloti di complemento;
   e) ammissione ufficiali in ferma prefissata alla rafferma annuale;
   f) concorsi ufficiali del ruolo normale a nomina diretta;
   g) concorsi ufficiali dei ruoli speciali;
   h) concorsi ufficiali direttori e vice direttori di banda delle Forze armate;
   i) ammissione alla ferma biennale degli ufficiali di complemento;
   l) concorsi per reclutamento allievi marescialli di Esercito italiano, Marina militare e Aeronautica militare e allievi ispettori dell'Arma dei carabinieri;
   m) concorsi per il reclutamento allievi sergenti di Esercito italiano, Marina militare e Aeronautica militare e allievi sovrintendenti dell'Arma dei carabinieri;
   n) concorsi per il reclutamento degli orchestrali delle Forze armate;
   o) concorsi per volontari;
   p) concorsi per transito nel servizio permanente dei volontari in ferma o rafferma;
   q) concorsi per transito dei volontari in ferma o rafferma nelle Forze di polizia;
   r) concorsi straordinari per il transito in servizio permanente e ulteriori concorsi assimilabili ai precedenti;
   s) ammissioni ai corsi di formazione e alle carriere di ufficiali, sottufficiali, graduati e militari di truppa.
2. In relazione alla rilevante finalità di interesse pubblico di instaurazione del rapporto di lavoro, ai sensi dell'articolo 112 del decreto n. 196, il trattamento dei dati sensibili e giudiziari in materia di assunzione del personale civile della Difesa avviene nell'ambito dei seguenti procedimenti e attività:

a) assunzione personale delle aree funzionali;

b) assunzione dirigenti;

c) assunzione categorie protette.

3. Il trattamento dei dati sensibili e giudiziari è effettuato ai sensi dei libri IV e V del codice e delle norme di legge sull'assunzione del personale civile e delle categorie protette.
4. I tipi di dati trattati in relazione a quanto indicato nei commi 1 e 2 sono i seguenti:
   a) stato di salute:

      1) patologie attuali;

      2) patologie pregresse;

      3) terapie in corso;

      4) anamnesi familiare;

   b) dati di carattere giudiziario.

5. Le particolari forme di elaborazione dei dati, per le finalità di seguito indicate, sono le seguenti:
   a) comunicazione agli enti internazionali presso i quali il personale militare presta servizio, con conseguente trasferimento dei dati all'estero, ai sensi dell' articolo 43 del decreto n. 196, ai fini della necessaria notifica di atti afferenti alla corretta gestione del rapporto di lavoro, quali quelli relativi agli accertamenti sanitari connessi all'idoneità al servizio militare, ovvero per le comunicazioni di carattere giudiziario con riflessi sullo stato giuridico e sull'impiego, limitatamente ai casi in cui ciò risulti indispensabile ai fini dell'adozione dei provvedimenti di competenza;
   b) comunicazione all'Ufficio centrale del bilancio presso il Ministero della difesa e alla Corte dei conti, ai fini della registrazione dei decreti di assunzione di personale appartenente alle categorie protette.
6. Il trattamento dei dati di cui ai commi 1 e 2 e il relativo flusso informativo comprendono:
   a) l'acquisizione delle domande di assunzione;

   b) il controllo dei requisiti per l'assunzione;

   c) la raccolta delle informazioni circa il possesso delle qualità morali e di condotta da parte degli aspiranti all'assunzione;

   d) l'organizzazione delle prove d'idoneità e la convocazione dei candidati;

   e) lo svolgimento delle prove d'idoneità;

   f) la comunicazione dei risultati delle prove;

   g) la richiesta e l'acquisizione dei documenti attestanti il possesso di tutti i requisiti dichiarati, procedimenti di nomina.

7. Le comunicazioni di dati sensibili anche mediante trasferimento dei dati all'estero avvengono esclusivamente con riguardo alla fase del controllo dei decreti di assunzione delle categorie protette, ovvero nell'ipotesi in cui l'interessato si trovi a prestare servizio presso un organismo internazionale e si renda necessario notificargli atti attraverso questo ultimo.
8. Si può procedere, altresì, a forme di estrazione e comunicazione dei dati in caso di ulteriori accertamenti sanitari richiesti dall'interessato presso gli organi medico-legali di secondo grado dell'Amministrazione; in tale caso la comunicazione avviene a richiesta dell'interessato.

Art. 1056 Documentazione del personale militare e civile

1 In relazione alla rilevante finalità di interesse pubblico della gestione del rapporto di impiego, di servizio o di lavoro, ai sensi dell'articolo 112 del decreto n. 196, il trattamento dei dati sensibili e giudiziari in materia di documentazione del personale militare e civile della Difesa avviene nell'ambito dei seguenti procedimenti e attività:

a) gestione della documentazione caratteristica e matricolare;

b) rilascio attestazione per benefici combattentistici;

c) rilascio carta multiservizi difesa;

d) cancellazione dalla documentazione matricolare di riferimenti a sentenze, ai sensi della legge sul casellario giudiziale;

e) aggiornamento documentazione matricolare;

f) cancellazione dalla documentazione matricolare di eventuali riferimenti a sanzioni disciplinari;

g) impianto custodia e aggiornamento degli stati di servizio e della documentazione caratteristica.

2 Il trattamento dei dati sensibili e giudiziari è effettuato ai sensi dei libri IV e V del codice e della normativa sul rapporto di lavoro del personale civile.

3 I tipi di dati trattati in relazione a quanto indicato nel comma 1 sono i seguenti:

a) convinzioni:

1) politiche;

2) sindacali;

b) stato di salute:

1) patologie attuali;

2) patologie pregresse;

3) terapie in corso;

4) anamnesi familiare;

c) dati di carattere giudiziario.

4 Nessuno dei procedimenti, a eccezione di quelli presupposti al riconoscimento dei benefici previdenziali e assistenziali e limitatamente ai dati strettamente indispensabili, consente la comunicazione dei dati sensibili ad altri enti della pubblica amministrazione.
5 Con riguardo alla documentazione caratteristica, personale e matricolare, ne è prevista la compilazione, l'aggiornamento e la custodia con la trasmissione dei giudizi e la visione integrale da parte dell'interessato.
6 La documentazione caratteristica non reca al proprio interno dati idonei a rivelare lo stato di salute del valutato, ove non strettamente indispensabile.
7 Nell'ambito della documentazione matricolare del personale militare, nei fascicoli personali del personale civile e nella cartella personale per il personale militare sono contenuti dati sanitari, nonché dati riguardanti procedimenti o provvedimenti giudiziari e disciplinari; nei fascicoli personali per il personale civile, possono inoltre essere contenuti dati riguardanti le convinzioni politiche o sindacali in relazione all'applicazione di istituti previsti dalla disciplina di rango legislativo e regolamentare dei rapporti di lavoro.

Art. 1057 Gestione del rapporto di impiego o di servizio del personale militare e del rapporto di lavoro del personale civile

1. In relazione alla rilevante finalità di interesse pubblico della gestione del rapporto di impiego o di servizio, ai sensi dell'articolo 112 del decreto n. 196, il trattamento dei dati sensibili e giudiziari nella specifica materia, con riguardo al personale militare, avviene nell'ambito dei seguenti procedimenti e attività:
   a) il collocamento in aspettativa per motivi sanitari e per motivi privati;
   b) la perdita del grado e reintegrazione nel grado;
   c) la cessazione dal servizio;
   d) la promozione al grado superiore per ufficiali, sottufficiali, graduati e militari di truppa;
   e) l'iscrizione nel ruolo d'onore;
   f) il collocamento in congedo per permanente inabilità al servizio militare incondizionato;
   g) la revoca del provvedimento di riforma;
   h) la rideterminazione delle anzianità nel ruolo e di grado;
   i) il transito di ruolo;
   j) il transito nei ruoli del personale civile per accertata permanente inidoneità fisica al servizio militare;
   k) la cessazione dal servizio d'autorità;
   l) la formazione delle aliquote di avanzamento;
   m) l'esclusione dall'aliquota di avanzamento, sospensione della valutazione, cancellazione dal quadro di avanzamento per mancanza di requisiti;
   n) le rettifiche della decorrenza delle promozioni;
   o) il transito dall'ausiliaria nella riserva;

p) le dimissioni e i proscioglimenti dalla ferma ufficiali, sottufficiali, graduati, militari di truppa, compresi gli allievi delle scuole e degli istituti delle Forze armate;

q) i richiami in servizio e la cessazione dagli stessi;

r) le procedure concorsuali per avanzamento;

s) la riammissione in servizio;

t) le procedure selettive interne diverse dall'accesso iniziale nell'Amministrazione militare e per assunzione di incarichi in particolari specialità.

2. In relazione alla rilevante finalità di interesse pubblico della gestione del rapporto di lavoro, ai sensi dell'articolo 112 del decreto n. 196, il trattamento dei dati sensibili e giudiziari nella specifica materia, con riguardo al personale civile della Difesa, avviene nell'ambito dei seguenti procedimenti e attività:

a) le procedure di riqualificazione del personale appartenente alle aree funzionali;

b) il conferimento di incarichi dirigenziali, l'assunzione personale delle aree funzionali.

3. Il trattamento dei dati sensibili e giudiziari è effettuato ai sensi dei libri IV e V del codice e della normativa sull'assunzione e il rapporto di lavoro del personale civile.
4. I tipi di dati trattati in relazione a quanto indicato nei commi 1 e 2 sono i seguenti:
   a) a) stato di salute:

      1) patologie attuali;

      2) patologie pregresse;

      3) terapie in corso;

      4) anamnesi familiare;

   b) b) dati di carattere giudiziario.

5. Le particolari forme di elaborazione dei dati, per le finalità di seguito indicate, sono le seguenti:
   1) comunicazione agli enti internazionali presso i quali il personale militare presta servizio, anche mediante trasferimento dei dati all'estero, ai sensi dell'articolo 43 del decreto n. 196, ai fini della necessaria notifica di atti incidenti sullo stato giuridico e sull'avanzamento dell'interessato;
   2) comunicazione all'Ufficio centrale del bilancio presso il Ministero della difesa e Corte dei conti, con riguardo alla registrazione dei decreti che incidono sullo stato giuridico del personale legati a ragioni di carattere sanitario o giudiziario; la comunicazione di dati sensibili e giudiziari all'esterno è prevista con esclusivo riguardo alla fase del controllo e del perfezionamento degli atti;

3) comunicazione al Ministero delle infrastrutture e dei trasporti, limitatamente alla gestione del rapporto di lavoro relativo al personale del Corpo delle capitanerie di porto;
4) comunicazione ai dicasteri presso i quali transiti il personale volontario in ferma, ai fini della corretta gestione del rapporto di lavoro.

Art. 1058 Impiego del personale

1. In relazione alla rilevante finalità di interesse pubblico di gestione del rapporto di impiego o di servizio, ai sensi dell'articolo 112 del decreto n. 196, il trattamento dei dati sensibili e giudiziari, in materia di impiego del personale militare, avviene nell'ambito dei seguenti procedimenti e attività:

a) pianificazione pluriennale dell'impiego;
b) ordini di trasferimento per la dislocazione delle risorse umane sul territorio nazionale e all'estero;
c) trasferimenti di sede a domanda;
d) ammissione: revoca, anticipazione e rinvio frequenza corsi obbligatori e non obbligatori;
e) impiego conseguente a qualificazione, dequalificazione e abilitazioni varie;
f) trasferimento a domanda ai sensi della legge 5 febbraio 1992, n. 104;
g) trasferimenti per mandati politici rappresentativi;
h) assegnazioni temporanee;
i) rilascio passaporto di servizio e rilascio tessere personali di riconoscimento;
j) nomine ad alte cariche militari;
k) transito categoria/specialità dei sottufficiali;
l) ammissione dei sottufficiali ai corsi per aerosoccorritori ed eventuali altri corsi;
m) assegnazione a domanda di accompagnatori di grandi invalidi;
n) attribuzione, revoca ovvero cambio di categoria ovvero incarico;
o) selezione personale da avviare all'estero in posti interforze e multinazionali;
p) esonero da specializzazioni, qualificazioni o abilitazioni varie;
q) trasferimenti temporanei;
r) assegnazione, proroga e revoca alloggi di servizio.

2. In relazione alla rilevante finalità di interesse pubblico di gestione del rapporto di lavoro, ai sensi dell'articolo 112 del decreto n. 196, il trattamento dei dati sensibili e giudiziari, in materia di impiego del personale civile della Difesa, avviene nell'ambito dei seguenti procedimenti e attività:

a) trasferimenti, comandi, fuori ruolo;

b) passaggio diretto di personale tra amministrazioni diverse;

c) riconversione professionale;

d) mutamento di mansioni per inidoneità psico-fisica;

e) rilascio del passaporto di servizio.

3. Il trattamento dei dati sensibili e giudiziari è effettuato ai sensi dei libri IV e V del codice e della normativa sul rapporto di lavoro del personale civile.

4. I tipi di dati trattati in relazione a quanto indicato nei commi 1 e 2 sono i seguenti:

a) stato di salute:

1) patologie attuali;

2) patologie pregresse;

3) terapie in corso;

4) anamnesi familiare;

b) dati di carattere giudiziario.

5. Le particolari forme di elaborazione dei dati, per le finalità di seguito indicate, sono le seguenti:

a) comunicazione alle amministrazioni di destinazione del personale in posizione di comando.

6. In caso di dislocazione di equipaggi militari marittimi o aeronautici o di reparti o di contingenti multinazionali interforze all'estero in Paesi terzi per operazioni o esercitazioni militari, viene posto in essere il trasferimento dei relativi dati ai sensi dell'articolo 43 del decreto n. 196.

Art. 1059 Assenze per motivi di salute e di famiglia

1. In relazione alla rilevante finalità di interesse pubblico della gestione del rapporto di impiego, di servizio o di lavoro, ai sensi dell'art. 112 del decreto n. 196, il trattamento dei dati sensibili in materia di assenze per motivi di salute e di famiglia, con riguardo al personale militare e civile della Difesa, avviene nell'ambito dei seguenti procedimenti, attività ed eventi:

a) assenze per malattia;

b) licenza straordinaria di convalescenza e aspettative per motivi di salute;

c) ricovero;

d) tutela dei dipendenti in particolari condizioni psico-fisiche (tossicodipendenza e alcoolismo);

e) tutela dei dipendenti portatori di handicap;

f) congedi per maternità e paternità;

g) congedi parentali;

h) congedi e i permessi per l'assistenza a portatori di handicap;

i) congedi per eventi e cause particolari;

j) aspettativa per motivi privati;

k) licenze straordinarie e permessi per gravi motivi di famiglia e per esigenze personali.

2. Il trattamento dei dati sensibili è effettuato ai sensi dei libri IV e V del codice e della normativa sul rapporto di lavoro del personale civile.

3. I tipi di dati trattati in relazione a quanto indicato nel comma 1 sono i seguenti:

a) stato di salute:

1) patologie attuali;

2) patologie pregresse;

3) terapie in corso;

4) anamnesi familiare;

b) dati di carattere giudiziario.

4. Le particolari forme di elaborazione dei dati, per le finalità di seguito indicate, sono le seguenti:

a) comunicazione alle aziende sanitarie locali per l'accertamento dei requisiti di legge.

5. I dati pervengono agli uffici competenti in materia di gestione del personale, su iniziativa del dipendente, ovvero dietro richiesta dell'Amministrazione e sono custoditi in forma cartacea nel fascicolo personale.

6. Su richiesta dell'interessato possono essere raccolti anche dati relativi ai propri familiari, ai fini dell'applicazione di istituti previsti dalla disciplina normativa dei rapporti di lavoro, nonché per lo svolgimento del rapporto di impiego fra l'interessato e l'Amministrazione della difesa.

c) 6-bis. I dati relativi alla diagnosi apposta sul certificato medico del personale militare possono essere utilizzati dal competente organo della sanità militare per le finalità dirette ad accertare la persistenza dell'idoneità psico-fisica ad attività istituzionali connesse alla detenzione o all'uso delle armi, ovvero comunque connotate da rischio o controindicazioni all'impiego e, in caso di accertata inidoneità, comunicati alle Commissioni mediche per l'adozione dei provvedimenti conseguenti. Vengono comunicati al superiore diretto, invece, solo i dati riguardanti l'inidoneità privi di elementi riguardanti la diagnosi. Le disposizioni del presente comma si applicano anche al Corpo della Guardia di finanza.

Art. 1060 Sicurezza e igiene sul lavoro e attività medico legale per i dipendenti

1. In relazione alle rilevanti finalità di interesse pubblico della gestione del rapporto di impiego, di servizio o di lavoro e dell'applicazione della normativa in materia di igiene e sicurezza nei luoghi di lavoro, ai sensi degli articoli 85 e 112 del decreto n. 196, il trattamento dei dati sensibili e giudiziari, in materia di sicurezza e igiene sul lavoro e attività medico legali della Difesa per i dipendenti, avviene nell'ambito dei seguenti procedimenti, attività ed eventi:

a) pratiche sanitarie relative alla concessione di cure termali, idropiniche, inalatorie;

b) infortuni sul lavoro;

c) accertamento malattie professionali personale civile;

d) riconoscimento lesioni o infermità dipendenti da causa di servizio;

e) equo indennizzo;

f) vaccinazione personale militare e civile;

g) tenuta cartella sanitaria personale militare e civile;

h) accertamento del possesso dei requisiti qualificanti per l'accesso a specifici impieghi;

i) verifica requisiti previsti in materia di sicurezza nell'ambiente di lavoro; l) verifiche fattori di rischio;

m) sorveglianza sanitaria di medicina del lavoro;

n) infortuni extra-lavorativi;

o) collocamento in aspettativa;

p) indennità speciale una tantum per le Forze di polizia;

q) attività di profilassi individuale e di reparto o di equipaggio;

r) aspetti sanitari di radio protezionistica;

s) comunicazioni e notifiche di assenze per malattie/lesioni gravi comportanti il collocamento in aspettativa;

t) inabilità permanente, ovvero morte del personale.

2. Il trattamento dei dati sensibili è effettuato ai sensi delle seguenti norme primarie:

a) legge 30 aprile 1962, n. 283;

b) decreto del Presidente della Repubblica 30 giugno 1965, n. 1124;

c) legge 11 luglio 1980, n. 312;

d) decreto legislativo 9 aprile 2008, n. 81;

e) decreto legislativo 17 marzo 1995, n. 230;

f) decreto legislativo 26 maggio 2000, n. 241;

g) legge 24 ottobre 2000, n. 323;

h) decreto-legge 29 dicembre 2000, n. 393, convertito, con modificazioni, dalla legge 28 febbraio 2001, n. 27;

i) legge 16 gennaio 2003, n. 3;

j) decreto legislativo 6 novembre 2007, n. 193.

3. I tipi di dati trattati in relazioni a quanto indicato nel comma 1 sono i seguenti:

d) a) stato di salute:

1) patologie attuali;

2) patologie pregresse;

3) terapie in corso;

4) anamnesi familiare;

b) dati di carattere giudiziario.

4. Le particolari forme di elaborazione dei dati, per le finalità di seguito indicate, sono le seguenti:

a) comunicazione al Comitato di verifica presso il Ministero dell'economia e delle finanze, per il previsto parere in materia di cause di servizio e di equo indennizzo;

b) comunicazione all'Autorità di pubblica sicurezza e, per il solo personale civile, all'Istituto nazionale di assicurazione per gli infortuni sul lavoro e all'organo di vigilanza presso le aziende sanitarie locali, per gli infortuni sul lavoro;

c) comunicazione all'Istituto superiore per la prevenzione e la sicurezza sul lavoro e all'organo di vigilanza presso le aziende sanitarie locali, ai fini della trasmissione della cartella sanitaria dei lavoratori sottoposti a sorveglianza sanitaria;

d) comunicazione agli enti internazionali presso i quali il personale militare presta servizio, con conseguente trasferimento dei dati all'estero, ai sensi dell'articolo 43 del decreto n. 196, ai fini della necessaria notifica di atti afferenti alla corretta gestione del rapporto di lavoro.

5. La raccolta dei dati sensibili avviene presso l'interessato e presso le strutture sanitarie, a cura del personale sanitario, in relazione ai procedimenti avviati a iniziativa di parte o d'ufficio.

6. La trattazione e la comunicazione dei dati sensibili concernenti lo stato di salute sono attuate dagli uffici periferici e centrali competenti alla trattazione delle varie fasi del procedimento.

Art. 1061 Monitoraggio e ricerca scientifica

2. In relazione alle rilevanti finalità di interesse pubblico della gestione del rapporto di impiego, di servizio o di lavoro, dei compiti del Servizio sanitario nazionale e degli scopi scientifici, ai sensi degli articoli 85, 98 e 112 del decreto n. 196, il trattamento dei dati sensibili in materia di ricerca scientifica e monitoraggio sanitario del personale militare e civile della Difesa impiegato in missioni internazionali avviene ai sensi del presente articolo.

3. Il trattamento dei dati sensibili è effettuato ai sensi del decreto-legge 29 dicembre 2000, n. 393, convertito, con modificazioni, dalla legge 28 febbraio 2001, n. 27 e del decreto-legge 20 gennaio 2004, n. 9, convertito, con modificazioni, dalla legge 12 marzo 2004, n. 68.

4. I tipi di dati trattati in relazione a quanto indicato nel comma 1 sono i seguenti:

a) stato di salute:

1) patologie attuali;

2) patologie pregresse;

3) terapie in corso;

4) anamnesi familiare.

5. Le particolari forme di elaborazione dei dati, per le finalità di seguito indicate, sono le seguenti:

a) comunicazione dei dati sanitari del personale impiegato in missioni internazionali agli organi preposti dalla normativa di settore a svolgere l'attività di ricerca scientifica e di monitoraggio.

6. L'adesione alle campagne di monitoraggio è volontaria in ogni sua fase e a tale scopo, in occasione di ciascuna visita medica l'interessato rilascia apposita dichiarazione di voler aderire alla campagna di monitoraggio.

7. Il monitoraggio consiste in una serie di visite mediche e di accertamenti di laboratorio che possono anche essere svolti oltre che dalle strutture sanitarie militari in territorio nazionale e all'estero, anche dalle strutture sanitarie del Servizio sanitario nazionale, secondo le procedure previste dalla normativa di settore.

8. La raccolta dei dati sensibili avviene presso l'interessato e presso le strutture sanitarie a cura del personale sanitario.

9. Il trattamento dei dati personali di carattere sanitario avviene esclusivamente nel caso in cui l'utilizzo di informazioni personali sulla salute delle persone interessate sia ritenuto indispensabile per svolgere l'attività di monitoraggio e la ricerca scientifica prevista dalla legge, non essendo sufficiente l'utilizzo di dati anonimi o di dati personali di natura diversa.

10. Le modalità di esecuzione del monitoraggio avvengono comunque nel rispetto dei limiti e secondo le modalità indicate dalle leggi di riferimento e dei relativi regolamenti di attuazione.

Art. 1062 Assistenza sanitaria in favore dei dipendenti e dei terzi

1 In relazione alla rilevante finalità di interesse pubblico connessa con i compiti degli organismi sanitari pubblici, ai sensi dell'articolo 85 del decreto n. 196, il trattamento dei dati sensibili e giudiziari, in materia di assistenza sanitaria della Difesa in favore dei dipendenti e dei terzi, avviene nell'ambito dei seguenti procedimenti, attività ed eventi:

a) soccorso e assistenza sanitaria di emergenza;

b) assistenza specialistica ambulatoriale e di riabilitazione;

c) attività immuno-trasfusionale;

d) ricovero ospedaliero;

e) attività autoptica;

f) tenuta cartella sanitaria;

g) infortuni extra-lavorativi;

h) attività di profilassi individuale e collettiva;

i)aspetti sanitari di radio protezionistica;

j) denuncia di malattie infettive.

2 Il trattamento dei dati sensibili e giudiziari è effettuato ai sensi delle seguenti norme di legge:

a) regio decreto 27 luglio 1934, n. 1265;

b) decreto del Presidente della Repubblica 27 marzo 1969, n. 128;

c) legge 26 luglio 1975, n. 354;

d) legge 23 dicembre 1978, n. 833;

e) legge 13 maggio 1978, n. 180;

f) decreto legislativo 6 settembre 1989, n. 322;

g) legge 4 maggio 1990, n. 107;

h) decreto del Presidente della Repubblica 10 settembre 1990, n. 285;

i) legge 25 febbraio 1992, n. 210;

l) decreto legislativo 30 dicembre 1992, n. 502;

m) legge 29 dicembre 1993, n. 578;

n) decreto legislativo 17 marzo 1995, n. 230;

o) legge 3 aprile 2001, n. 120;

p) decreto-legge 18 settembre 2001, n. 347, convertito, con modificazioni dalla legge 16 novembre 2001, n. 405;

q) legge 21 ottobre 2005, n. 219.

3 I tipi di dati trattati in relazione a quanto indicato nel comma 1 sono i seguenti:

a) stato di salute:

1) patologie attuali;

2) patologie pregresse;

3) terapie in corso;

4) anamnesi familiare;

b) dati di carattere giudiziario.

4 Le particolari forme di elaborazione dei dati, per le finalità di seguito indicate, sono le seguenti:

a) comunicazione all'azienda sanitaria di residenza dell'interessato, nei casi previsti dalla normativa di settore;

b) comunicazione agli ospedali pubblici o privati per la ricerca posti letto, per trasferimenti del malato;

c) comunicazione all'autorità giudiziaria e alle Forze di polizia;

d) comunicazione al Ministero della salute e alla azienda sanitaria locale, per la denuncia di casi di malattie infettive e diffusive;

e) comunicazione ai centri di coordinamento regionale immuno-trasfusionali;

f) riscontro a esami commissionati da presidi ospedalieri e da unità operative di medicina generale;

g) comunicazione al comune ove è avvenuto il decesso;

h) comunicazione all'autorità giudiziaria, ove la comunicazione del decesso sia prevista da obblighi di legge.

5 In caso di soccorso e assistenza sanitaria di emergenza:

a) i dati afferenti allo stato di salute della persona soccorsa sono acquisiti dall'operatore al momento della richiesta di intervento e sono da questi comunicati agli operatori del mezzo di soccorso;

b) durante il trasporto sono riportate nella scheda di soccorso i dati anagrafici, l'anamnesi, ove possibile, e le operazioni di assistenza compiute; nel caso in cui il paziente abbia necessità di ricovero, viene trasportato presso l'ospedale più idoneo al trattamento della patologia;

c) presso l'ospedale militare il personale infermieristico procede all'accoglienza e alla compilazione della scheda di TRIAGE con la relativa assegnazione del codice colore di priorità di accesso agli ambulatori; il medico di pronto soccorso completa il dato di TRIAGE con i dati clinico-anamnestici di pertinenza medica, i quali vengono trasmessi ad altro personale medico per consentire gli ulteriori accertamenti urgenti, ovvero per l'eventuale trasferimento in regime di ricovero presso altra struttura ospedaliera. In caso di dimissione dal pronto soccorso, il personale sanitario addetto procede all'archiviazione della pratica, dopo aver consegnato la copia integrale dei documenti all'utente.

6 In caso di assistenza specialistica ambulatoriale e di riabilitazione:

a) il trattamento dei dati è correlato all'erogazione in regime ambulatoriale di prestazioni specialistiche, di diagnostica strumentale e di laboratorio, di riabilitazione;

b) la prescrizione può essere effettuata dal medico militare, presso il comando o ente d'appartenenza dell'interessato, dal medico di medicina generale o da altro medico del servizio sanitario regionale ed è utilizzata dal paziente ai fini della prenotazione della prestazione presso la struttura sanitaria militare;

c) il referto delle prestazioni di diagnostica strumentale e di laboratorio è conservato in forma cartacea e informatica;

d) i dati relativi all'anamnesi familiare sono raccolti presso l'interessato solamente quando ciò sia strettamente indispensabile per la diagnosi e la cura della salute;

e) con riguardo alla riabilitazione i dati sensibili concernono lo stato di salute e di autonomia del soggetto, con le indicazioni del quadro riabilitativo e assistenziale ritenuto necessario.

7 In caso di attività immuno-trasfusionale:

a) i dati riguardano donatori, sacche e riceventi, per garantire la tracciabilità di ogni unità di emocomponenti; i dati relativi al donatore contenuti nella scheda di cui al decreto del Ministro della salute 3 marzo 2005, pubblicato nella Gazzetta Ufficiale del 13 aprile 2005, n. 85, sono trattati nell'ambito del processo di selezione del donatore a cura della struttura trasfusionale che ne cura la conservazione;

b) le unità di sangue e di emocomponenti vengono raccolti in sacche etichettate conformemente al decreto del Ministro della sanità 25 gennaio 2001, pubblicato nella Gazzetta Ufficiale del 3 aprile 2001, n. 78, le quali, in particolare, recano il numero identificativo della donazione attraverso il quale è possibile risalire al donatore, ove ciò risulti necessario;

c) i dati relativi al ricevente sono trattati e conservati sia dalla struttura di immuno-ematologia e trasfusionale, sia dalla struttura di degenza presso la quale il paziente è sottoposto al trattamento trasfusionale.

8 In caso di ricovero ospedaliero:

a) il trattamento dei dati riguarda le attività collegate alle attività di ricovero ospedaliero che può avvenire sia in modo programmato, sia in urgenza. Nell'ambito dell'attività di ricovero ospedaliero il trattamento dei dati è conciato alle seguenti attività:

1 cartelle cliniche di ricovero;

2 diari clinici relativi ai ricoverati;

3 registri nosologici;

4 registri delle prenotazioni;

5 schede di dimissione;

6 relazione clinica di dimissione diretta al medico di famiglia;

7 archivi di attività diagnostiche e terapeutiche;

8 registri di sala operatoria;

9 registri delle trasfusioni;

10 registri dei decessi, delle autopsie e delle certificazioni di morte;

11 attività amministrativo contabili: registro della lamentele degli utenti;

b) lo stesso può dar luogo al trattamento dei dati giudiziari quando questo riguardi cittadini detenuti o internati;

c) in caso di decesso presso la struttura ospedaliera militare si eseguono attività certificatorie finalizzate alla autorizzazione alla sepoltura o alla cremazione;

d) l'attività autoptica viene svolta solamente per gli accertamenti diagnostici in caso di decesso in cui sussistono dubbi sulla causa della morte;

e) l'ospedale militare redige le schede di morte con finalità epidemiologica e statistica;

f) la raccolta dei dati sensibili avviene presso l'interessato e presso le strutture sanitarie pubbliche e private dai quali viene trasferito il malato.

Art. 1063 Attività medico legale in favore di terzi

1. In relazione alla rilevante finalità di interesse pubblico connessa con i compiti degli organismi sanitari pubblici, ai sensi dell'articolo 85 del decreto n. 196, il trattamento dei dati sensibili e giudiziari, in materia di attività medico legali della Difesa in favore dei terzi, avviene nell'ambito dei seguenti procedimenti, attività ed eventi:

a) attività medico-legale in favore di soggetti estranei all'Amministrazione, al fine del rilascio di abilitazioni, licenze, attestati aeronautici, ovvero per il riconoscimento di benefici pensionistici, assistenziali;

b) risarcimento danni da emotrasfusione;

c) attività medico-legale in sede giurisdizionale e giustiziale, su richiesta dell'autorità giudiziaria, dell'avvocatura dello Stato e di tutte le Amministrazioni dello Stato; soccorso e assistenza sanitaria di emergenza.

2. Il trattamento dei dati sensibili e giudiziari è effettuato ai sensi delle seguenti norme primarie:

a) legge 11 marzo 1926, n. 416;

b) legge 23 dicembre 1978, n. 833;

c) legge 22 dicembre 1980, n. 913;

d) decreto del Presidente della Repubblica 9 ottobre 1990, n. 309;

e) legge 8 agosto 1995, n. 335;

f) legge 21 ottobre 2005, n. 219.

3. I tipi di dati trattati in relazione a quanto indicato nel comma 1 sono i seguenti:

a) stato di salute:

1) patologie attuali;

2) patologie pregresse;

3) terapie in corso;

4) anamnesi familiare;

b) dati di carattere giudiziario.

4. Le particolari forme di elaborazione dei dati, per le finalità di seguito indicate, sono le seguenti:

a) comunicazione al datore di lavoro privato o pubblica amministrazione dell'interessato sottoposto all'accertamento della idoneità a svolgere le specifiche mansioni, limitatamente al giudizio d'idoneità;

b) comunicazione al datore di lavoro dell'interessato al fine del riconoscimento di benefici pensionistici;

c) comunicazione agli ospedali pubblici o privati per la ricerca posti letto, per trasferimenti del malato;

d) comunicazione alla Motorizzazione civile per il rilascio e il rinnovo della patente di guida civile;

e) comunicazione alle prefetture-uffici territoriali del Governo e questure, per finalità connesse al rilascio del porto d'armi limitatamente al giudizio di idoneità;

f) comunicazione ai Servizi di assistenza sanitaria naviganti (SASN);

g) comunicazione all'Istituto nazionale per la previdenza sociale, ai fini previdenziali.

5. La raccolta dei dati avviene presso l'interessato o presso il datore di lavoro con riguardo alla documentazione strettamente necessaria all'espletamento dell'attività medico-legale richiesta; la suddetta raccolta avviene presso le strutture sanitarie e a cura di personale sanitario.

6. Il dato viene archiviato presso la struttura sanitaria secondo le disposizioni di sicurezza dettate dalla normativa vigente.

7. Le amministrazioni pubbliche o private possono richiedere alle strutture sanitarie militari pareri e consulenze medico-legali in materia di dipendenza da causa di servizio, benefici accessori e ogni altro indennizzo previsto da istituti normativi che contemplano la competenza

di accertamento presso organi sanitari del Ministero della difesa; tali organi effettuato l'accertamento sanitario delle condizioni psico-fisiche dell'interessato nell'ambito delle loro competenze e predispongono il parere o la consulenza medico-legale da comunicare all'Amministrazione richiedente.

8. La struttura sanitaria militare trasmette alla Motorizzazione civile il certificato di idoneità, recante l'eventuale obbligo di protesi correttive per la vista e l'udito, ai fini del rilascio o del rinnovo delle patenti per la conduzione di veicoli; analoga comunicazione viene effettuata alle competenti questure e prefetture-uffici territoriali del Governo per la licenza del porto d'armi.

9. Gli organi sanitari dell'Aeronautica militare effettuano, ai sensi della normativa vigente, visite mediche di accertamento dell'idoneità psico-fisica dei titolari di licenza o attestati aeronautici civili; le visite riguardano privati cittadini, dipendenti di compagnie commerciali, nonché personale di altre amministrazioni, ivi incluse le Forze di polizia e i Corpi armati dello Stato. I dati sanitari raccolti sono esclusivamente quelli strettamente indispensabili alla formulazione dei giudizi di idoneità ovvero inidoneità psico-fisica; tali giudizi sono comunicati al datore di lavoro privato o pubblico, nonché agli organi dell'aviazione civile e ai servizi di assistenza sanitaria ai naviganti.

Art. 1064 Disciplina

1. In relazione alla rilevante finalità di interesse pubblico di gestione del rapporto di impiego o di servizio, ai sensi dell'articolo 112 del decreto n. 196, il trattamento dei dati sensibili e giudiziari, in materia di disciplina del personale militare, avviene nell'ambito dei seguenti procedimenti e attività:

a) procedimento disciplinare per l'irrogazione di una sanzione disciplinare di corpo;
b) cessazione degli effetti delle sanzioni disciplinari di corpo;
c) controllo di legittimità in materia di sanzioni disciplinari di corpo;
d) esame di provvedimenti giurisdizionale a fini disciplinari;
e) procedimenti per l'applicazione delle sanzioni disciplinari di stato;
f) reintegrazione nel grado a seguito di perdita del grado quale sanzione di stato;
g) applicazione, cessazione degli effetti e revoca di misure disciplinari precauzionali;
h) trattazione delle istanze per conferire con le autorità centrali e periferiche;
i) comunicazione al prefetto dei casi di tossicodipendenza.

2. In relazione alla rilevante finalità di interesse pubblico di gestione del rapporto di lavoro, ai sensi dell'articolo 112 del decreto n. 196, il trattamento dei dati sensibili e giudiziari, in materia di disciplina del personale civile della Difesa, avviene esclusivamente nell'ambito dei procedimenti disciplinari.

3. Il trattamento dei dati sensibili e giudiziari è effettuato ai sensi dei libri IV e V del codice e della normativa sul rapporto di lavoro del personale civile.

4. I tipi di dati trattati in relazioni a quanto indicato nei commi 1 e 2 sono i seguenti:

a) stato di salute:
   1) patologie attuali;
   2) patologie pregresse;
   3) terapie in corso;

c) dati di carattere giudiziario.

5. Le particolari forme di elaborazione dei dati, per le finalità di seguito indicate, sono le seguenti:

a) comunicazione al Prefetto ai fini dell'applicazione delle sanzioni amministrative previste dall'articolo 75, del decreto del Presidente della Repubblica 9 ottobre 1990, n. 309, in materia di tossicodipendenza;
b) comunicazione prevista dall' articolo 929 del codice di sottoporsi agli accertamenti sanitari.

Art. 1065 Ispezioni, inchieste e responsabilità civile, amministrativa e contabile

1. In relazione alle rilevanti finalità di interesse pubblico di gestione del rapporto di impiego, di servizio o di lavoro e di controllo e ispettive, ai sensi degli articoli 67 e 112 del decreto n. 196, il trattamento dei dati sensibili e giudiziari, in materia di ispezioni, inchieste e responsabilità civile amministrativa e contabile del personale militare e civile della Difesa, avviene nell'ambito dei seguenti procedimenti e attività:

a) inchieste volte all'accertamento di responsabilità amministrativa, contabile e civile;
b) inchieste sommarie e formali su gravi incidenti, inclusi quelli di volo;
c) denunce di reato e di danno erariale;

d) attività ispettiva volta all'accertamento della legittimità, dell'imparzialità, dell'efficienza e dell'efficacia dell'azione amministrativa;
e) recupero danno erariale;
f) riscossione dei crediti liquidati dalla Corte dei conti con sentenza o ordinanza esecutiva;
g) evasione di istanze ed esposti vari.

2. Il trattamento dei dati sensibili e giudiziari è effettuato ai sensi della vigente normativa di legge in materia di controlli e di responsabilità civile, amministrativa e contabile.

3. I tipi di dati trattati in relazioni a quanto indicato nel comma 1 sono i seguenti:
   a) stato di salute:
      1) patologie attuali;
      2) patologie pregresse;
      3) terapie in corso;
      4) anamnesi familiari;
   b) dati di carattere giudiziario.

4. Le particolari forme di elaborazione dei dati, per le finalità di seguito indicate, sono le seguenti:
   a) comunicazione alla Corte dei conti per responsabilità amministrativa e contabile;
   b) comunicazione alle altre autorità giudiziarie, con riguardo a notizie rilevanti sotto il profilo giudiziario, emerse nel corso delle indagini.

5. La commissione di inchiesta o l'ufficiale inquirente, nominati al fine di accertare possibili responsabilità di carattere amministrativo, contabile o civile, possono trattare nello svolgimento delle indagini dati giudiziari e sensibili delle persone coinvolte negli accertamenti, nei limiti in cui ciò risulti indispensabile all'espletamento delle attività ispettive; tali dati possono essere ricompresi:
   a) nella denuncia alla procura generale della Corte dei conti;
   b) nella successiva comunicazione dell'esito dell'inchiesta alla medesima Corte dei conti;
   c) nelle eventuali risultanze disciplinari o penali che fungono da presupposto dell'azione ispettiva.

6. La commissione di investigazione per gli incidenti di volo trasmette i risultati dell'indagine, che può comprendere dati afferenti lo stato di salute, nonché dati giudiziari, all'alto comando da cui dipende il velivolo; quest'ultimo invia la documentazione alle autorità competenti per l'eventuale denuncia alla Corte dei conti.

7. L'ufficiale inquirente, per le inchieste sommarie, e la commissione d'inchiesta, per le inchieste formali, comunicano gli esiti delle indagini all'autorità che ha disposto l'inchiesta e provvedono alle comunicazioni alle autorità giudiziarie competenti, secondo la normativa vigente, ove emergano danni erariali o commissione di reati.

Art. 1066 Rimborso delle spese legali

1. In relazione alla rilevante finalità di interesse pubblico di gestione del rapporto di impiego o di servizio, ai sensi dell'articolo 112 del decreto n. 196, il trattamento dei dati giudiziari, in materia di rimborso delle spese legali per il personale militare, avviene nell'ambito dei seguenti procedimenti e attività:

a) istruttoria dell'istanza di rimborso di spese legali;
b) valutazione dei pareri gerarchici e della connessione dei fatti con il servizio od obblighi istituzionali;
c) pagamento delle spese legali e di giudizio a seguito di conforme giudizio di congruità dell'Avvocatura generale dello Stato;
d) trattazione delle istanze di gratuito patrocinio;
e) istruttoria delle istanze di anticipo spese legali;
f) valutazione di pareri gerarchici;
g) valutazione rispondenza dei fatti ai requisiti previsti dalla normativa specifica;
h) pagamento delle somme di rimborso in anticipo.

2. In relazione alla rilevante finalità di interesse pubblico di gestione del rapporto di impiego o di servizio, ai sensi dell'articolo 112 del decreto n. 196, il trattamento dei dati giudiziari, in materia di rimborso delle spese legali per il personale civile della Difesa, avviene nell'ambito dei seguenti procedimenti e attività:

a) liquidazione spese di giudizio;
b) liquidazione somme spettanti per rivalutazione e interessi moratori.

3. Il trattamento dei dati giudiziari è effettuato ai sensi dei libri IV, V e VI del codice, della normativa sul rapporto di lavoro del personale civile e di quella processuale vigente.

4. Le particolari forme di elaborazione dei dati, per le finalità di seguito indicate, sono le seguenti:

a) comunicazione all'Avvocatura generale dello Stato per l'acquisizione del prescritto parere di congruità;
b) comunicazione all'Ufficio centrale del bilancio presso il Ministero della difesa, ai fini del pagamento delle somme riconosciute all'interessato a titolo di rimborso.

5. Ai fini del corretto espletamento del procedimento di rimborso delle spese legali, vengono necessariamente in trattazione i dati giudiziari, e in particolare la sentenza di assoluzione del pubblico dipendente e il suo integrale contenuto.

6. I principali tipi di trattamento sono l'acquisizione e l'esame di atti giudiziari, la loro valutazione ai fini dell'accertamento della connessione diretta dei fatti contestati con il servizio e, in definitiva, della sussistenza del diritto al rimborso.

7. L'attività procedimentale comporta la comunicazione, archiviazione e, ove del caso, distruzione secondo modalità previste dalla normativa vigente.

Art. 1067 Ricompense, onorificenze e riconoscimenti

1. In relazione alla rilevante finalità di interesse pubblico di conferimento di onorificenze e ricompense, ai sensi dell'articolo 69 del decreto n. 196, il trattamento dei dati sensibili e giudiziari, in materia di ricompense, onorificenze e riconoscimenti, avviene nell'ambito dei seguenti procedimenti e attività:

a) concessione di ricompense, onorificenze, riconoscimenti e decorazioni;
b) formazione dell'Albo d'oro.

2. Il trattamento dei dati sensibili e giudiziari è effettuato ai sensi dei libri IV, V e VI del codice, e della normativa sulla concessione delle ricompense al valor civile e delle onorificenze dell'ordine al merito della Repubblica italiana.

3. I tipi di dati trattati in relazione a quanto indicato nel comma 1 sono i seguenti:
   a) stato di salute:
      1) patologie attuali;
      2) patologie pregresse;
      3) terapie in corso;
   b) dati di carattere giudiziario;
   c) convinzioni politiche, limitatamente agli eventi bellici del secondo conflitto mondiale.

4. Le particolari forme di elaborazione dei dati, per le finalità di seguito indicate, sono le seguenti:
   a) comunicazione al Ministero dell'interno per l'istruttoria delle pratiche relative alla concessione delle medaglie al valore o merito civile;
   b) comunicazione alla Giunta per le onorificenze dell'ordine al merito della Repubblica italiana istituita presso la Presidenza del Consiglio dei Ministri;
   c) comunicazione all'Ufficio centrale del bilancio, per le onorificenze e le decorazioni il cui conferimento comporta spese aggiuntive.

5. I dati necessari sono acquisiti presso l'interessato o presso i terzi esclusivamente allo scopo di verificare la sussistenza dei requisiti e dei presupposti per la concessione delle onorificenze, dei riconoscimenti, delle ricompense e delle decorazioni.

6. La trattazione delle pratiche relative ai militari caduti e dispersi in tempo di guerra e di grave crisi internazionale, ai fini della formazione dell'Albo d'oro, comporta il trattamento di dati sensibili indicati nel comma 2, nel rispetto del principio di stretta indispensabilità.

Art. 1068 Distacchi per assunzione di cariche politiche e sindacali

1. In relazione alla rilevante finalità di interesse pubblico di gestione del rapporto di impiego o di servizio, ai sensi dell'articolo 112 del decreto n. 196, il trattamento dei dati sensibili, in materia di distacchi per assunzione di cariche politiche del personale militare, avviene nell'ambito dei seguenti procedimenti e attività:
   a) collocamento in aspettativa senza assegni per militari eletti al Parlamento nazionale, quello europeo, nei Consigli regionali e degli enti territoriali;
   b) permessi e licenze per la partecipazione alle sedute dei Consigli di enti territoriali.

2. In relazione alla rilevante finalità di interesse pubblico di gestione del rapporto di lavoro, ai sensi dell'articolo 112 del decreto n. 196, il trattamento dei dati sensibili, in materia di distacchi per assunzione di cariche politiche e sindacali del personale civile della Difesa, avviene nell'ambito dei seguenti procedimenti e attività:

a) distacchi, aspettative, permessi sindacali;
b) aspettative e permessi per cariche pubbliche elettive;
c) aspettative e permessi per funzioni pubbliche.

3. Il trattamento dei dati sensibili è effettuato ai sensi dei libri IV e V del codice della normativa sul rapporto di lavoro del personale civile.

4. I tipi di dati trattati in relazioni a quanto indicato nei commi 1 e 2 sono i seguenti:

a) convinzioni:
   1) politiche;
   2) sindacali.

5. Le particolari forme di elaborazione dei dati, per le finalità di seguito indicate, sono le seguenti:

1) comunicazione alla Presidenza del Consiglio dei Ministri - Dipartimento della funzione pubblica ai sensi dell'articolo 50 del decreto legislativo 30 marzo 2001, n. 165;
2) comunicazione alle istituzioni rappresentative presso cui il personale svolge il proprio mandato rappresentativo.

6. I dati pervengono agli uffici competenti in materia di gestione del personale, su iniziativa del dipendente, ovvero previa richiesta dell'Amministrazione. Sono custoditi, in forma cartacea, nel fascicolo personale, nonché comunicati alla Presidenza del Consiglio dei Ministri - Dipartimento della funzione pubblica e alle istituzioni rappresentative presso le quali l'interessato espleta il proprio mandato.

7. La trattazione dei dati sindacali si riferisce esclusivamente al personale civile.

Art. 1069 Trattamento economico continuativo fisso ed eventuale del personale in attività di servizio

1. In relazione alla rilevante finalità di interesse pubblico di gestione del rapporto di impiego o di servizio, ai sensi dell'articolo 112 del decreto n. 196, il trattamento dei dati sensibili e giudiziari, in materia di trattamento economico continuativo fisso ed eventuale del personale militare in attività di servizio, avviene nell'ambito dei seguenti procedimenti e attività:
   a) decretazioni stipendiali ufficiali;
   b) determinazioni stipendiali sottufficiali e truppa in servizio permanente;
   c) determinazioni stipendiali in via provvisoria a ufficiali, sottufficiali, graduati e militari di truppa conseguenti a: nomine, promozioni, ricostruzioni di camera, attribuzione benefici convenzionali, disposizioni di legge, revoca sospensione dall'impiego, richiamo dall'ausiliaria o dalla riserva, decesso, collocamento ausiliaria, congedo assoluto, complemento o riserva;
   d) determinazione di attribuzione indennità operative e supplementari;
   e) individuazione categorie personale aventi titolo all'indennità di rischio;
   f) maggiorazione indennità operativa di base;
   g) autorizzazione alla proroga dell'indennità di aeronavigazione.

2. In relazione alla rilevante finalità di interesse pubblico di gestione del rapporto di lavoro, ai sensi dell'articolo 112 del decreto n. 196, il trattamento dei dati sensibili e giudiziari, in materia di trattamento economico continuativo fisso ed eventuale del personale civile della Difesa in attività di servizio, avviene nell'ambito dei seguenti procedimenti e attività:
   a) determinazioni stipendiali;
   b) liquidazione trattamenti economici fissi, accessori ed eventuali;
   c) ritenute quote associative per versamento organizzazioni sindacali;
   d) sospensione erogazione e corresponsione indennità alimentare;
   e) cessione del quinto;
   f) obblighi contributivi, invalidità vecchiaia superstiti;
   g) obblighi assicurativi;
   h) obblighi fiscali;
   i) rimborso spese di missione.

3. Il trattamento dei dati sensibili e giudiziari è effettuato ai sensi dei libri IV, V e VI del codice e della normativa sul rapporto di lavoro del personale civile.

4. I tipi di dati trattati in relazione a quanto indicato nei commi 1 e 2 sono i seguenti
   a) convinzioni:
      1) sindacali;
   b) stato di salute:
      1 patologie attuali;
      2 patologie pregresse;
      3 terapie in corso;
      4 anamnesi familiare;
   c) dati di carattere giudiziario.

5. Le particolari forme di elaborazione dei dati, per le finalità di seguito indicate, sono le seguenti:
   a) comunicazione all'Ufficio centrale del bilancio presso il Ministero della difesa e la Corte dei conti, con riguardo alla registrazione dei decreti attributivi di benefici economici connessi allo stato di salute;
   b) comunicazione all'Istituto nazionale di previdenza per i dipendenti delle amministrazioni pubbliche, ai fini dell'assolvimento agli obblighi contributivi;
   c) comunicazione all'Istituto nazionale per le assicurazioni contro gli infortuni sul lavoro, per gli obblighi assicurativi;
   d) comunicazione al Ministero dell'economia e delle finanze, ai fini dell'assolvimento degli obblighi fiscali nonché della gestione del trattamento economico del personale civile.

6. L'elaborazione dei dati relativi allo stato di salute e di carattere giudiziario e il relativo flusso riguardano esclusivamente profili che incidono sulla retribuzione economica dell'interessato e vengono gestiti, con modalità informatiche protette e nel rispetto del principio dell'indispensabilità, dagli enti dell'amministrazione della Difesa dell'area tecnico amministrativa e tecnico-operativa preposti alla gestione stipendiale del personale.

7. È prevista, per il solo personale civile, la comunicazione al sistema informatico del Ministero dell'economia e delle finanze dei dati riguardanti le ritenute delle quote associative, per il versamento alle organizzazioni sindacali.

Art. 1070 Trattamento economico di quiescenza ordinario e privilegiato

1. In relazione alle rilevanti finalità di interesse pubblico di gestione del rapporto di impiego o di servizio e di concessione di benefici economici e abilitazioni, ai sensi degli articoli 68 e 112 del decreto n. 196, il trattamento dei dati sensibili e giudiziari, in materia di trattamento economico di quiescenza ordinario e privilegiato del personale militare, avviene nell'ambito dei seguenti procedimenti e attività:

a) liquidazione pensioni normali dirette del personale militare, a seguito di cessazione dal servizio per raggiunti limiti di età, infermità, dimissioni;
b) riliquidazione dei trattamenti pensionistici;
c) liquidazione e riliquidazione della speciale elargizione;
d) liquidazione assegno vitalizio e speciale assegno vitalizio;
e) liquidazione indennizzo privilegiato aeronautico;
f) liquidazione indennità una tantum per paraplegici;
g) riconoscimento dipendenza da causa di servizio del personale in congedo;
h) accertamenti relativi all'ascrivibilità a categoria di pensione delle infermità e richiesta di parere sulla dipendenza da causa di servizio;
i) pensioni di reversibilità;
l) provvidenze in favore di grandi invalidi;
m) assegno sostitutivo dell'accompagnatore.

2. In relazione alle rilevanti finalità di interesse pubblico di gestione del rapporto di lavoro e di concessione di benefici economici e abilitazioni, ai sensi degli articoli 68 e 112 del decreto n. 196, il trattamento dei dati sensibili e giudiziari, in materia di trattamento economico di quiescenza ordinario e privilegiato del personale civile della Difesa, avviene nell'ambito dei seguenti procedimenti e attività:

a) pensione privilegiata diretta e di reversibilità;
b) pensione di inabilità;
c) liquidazione speciale elargizione;

d) provvidenze a favore di cittadini deceduti o divenuti invalidi a causa di ordigni bellici in tempo di pace.

3. Il trattamento dei dati sensibili e giudiziari è effettuato ai sensi dei libri IV, V e VII del codice e della normativa sul trattamento di quiescenza e di fine rapporto del personale civile.

4. I tipi di dati trattati in relazione a quanto indicato nei commi 1 e 2 sono i seguenti:

a) stato di salute:
   1) patologie attuali;
   2) patologie pregresse;
   3) terapie in corso;
   4) anamnesi familiare;
b) dati di carattere giudiziario.

5. Le particolari forme di elaborazione dei dati, per le finalità di seguito indicate, sono le seguenti:

a) comunicazione agli enti previdenziali per l'erogazione del trattamento pensionistico;
b) comunicazione all'Ufficio centrale del bilancio presso il Ministero della difesa e la Corte dei conti, con riguardo alla registrazione dei decreti che dispongono l'erogazione del trattamento pensionistico e di altri riconoscimenti economici legati alle condizioni di salute degli interessati;
c) comunicazione al Comitato di verifica per le cause di servizio, per il previsto parere;
d) comunicazione alle aziende sanitarie locali per l'accertamento delle condizioni di incollocabilità;
e) comunicazione al Ministero dell'economia e delle finanze, per l'erogazione dell'assegno mensile sostitutivo dell'accompagnatore.

6. I dati sanitari e giudiziari, attinenti al trattamento pensionistico e ad altre provvidenze di carattere previdenziale concesse all'interessato o ai superstiti, sono acquisiti dagli uffici competenti presso l'interessato o presso gli altri soggetti pubblici coinvolti nel procedimento.

7. I dati che vengono comunicati all'ente previdenziale sono esclusivamente quelli indispensabili all'impianto e all'aggiornamento della pratica pensionistica.

8. Forme di trattamento mediante trasmissione all'esterno avvengono su richiesta del dipendente in caso di rideterminazione delle infermità o di impugnazione delle determinazioni medico-legali dell'organo medico-legale di secondo grado.

9. Relativamente al riconoscimento dell'assegno mensile sostitutivo dell'accompagnatore ai grandi invalidi, si procede alla trasmissione delle domande, complete della indispensabile documentazione, al Ministero dell'economia e delle finanze; al medesimo fine vengono comunicati al Ministero dell'economia e delle finanze gli elenchi nominativi:

a) dei grandi invalidi di guerra e per servizio, che alla data del 15 gennaio 2003 fruivano di un accompagnatore in servizio obbligatorio di leva o del servizio civile;
b) dei grandi invalidi che hanno perso l'accompagnatore entro il 30 aprile 2005;
c) dei grandi invalidi di guerra e per servizio che hanno fatto richiesta dell'accompagnatore almeno una volta nel triennio antecedente alla data di entrata in vigore della legge 27 dicembre 2002, n. 288 e ai quali gli enti preposti non sono stati in grado di assicurarlo.

Art. 1071 Provvidenze, assistenza e attività ricreative

1. In relazione alla rilevante finalità di interesse pubblico di gestione del rapporto di impiego o di servizio, ai sensi dell'articolo 112 del decreto n. 196, il trattamento dei dati sensibili, in materia di provvidenze, assistenza e attività ricreative per il personale militare, avviene nell'ambito dei seguenti procedimenti e attività:

a) concessione sussidi in denaro;
b) concessione borse di studio a favore dei figli disabili del personale;
c) rimborso soggiorno ai familiari dei militari deceduti, in pericolo di vita e in casi di particolare gravità;
d) concessione prestiti da parte delle Casse ufficiali e sottufficiali;
e) liquidazione indennità supplementare;
f) interventi assistenziali (sussidi) a favore del personale civile e militare per interventi di alta chirurgia o di particolare gravità;
g) malattie;
h) prestazioni sanitarie fruite all'estero;
i) applicazione di protesi.

2. In relazione alla rilevante finalità di interesse pubblico di gestione del rapporto di lavoro, ai sensi dell'articolo 112 del decreto n. 196, il trattamento dei dati sensibili, in materia di

provvidenze, assistenza e attività ricreative per il personale civile della Difesa, avviene nell'ambito dei seguenti procedimenti e attività:

a) concessione sussidi in denaro;
b) borse di studio;
c) rimborso spese di cura.

3. Il trattamento dei dati sensibili e giudiziari è effettuato ai sensi dei libri IV, V, VI e VII del codice e della normativa sul trattamento economico, di quiescenza e di fine rapporto del personale civile.

4. I tipi di dati trattati in relazioni a quanto indicato nei commi 1 e 2 sono i seguenti:
   a) stato di salute:
      1) patologie attuali;
      2) patologie pregresse;
      3) terapie in corso;
      4) anamnesi familiare.

5. Le particolari forme di elaborazione dei dati, per le finalità di seguito indicate, sono le seguenti:
   a) comunicazione all'Ufficio centrale del bilancio presso il Ministero della difesa, per il controllo di legittimità dei provvedimenti con cui sono erogate le somme in favore del personale.

6. I dati vengono forniti dall'interessato che chiede di fruire dei servizi o dei benefici; il dato sanitario è acquisito ai fini della valutazione della sussistenza dei presupposti all'ammissione al beneficio richiesto. L'archiviazione delle certificazioni mediche avviene anche in forma cartacea.

7. I dati vengono conservati solo al fine di attestare l'avvenuta verifica della sussistenza del diritto all'erogazione del beneficio.
8. Si può procedere, altresì, a forme di estrazione e trasmissione dei dati all'interno dell'Amministrazione difesa, in caso di ulteriori accertamenti sanitari richiesti dall'interessato presso gli organi medico-legali di secondo grado; in tale caso la comunicazione avviene a richiesta del dipendente.

Art. 1072 Demanio

1. In relazione alla rilevante finalità di interesse pubblico connessa con la materia tributaria, ai sensi dell'articolo 66 del decreto n. 196, il trattamento dei dati sensibili, in materia di gestione del demanio militare, avviene nell'ambito dei seguenti procedimenti e attività:
   a) gestione patrimonio immobiliare della Difesa;
   b) procedure di sfratto, di espropriazione e di occupazione;
   c) servitù militari.

2. Il trattamento dei dati sensibili e giudiziari è effettuato ai sensi del libro II del codice, del codice civile e del decreto-legge 30 settembre 2003, n. 269, convertito, con modificazioni, dalla legge 24 novembre 2003, n. 326.

3. I tipi di dati trattati in relazione a quanto indicato nel comma 1 sono i seguenti:
   a) stato di salute:
      1 patologie attuali;
      2 patologie pregresse;
      3 terapie in corso.

4. Le operazioni eseguite in relazione a quanto indicato nel comma 1 sono le seguenti:
   a) trattamento ordinario dei dati:
      1 raccolta presso gli interessati;
      2 elaborazione in forma cartacea e con modalità informatizzate.

5. Nell'ambito dei procedimenti relativi alla gestione del demanio e del patrimonio della Difesa e, in particolare dei procedimenti di sfratto, di occupazione e di espropriazione, l'Amministrazione, ai fini dell'adozione del provvedimento, può dover valutare dati afferenti allo stato di salute acquisiti presso l'interessato, ovvero da questi prodotti allo scopo di tutelare i propri interessi.

Art. 1073 Atti di sindacato ispettivo, di indirizzo e di controllo

1. In relazione alla rilevante finalità di interesse pubblico connessa con la documentazione dell'attività istituzionale di organi pubblici e con l'attività di sindacato ispettivo, di indirizzo e di controllo, come definite dai regolamenti del Senato della Repubblica e della Camera dei deputati,

il trattamento dei dati sensibili e giudiziari, ai sensi degli articoli 65 e 67 del decreto n. 196, in materia di atti di sindacato ispettivo di pertinenza della Difesa avviene ai sensi del presente articolo.

2. I tipi di dati trattati in relazione a quanto indicato nel comma 1 sono i seguenti:
   a) stato di salute:
      1 patologie attuali;
      2 patologie pregresse;
      3 terapie in corso;
      4 anamnesi familiare;
   b) dati di carattere giudiziario;
   c) convinzioni politiche, filosofiche, religiose, sindacali e di altro genere e vita sessuale, limitatamente alla trattazione degli atti di sindacato ispettivo, di indirizzo e di controllo.

3. Le particolari forme di elaborazione, per le finalità di seguito indicate, sono le seguenti:
   1) comunicazione all'organo richiedente per la formulazione della risposta all'interrogazione o all'atto di sindacato ispettivo, limitatamente ai dati indispensabili.

4. Il trattamento è volto a predisporre gli elementi di risposta agli atti di sindacato ispettivo, ovvero le informazioni necessarie alla replica o al parere del Governo su mozioni o risoluzioni, d'interesse dell'Amministrazione della difesa, per consentire il corretto svolgersi della funzione di controllo delle Camere.

5. La predisposizione degli schemi di risposta riguarda anche gli interventi del Ministro o dei Sottosegretari, in occasione di interrogazioni, interrogazioni a risposta immediata, interpellanze, e informative urgenti in Commissione o in Assemblea.

6. La trasmissione delle risposte concerne solo le interrogazioni a risposta scritta, ed è diretta ai parlamentari interroganti e alla Camera di appartenenza degli stessi.

7. L'acquisizione e il trattamento dei dati sensibili e giudiziari avviene di volta in volta in ragione delle tematiche e delle materie su cui si incentrano gli atti di sindacato ispettivo di interesse, solamente laddove strettamente indispensabili.

8. Il trattamento di dati sensibili e giudiziari avviene nel rispetto del principio di stretta indispensabilità sia nell'attività di predisposizione dello schema di risposta, sia, in particolare, nella comunicazione agli organi interroganti.

Art. 1074 Gestione del contenzioso giudiziale e stragiudiziale

1. In relazione alle rilevanti finalità di interesse pubblico di gestione del rapporto di impiego, di servizio o di lavoro e di applicazione di norme in materia di ricorsi ed esercizio del diritto di difesa in sede amministrativa e giudiziaria, ai sensi degli articoli 71 e 112 del decreto n. 196, il trattamento dei dati sensibili e giudiziari, in materia di gestione del contenzioso giudiziale e stragiudiziale della Difesa, avviene nell'ambito dei seguenti procedimenti e attività:
   a) attività rivolta alla tutela degli interessi dell'amministrazione in sede amministrativa, di giurisdizione ordinaria o amministrativa e di giurisdizione amministrativa speciale, o militare, nonché in sede stragiudiziale;
   b) costituzione di parte civile in procedimenti penali;
   c) risarcimento danni;
   d) procedure esecutive.

2. Il trattamento dei dati giudiziari, nonché di quelli idonei a rivelare lo stato di salute, è effettuato ai sensi dei libri IV e V del codice, della normativa sul rapporto di lavoro del personale civile, del decreto del Presidente della Repubblica 24 novembre 1971, n. 1199 sui ricorsi amministrativi e di quella processuale vigente in materia penale, civile e amministrativa.
3. I tipi di dati trattati in relazione a quanto indicato nel comma 1 sono i seguenti:
   a) stato di salute:
      1 patologie attuali;
      2 patologie pregresse;
      3 terapie in corso;
      4 anamnesi familiare;
   b) dati di carattere giudiziario.

4. Le particolari forme di elaborazione per le finalità di seguito indicate:
   a) comunicazione alle autorità giudiziarie;

b) comunicazione all'Avvocatura generale dello Stato, allo scopo di fornire gli elementi di fatto e di diritto necessari per la difesa dell'Amministrazione;
c) comunicazione al Consiglio di Stato, per l'acquisizione del parere, e Presidenza della Repubblica, nell'ambito dei ricorsi straordinari al Capo dello Stato;
d) comunicazione al Collegio di conciliazione, di cui all'art. 66 del decreto legislativo n. 165 del 2001, per le controversie individuali del personale civile;
e) comunicazione alla Presidenza del Consiglio di Ministri e all'Avvocatura generale dello Stato, per la costituzione di parte civile nei procedimenti penali;
f) comunicazione alle compagnie assicuratrici, per il recupero delle somme erogate a vuoto a favore del dipendente danneggiato.

5. Gli uffici dell'Amministrazione competenti a trattare il contenzioso effettuano il trattamento dei dati sensibili e giudiziari nella misura in cui ciò sia indispensabile per fornire all'Avvocatura generale dello Stato e alle autorità giudiziarie gli elementi necessari per la tutela degli interessi della Difesa in sede giudiziaria e stragiudiziale, ovvero per istruire la pratica relativa a un ricorso straordinario al Capo dello Stato; dietro richiesta dell'autorità giudiziaria possono essere forniti dati sensibili e giudiziari di cui sia in possesso l'Amministrazione.

6. Nelle memorie scritte depositate dall'Amministrazione presso il collegio di conciliazione, di cui all'art. 66 del decreto legislativo n. 165 del 2001, possono essere contenuti dati sensibili e giudiziari necessari nella misura in cui ciò sia strettamente indispensabile ai fini dell'esperimento del tentativo di conciliazione.

Art. 1075 Norme comuni in materia di raccolta, archiviazione e custodia dei dati

1. Le operazioni comuni eseguite in relazione al trattamento dei dati di cui al capo II sono le seguenti:
   a) raccolta presso gli interessati e presso terzi;
   b) elaborazione in forma cartacea e con modalità informatizzate.

2. I dati di cui all' articolo 1072 vengono raccolti esclusivamente presso gli interessati.

3. I dati di cui al presente capo:

a) sono archiviati su supporto cartaceo o informatico presso le strutture deputate al trattamento degli stessi e vengono custoditi in appositi locali muniti di serratura o, per i dati di carattere sanitario, in armadi dotati di serratura posti in locali accessibili esclusivamente al personale autorizzato;
b) ove custoditi in elaboratori elettronici, sono accessibili solamente al personale in possesso di credenziali di autenticazione informatica.

ALLEGATO B – TRATTAMENTO EFFETTUATO CON APPLICATIVI ESTERNI ALLA DIREZIONE

DESCRIZIONE	TIPO DI DATI	DENOMINAZIONE	U.O. INTERESSATA	GESTORE	PROTEZIONI
Sistema per la gestione integrata della contabilità economica e finanziaria	Economico-finanziari	SICOGE	VDA Servizi Amministrativi (SA) degli UU.TT.	Ragioneria Generale dello Stato	Livello applicativo: utente e password (doppia autenticazione) con l'apposizione della firma digitale da parte del Dirigente dell'Amministrazione
Valutazione dirigenziale	Personali, identificativi, sensibili,	SIRIDI	UD	O.I.V. DIFESA	Livello applicativo: utente e password
Protocollo Informatico	Personali, identificativi, sensibili, giudiziari	ADHOC	Vice Direzioni, Reparti, uffici, divisioni, servizi UU.TT. e loro articolazioni	SEGREDIFESA	Livello applicativo: login con CMD o con ruolo
Gestione Capitoli Straordinari FF.AA.	Personali, identificativi, sensibili	GEFIS WEB	UD UTT (UD)	SEGREDIFESA	Livello applicativo: utente e password

ALLEGATO B

Fogli di viaggio	Personali, identificativi,	SIIMP	UD UTT (UD e SA)	SEGREDIFESA–UGCRA	Livello applicativo: utente e password
Rilevazione presenze	Personali, identificativi, sensibili	WEB ACCESSI 2	UD UTT (UD)	Comando C4 Difesa	Livello applicativo: CMD
Acquisizione dati emissione CMD	Personali, identificativi, sensibili (eventuali)	Portale CMD modello AT elettronico	UD	Comando C4 Esercito	Livello applicativo: CMD
Sistema finanziario dell'Amministrazione Difesa	Economici	SIFAD OBJ SIFAD OIV	UPGFC	SMD – U.G.P.P.B. O.I.V. DIFESA	Livello applicativo: utente e password
Sistema Informativo Personale Civile	Personali, identificativi, sensibili	INFOCIV	UD	PERSOCIV	Livello applicativo: utente e password
Rilevazione Performances Personale Civile non dirigenziale della Difesa	Personali, identificativi, sensibili (valutazione performance)	INFOPERF	UD	PERSOCIV	Livello applicativo: utente e password
Portale Gestione Infortuni sul lavoro	Personali, identificativi, sanitari, sensibili	INAIL	DIREZIONE UU.TT. (Direzione)	INAIL	Livello applicativo: utente e password
Sistema Gestione Operativa Personale	Personali, identificativi, sensibili	GOPERS	Tutte le UU.OO.	C4 Difesa	Livello applicativo: utente e password

ALLEGATO B

Ubicazione fisica dei supporti per la memorizzazione: presso la sala server di SGD-MARSALA (ove non diversamente specificato); Tipologia di dispositivi per l'accesso: personal computer; Tipologia di interconnessione: rete intranet Difesa.

ALLEGATO C – TRATTAMENTO EFFETTUATO CON APPLICATIVI DELLA DIREZIONE

Descrizione sintetica attività	Tipo di dati trattati	Banca dati	Unità organizzative utilizzatrici/ Personale dipendente	Autore	Responsabile del trattamento	Misure di sicurezza adottate
Protocollo informatico (storico)	Personali Identificativi Sensibili Giudiziari	SICOR	UPGFC	Ditta Mythos	UPGFC	Su 3 livelli: a livello di rete (controllo e profilo di accesso); a livello Data Base (DBA) (consenso di connessione); a livello di applicativo (accesso funzionale).
Gestione attività per il rilascio/rinnovo N.O.S.	Personali Identificativi Giudiziari	NOS	UD UU.TT. (UD)	UD	UD	Gestione su computer *stand alone* (non in rete) Livello applicativo: utente e password

ALLEGATO D – MODULO DI ASSUNZIONE DI RESPONSABILITA'

MODULO PER PERSONALE DIPENDENTE

COMANDO C4 DIFESA

Roma – Via Stresa, 31/B

MODULO DI ASSUNZIONE DI RESPONSABILITA'

Con il presente modulo d'Assunzione di Responsabilità il sottoscritto ..... in servizio presso .....
(grado/qualifica cognome e nome)
in..... telefono ufficio ..... assegnatario della casella di posta elettronica dell'Amministrazione Difesa ..... e utente del PC con indirizzo IP ..... e con scheda di rete avente indirizzo MAC.....

dichiara di essere a conoscenza che:

a) il PC affidatogli dall'Amministrazione Difesa deve essere utilizzato esclusivamente per adempiere alle sole esigenze d'istituto a lui demandate. La possibilità d'uso di Internet è consentita unicamente per incrementare l'efficienza e la produttività del proprio lavoro e NON per scopi personali;
b) l'user-ID assegnato e la password di accesso devono essere custoditi e mantenuti strettamente riservati e non devono essere condivisi con altri utenti;
c) non è consentito detenere dati personali sul PC in questione;
d) l'indirizzo di posta elettronica (e-mail) assegnatogli, ancorché nella forma nome.cognome@.....difesa.it, non ha caratteristiche di privatezza ma costituisce normale strumento di lavoro e ne è vietato l'utilizzo per scopi personali. L'assegnatario è tenuto ad informare di tale caratteristica i terzi a cui comunica il citato indirizzo e-mail;
e) l'utilizzo di apparati di sicurezza (firewall IDS) e di filtraggio della posta indesiderata (firewall-antispam) devono inevitabilmente analizzare in modo autonomo ed automatico il traffico Internet e della posta elettronica per svolgere il loro compito;
f) deve dare comunicazione immediata al Comando C4 Difesa dell'eventuale perdita di riservatezza della password e al Capo Ufficio/Servizio della eventuale cessazione di utilizzo della rete;
g) è vietato immettere, trasmettere, diffondere qualsiasi materiale che non può essere distribuito legalmente via rete telematica (**vedi disposizioni di legge di seguito indicate**);
h) è vietato modificare la configurazione del PC in dotazione. Nel caso in cui si presentasse l'esigenza di utilizzare nuovo software, ciò può avvenire solo previa autorizzazione del proprio Capo Ufficio/Servizio, che ne valuterà l'effettiva necessità prima, e successivamente inoltrerà la richiesta al GEIRD (apertura ticket) il quale provvederà ad eseguirne l'installazione.
i) le disposizioni legislative sulla tutela giuridica del software considerano i programmi per elaboratore alla stregua di opere letterarie protette dalle vigenti leggi in materia;
j) la riproduzione permanente/temporanea, totale/parziale di software acquisito dal commercio o prodotto dall'Amministrazione Difesa deve essere autorizzata dai titolari dei diritti di proprietà sullo stesso;

firma per accettazione _____

1 di 2

k. chiunque abusivamente duplica software per uso su elaboratori o sapendo o, avendo motivo di sapere che si tratta di copie non autorizzate, lo distribuisce, lo vende, lo detiene a scopi commerciali/personali, è soggetto alla pena prevista dalla vigente legislazione che comporta reclusione e sanzioni economiche. Alla stessa pena è soggetto chi mette in atto sistemi tendenti a facilitare la rimozione arbitraria e l'elusione funzionale dei dispositivi applicati a protezione dei software per uso su elaboratori;

l. lo scarico dalla rete (download) di opere protette dal copyright (musiche, filmati, programmi etc. etc.) non è consentito a nessun titolo ed è soggetto a sanzione in conformità dalle vigenti leggi;

m. la detenzione sul proprio elaboratore di contenuti pedo-pornografici è vietata e soggetta a sanzione in conformità alle vigenti leggi;

n. non sono consentite azioni tendenti a nascondere la propria identità, a molestare o arrecare danno sull'attività degli elaboratori di altri utenti o ad acquisire dati/informazioni/privilegi a cui non si ha diritto.

Qualsiasi inadempienza a quanto dichiarato nel presente documento provocherà l'immediata sospensione del servizio rete Internet. Il Comando C4 Difesa può interrompere il servizio prestato al sottoscritto anche solo per palese violazione del codice di buon comportamento.

Il Comando C4 Difesa provvederà a fornire consulenza sulle configurazioni ideali da realizzare sui computer attraverso il supporto del GEIRD (tel. 24444). I dati di questo modulo saranno utilizzati dal Comando, titolare del trattamento degli stessi, nel rispetto del D.Lgs. 196 in data 30/06/2003.

Si riportano per opportuna informazione le normative che regolano l'argomento oggetto del presente modulo:

- Netiquette, "galateo di internet";
- D.P.R. n.144 in data 27/07/2005 "Misure urgenti per il contrasto del terrorismo internazionale";
- D.Lgs. 196 in data 30/06/2003, "Codice di protezione dei dati personali";
- D.P.R. n. 513 in data 10/11/1997, "Regolamento contenente i criteri e le modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici (a norma dell'art. 15, comma 2 della Legge in data 15/03/1997 n. 59", delega al governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della Pubblica amministrazione e la semplificazione amministrativa);
- Legge n. 633 in data 22/04/1941 in materia di disposizioni sul diritto di autore, con l'aggiornamento del comma 1/b aggiunto dall'art. 1 del D.Lgs. 29/12/92, n. 518 (attuazione direttiva 91/250/CEE relativa alla tutela giuridica dei programmi per elaboratore);
- Art. 615 del Codice Penale in merito all'accesso abusivo ad un sistema informatico o telematico;
- Legge 23 dicembre 1993 n. 547 "Modificazioni ed integrazioni delle norme del codice penale e del codice di procedura penale in tema di criminalità informatica".
- Codice dell'Amministrazione Digitale (CAD) in vigore a decorrere dal 1 gennaio 2006
- Direttiva n. 2/2009 della presidenza del Consiglio dei Ministri – Dip. della Funz. Pubbl.

Le normative suindicate sono anche consultabili al seguente indirizzo: https//archimede.difesa.it

Firma per accettazione

_____

Roma _____