ATC RC1

NORME COMPORTAMENTALI

Soggetti autorizzati al trattamento di dati personali

Indice

Introduzione

Il presente documento costituisce una appendice alla policy privacy dell'Ambito Territoriale di Caccia RC1, contenente istruzioni operative per il corretto utilizzo dei sistemi informatici presenti all'interno dell'Ente nell'ambito delle attività di trattamento dei dati personali o sensibili. Lo scopo è quello di ridurre e contenere i rischi di danneggiamento o dispersione dei dati trattati, a causa di un uso non corretto o illecito dei sistemi informatici da parte del personale autorizzato al trattamento. I dati personali devono essere trattati:

a) in osservanza dei criteri di riservatezza;

b) in modo lecito e secondo correttezza;

c) per un periodo di tempo non superiore a quello necessario agli scopi per i quali sono stati raccolti o successivamente trattati;

d) nel pieno rispetto delle misure di sicurezza predisposte, custodendo e controllando i dati oggetto di trattamento in modo da evitare i rischi, anche accidentali, di distruzione o perdita, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

1. Altri riferimenti

In relazione all'ente ed alla pianificazione delle attività di trattamento dei dati, si definisce soggetto autorizzato, all'interno di una organizzazione e secondo la normativa europea, chiunque effettui operazioni di trattamento, pertanto è *«persona autorizzata al trattamento dei dati personali sotto l'autorità diretta del titolare».*

Si consiglia la consultazione ed il raffronto dei seguenti documenti e fonti:

• REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);

- D. Lgs n.101/2018

• https://www.garanteprivacy.it/

• Codice in materia di protezione dei dati personali, decreto legislativo 30 giugno 2003, n.196.

1.1 Organizzazione del documento

Il documento è suddiviso in quattro parti:

- **Sicurezza fisica:** norme per la custodia e la protezione dei dati e degli strumenti utilizzati per effettuarne il trattamento;

- **Sicurezza logica:** contromisure adeguate a garantire la protezione e la riservatezza dell'accesso ai dati ed agli strumenti utilizzati per il loro trattamento;
- **Istruzioni agli autorizzati del trattamento dei dati:** indicazioni utili per la corretta gestione e custodia degli account di accesso ai sistemi informatici utilizzati per il trattamento dei dati;
- **Sicurezza del software e dell'hardware:** norme per la corretta gestione degli apparati informatici e del software installato su di essi;
- **Sanzioni per inosservanza delle norme:** sanzioni a carico dell'autorizzato in caso di violazioni delle istruzioni operative.

2 Sicurezza fisica

I dati personali sia in forma cartacea che elettronica devono essere protetti in modo da impedirne l'accesso a persone non autorizzate con l'obiettivo di non violare la privacy rendendo pubblici dati di natura riservata e al tempo stesso di preservarne l'integrità. La sicurezza fisica riguarda quelle misure adottate al fine di impedire l'accesso di persone non autorizzate ai dati (qualora siano archiviati su supporti cartacei) o ai dispositivi informatici utilizzati per il trattamento, l'elaborazione automatica e l'archiviazione dei dati stessi. Le misure di sicurezza fisica riguardano anche le procedure organizzative e gli strumenti adottati al fine di garantire l'integrità e la conservazione dei dati a fronte di eventi straordinari dovuti a cause naturali o provocati al fine di danneggiare l'Ente. Le misure, in parte attuate ed in parte da implementarsi, richiedono l'ubicazione dei dati (cartacei o

su supporti informatici) in locali protetti da serrature e che richiedono un accesso controllato. I documenti cartacei devono essere archiviati in mobili protetti da serrature e deve essere tracciato l'iter secondo procedure definite. La verifica della corretta adozione di quanto previsto dalle procedure da parte dei soggetti autorizzati e la definizione delle procedure stesse è in capo ai Designati al trattamento dei dati. I designati di area sono figure apicali che, nell'ambito del rapporto di lavoro instaurato con il Titolare e tenuto conto delle mansioni assegnate, sono deputati di per sé al controllo e tenuti agli adempimenti legati alla propria funzione.

Nel caso di trattamento informatico sono in vigore procedure di controllo d'acceso ai locali dove sono ubicati gli altri sistemi informatici utilizzati per il trattamento di dati personali. I Designati del trattamento provvedono ad attuare le misure di protezione ad archivi contenenti dati personali in modo da impedirne l'accesso a persone non autorizzate. Gli autorizzati accedono ai dati personali nello svolgimento delle proprie mansioni ed evitano comportamenti che possano pregiudicare la riservatezza dei dati. Per esigenze specifiche possono chiedere indicazioni e direttive al Designato di area di loro pertinenza e precedentemente menzionato.

3 Sicurezza logica

La sicurezza logica riguarda l'accesso ai dati personali trattati attraverso procedure informatiche e viene realizzata assicurando che gli accessi ai sistemi informativi avvengano secondo modalità predefinite, tali da garantire un elevato livello di robustezza ed affidabilità. In particolare le misure di sicurezza logica mirano ad identificare i soggetti che accedono ai sistemi informatici adibiti al trattamento di dati, in modo tale da assicurare che soltanto i soggetti autorizzati a compiere un determinato trattamento possano accedere ai dati di propria competenza. Tale identificazione avviene utilizzando un codice identificativo personale (username) associato univocamente ad ogni singolo incaricato ed una parola chiave (password). Tutti gli autorizzati devono rispettare le seguenti disposizioni:

a. Il dipendente autorizzato a cui è stato assegnato un account di identificazione (una coppia formata da uno username e da una password) per l'accesso alla rete informatica e/o all'utilizzo di applicazioni informatiche centralizzate o locali, è responsabile di tutto quanto accade a seguito di operazioni abilitate dal proprio codice identificativo personale.

b. L'autorizzato gestisce le proprie password secondo i principi di liceità, correttezza e riservatezza e secondo le disposizioni riportate nel presente documento.

c. L'autorizzato custodisce le password in modo riservato e non le comunica a nessun altro.

d. L'autorizzato esercita tutte le azioni necessarie per evitare che altre persone abbiano accesso alla sua stazione di lavoro. A tal fine quando si allontana dalla

propria stazione esce dal sistema (logoff) o blocca il personal computer con la password di uno screen saver. L'autorizzato cambia la password al primo accesso ed almeno ogni 6 mesi.

f. Oltre a queste misure, che ogni singolo addetto al trattamento è tenuto ad adottare, l'Ente ha messo in atto e si impegna a gestire contromisure di sicurezza logica, quali firewall ed altri sistemi di filtraggio del traffico di rete, per impedire l'accesso al sistema informativo dell'ATC RC1 da parte di utenti non autorizzati.

4 Istruzioni ai soggetti autorizzati al trattamento dei dati

Nel pieno rispetto del REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO e tenuto conto delle attività svolte nell'ambito della Struttura di appartenenza, l'incaricato dovrà effettuare trattamenti di dati personali di competenza attenendosi scrupolosamente alle seguenti istruzioni ed ad ogni ulteriore indicazione, anche verbale, che potrà essere fornita dal Titolare del Trattamento o dal Designato di area.

Le Misure di sicurezza devono "garantire un livello di sicurezza adeguato al rischio" del trattamento (art. 32, paragrafo 1); non potranno più sussistere obblighi generalizzati di adozione di misure "minime" di sicurezza *(ex art. 33 Codice)* poiché tale valutazione sarà rimessa, caso per caso, al titolare in rapporto ai rischi specificamente individuati come da art. 32 del regolamento.

Il Regolamento pone con forza l´accento sulla "responsabilizzazione" (accountability nell´accezione inglese) del Titolare **–** ossia, sull´**adozione di**

comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l´applicazione del regolamento *(si vedano artt. 23-25, in particolare, e l´intero Capo IV del regolamento)*. Si tratta di un approccio basato sul rischio e su misure di accountability.

Il primo fra tali criteri è sintetizzato dall´espressione inglese **"data protection by default and by design"** *(si veda art. 25)*, ossia dalla necessità di configurare il trattamento prevedendo fin dall´inizio le garanzie indispensabili "al fine di soddisfare i requisiti" del regolamento e tutelare i diritti degli interessati – tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati.

Le misure sono distinte in funzione delle seguenti modalità di trattamento dei dati:

- senza l'ausilio di strumenti elettronici (es. dati in archivi cartacei o su supporto magnetico/ottico);
- con strumenti elettronici (PC)

4.1 Trattamenti senza l'ausilio di strumenti elettronici

I dati personali conservati su supporti di tipo elettronico sono sottoposti alle stesse misure di protezione relative ai supporti cartacei. Nel caso in cui esistano copie o riproduzioni di documenti che contengono dati personali, esse devono essere protette con le stesse misure di sicurezza applicate agli originali.

Custodia

• I documenti contenenti dati personali, devono essere custoditi in modo da non essere accessibili a persone non autorizzate del trattamento (es. armadi o cassetti chiusi a chiave).

• I documenti contenenti dati personali prelevati dagli archivi per l'attività quotidiana, devono esservi riposti a fine giornata.

• I documenti contenenti dati personali non devono rimanere incustoditi su scrivanie o tavoli di lavoro.

Comunicazione

L'utilizzo dei dati personali deve avvenire in base al principio del "need to know" e cioè essi non devono essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie mansioni lavorative (anche se queste persone sono a loro volta autorizzate del trattamento). I dati non devono essere comunicati all'esterno della struttura e comunque a soggetti terzi se non previa autorizzazione.

Distruzione

• Qualora sia necessario distruggere i documenti contenti dati personali, questi devono essere distrutti utilizzando gli appositi apparecchi "distruggi documenti" o, in assenza, devono essere sminuzzati in modo da non essere più ricomponibili.

• I supporti magnetici od ottici contenenti dati personali devono essere cancellati prima di essere riutilizzati. Se ciò non è possibile, essi devono essere distrutti.

4.1.1 Istruzioni per il trattamento di dati sensibili e/o giudiziari

• I documenti o i supporti di tipo magnetico/ottico che contengono dati sensibili e/o giudiziari devono essere controllati e custoditi dai dipendenti autorizzati, i quali devono impedire l'accesso a persone prive di autorizzazione. Ad esempio la consultazione di documenti/certificati per l'inserimento in procedure informatiche di gestione/amministrazione del personale di dati relativi a permessi sindacali, assenze per malattie ecc., deve avvenire per il tempo strettamente necessario alla digitazione stessa e, subito dopo, i documenti devono essere archiviati in base alle presenti istruzioni.

• L'archiviazione dei documenti cartacei contenenti dati sensibili e/o giudiziari deve avvenire in locali ad accesso controllato, utilizzando armadi o cassetti chiusi a chiave.

4.2 Trattamenti con l'ausilio di mezzi elettronici

Al fine di poter trattare i dati mediante dispositivi informatici, deve essere prevista una procedura di autenticazione che consenta l'identificazione dei soggetti autorizzati allo specifico trattamento, attraverso "credenziali di autenticazione". Esse consistono in un user-ID associato ad una parola chiave segreta (password). Le user-ID individuali per l'accesso alle applicazioni NON devono essere MAI condivise da più utenti (anche se autorizzati del trattamento). Nel caso in cui occorre permettere l'accesso da parte di altri utenti, è necessario richiedere

l'autorizzazione al Designato di area del trattamento. Per i PC collegati in rete gli autorizzati devono farsi identificare per poter accedere alle rete dell'Ente. Tutti gli autorizzati che utilizzano un personal computer per il trattamento di dati personali non collegato in rete devono proteggere l'accesso alla propria postazione di lavoro attivando una password come previsto dalle funzionalità di protezione del PC.

4.2.1 Gestione delle password

La scelta delle password da parte dell'autorizzato deve essere ponderata in quanto un utilizzo improprio della stessa è il modo più facile per un accesso illecito da parte di terzi alla rete e/o all'applicazione, e di conseguenza ai dati in essi custoditi a tutti gli effetti risultando con l'identità di un altro utente. Una password deve essere facile da ricordare ma, allo stesso tempo, difficile da individuare. Questa sezione offre dei suggerimenti su come scegliere e proteggere la propria password. Queste linee guida rivestono un'importanza particolare se si lavora con materiale sensibile. Nella gestione delle password è necessario osservare pertanto le seguenti indicazioni:

1. NON comunicare a NESSUN altro dipendente autorizzato/collega le proprie password.

2. NON scrivere le proprie password su supporti facilmente rintracciabili e soprattutto in prossimità della postazione di lavoro utilizzata.

3. NON scegliere password corrispondenti a parole presenti in un dizionario, sia della lingua italiana che di lingue straniere. Non utilizzare nemmeno parole del

dizionario in senso inverso. 4. NON usare parole che possano essere facilmente riconducibili all'identità dell'utente come, ad esempio, il codice fiscale, il nome del coniuge o dei figli, la data di nascita, il numero di telefono, la targa della propria auto, il nome della via in cui si abita o addirittura la stessa ID. NON usare come password parole ottenute da una combinazione di tasti vicini alla tastiera.

5. NON usare la stessa password per l'accesso a sistemi ed applicativi differenti.

6. NON comunicare password vecchie e non più in uso in quanto potrebbe essere possibile ricavare da questi dati regole empiriche o personali che l'autorizzato utilizza per generare le proprie password.

7. Cambiare le password (almeno ogni sei mesi).

8. Utilizzare password lunghe almeno 8 caratteri od il massimo consentito dal sistema utilizzando un misto di lettere, numeri e segni di interpunzione.

9. Nel digitare la password accertarsi che non ci sia nessuno che osservi e sia in grado di vedere od intuire i caratteri digitati sulla tastiera.

4.2.2 Suggerimenti utili in presenza di ospiti o terze parti

A conclusione del paragrafo si ribadisce come gli autorizzati del trattamento debbono impedire l'accesso ai dati in loro possesso da parte di chi non è autorizzato. Qui si indicano poche regole di buona condotta che ogni autorizzato del trattamento di dati dovrebbe seguire in occasione di visite esterne o particolari situazioni di "minaccia" per la segretezza dei dati.

Esse sono ad esempio

• Fare attendere gli ospiti in luoghi in cui non siano presenti informazioni riservate o dati personali.

• Se è necessario allontanarsi dalla scrivania in presenza di ospiti, riporre i documenti e attivare il salvaschermo del PC.

• Segnalare qualsiasi anomalia del pc al Designato di area e questi a sua volta all'Amministratore di sistema.

Le norme riportate in questa sezione sono finalizzate ad aumentare la sicurezza dei singoli sistemi informatici utilizzati per il trattamento dei dati. Il rispetto di tali norme garantisce anche che non vengano compromesse le misure di sicurezza del sistema informativo dell'Ente ad opera di un utente regolarmente autorizzato, ma che inconsapevolmente adotta comportamenti in grado di violare l'integrità del sistema (installazione inconsapevole di virus o di "trojan horse"). L'autorizzato non può installare sulla propria postazione di lavoro programmi non attinenti alle normali attività d'ufficio né nuovi programmi. Gli utenti non possono modificare le configurazioni hardware e software. Se un autorizzato rileva un problema nell'ambito dell'utilizzo del sistema informatico relativo al trattamento di dati in corso che può compromettere la sicurezza dei dati ne dà immediata comunicazione al Designato di area del trattamento dei dati. Quest'ultimo provvede ad inoltrare la comunicazione, che analizza il problema segnalato ed adotta tutte le misure tecniche necessarie a risolverlo. Gli utenti che hanno accesso alla rete Internet mediante un personal computer in ambiente Microsoft Windows, verificano sul sito ufficiale della Microsoft (http://www.microsoft.com), con cadenza almeno mensile, le correzioni software per problemi di sicurezza

applicabili alla propria versione di sistema operativo. Utilizzando la funzione "Windows Update" del proprio sistema operativo Microsoft Windows è possibile rilevare la presenza di correzioni software per problemi di sicurezza, l'utente è tenuto a scaricare ed installare tali aggiornamenti sul proprio PC seguendo le indicazioni riportate sul sito Microsoft. Anche gli utenti di postazioni di lavoro non Windows (es.: Linux RedHat, Apple MacOS X, ecc.) hanno la possibilità di scaricare gli aggiornamenti e le correzioni del proprio sistema operativo, utilizzando funzioni analoghe presenti sulla propria macchina.

5.1 Protezione da virus informatici

I virus informatici rappresentano una delle minacce principali per la sicurezza dei sistemi informativi e dei dati in esso presenti. Un virus informatico può modificare e/o cancellare i dati in esso contenuti, può compromettere la sicurezza e la riservatezza di un intero sistema informativo, può rendere indisponibile tutto o parte del sistema, compresa la rete di trasmissione dati. Al fine di non aumentare il livello di rischio di contaminazione da virus è opportuno:

1. accertarsi che sul proprio computer sia sempre operativo il programma antivirus in uso dall'Ente, aggiornato e con la funzione di monitoraggio attiva;

2. sottoporre a controllo con il programma installato sul proprio PC, tutti i supporti di provenienza esterna prima di eseguire files in esso contenuti;

3. accertarsi sempre della provenienza dei messaggi di posta elettronica contenenti allegati; nel caso che il mittente dia origine a dubbi, cancellare direttamente il messaggio senza aprire gli allegati

4. non condividere con altri computer il proprio disco rigido o una cartella di files senza password di protezione in lettura/scrittura;

5. limitare la trasmissione tra computer in rete di file eseguibili e di sistema;

6. non scaricare da Internet programmi o file non inerenti l'attività lavorativa o comunque sospetti.

5.2 Backup dei dati

L'Ente adotta misure per l'esecuzione di backup dei dati presenti sui sistemi informatici utilizzati per il trattamento dei dati. Tali misure tengono conto dei seguenti aspetti:

• la frequenza del backup deve essere commisurata alla frequenza con cui i dati sono aggiornati;

• la politica di backup deve consentire un agevole ripristino delle informazioni e dei dati, qualora questi dovessero risultare corrotti o dovessero subire manomissioni o danneggiamenti durante la normale operatività degli incaricati o a causa di accessi fraudolenti al sistema;

• gli autorizzati che trattano i dati sui propri PC non collegati in rete o di cui non sono previsti backup centralizzati, devono provvedere al backup dei dati frequenti e custodire i supporti in luogo sicuro e ad accesso controllato.

5.3 Utilizzo della rete Internet

Il sistema informativo ed i dati in esso contenuti possono subire gravi danneggiamenti per un utilizzo improprio della connessione alla rete Internet; inoltre, come detto, attraverso la rete, possono essere nel sistema virus informatici e possono penetrare utenti non autorizzati. Al fine di evitare questi pericoli, è opportuno attenersi alle regole seguenti:

1. utilizzare la connessione ad Internet esclusivamente per lo svolgimento dei propri compiti istituzionali;
2. non diffondere messaggi di posta elettronica di provenienza dubbia;
3. non utilizzare la casella postale assegnata dall'Ente per fini privati e personali;
4. gli utenti devono essere a conoscenza degli articoli del codice penale 615 ter – "Accesso abusivo ad un sistema informatico e telematico", 615 quater – "Detenzione e diffusione abusiva di codici di accesso a sistemi informatici e telematica", 615 quinquies – "Diffusione di programmi diretti a danneggiare ed interrompere un sistema informatico", nonché del Decreto Legge 22 Marzo 2004 n. 72 convertito in legge con modificazioni dalla Legge 21 Maggio 2004 n. 128 (Legge Urbani) che sanziona la condivisione e/o fruizione di file relativi ad un'opera cinematografica od assimilata protetta da Diritti d'autore. Si ribadisce il fatto che nessun utente della rete informatica è autorizzato ad installare sulla propria postazione di lavoro software non previsto dalla configurazione predisposta. È pertanto vietato effettuare il download e l'installazione di programmi dalla rete Internet.

6 Sanzioni per inosservanza delle norme

Le presenti istruzioni operative sono impartite ai sensi delle normative vigenti in materia di privacy, l'inosservanza delle quali da parte dell'autorizzato può comportare sanzioni anche di natura penale a suo carico.

Responsabile della Protezione dei dati – Data Protection Officer è l'Avv. Lucia Lipari, raggiungibile al mob. 3294203914 o all'indirizzo avv.lucialipari@pec.it