REGOLAMENTO

PROTEZIONE DEI DATI PERSONALI DELLA FONDAZIONE ACCADEMIA NAUTICA DELL'ADRIATICO

I. INTRODUZIONE

1. PREMESSA

A seguito dell'introduzione del Regolamento Generale sulla protezione dei dati personali - GDPR (2016/679/UE) la Fondazione Accademia Nautica dell'Adriatico adotta il presente Regolamento interno per assicurare la conformità delle attività di trattamento realizzate, nonché il rispetto di ogni disposizione della normativa vigente in materia di protezione dei dati personali e garantire adeguati livelli di sicurezza delle informazioni.

In questo documento sono individuate regole precise per il trattamento dei dati personali anche attraverso l'utilizzo degli strumenti informatici a disposizione dei dipendenti.

2. SCOPO, CAMPO DI APPLICAZIONE

Lo scopo primario del presente Regolamento interno è quello recepire quanto previsto GDPR (2016/679/UE) in merito alla protezione dei diritti e le libertà fondamentali delle persone fisiche ed in particolare la protezione dei dati personali definendo nuovi ruoli e responsabilità coinvolgendo tutte le funzioni, i processi, le tecnologie, i dati ed in particolare, tutte le informazioni che, direttamente oppure indirettamente, identificano un soggetto residente nell'UE.

Questo documento definisce un insieme di norme comportamentali a cui devono uniformarsi nell'ambito delle attività che implicano un trattamento di dati ed informazioni: i dipendenti, i collaboratori, le terze parti ed in generale quelli che sono definiti come soggetti interni ed esterni che operano per la Fondazione.

3. SOGGETTI COINVOLTI DAL GDPR

- La Persona Fisica a cui si riferiscono i dati personali (*Data subject)*
- Il titolare del trattamento - Fondazione Accademia Nautica dell'Adriatico (*Data Controller*)
- La persona autorizzata al trattamento (dipendenti e collaboratori parasubordinati)
- Il responsabile del trattamento – (*Data Processor*)
- Il responsabile della protezione dei dati *(DPO-Data Protection Officer)*
- Il Garante per la protezione dati personali *(I-DPA - Italian Data Protection Authority)*

3.1. Esempi di Persona Fisica (*Data subject)*

- Componenti degli Organi statutari
- Management e dipendenti della Fondazione
- Collaboratori coordinati e continuativi
- Consulenti e collaboratori occasionali
- Personale operante a fronte di accordi di distacco o di un comando
- Allievi partecipanti ai corsi tenuti dalla Fondazione
- Docenti ed Istruttori che operano a vario titolo
- Collaboratori a qualsiasi titolo di imprese fornitrici di beni, servizi o lavori che realizzano opere in favore della Fondazione
- Personale di altre entità presenti in forza di convenzioni o accordi inter-istituzionali
- Visitatori, ospiti di vario genere partecipanti alle iniziative pubbliche organizzate dalla Fondazione quali seminari, conferenze, ecc.

3.1.1 Diritti della Persona Fisica

La persona fisica diventa soggetto interessato che con il GDPR acquisisce una serie di diritti:

- ✓ Violazione dei dati (Data Breach): notifica all'Autorità di Controllo e all'interessato in caso di violazione senza ingiustificato ritardo
- ✓ Diritto di accesso: prevede in ogni caso il diritto di ricevere una copia dei dati personali oggetto di trattamento. Fra le informazioni che il Titolare deve fornire non rientrano le "modalità" del trattamento, mentre occorre indicare il periodo di conservazione previsto
- ✓ Diritto di cancellazione (diritto all'oblio): si configura come un diritto alla cancellazione dei propri dati personali in forma rafforzata. Si prevede l'obbligo per i titolari del trattamento (se hanno "reso pubblici" i dati personali dell'interessato: ad esempio, pubblicandoli su un sito web) di informare della richiesta di cancellazione altri titolari che trattano i dati personali cancellati, compresi "qualsiasi link, copia o riproduzione" (art. 17, paragrafo 2). L'interessato ha il diritto di chiedere la cancellazione dei propri dati, per esempio, anche dopo revoca del consenso al trattamento (art. 17, paragrafo 1)
- ✓ Diritto di limitazione del trattamento: si tratta di un diritto diverso e più esteso rispetto al "blocco" del trattamento di cui all'art. 7, comma 3, lettera a), del Codice, in particolare, è esercitabile non solo in caso di violazione dei presupposti di liceità del trattamento (quale alternativa alla cancellazione dei dati stessi)
- ✓ Diritto di rettifica: diritto dell'interessato a modificare i propri dati personali
- ✓ Diritto di opposizione: diritto dell'interessato di opporsi al trattamento di dati personali che lo riguardano, realizzati in ragione dell'esecuzione di un compito di pubblico interesse o del legittimo interesse del titolare. L'interessato può sempre opporsi al trattamento per finalità di marketing diretto.
- ✓ Diritto alla portabilità dei dati: diritto dell' interessato a trasferire i propri dati personali. Non si applica ai trattamenti non automatizzati (quindi non si applica agli archivi o registri cartacei) e sono previste specifiche condizioni per il suo esercizio; in particolare, sono portabili solo i dati trattati con il consenso dell'interessato o sulla base di un contratto stipulato con l'interessato (quindi non si applica ai dati il cui trattamento si fonda sull'interesse pubblico o sull'interesse legittimo del titolare, per esempio), e solo i dati che siano stati "forniti" dall'interessato al titolare

La Fondazione Accademia Nautica dell'Adriatico quale policy di comportamento mette in atto tutte le misure necessarie per garantire i diritti, indicati dal Regolamento GDPR, dei soggetti interessati.

3.2. Titolare del Trattamento (Data Controller)

E' l'organizzazione nel suo complesso, nella persona del suo ***Legale Rappresentante*** che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza.

3.3 Persona autorizzate al trattamento

È il dipendente o collaboratore che realizza attività di trattamento sotto la diretta autorità della Fondazione

3.4 Responsabile del trattamento (Data Processor)

È la persona fisica o giuridica, autorità pubblica, servizio o altro organismo che tratta dati personali per conto del "Titolare del Trattamento". Il Responsabile del trattamento deve presentare garanzie

sufficienti per mettere in atto misure tecniche e organizzative adeguate affinché il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato (Persona Fisica).

3.5 Responsabile della protezione dei dati (Data Protection Officer - DPO)

Tale funzione dovrebbe sostenere gli incaricati della conformità e farsi carico della responsabilità di coordinare gli sforzi per la protezione dei dati e fornire formazione organizzativa per assicurarne l'efficacia.

E' la persona fisica nominata dal Titolare del trattamento dati che, ai sensi degli artt. 37-39 del GDPR, operando in modo indipendente rispetto all'organizzazione, consiglia il Titolare riguardo obblighi, requisiti ed evoluzione normativa, realizza verifiche interne sulla corretta applicazione delle disposizioni normative e del sistema di gestione per la protezione dei dati personali definite dal Titolare, assiste il Titolare sulla valutazione di impatto e sull'analisi del rischio e rappresenta il punto di contatto per interessati e Garante Privacy.

In base all'articolo 37, paragrafo 1, del GDPR, la nomina di un DPO è obbligatoria se il trattamento è svolto da un'autorità pubblica o da un organismo pubblico oppure per alcune tipologie di aziende che monitorano una notevole mole di dati. Con aggiornamento del presente documento ad aprile 2023, si ritiene che le attività principali dell'Accademia non soddisfino il criterio della "larga scala" e che pertanto non sia obbligatoria la designazione di un DPO come riportato nel documento "ACCOUNTABILITY ASSESSMENT Valutazione DPO" AA2 del 27/08/2019 rev. 10/04/2023.

II. DATA PROTECTION BY DESIGN

Il piano operativo di conformità al GDPR si attua nell'organizzazione della Fondazione attraverso sei fasi rispondendo al requisito di organizzare le operazioni per fornire servizi "conformi fin dalla progettazione" (by design) senza sacrificare l'agilità della Fondazione stessa:

1. eseguire la valutazione iniziale (delle esigenze di conformità al GDPR)
2. identificare le priorità di conformità (nell'elaborazione di informazioni personali identificabili)
3. concludere una valutazione di impatto
4. implementazione del piano d'azione (con azioni correttive e preventive modellando i processi di business)
5. tener traccia degli incidenti (capacità di reporting)
6. dimostrare di essere conformi (alla dirigenza e alle autorità di vigilanza)

1. PRIORITA' DI CONFORMITA'

Il GDPR ha l'obiettivo di regolare il ciclo di vita dei dati. La Fondazione effettua periodicamente l'inventario dei dati personali trattati internamente o da terzi per conto della Fondazione, indentificandone le modalità , le finalità e necessità del trattamento.

La classificazione e mappatura delle informazioni per soggetto, processo e tecnologia consentano di stabilirne l'utilizzo, mentre l'attribuzione ai dati di una priorità, agevola a valutare la necessità. L'incrocio di questi aspetti evidenzia le interazioni con i dati personali più critiche per un'ulteriore valutazione dei requisiti di conformità.

Tutte le informazioni direttamente o indirettamente riferibili a persone fisiche costituiscono dati personali. Ciò significa che le informazioni che da sole non identificano un soggetto, ma che lo fanno se raggruppate con altre informazioni o specifici identificativi , devono essere considerate dati personali. Tutte le attività di trattamento di dati personali devono rispettare i principi applicabili previsti dal GDPR e pertanto si rende necessario un censimento delle informazioni trattate, dei flussi e dei soggetti coinvolti.

2. TRACCIABILITA' DEGLI INCIDENTI

Il GDPR richiede che il Titolare del trattamento notifichi all'autorità di controllo competente le violazioni di dati personali subite, entro 72 ore dal momento in cui ne è venuto a conoscenza, salvo sussistano determinate condizioni per cui risulti improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche (art.33).

Allo stesso modo il GDPR richiede che il titolare del trattamento notifichi ai soggetti interessati la violazione di dati personali, quando tale violazione possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche (art. 34).

Le disposizioni sono rispettate attraverso un monitoraggio continuo delle attività di trattamento dei dati e con il tracciamento delle violazioni subite, al fine di documentare la natura della violazione e le azioni intraprese di volta in volta.

A tale scopo sono registrati nel Registro delle violazioni: data e ora della conoscenza della violazione, la descrizione della violazione rilevata, data e ora della notifica all'Autorità competente, data e ora della notifica ai soggetti interessati, la gravità assegnata le azioni correttive attuate per risolvere l'incidente ed ridurre il rischio che si ripresenti, il rischio per i soggetti interessati.

3. DIMOSTRAZIONE DI CONFORMITA'

Il GDPR richiede che al titolare del trattamento di essere in grado di fornire informazioni specifiche che dimostrino la conformità delle attività di trattamento,. Tra le evidenze che possono essere portate a dimostrazione della conformità delle attività di trattamento, si indicano a titolo esemplificativo le seguenti:

- Registro delle attività di trattamento (art. 30)
- Procedura per la gestione delle violazioni di dati personali e registro delle violazioni (art. 33)
- Adozione di misure tecniche e organizzative adeguate al rischio e valutazione d'impatto (artt. 32, 35)
- Conclusione dei contratti che dispongono della materia del trattamento di dati personali tra titolare e responsabili del trattamento (art. 28)
- Autorizzazione al trattamento e istruzioni per i soggetti incaricati (dipendenti e collaboratori parasubordinati) che svolgono attività di trattamento sotto la diretta autorità del titolare

III. MODELLO ORGANIZZATIVO

1. CLASSIFICAZIONE DEL PATRIMONIO INFORMATIVO DELLA FONDAZIONE

Informazioni pubbliche: sono le informazioni liberamente trattabili da soggetti attraverso i mezzi di comunicazione messi a disposizione dalla Fondazione (sito internet, pubblicazioni, comunicati, ecc.). Queste informazioni non richiedono da parte dei soggetti particolari attenzioni di riservatezza. La divulgazione di tali informazioni non presenta implicazioni per la Fondazione in quanto si tratta di informazioni pubbliche che possono essere diffuse.

Informazioni interne: sono le informazioni che possono essere trattate da soggetti esclusivamente all'interno dei processi e del contesto organizzativo della Fondazione attraverso i canali istituzionali messi a disposizione (e-mail, intranet, sito internet, aree di scambio su server interni e sul cloud, computer, ecc.). Queste informazioni richiedono da parte dell'utilizzatore una particolare attenzione nel trattamento, in quanto la loro divulgazione rappresenta una violazione dei vincoli di riservatezza ai quali è legato ogni utilizzatore con un possibile impatto legale

Dati personali e informazioni riservate: sono le informazioni che possono essere trattate soggetti autorizzati in rapporto al ruolo ricoperto nell'organizzazione e di una precisa finalità di trattamento individuata dal Titolare o dal Responsabile del trattamento. Tali informazioni devono essere comunicate solo a soggetti legittimati, valutando lo strumento di comunicazione più appropriato messo a disposizione della Fondazione in quanto la loro diffusione può avere un rilevante impatto legale (per esempio, violazione della normativa in materia di protezione di dati personali), d'immagine e di competitività per la Fondazione.

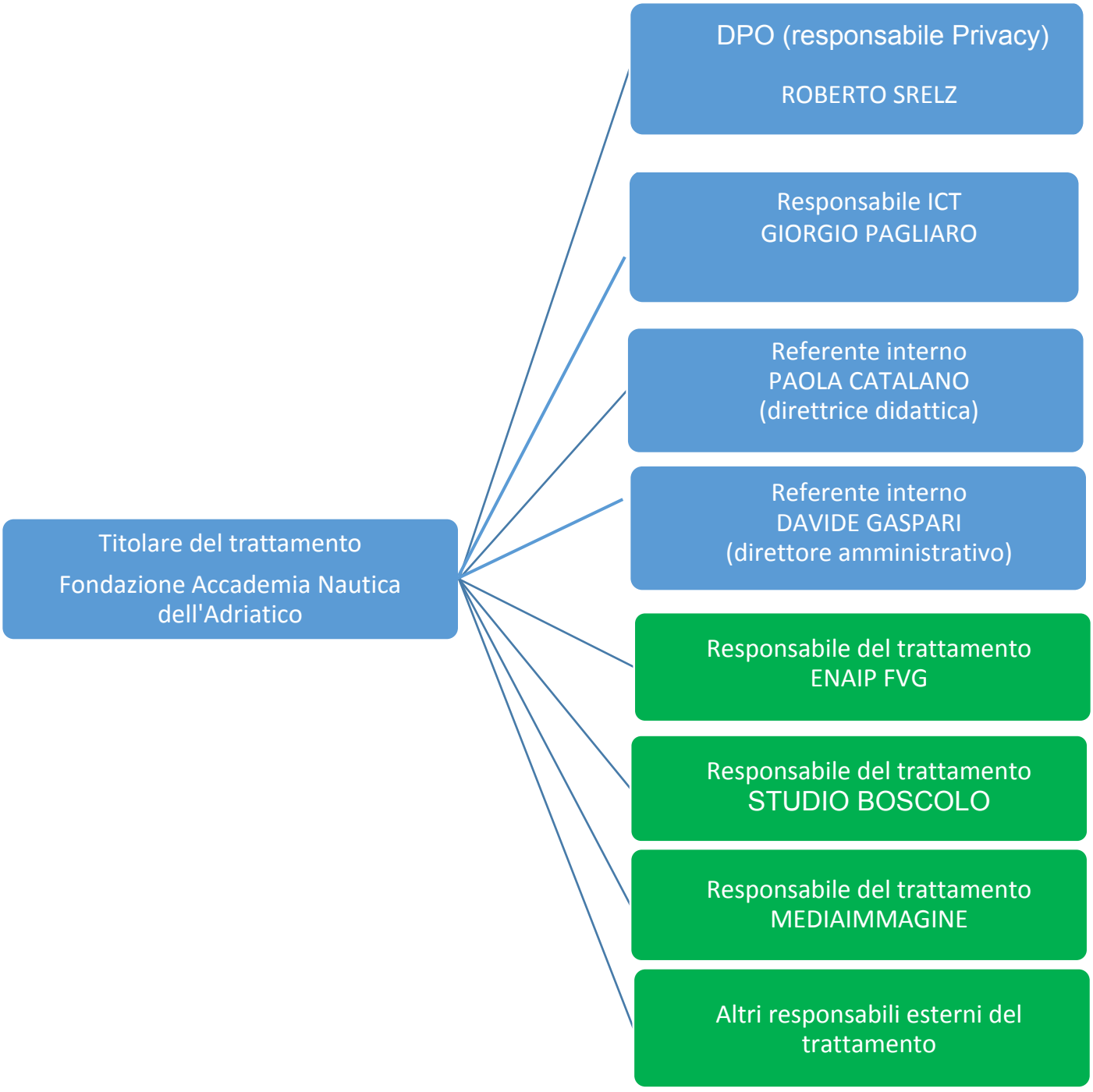
L'art. 35 del Reg. UE 2016/679 (GDPR) prevede che quando un tipo di trattamento, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare effettua una valutazione d'impatto (DPIA).

Si ritiene di non dover obbligatoriamente sottoporre a DPIA alcuna attività di trattamento attualmente realizzata dalla Fondazione Accademia Nautica dell'Adriatico, poiché in nessun caso sono soddisfatti almeno due criteri indicati dal WP29, e data la natura, oggetto, contesto e finalità del trattamento non si ritiene che tali attività possano comportare un rischio elevato per i diritti e le libertà dei soggetti interessati come riportato nel documento "ACCOUNTABILITY ASSESSMENT Valutazione DPIA" AA1 del 27/08/2019 rev. 10/04/2023.

2. MODELLO ORGANIZZATIVO DI RESPONSABILITÀ

Nell'ambito della conformità al GDPR e sulla base del proprio organigramma, la Fondazione ha definito e formalizzato un Modello Organizzativo di responsabilità finalizzato al corretto trattamento dei dati personali.

Il Modello Organizzativo identifica diversi Responsabili del trattamento, il Coordinatore Privacy, ed i referenti interni a cui sono state demandate le mansioni e monitoraggio dei processi interni in materia di protezione dei dati personali.



2.1. REFERENTI INTERNI E COORDINATORE PRIVACY

Ai referenti interni sono affidate le responsabilità come definite all'interno del seguente documento:

- ✓ Registro delle attività di trattamento

Il Registro identifica dettagliatamente il perimetro di responsabilità dei soggetti Referenti per i seguenti argomenti relativi il trattamento dei dati personali degli interessati:

- ✓ Categoria
- ✓ Modalità
- ✓ Operazioni
- ✓ Finalità
- ✓ Tipologia supporti
- ✓ Trasferimento verso paesi terzi
- ✓ Misure di sicurezza tecniche ed organizzative

Il trattamento sarà svolto in forma manuale e tramite elaborazione elettronica e digitale *(modalità di trattamento),* nel rispetto di quanto previsto dall'art. 32 del GDPR 2016/679 da parte di personale appositamente incaricato e potranno essere trattati anche da terzi in qualità di responsabili del trattamento appositamente individuati per le esigenze connesse all'adempimento delle finalità di gestione.

Ogni Referente interno è tenuto e si impegna a:

- ✓ trattare i dati personali solo sulla base alle indicazioni del presente regolamento, somministrando ai soggetti interessati le informative ed i moduli di consenso codificati nel Sistema di Gestione Qualità dell'Accademia Nautica dell'Adriatico nella versione più aggiornata;
- ✓ garantire che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
- ✓ adottare tutte le misure tecniche e organizzative necessarie al fine di garantire un livello di sicurezza adeguato al rischio;
- ✓ finalizzare gli accordi in materia di trattamento di dati personali ai sensi dell'art. 28 Reg. UE 2016/679 con i "Responsabili esterni" per l'affidamento di attività di trattamento di dati personali della struttura organizzativa interna di propria competenza secondo le indicazioni del Coordinatore Privacy e del Titolare;
- ✓ supervisionare le procedure di cancellazione dei dati personali al termine del loro periodo di conservazione indicate, sia in forma cartacea che elettronica; preoccupandosi di cancellare anche eventuali copie esistenti dopo che è terminata la prestazione dei servizi relativi al trattamento (su indicazione del Titolare del trattamento), notificando l'avvenuto buon esito al Coordinatore Privacy.
- ✓ mettere a disposizione del Coordinatore Privacy e del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto dei suoi obblighi nonché contribuire, se richiesto, alle attività di riesame interno e alle ispezioni realizzate dalle Autorità competenti
- ✓ rispettare, in ogni caso e al pari di ogni altro dipendente e collaboratore, le istruzioni indicate in specifici atti di autorizzazione, policies, regolamenti e procedure aziendali.

Il Coordinatore Privacy è tenuto e si impegna a:

- ✓ assistere il Titolare del trattamento nell'adozione di adeguate misure tecniche e organizzative, tenendo conto della natura del trattamento, coadiuvare il Titolare e gli uffici preposti al fine di soddisfare l'obbligo di dare seguito alle richieste per l'esercizio dei diritti dell'interessato (quali il diritto di accesso ai dati personali, il diritto di rettifica, il diritto di cancellazione, il diritto alla limitazione del trattamento, il diritto alla portabilità dei dati, il diritto di opposizione);
- ✓ assistere il Titolare del trattamento nel garantire il rispetto degli obblighi in materia di tutela della sicurezza dei dati, tenendo conto della natura del trattamento e delle informazioni a disposizione del Referente interno;
- ✓ mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto dei suoi obblighi, nonché contribuire alle attività di riesame interno e alle ispezioni realizzate dalle Autorità competenti
- ✓ rispettare, in ogni caso e al pari di ogni altro dipendente e collaboratore, le istruzioni indicate in specifici atti di autorizzazione, policies e procedure aziendali

2.2. RESPONSABILI ESTERNI DEL TRATTAMENTO DATI (DATA PROCESSOR)

Sono designati alcuni soggetti prestatori di servizi esternalizzati alla Fondazione come specialisti per la sicurezza (DPS) e Responsabili del trattamento dei dati personali per conto del Titolare del trattamento. Le istruzioni in merito alle modalità del trattamento dei dati personali realizzato per conto del Titolare sono formalizzate e sottoscritte tra le parti attraverso accordi in materia di trattamento dei dati personali ai sensi dell'art.28 Reg. UE 2016/679 GDPR. Il Responsabile del trattamento dovrà essere designato attraverso un contratto che dovrà essere redatto in forma scritta, anche in formato elettronico, e dovrà disciplinare, tra l'altro, i seguenti aspetti:

- ✓ durata del trattamento,
- ✓ la natura e la finalità del trattamento,
- ✓ il tipo di dati personali
- ✓ le categorie di interessati
- ✓ l'autorizzazione generale o specifica per ricorrere a sub-responsabili
- ✓ gli obblighi e i diritti del titolare del trattamento

A cura del Referente interno o di un suo delegato, dovrà essere mantenuto aggiornato il Registro delle attività di trattamento della Fondazione, nella parte dedicata ai Responsabili del trattamento.

2.3. INFRASTRUTTURA PER LA CONSERVAZIONE DATI PERSONALI

I dati personali degli interessati e tutti i documenti interni comprovanti la corretta applicazione delle disposizioni del GDPR sono mantenuti in formato elettronico nel Cloud Microsoft 365, SharePoint e Synology NAS Fileserver dopo l'iniziale elaborazione / trattamento all'interno dei supporti di memorizzazione (HD) degli endpoint computer assegnati agli operatori (notebook, desktop computer, all-in-one computer, …).

La struttura delle cartelle (directory) è definita nella procedura del Sistema di Gestione certificato ISO9001:2015 identificata come FAN(2019)-05 "Gestione Documenti e Dati"

2.4 PERIODO DI CONSERVAZIONE DATI

È stabilito un termine per la cancellazione / eliminazione dei dati personali dal momento della loro acquisizione salvo che le finalità perseguite per lo specifico trattamento possano essere conseguite entro un periodo di tempo diverso ovvero sia diversamente stabilito dalla Legge.

Con periodicità triennale i Referenti interni provvederanno all'identificazione dei dati non necessari oppure che superano il termine di conservazione in modo da attivare il processo di cancellazione /eliminazione, sulla base delle procedure e misure tecniche sviluppate e adottate dal Titolare.

III. POLICY DI COMPORTAMENTO

3.1. PRINCIPI GENERALI DEL TRATTAMENTO

Il trattamento di dati personali rappresenta qualunque operazione o sequenza di operazioni attuate su un dato di una persona fisica anche senza l'ausilio di strumenti elettronici.

3.2 GESTIONE DEI LOCALI E DELLE RISORSE

Tutti i locali e tutte le risorse messe a disposizione dalla Fondazione devono essere utilizzati e custoditi con la massima diligenza al fine di garantire un'efficiente conduzione dell'attività lavorativa ed un adeguato livello di sicurezza delle informazioni applicando il presente regolamento interno.

3.2 ACCESSO AGLI UFFICI ED AREE PROTETTE

L'accesso agli uffici, alle aree riservate ed agli archivi cartacei, è permesso ai soggetti autorizzati in base a precise e motivate esigenze lavorative.

I visitatori, gli ospiti di vario genere e gli allievi dovranno essere adeguatamente istruiti dal personale autorizzato in merito alle caratteristiche dell'ambiente, ai rischi presenti, alle norme comportamentali previste e alle procedure da attuare per prevenire o gestire situazioni di emergenza e di rischio.

3.3. RIPRESE VIDEO-AUDIO-FOTOGRAFICHE

Qualsiasi ripresa video-audio-fotografica deve essere realizzata rispettando i diritti delle singole persone coinvolte.

Soggetti interni: per ragioni connesse alla propria attività lavorativa le riprese video-audio-fotografiche devono essere autorizzate dal proprio Referente interno. Tali riprese possono essere utilizzate esclusivamente per finalità lavorative e non possono essere divulgate al di fuori del contesto istituzionale in cui sono state realizzate.

Al di fuori di questa casistica non è consentito effettuare riprese video-audio-fotografiche in qualunque area delle sedi operative della Fondazione salvo esplicita autorizzazione scritta.

I Soggetti interni potranno essere fotografati e/o ripresi in occasione di eventi, seminari e momenti di formazione. In questi casi, le immagini e le riprese potranno essere utilizzate per scopi e comunicazioni istituzionali.

Soggetti esterni: non è consentito effettuare riprese video-audio-fotografiche in qualunque area delle sedi operative della Fondazione salvo esplicita autorizzazione scritta. Il soggetto interno referente della visita è tenuto a far rispettare queste prescrizioni.

3.4 POSTAZIONI DI LAVORO

L'utilizzo della postazione di lavoro e il conseguente accesso ai documenti, atti e archivi è consentito nei limiti della propria funzione e dei propri incarichi.

La propria scrivania deve essere mantenuta in ordine, verificando di non lasciare documenti e atti riservati senza un proprio controllo all'accesso di terzi, in momenti di pausa, terminata la giornata di lavoro e/o in periodi di assenza.

3.5 MISURE FISICHE DI CUSTODIA DI DOCUMENTI E ATTI CARTACEI

I dati ed i supporti cartacei necessari per lo svolgimento delle mansioni lavorative devono essere custoditi in armadi o cassettiere del contesto organizzativo in cui si opera. I documenti dovranno essere riposti correttamente durante i periodi di temporanea assenza ed al termine dell'attività lavorativa negli appositi archivi.

Gli archivi di documenti e atti contenenti dati sensibili dovranno essere custoditi in armadi chiusi a chiave oppure in alternativa dovranno essere chiusi a chiave i locali contenenti gli archivi.

L'eliminazione fisica di ogni documento cartaceo o supporto informatico contenente dati e informazioni aziendali e/o personali deve essere effettuata solo utilizzando gli appositi strumenti distruggi documenti messi a disposizione.

Non devono essere lasciati documenti incustoditi presso i dispositivi di stampa o copia.

3.6 GESTIONE DEI DATI PERSONALI E AZIENDALI

Ogni soggetto è responsabile dei dati e delle informazioni delle quali entra in possesso per lo svolgimento della sua attività lavorativa. Deve quindi trattare i dati e le informazioni adottando ogni idonea misura di sicurezza al fine di tutelarne la riservatezza, la sicurezza, l'integrità ed il corretto utilizzo.

I dati e le informazioni potranno essere comunicate a terze parti esclusivamente nell'ambito della propria funzione e secondo le finalità connesse alla propria attività lavorativa.

È vietata la comunicazione di dati e informazioni verso terzi che possano arrecare danno all'immagine, alla reputazione, alla produttività, alla proprietà intellettuale e del know-how o che possano violare i vincoli contrattuali e di legge connessi al rapporto di lavoro.

È assolutamente vietata la divulgazione a terzi di informazioni riservate, confidenziali o comunque di proprietà del Titolare. In caso di violazione, il Titolare si riserva di avviare i relativi provvedimenti disciplinari, nonché le azioni civili e penali consentite.

Si ricorda, inoltre, che la diffusione illecita di dati e informazioni potrebbe configurare, oltre alla violazione del presente regolamento, la violazione di norme con conseguenze sia civili che penali a carico del responsabile dell'illecita diffusione, nonché come violazione della normativa che regola il rapporto di lavoro.

3.7 STRUMENTI INFORMATICI

L'utilizzo degli strumenti informatici in dotazione è di carattere professionale. In deroga a tale principio la Fondazione autorizza un moderato e ragionevole utilizzo privato. Tale utilizzo deve essere limitato ed ispirato a criteri di buon senso e non dovrà ostacolare l'utilizzo professionale. Lo spazio dello strumento affidato utilizzato a fini "privati" (ad esempio dislocazione di file dati, foto o filmati), dovrà perciò essere limitato, ben identificato e non dovrà precludere e limitare quello dedicato all'utilizzo professionale.

Tutti gli strumenti dovranno essere bloccati e protetti da password, se lasciati incustoditi.

Gli strumenti dovranno essere spenti o messi in modalità a basso consumo se non usati per più di un'ora, a meno di motivate esigenze tecniche o di manutenzione.

3.8 CUSTODIA DEGLI STRUMENTI INFORMATICI

Gli strumenti informatici di proprietà della Fondazione devono essere custoditi dall'utilizzatore con cura e diligenza prevenendo possibili danneggiamenti che ne compromettano il corretto funzionamento ed evitando di lasciarli incustoditi in ambienti pubblici.

In caso di furto o danneggiamento di beni, l'utilizzatore dovrà informare immediatamente il servizio helpdesk@accademianautica.it e presentare formale denuncia alle autorità di pubblica sicurezza e inviarne copia al servizio helpdesk@accademianautica.it sopra menzionato per l'attivazione degli atti formali di scarico e di attivazione eventuali coperture assicurative esistenti.

3.9 GESTIONE DELLE CREDENZIALI DI ACCESSO E DELLE PASSWORD

Le credenziali di autenticazione per l'accesso alla rete e per altri servizi vengono assegnate all'utilizzatore e sono modificabili dallo stesso consistono in un username ed una password riservata che dovrà venir custodita dall'utilizzatore con la massima diligenza e non divulgata.

Ogni utilizzatore è responsabile della sicurezza e di qualunque operazione effettuata utilizzando le proprie credenziali. È proibito accedere alla rete e ai programmi con credenziali diverse dalle proprie o in maniera anonima.

Le password devono essere gestite in modalità sicura in base alla policy definita dalla Fondazione Accademia Nautica all'interno dell'ambiente Microsoft 365 in dotazione.

3.10 GESTIONE E PROTEZIONE DEI DATI

L'accesso ai dati è consentito nei limiti della propria funzione organizzativa e della propria attività lavorativa. I dischi di rete presenti sui server interni e nel Cloud sono a disposizione della Fondazione e sono aree di condivisione di informazioni professionali / lavorative e non possono in alcun modo essere utilizzate per scopi diversi.

Qualunque file che non sia inerente all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità vengono svolte regolari attività di controllo, amministrazione, backup e mirroring dei dati in ambiente Cloud.

Si ricorda che i dischi locali installati su notebook o personal computer non sono soggetti ad operazioni di backup, la responsabilità del salvataggio dei dati ivi contenuti è pertanto a carico del singolo utilizzatore attraverso l'uso delle aree disponibili nel Cloud della Fondazione.

Gli utilizzatori che trattengono dati di Fondazione su supporti quali memorie USB o dischi locali per i quali non è previsto backup, sono responsabili del salvataggio degli stessi e di eventuali danni alla Fondazione o a terzi anche di natura civilistica causati dalla loro perdita o sottrazione.

L'utilizzo a qualsiasi titolo di memorie rimovibili (ad esempio) USB e di servizi Cloud diversi da Microsoft 365 di Accademia è potenziale fonte di minacce informatiche, per tanto è sconsigliato, limitato o impedito su notebook o personal computer in uso presso le sedi della Fondazione.

È vietato il salvataggio di dati e informazioni di carattere aziendale in sistemi di Cloud pubblica (Dropbox, GoogleDrive, ecc.) non esplicitamente autorizzati in forma scritta dall' Amministratore di Sistema (Responsabile ICT).

3.11 GESTIONE DELLA POSTA ELETTRONICA

L'assegnazione di una casella di posta elettronica (@accademianautica.it e .com) è di carattere professionale. In deroga a tale principio è consentito un moderato e ragionevole utilizzo privato.

La Fondazione, prevede che ad ogni messaggio in uscita sia automaticamente aggiunto un breve testo di avviso al ricevente della natura potenzialmente riservata del messaggio.

Gli utilizzatori dell'e-mail della Fondazione sono responsabili dell'utilizzo della stessa e devono mantenere un corretto comportamento nell'utilizzo della posta elettronica. In particolare, i soggetti devono seguire le seguenti disposizioni:

- ✓ non inviare né conservare messaggi di posta elettronica e/o allegati dal contenuto offensivo, molesto, volgare, blasfemo, xenofobo, razziale, pornografico o comunque inappropriato o illegale;
- ✓ prestare la massima attenzione nell'inoltro di e-mail riportanti contenuti e indirizzi e-mail di precedenti comunicazioni;
- ✓ prestare la massima attenzione ad e-mail sospette, avvisando l'Amministratore di Sistema (Responsabile ICT) in caso di dubbi sulla provenienza/contenuto delle stesse;
- ✓ creare una sezione denominata "Posta personale" all'interno della propria casella di posta, alla quale gli Amministratori di Sistema non potranno accedere se non per gravi motivi di sicurezza informatica.

Per motivi di sicurezza informatica ed in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, l'accesso alla casella di posta dell'utilizzatore potrà essere gestita dagli Amministratore di Sistema (Responsabile ICT) su richiesta del Coordinatore Privacy al fine di verificare il contenuto dei messaggi e ad inoltrare al Titolare del Trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa.

La Posta Elettronica Certificata (PEC) può essere utilizzata dalle persone specificatamente autorizzate solamente per motivi professionali.

3.12 UTILIZZO DELLA NAVIGAZIONE INTERNET

L'accesso a Internet è fornito principalmente per scopo professionale, per accedere a informazioni e contenuti necessari allo svolgimento dell'attività lavorativa. Essendo uno strumento di lavoro, gli utilizzatori cui si attribuisce l'accesso, sono responsabili del suo corretto utilizzo. Analogamente a quanto avviene per la posta elettronica, è consentito un moderato e ragionevole utilizzo privato, limitato ed ispirato a criteri di buon senso senza ostacoli all'attività professionale.

Il numero e la durata degli accessi a Internet possono essere registrati. La consultazione di tali registrazioni può avvenire solo in forma anonima e aggregata salvo i casi previsti dalla legge e dal mancato rispetto del presente regolamento interno. Gli eventuali controlli compiuti dagli Amministratori di Sistema potranno avvenire mediante un sistema di analisi dei file giornale. Gli utilizzatori devono seguire le seguenti regole di navigazione della rete Internet:

- ✓ è tassativamente vietato scaricare materiale e programmi in violazione della legislazione sui diritti di autore, che siano essi appartenenti a persone o aziende, coperti da copyright,

brevetto o proprietà intellettuale, ivi compresa l'installazione o la distribuzione di software che non sia specificatamente licenziato per essere utilizzato all'interno della Fondazione;

- ✓ è tassativamente vietato navigare siti e scaricare materiale pericoloso/vietato o avente contenuti illegali (contenuto offensivo, molesto, volgare, blasfemo, xenofobo, razziale, pornografico, pedopornografico, terrorismo o comunque inappropriato o illegale);
- ✓ è vietato effettuare copia non autorizzata di materiale coperto da copyright compreso ma non limitato a digitalizzazione e distribuzione di foto da riviste, libri o altre fonti, musica o materiale video;
- ✓ è vietato utilizzare l'infrastruttura tecnologica di Fondazione per procurarsi e diffondere materiale in violazione con le normative vigenti;
- ✓ è vietato effettuare attività che possano generare dei problemi di sicurezza o danneggiare le comunicazioni sulla rete;
- ✓ è vietato eseguire qualsiasi forma di monitoraggio della rete che permetta di catturare dati non espressamente inviati all' host dell'utilizzatore (sniffing) a meno che questa attività non faccia parte dei compiti dell'utilizzatore e quindi formalmente autorizzata dagli amministratori di sistema, anche a fini didattici;
- ✓ è vietato aggirare le procedure di autenticazione o la sicurezza di qualunque host, rete, account.

3.13. ACCESSO INTERNET PER UTILIZZATORI ESTERNI

È previsto un sistema per consentire l'accesso e la navigazione in Internet sicuri ad utilizzatori esterni che non abbiano a disposizione le credenziali Microsoft 365 di Accademia Nautica. Il numero, la durata degli accessi ad Internet e le quantità di dati (non la natura, la provenienza o destinazione o qualità degli stessi) scambiate sono costantemente registrate nel rispetto della vigente normativa applicabile, con particolare riguardo al Reg. UE 2016/679. La registrazione viene mantenuta solo per lo stretto tempo necessario a garantire la sicurezza.

3.14. COMUNICAZIONE DI DATI E INFORMAZIONI ATTRAVERSO SOCIAL MEDIA

È vietato pubblicare in internet attraverso Social media, forum, chat, blog, siti internet, dati ed informazioni di carattere aziendale (informazioni, documenti, appunti, commenti personali o di terzi, foto, video, audio, ecc..) che possano arrecare danno all'immagine, alla reputazione, alla produttività, alla proprietà intellettuale e del know-how o che possano violare i vincoli contrattuali e di legge connessi al rapporto di lavoro.

È consentita la divulgazione di informazioni già rese pubbliche dalla Fondazione.

3.15. SISTEMI DI MONITORAGGIO RETE AZIENDALE

Per motivi di sicurezza del sistema informatico, per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, ecc.) o per finalità di controllo e programmazione dei costi aziendali (ad esempio, verifica costi di connessione ad Internet, traffico telefonico, ecc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà del Titolare, per il tramite dell' Amministratore di Sistema (Responsabile ICT) e

nel rispetto del Regolamento UE 2016/679 (GDPR), accedere direttamente a tutti gli strumenti informatici della Fondazione.

Periodicamente e in presenza di anomalie, l'Amministratore di Sistema (Responsabile ICT) effettua verifiche di funzionalità approfondite che potranno determinare segnalazioni ed avvisi generalizzati diretti agli utilizzatori della funzione organizzativa in cui è stata rilevata l'anomalia stessa e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

Controlli su base individuale potranno essere compiuti solo in caso di successive ulteriori anomalie.

Gli Amministratori di Sistema e gli specialisti della sicurezza incaricati (DPS) effettuano inoltre forme di controllo di carattere impersonale sulla rete e su tutti i dispositivi che la compongono.

In nessun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

La Fondazione è tenuta comunque a denunciare all'autorità giudiziaria tutti i comportamenti contrari alla legge, anche rilevati da analisi di tipo impersonale.

3.16. UTILIZZO DELLA FIRMA DIGITALE

La Firma Digitale deve essere utilizzata esclusivamente dal titolare della firma o da chi delegato.

3.17. UTILIZZO DELLA PEC – POSTA ELETTRONICA CERTIFICATA

La posta elettronica certificata è un e-mail che garantisce ora e data di spedizione e di ricezione, provenienza ed integrità del contenuto. La PEC consente di inviare e ricevere messaggi con lo stesso valore legale di una raccomandata con avviso di ricevimento.

Il limite della PEC è quello di non poter dimostrare il testo di eventuali allegati ma solo la loro presenza (salvo che questi siano stati firmati con la firma elettronica).

La PEC deve essere utilizzata esclusivamente dal titolare o da chi delegato che dovrà attenersi alle seguenti disposizioni:

- ✓ verificare sempre che la casella di PEC sia sufficientemente capiente;
- ✓ non eccedere i limiti dimensionali del messaggio inviato, ci sono limiti definiti dal gestore che fornisce il servizio ad Accademia;
- ✓ non cancellare per nessun motivo nessuno dei messaggi in entrata o in uscita.
- ✓ le PEC di Accademia non può essere utilizzata per comunicazioni e affari privati e/o personali.

Non è corretta la conservazione delle Pec secondo le seguenti forme:

- ✓ l'archiviazione delle PEC nel proprio computer, non è garantito il valore legale in quanto non si è in presenza di conservazione a norma se non sono rispettati i requisiti di legge;
- ✓ la stampa su carta e l'archiviazione fisica del documento. La tradizionale conservazione della stampa del documento PEC non garantisce la conformità all'originale informatico.

3.18. PERDITA DELLE CONDIZIONI DI PERSONA AUTORIZZATA AL TRATTAMENTO

In caso di perdita delle condizioni di Persona autorizzata al Trattamento dati o di cessazione del rapporto con la Fondazione, valgono le seguenti regole operative:

- ✓ le credenziali per l'accesso ai sistemi e alla posta elettronica vengono disattivate;
- ✓ è facoltà della Fondazione effettuare eventuali operazioni di conservazione di e-mail di carattere professionale di utilizzatori non più appartenenti all'organizzazione;
- ✓ le e-mail nella "Posta personale" saranno, al contrario, cancellate.

Tali attività sono effettuate dall'Amministratore di Sistema (Responsabile ICT) autorizzato alla gestione della posta elettronica, che potranno pertanto avere accesso, per esclusive ragioni di carattere tecnico e solo ove non sia evitabile, a dati personali conservati all'interno delle caselle di posta.

3.19. RESPONSABILITÀ E SANZIONI

È fatto obbligo a tutti i Soggetti interni ed utilizzatori dei sistemi informatici della Fondazione di osservare le disposizioni portate a conoscenza con il presente regolamento interno.

Il mancato rispetto o la violazione del presente regolamento è perseguibile e con provvedimenti disciplinari da parte della Direzione della Fondazione, nonché con tutte le azioni civili e penali consentite.

Chiunque non rispetti il presente Regolamento potrà essere soggetto all'immediata sospensione dell'accesso agli strumenti informatici.

3.20. AGGIORNAMENTO E REVISIONE REGOLAMENTO INTERNO

Il presente regolamento è soggetto a revisione periodica, che potrà avvenire a seguito di cambiamenti organizzativi e normativi o necessità istituzionali. Tutte le future modifiche al presente regolamento verranno opportunamente comunicate agli utilizzatori interni attraverso comunicazione tramite e-mail e se necessario rese pubbliche sul sito internet www.accademinautica.it

4.0 CENNI DI CYBERSECURITY

La maggior parte degli incidenti è legata ad errori umani. Il fattore umano è, di fatto, l'anello debole della sicurezza informatica. Solo in Italia si è stimato che il 53% degli incidenti sono dovuti a cause endogene (password deboli, uso di strumenti aziendali con connessioni pubbliche, navigazione in siti non sicuri, trasporto di dati confidenziali su memorie USB, ecc.), a cui devono sommarsi i tentativi di ***phishing,*** che aumentano sempre più.

Nel 2017 almeno il 45% delle aziende italiane sono state colpite da attacchi informatici, per un danno stimato di circa 10 miliardi di euro. Di questi attacchi, la maggior parte sono stati causati da persone interne all'azienda in modo accidentale, a causa dell'uso scorretto degli strumenti aziendali o della scarsa attenzione e consapevolezza in merito ai rischi.

Dal 2018 a oggi, gli attacchi con impatto significativo sono aumentati del 38% mediamente ogni anno. Nel 2018 la media era di **129 attacchi gravi** avvenuti con successo **ogni mese**. Il numero di casi censiti, orientati a finalità di cybercrime e furto di dati personali, è aumentato del 99% rispetto al 2017 (Fonte: Rapporto Clusit 2019). Nel 2022, il numero di cyberattacchi è stato di 1 ogni 39 secondi, con il **95% delle violazioni effettive dovuto a errore umano** e misure di sicurezza insufficienti. Il rapporto IBM-Ponemon Institute 2019 sui **costi di un *data breach*** mostrava che un incidente informatico da cui derivi una violazione di dati personali costa ad un'azienda circa €150 per ogni record compromesso, con una media di circa 22.600 record compromessi per ogni violazione grave; **nel 2025 la previsione attuale indica un costo complessivo a livello mondiale di 5 mila miliardi euro**. Spesso si parla di "incidenti informatici". Il termine incidente lascia pensare ad una casualità, ma è bene non lasciarsi ingannare, poiché non c'è nulla di casuale. L'industria del cybercrime rimane una minaccia concreta e reale, molto più reale e vicina di quanto si possa immaginare, a causa della sua natura subdola. La principale difesa contro gli attacchi informatici è la consapevolezza delle proprie azioni quando ci si trova ad operare in situazioni esposte a rischi, come l'uso di Internet, dei dispositivi mobili o della posta elettronica.

Non abbiate mai paura di segnalare dubbi o episodi che possano mettere a rischio la sicurezza delle informazioni. La sicurezza informatica delle imprese è fatta di persone **competenti, consapevoli e proattive**.

Nei paragrafi successivi saranno introdotte alcune brevi nozioni riguardanti le principali minacce informatiche ed alcuni consigli per difendersi.

4.1: LE PIÙ COMUNI MINACCE INFORMATICHE

Gli attacchi informatici più comuni e più frequenti avvengono tramite l'utilizzo della posta elettronica e di internet, e consistono nelle seguenti categorie di attacco:

1. **Phishing**: tentativo di truffa veicolato tramite email con il quale l'attaccante cerca di ingannare la vittima facendo pressioni psicologiche o fingendosi una persona o ente conosciuto. Spesso le email di phishing inducono la vittima a scaricare file contenenti software malevolo con cui compromettere i sistemi aziendali. Il phishing rientra nelle tecniche di c.d. "**social engineering**", lo sfruttamento di vulnerabilità umane (vanità, avidità, curiosità, altruismo, paura, ecc.), mirate a spingere le persone a fornire informazioni personali o particolarmente confidenziali, al fine di ottenere accesso ad account bancari o aziendali.
2. **Malware**: software malevolo solitamente contenuto in file allegati ad email o in file scaricati dal web che nei casi peggiori può rendere inutilizzabili tutti i dati contenuti nei server aziendali o essere la via d'ingresso per attacchi successivi all'infrastruttura dell'organizzazione.

Il **phishing** è probabilmente la tecnica di attacco più diffusa al mondo, e per questo motivo anche la più insidiosa. Le email di **phishing** sono sempre più sofisticate, e può anche capitare che l'attacco sia mirato ad una specifica persona, utilizzando dati veritieri con cui manipolare il destinatario, spesso acquisiti attingendo da database compromessi.

Nel 2018 si sono registrare numerose campagne di **phishing**, che rimane il primo vettore di diffusione dei malware. Si stima che circa il 50% degli utenti Internet riceva almeno una mail di phishing al giorno, e di questi, il 25% ne cade vittima, compromettendo la sicurezza dei sistemi aziendali ai quali accede. Nel 2022, le vittime di attacchi phishing che hanno effettivamente causato danni, nei soli Stati Uniti, sono state **300mila**.

4.2: COME DIFENDERSI DAL PHISHING E DAL SOCIAL ENGINEERING

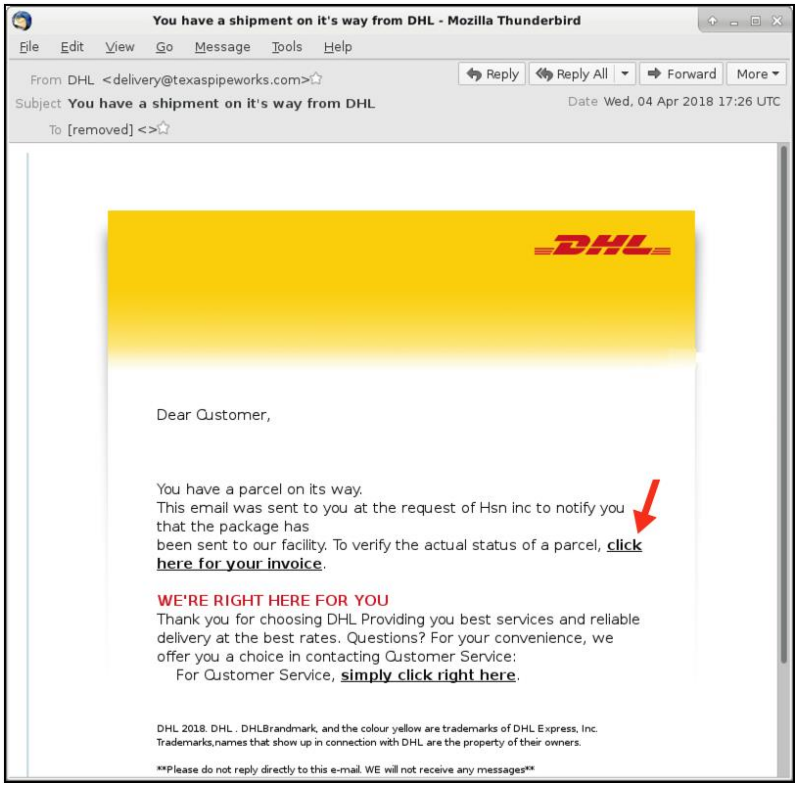
Difendersi dai tentativi di **phishing** è più insidioso di quanto possa sembrare. Alcuni tentativi di phishing possono risultare molto semplici da individuare, mentre altri, più mirati e meglio architettati, possono risultare assolutamente veritieri.

Solitamente le email di phishing **colgono di sorpresa l'utente**, con notizie inaspettate ad **elevato contenuto destabilizzante**. Se l'email ricevuta è completamente inaspettata, è presumibile ritenere che sia un tentativo di phishing.

Per ottenere successo, il phishing sfrutta principalmente tre fattori umani: **curiosità**, **paura**, **fretta**.

Per difendersi è necessario prestare la massima attenzione ai seguenti elementi:

1. Verificare sempre il mittente: spesso le email di phishing cercano di riprodurre indirizzi di mittenti ritenuti affidabili
2. Non aprire mai un link o un allegato immediatamente: la fretta è il nostro peggior nemico
3. Leggere attentamente il contenuto: le email di phishing sono spesso prodotte in modo industrializzato con l'utilizzo di traduttori automatici, e spesso contengono errori facilmente riconoscibili
4. Diffidare sempre dalle email con contenuti che incitano all'urgenza o che destano paura: solitamente le email di phishing sono strutturate in modo da spingere il destinatario a cliccare su link o scaricare allegati con il pretesto di scadenze immediate o eventi avversi nel caso in cui non si proceda
5. In caso di sospetti sulla legittimità della email, è bene accedere al sito interessato digitando manualmente nel browser il suo indirizzo, piuttosto che fare click su link presenti nel messaggio di posta elettronica
6. Anche se il messaggio proviene da una fonte affidabile, non è detto che sia sicuro. Le email **non sono un mezzo di comunicazione sicuro** e possono essere violate facilmente. In caso di dubbio, confrontatevi sempre con il mittente per valutare la veridicità del contenuto del messaggio
7. Fare attenzione a pubblicare informazioni relative al proprio lavoro su social network, poiché potrebbero essere utilizzate per mettere in atto tentativi di phishing mirati

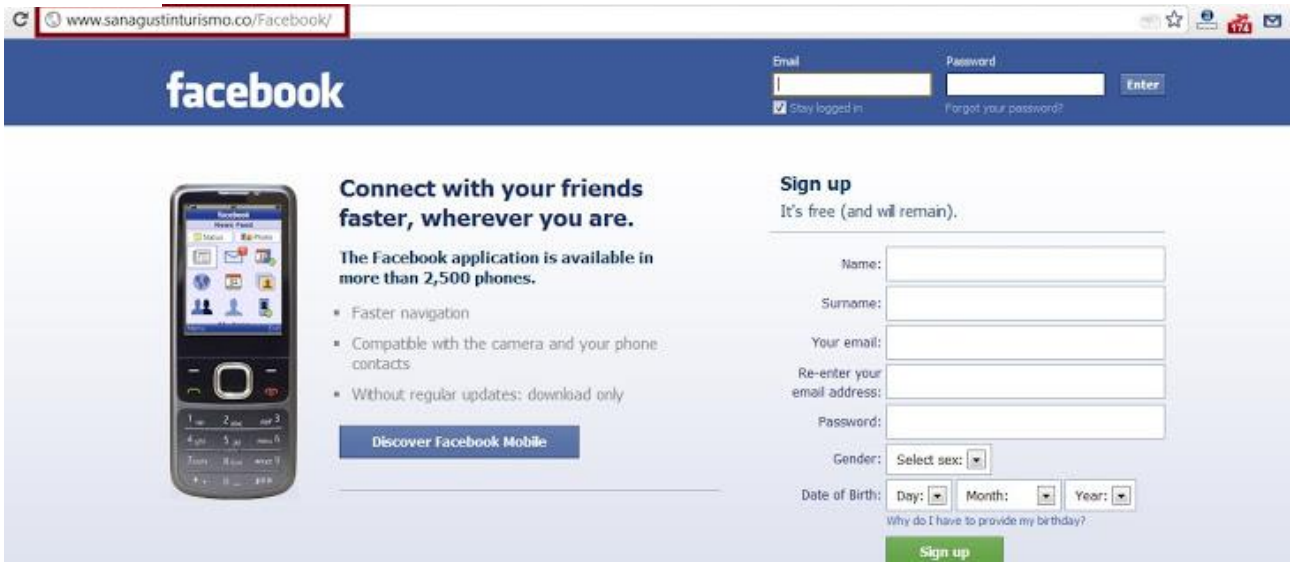


Tentativo di phishing con finta email DHL (l'indirizzo email del mittente è chiaramente non relativo a DHL) che induce il destinatario a cliccare su link e scaricare un file infetto – Fonte: www.cert-pa.it

Le email non sono l'unico strumento con cui veicolare tentativi di phishing.

Spesso all'interno delle email, che pur essendo realizzate da attaccanti malevoli possono essere del tutto innocue, sono contenuti link a siti web fittizi che assomigliano in tutto e per tutto al sito reale, in modo da convincere il destinatario ad inserire i propri dati personali, che saranno intercettati dall'attaccante.

Spesso il sito web è registrato con un nome di dominio molto simile a quello originale, e grazie all'utilizzo di caratteri ingannevoli è possibile rendere molto difficoltosa l'identificazione del sito fittizio a prima vista.



Nell'immagine un esempio banale di phishing attraverso un sito web che riproduce accuratamente la homepage di Facebook. Lo scopo dell'attaccante in questo caso è rubare le credenziali di accesso dell'utente, in modo da utilizzarle per accedere a servizi importanti, come gli account bancari o di servizi di pagamento, nel caso in cui la vittima abbia riutilizzato la stessa password.

Il **phishing** è soltanto uno strumento di attuazione di tecniche di **social engineering.**

Il social engineering è una tecnica umana e non qualcosa di fisico che può essere rimosso dal computer o evitato con l'uso di software di sicurezza. Un esempio "arcaico" di social engineering sono i malintenzionati che si spacciano per tecnici della distribuzione elettrica o del telefono per entrare nelle case delle vittime.

L'unico modo per prevenire il social engineering è essere consapevoli della sua esistenza anche su Internet e cercare di non cadere vittima di truffe.

Una forma particolare di **social engineering** è quella del "**CEO Fraud**", un tipo di truffa in cui i cybercriminali, attraverso infezioni malware o altre tecniche di social engineering, riescono ad impersonare i vertici aziendali per indurre i dipendenti, spesso dell'ufficio finance/amministrazione, ad effettuare trasferimenti di denaro sui loro conti.

Le vittime predilette di questi truffatori sono le piccole e medie aziende, in cui spesso manca una vera e propria consapevolezza di queste minacce.

Un eclatante caso di **CEO Fraud** in Italia ha riguardato un dirigente di Confindustria che, con una banalissima mail, è stato spinto a fare un bonifico di mezzo milione di euro su un conto sconosciuto, pensando che gli fosse stato chiesto dalla Direttrice generale, la cui email era stata compromessa. Il dirigente fu purtroppo licenziato in tronco ed i soldi mai recuperati.

4.3: COME PREVENIRE LE INFEZIONI MALWARE

La consapevolezza delle proprie azioni aiuta anche prevenire possibili infezioni malware che potrebbero causare danni disastrosi all'infrastruttura informatica aziendale.

Per quanto riguarda l'uso di internet e della posta elettronica, valgono le stesse raccomandazioni del paragrafo precedente, tuttavia, è bene utilizzare alcune altre accortezze per prevenire il rischio di un'infezione malware:

1. Evitare di scaricare **file eseguibili o allegati** provenienti da fonti non attendibili.
2. Non utilizzare dispositivi portatili sconosciuti, come ad esempio chiavette USB non identificate
3. Evitare di utilizzare email e dispositivi aziendali per scopi personali
4. Prestare attenzione a falsi avvisi (pop-up) di sicurezza: alcuni software malevoli possono veicolare messaggi simili a quelli degli antivirus, col solo scopo di installare software malevolo sul pc dell'utente
5. Non utilizzare smartphone personali privi di protezione antivirus per accedere alla rete aziendale

Gli allegati malevoli sono indubbiamente il metodo più diffuso e meno costoso di diffusione di malware. Il formato più utilizzato (47%) è il **documento Word (.doc),** seguito (17%) dal **documento Excel (.xls).** I documenti Office sono molto efficaci come mezzo d'infezione malware, poiché è semplice nascondere **macro** con codice malevolo, che si attiva quando l'utente attiva la macro.

5. DEFINIZIONI

Di seguito sono riportate le principali definizioni indicate dal GDPR:

Dato personale: qualsiasi informazione che identifica o rende identificabile una persona fisica e che può fornire dettagli sulle sue caratteristiche fisiche, fisiologiche, genetiche o psichiche, sulle sue abitudini, sul suo stile di vita, sulle sue relazioni personali, sul suo stato di salute o sulla sua situazione economica.

Dati identificativi: dati personali che permettono l'identificazione diretta di una persona fisica.

Dati appartenenti a categorie particolari: dati personali idonei a rivelare lo stato di salute (attinenti alla salute fisica o mentale, compresa la prestazione di servizi di assistenza sanitaria) e la vita sessuale, l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale di una persona fisica.

Dati genetici: dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla sua fisiologia o salute.

Dati biometrici: dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica e che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.

Dati giudiziari: dati idonei a rilevare informazioni riguardo provvedimenti in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.

Trattamento di dati personali: qualsiasi operazione compiuta con o senza l'ausilio di processi automatizzati e applicata a dati personali, o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento, 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.

Profilazione: qualsiasi forma di trattamento automatizzato di dati personali che consiste nell'utilizzo di tali dati per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica.

Pseudonimizzazione: trattamento dei dati personali effettuato in modo tale che tali dati non possano più essere attribuibili ad un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che i dati personali non siano attribuibili a una persona fisica identificata o identificabile.

Comunicazione di dati personali: dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, in base ad una precisa finalità ed una modalità certa e sicura di trattamento, anche mediante la loro messa a disposizione o consultazione.

Diffusione di dati personali: dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

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

Persona autorizzata al trattamento: persona fisica autorizzata a compiere operazioni di trattamento dati sotto la diretta autorità del titolare del trattamento e sulla base di precise istruzioni fornite con Regolamenti, policies e procedure adottati dal Titolare

Amministratore del Sistema Informatico (Responsabile ICT): persona fisica nominata dal Titolare e preposta alla gestione e sicurezza dei sistemi informativi attraverso l'applicazione delle misure necessarie al mantenimento della riservatezza, disponibilità e integrità del dato personale trattato nei sistemi informativi in conformità al presente Regolamento. **Data Protection Specialist** (Coordinatore Privacy): persona fisica nominata dal Titolare che ricopre il ruolo di consulente tecnico dello stesso e del Responsabile ICT in materia di politiche di sicurezza e GDPR

Strumenti informatici: stampanti, laptop, computer da tavolo, telefoni fissi, smartphone, tablet, e-book reader, telecamere IP, e, in generale, qualsiasi dispositivo in grado di connettersi a una rete IP.

Data Center: locale ad accesso limitato che ospita i server, i sistemi di calcolo e i dispositivi di networking, oltre che i sistemi di storage su cui sono residenti i dati.

Cloud Pubblica: modello di conservazione dati su computer in rete dove i dati stessi sono memorizzati su molteplici server virtuali generalmente ospitati presso strutture di terze parti o su server dedicati.

INFORMAZIONI DOCUMENTO

Data ultimo aggiornamento	Revisione	ID	Descrizione
16/06/2026	**9**	**FAN(2018)10**	Regolamento interno per la protezione dei dati personali nel rispetto del Reg. UE 2016/679.

Preparato	Verificato	Autorizzato	
R.Srelz	R.Srelz	S.Beduschi	

Data di prima adozione e distribuzione nell'organizzazione	25/05/2018