FRANCESCO PISANI & FIGLI S.P.A

Produzione Cartone Ondulato Scatolificio

03033 Arpino (FR) - S.S. 82 Valle del Uri - km. 66,200

tel. 0776882272 info@pisaniscatolificio.it

MANUALE DELLA. PRIVACY

Conforme al Decreto Legislativo del 3 giugno 2003, n. 196 (cosiddetto "Codice sulla privacy") e, in particolare, al nuovo Regolamento Europeo n. 2016/679

Revisione n. 5 del 31.01.2022

SOMMARIO

Allegati al Manuale

A) Regole per l'adozione delle misure di sicurezza.

B) Disciplinare per l'utilizzo della rete informatica

C) Procedura per la gestione delle violazioni – data breach

PARTE PRIMA: INTRODUZIONE

1. Principi normativi

Il presente Manuale ha lo scopo di definire le modalità procedurali, organizzative e tecniche necessarie a garantire la tutela e la sicurezza dei dati informatici e cartacei trattati della Francesco Pisani & Figli S.p.a, (di seguito anche "Società") in conformità a quanto stabilito dal Codice della Privacy (Decreto Legislativo n. 196 del 30/06/2003) e dal nuovo Regolamento Europeo n. 2016/679.

Il Manuale si presenta nella versione aggiornata al fine di recepire, in un unico testo, i precetti normativi introdotti di recente, sia in ambito nazionale che aziendale, in tema di trattamento dei dati personali (*D. Lgs. 196 del 30/06/2003 e ss.mm., regolamenti e codici deontologici succeduti negli ultimi anni, direttive e linee guida del Garante, Direttiva dell'UE 2000/58 sulla riservatezza nelle comunicazioni elettroniche e soprattutto Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27/04/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*).

L'obiettivo della Società è di costituire una sorta di vademecum per tutto il personale e i collaboratori della nostra azienda che, per quanto di loro competenza, sono tutti tenuti a conoscerne i contenuti e a rispettarne le prescrizioni.

A tale scopo il Manuale viene distribuito in forma controllata ad ogni Responsabile del trattamento, ad ogni Designato o Incaricato interno al trattamento dei dati personali nonché a tutto il personale per necessaria presa visione e conoscenza nonché viene pubblicato sul sito della Società al seguente indirizzo: http://www.pisaniscatolificio.it

L'avvenuta distribuzione è documentata tramite le firme di ricevuta poste in calce all'originale del documento tenuto e conservato dal Titolare del trattamento dei dati - Francesco Pisani & Figli S.p.a,- oppure dal Responsabile del Trattamento designato

A seguito di eventuali revisioni, il Titolare o il Responsabile provvederà ad eseguire la redistribuzione del Manuale ritirando le copie superate.

2. Allegati al Manuale

Vengono allegati a questo Manuale una serie di documenti tecnici atti a dare compiuta attuazione ai dettami della nuova "Privacy europea".

Tali documenti, ai quali viene data massima pubblicità e diffusione tramite la pubblicazione sul sito internet aziendale, sono:

A. Regole per l'adozione delle misure di sicurezza;

B. Disciplinare per l'uso della rete informatica;

C. Disciplinare per l'autorizzato al trattamento;

D. Procedura per la gestione delle violazioni – ***data breach***.

La normativa vigente lascia al Titolare ampia autonomia decisionale in merito alle modalità, alle garanzie e ai limiti del trattamento dei dati personali, nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel Regolamento. Pertanto questa Società si è impegnata sin da subito a far propri i dettami del Legislatore europeo relativi alla responsabilizzazione o *accountability* ed alla conformità o *compliance* anche attraverso la predisposizione di questo documento.

Al presente Manuale si trovano altresì allegati, e ne costituiscono parte integrante, i seguenti documenti atti garantire e dimostrare il rispetto degli obblighi procedurali indicati:

E) Informative alla clientela e ai fornitori aziendali.

F) Informative ai dipendenti e collaboratori aziendali.

G) Nomina del responsabile al trattamento dei dati

H) Nomina incaricati interni al trattamento

I) Elenco responsabili e incaricati al trattamento

PARTE SECONDA: DISPOSIZIONI GENERALI

3. DEFINIZIONI

Come stabilito dall'articolo n. 4 del Regolamento Europeo n. 2016/679, ai fini di questo disciplinare aziendale si intende per:

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»***: 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;

c) «***limitazione di trattamento***»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

d) «***profilazione»***: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali 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;

e) «***archivio***»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

g) «***destinatario***»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

h) «***terzo***»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

i) «***consenso dell'interessato***»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

l) «***violazione dei dati personali*** o ***data breach***»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

m) «***dati genetici***»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

n) «***dati biometrici***»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

o) «***dati relativi alla salute***»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute; a proposito delle tipologie di "dati" sopra indicate, si fa presente che il Regolamento Europeo non utilizza la definizione "dati sensibili" ma parla di "dati particolari"

p) <<***pseudonimizzazione***>>: sostituzione di materiale che identifica una persona con identificativi artificiali e con cifratura (codifica dei messaggi in modo che solo i soggetti autorizzati possano leggerli).

q) «***autorità di controllo***»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del Regolamento UE

Quelle sopra riportate rappresentano le "definizioni" su cui ha inciso maggiormente il nuovo Regolamento Europeo: per le altre "definizioni" si fa espresso rinvio al testo dell'articolo n. 4 del Regolamento Europeo n. 2016/679

4. TRATTAMENTO DI CATEGORIE PARTICOLARI DI DATI (EX DATI SENSIBILI)

Come stabilito dall'articolo n. 9 del Regolamento Europeo n. 2016/679, 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.

Detta disposizione non si applica, secondo il Regolamento UE, quando incorrono alcune condizioni nelle quali "*il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato*".

5. TRATTAMENTO DEI DATI PERSONALI RELATIVI A CONDANNE PENALI E REATI (DATI GIUDIZIARI)

Come stabilito dall'articolo n. 10 del Regolamento Europeo n. 2016/679, *"il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica.*"

Pertanto si prevede che il trattamento dei dati personali relativi a condanne penali e reati sia lecito solo quando sono rispettate – **congiuntamente** – le seguenti condizioni:

- vi sia una delle **basi giuridiche** di cui all'art. 6, paragrafo 1 del GDPR (consenso dell'interessato, trattamento necessario per dare esecuzione ad un contratto di cui l'interessato è parte o di misure precontrattuali adottate su richiesta dello stesso, trattamento necessario per adempiere ad un obbligo di legge sussistente in capo al Titolare, trattamento necessario per la salvaguardia di interessi vitali dell'interessato o di altra persona fisica; trattamento necessario per lo svolgimento di un compito di interesse pubblico o per il perseguimento di un legittimo interesse del Titolare).
- deve avvenire soltanto sotto il controllo dell'**autorità pubblica** oppure deve essere autorizzato dal diritto dell'Unione o degli Stati membri e che preveda garanzie appropriate per i diritti e le libertà degli interessati.

La dottrina prevalente, in merito al fondamento giuridico che consenta di trattare i dati relativi a condanne penali e reati per valutare l'attitudine lavorativa, ha ritenuto che l'autorizzazione da parte del diritto nazionale già risulti presente ai sensi dell'art. 8 del c.d. "Statuto dei Lavoratori" (L. 300/1970) che ne prevede il trattamento nell'ambito della valutazione dell'attitudine lavorativa.

Ebbene, deve rimarcarsi come il trattamento è consentito solo per la valutazione dell'attitudine professionale del lavoratore e non per l'assunzione, con il rispetto dei principi costituzionali di cui agli artt. 2, 3, 21 e 41 della Costituzione; vi è sempre possibilità del lavoratore/candidato di richiedere in sede giudiziale il risarcimento del danno per la mancata assunzione o per il licenziamento

intervenuto in violazione del divieto ex art. 8 statuto del lavoratori; vi sono delle sanzioni penali all'articolo 38 dello Statuto dei Lavoratori nel caso in cui il Datore di Lavoro non rispetti i limiti di cui all'articolo 8.

6. COMUNICAZIONE DI DATI VERSO L'ESTERNO

La comunicazione a soggetti terzi di dati di carattere personale e particolare, detenuti dal Titolare del Trattamento, deve avvenire unicamente in ragione delle finalità per le quali gli stessi sono stati acquisiti e di cui si è data contezza nell'informativa privacy consegnata e sottoscritta dagli interessati. La diffusione di dati che ecceda quanto su indicato, deve considerarsi illecita

7. TRATTAMENTO DEI DATI

La nostra Società deve, quindi, proteggere i dati personali in suo possesso attraverso un loro **"trattamento"** conforme alle disposizioni del Regolamento europeo ed in osservazione dei seguenti: adempimenti

a) Istituire e nominare i responsabili c/a gli incaricati al trattamento dei dati

b) Effettuare la raccolta dei dati nei casi previsti dal Regolamento europeo e solo a seguito di informativa e (quando previsto) consenso dell'interessato.

c) Eseguire il trattamento dei dati per finalità determinate, esplicite e legittime

d) Assicurarsi che i dati siano esatti, aggiornati, pertinenti, completi, e non eccedenti rispetto alle finalità del trattamento.

e) Garantire che i dati siano raccolti in modo lecito, corretto e trasparente e che siano conservati solo per il tempo necessario agli scopi per i quali sono stati raccolti e trattati.

f) Istituire un sistema di controllo degli accessi informatici aggiornando almeno annualmente i profili di autorizzazione.

g) Assicurare la riservatezza delle credenziali di accesso (password).

h) Assicurare la corretta composizione, custodia e modifica periodica delle passwords.

i) Disattivare le credenziali e passwords non utilizzate e non riassegnare credenziali o passwords già utilizzate.

j) Utilizzare e aggiornare software antivirus adeguati a proteggere il sistema informatico.

k) Assicurare adeguate metodologie di custodia del supporti removibili garantendone la distruzione nei cosi di inutilizzo a la loro formattazione nei casi di riutilizzo.

l) Garantire il salvataggio dei dati almeno settimanale.

m) Assicurare il ripristino dei dati in tempi certi.

n) Assicurare un adeguato controllo e la custodia degli atti e documenti cartacei riportanti dati personali

o) Informare tutto il personale sui comportamenti più rilevanti in materia di trattamento dati e formare tutto il personale incaricato al trattamento dei dati.

p) Verificare l'affidabilità e la corretta applicazione delle disposizioni atte a garantire la sicurezza e la protezione dei dati.

q) Assicurare e garantire il corretto uso e conservazione delle immagini ricavate dall'utilizzo della videosorveglianza

8. TRATTAMENTI OPERATI DALLA SOCIETA'

Di seguito sono decritti i trattamenti effettuati dalla Francesco Pisani & Figli Sp.a.

Finalità e descrizione del trattamento	**Fornitura dei prodotti (vendita)**
Interessati al trattamento:	Clienti
Natura dei dati trattati:	Dati diversi da quelli sensibili e giudiziari
Funzione interna autorizzata al trattamento	Commerciale - Vendite
Funzioni interne che concorrono al trattamento	Contabilità
Strutture esterne delegate al trattamento	Agenti di Vendita
Strumenti elettronici impiegati	Personal Computer
Descrizione banca dati	Software RTS
Ubicazione supporti memorizzazione	Commerciale - Contabilità
Sistemi di interconnessione	Rete locale
Descrizione supporti cartacei	Contratti, ordini, documenti
Ubicazione supporti cartacei:	Vendite - Contabilità - Archivio generale

Finalità e descrizione del trattamento:	**Approvvigionamento acquisti**
Interessati al trattamento	Fornitori
Natura dei dati trattati	Dati diversi da quelli sensibili e giudiziari
Funzione interna autorizzata al trattamento	Commerciale - Acquisti
Funzioni interne che concorrono al trattamento	Contabilità
Strumenti elettronici impiegati	Personal Computer

Strumenti elettronici impiegati	Software RTS
Ubicazione supporti di memorizzazione:	Commerciale - Contabilità
Sistemi di interconnessione	Rete locale
Descrizione supporti cartacei	Documenti contrattuali, contabili e fiscali
Ubicazione supporti cartacei	Acquisti- - Contabilità- Archivio generale

Finalità e descrizione del trattamento	**Gestione del personale**
Interessati al trattamento	Dipendenti e collaboratori Dati identificativi
Natura dei dati trattati	Dati sensibili (cartella sanitaria)
Funzioni interne autorizzata al trattamento	Risorse umane
Strutture esterne delegate al trattamento	Dott. Quaglieri
Strumenti elettronici impiegati	Personal Computer (dati identificativi)
Descrizione della banca dati	Software INAZ (dati identificativi)
Funzioni interne che concorre al trattamento	Contabilità
Ubicazione supporti di memorizzazione	Risorse umane (dati identificativi) Buste paga
Descrizione supporti cartacei	Cartella sanitaria Sala medica (cartella sanitaria)
Ubicazione supporti cartacei	Archivio generale (buste paga)

Finalità e descrizione del trattamento	**Gestione hardware e software (CED)**
Interessati al trattamento	Dipendenti, clienti e fornitori
Natura dei dati trattati:	Dati diversi da quelli sensibili e giudiziari
Funzioni interne autorizzata al trattamento	CED
Strutture esterne delegate al trattamento	INAZ/RTS/RI//BS/MS
Strumenti elettronici impiegati:	Personal computer
Descrizione della banca dati	Software RTS/INAZ/Arnet Solution
Sistemi di interconnessione	Rete locale

PARTE TERZA: DIRITTI DELL'INTERESSATO

9. INFORMATIVA SUL TRATTAMENTO DEI DATI

Come stabilito dall'articolo n. 13 del Regolamento Europeo n. 2016/679, in caso di raccolta presso l'interessato di dati che lo riguardano, il Titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni:

a. l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
b. b. i dati di contatto del Responsabile della protezione dei dati (D.P.O.);
c. le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
d. qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f) del Regolamento UE, i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
e. gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
f. ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione, nei termini previsti dal Regolamento UE.

In aggiunta alle informazioni di cui sopra, nel momento in cui i dati personali sono ottenuti, il Titolare del trattamento fornisce all'interessato le seguenti ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente:

g. il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
h. l'esistenza del diritto dell'interessato di chiedere al Titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
i. qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a) del Regolamento UE, l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
j. il diritto di proporre reclamo a un'autorità di controllo;
k. se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
l. l'eventuale esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4 del Regolamento UE, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Per quanto concerne il periodo di conservazione dei dati personali raccolti da questa Società, i dati verranno conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello strettamente necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati, come previsto dalla normativa vigente.

10. CONSENSO AL TRATTAMENTO DEI DATI: PRINCIPI GENERALI

Il Regolamento UE conferma che ogni trattamento deve trovare fondamento in un'idonea base giuridica; i fondamenti di liceità del trattamento sono indicati all'art. 6 del Regolamento. In particolare:

- il consenso deve essere "**esplicito**" o il trattamento deve basarsi sul verificarsi dei casi previsti dal GDPR;
- deve essere, in tutti i casi, **libero, specifico, informato e inequivocabile** e non è ammesso il consenso tacito o presunto (non è quindi possibile utilizzare "caselle pre-spuntate" su un modulo);
- deve essere manifestato attraverso "**dichiarazione o azione positiva inequivocabile"** (per approfondimenti, si vedano considerando 39 e 42 del regolamento).

11. DIRITTO DI ACCESSO DELL'INTERESSATO

Come stabilito dall'articolo n. 15 del Regolamento Europeo n. 2016/679, l'interessato ha il diritto di ottenere dal Titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:

m. le finalità del trattamento;

n. le categorie di dati personali in questione;

o. i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;

p. quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

q. l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica ola cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;

r. il diritto di proporre reclamo a un'autorità di controllo;
s. qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
t. l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Oltre al rispetto delle prescrizioni relative alle modalità di esercizio di questo diritto, il Titolare può consentire agli interessati di consultare direttamente, da remoto e in modo sicuro, i propri dati personali.

Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'articolo 46 relative al trasferimento. Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento.

12. DIRITTO DI RETTIFICA

Come stabilito dall'articolo n. 16 del Regolamento Europeo n. 2016/679, **l'interessato ha il diritto di ottenere dal Titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo.** Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

13. DIRITTO ALLA CANCELLAZIONE (DIRITTO ALL'OBLIO)

Come stabilito dall'articolo n. 17 del Regolamento Europeo n. 2016/679, **in capo all'interessato è riconosciuto il diritto "all'oblio", che si configura come un diritto alla cancellazione dei propri dati personali in forma rafforzata.** Si prevede, infatti, l'obbligo per i Titolari (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" (si veda art. 17, paragrafo 2 del Regolamento UE).

14. DIRITTO DI LIMITAZIONE AL 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), bensì anche se l'interessato chiede la rettifica dei dati (in attesa di tale rettifica da parte del titolare) o si oppone al loro trattamento ai sensi dell'art. 21 del regolamento (in attesa della valutazione da parte del titolare).

Esclusa la conservazione, ogni altro trattamento del dato di cui si chiede la limitazione è vietato a meno che ricorrano determinate circostanze (consenso dell'interessato, accertamento diritti in sede giudiziaria, tutela diritti di altra persona fisica o giuridica, interesse pubblico rilevante). **Il diritto alla limitazione prevede che il dato personale sia "contrassegnato" in attesa di determinazioni ulteriori; pertanto, è opportuno che il Titolare preveda nei propri sistemi informativi (elettronici o meno) misure idonee a tale scopo.**

15. DIRITTO ALLA PORTABILITA' DEI DATI

Si tratta di uno dei nuovi diritti previsti dal regolamento, anche se non è del tutto sconosciuto ai consumatori (si pensi alla portabilità del numero telefonico). Non si applica ai trattamenti non automatizzati (quindi non si applica agli archivi o registri cartacei); 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**.

Inoltre, il Titolare deve essere in grado di trasferire direttamente i dati portabili a un altro titolare indicato dall'interessato, se tecnicamente possibile.

16. DIRITTO DI OPPOSIZIONE

Come stabilito dall'articolo n. 21 del Regolamento Europeo n. 2016/679, l'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei

dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f) del medesimo Regolamento, compresa la profilazione sulla base di tali disposizioni.

Il Titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

17. PROCESSO DECISIONALE AUTOMATIZZATO (PROFILAZIONE)

Come stabilito dall'articolo n. 22 del Regolamento Europeo n. 2016/679, l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona. Tale principio non si applica nel caso in cui la decisione:

- sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;
- sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà dei legittimi interessi dell'interessato;
- si basi sul consenso esplicito dell'interessato.

PARTE QUARTA: TITOLARE E RESPONSABILE DEL TRATTAMENTO

18. TITOLARE DEL TRATTAMENTO

Il "Titolare" del trattamento dei dati personali è la persona fisica, giuridica, la Pubblica Amministrazione, e qualsiasi altro Ente, Associazione od organismo cui competono le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, compreso il profilo della sicurezza.

Il Titolare del trattamento dei dati personali, ai sensi e per gli effetti del Regolamento Europeo e del Codice della privacy, è **la Francesco Pisani & Figli S.p.a.**

Il Titolare provvede:

a. a richiedere al Garante per la protezione dei dati personali l'eventuale autorizzazione al trattamento dei dati personali, nei casi previsti dalla vigente normativa e ad assolvere all'eventuale obbligo di notificazione e comunicazione (DPIA);

b. a nominare con atto deliberativo i Responsabili del trattamento dei dati personali, impartendo ad essi, per la corretta gestione e tutela dei dati personali, i compiti e le necessarie istruzioni, in relazione all'informativa agli interessati, alla tipologia dei dati da trattare, alle condizioni normative previste per il trattamento dei dati, alle modalità di raccolta, comunicazione e diffusione dei dati, all'esercizio dei diritti dell'interessato previsti dall'art. 7 del Codice della Privacy e all'articolo 12 del Regolamento UE, all'adozione delle misure di sicurezza per la conservazione, alla protezione e sicurezza dei dati;

c. a nominare il Data Protection Officer, come stabilito dall'articolo 37 del Regolamento UE;

d. a disporre periodiche verifiche sul rispetto delle istruzioni impartite, anche con riguardo agli aspetti relativi alla sicurezza dei dati; e. a mettere in atto misure tecniche e organizzative adeguate a garantire che il trattamento dei dati sia effettuato conformemente al presente Regolamento.

Si dà evidenza, inoltre, del fatto che il Regolamento UE pone con forza l'accento sulla "responsabilizzazione" (a***ccountability***) di titolari e responsabili, ovverossia sull'adozione di comportamenti tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento. Si tratta di una grande novità per la protezione dei dati in quanto viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali, nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel regolamento.

Questa Società sta lavorando attivamente per far proprio l'approccio del Legislatore europeo relativo all'accountability.

19. DESIGNATO O AUTORIZZATO AL TRATTAMENTO DEI DATI

La previsione della figura del c.d." Responsabile interno" trovava la propria fonte normativa di diritto interno nell'art. 29 del Codice privacy (abrogato dal D.Lgs 101/2018), che appunto consentiva al Titolare di nominare un Responsabile scelto tra le risorse umane della propria azienda.

Nel nuovo regolamento europeo (art. 4, par. 1, n. 8 GDPR) il Responsabile del trattamento è la persona fisica, giuridica, pubblica amministrazione, il servizio o altro organismo che tratta dati personali per conto del titolare. Si tratta dunque di un soggetto, distinto dal titolare, che deve essere in grado di fornire garanzie al fine di assicurare il pieno rispetto delle norme in materia di protezione dei dati personali, nonché di garantire la tutela dei diritti dell'interessato (Art. 28, par. 1, GDPR).

Il nuovo Regolamento Europeo disciplina in sostanza i compiti di un Responsabile "**esterno"** senza più contemplare la figura del responsabile "interno", in quanto descrive funzioni, competenze e responsabilità che soltanto un soggetto esterno all'azienda può garantire.

Il **Considerando 81** del Regolamento, appunto, dispone: << … *quando affida delle attività di trattamento a un responsabile del trattamento* ***il titolare del trattamento dovrebbe ricorrere unicamente a responsabili del trattamento che presentino garanzie sufficienti, in particolare in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto misure tecniche e organizzative che soddisfino i requisiti del presente regolamento, anche per la sicurezza del trattamento*** *… al termine del rapporto o del trattamento, dovrà restituire i dati personali ricevuti o provvedere alla loro cancellazione, salvo che il diritto dell'Unione o degli Stati membri cui è soggetto il responsabile del trattamento prescriva la conservazione dei dati personali.>>*.

Questa Società, in continuità con le scelte organizzative assunte negli anni, ha deciso di conferire l'incarico di **Autorizzati al trattamento dei dati** a quei dirigenti o funzionari apicali che già ricoprivano il ruolo di Responsabili interni al trattamento dei dati e che sono in grado di garantire la sicurezza dei dati in ambito privacy rispondendo con diversi livelli di autonomia alle direttive del Titolare del Trattamento.

L'Autorizzato al trattamento dei dati deve:

- individuare gli Incaricati del trattamento;

- fornire istruzioni operative;

- attuare gli obblighi di formazione ed acquisizione del consenso nei confronti degli interessati;

- predisporre la notificazione del data breach;

- garantire l'esercizio dei diritti dell'interessato, collaborare con il Garante per l'attuazione delle prescrizioni ed aggiornare il sistema di sicurezza idoneo. Ad esempio è possibile avere un autorizzato solo per il "riscontro all'interessato" che provveda a riscontrare i reclami del Cliente;

- non può nominare altri designati ma può avvalersi di collaboratori d'ufficio.

- tenendo conto del livello di autonomia concessa dal Titolare nella delega al trattamento, assistere il Titolare con misure tecniche ed organizzative adeguate, al fine di soddisfare l'obbligo del Titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato secondo quanto previsto nella normativa vigente;

- mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti nel presente Regolamento;

- contribuire alle attività di verifica del rispetto del regolamento, comprese le ispezioni, realizzate dal titolare del trattamento o da altro soggetto da questi incaricato.

20. RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI

Nell'ambito di queta Società sono individuati, quali **Responsabili esterni al trattamento dei dati**, i soggetti esterni che, per svolgere la propria attività sulla base di una convenzione o un contratto sottoscritto con l'Azienda, trattino dati di cui è titolare la Francesco Pisani & Figli S.p.a. e qualora siano in possesso dei requisiti previsti dall'articolo 28 del Regolamento EU (esperienza, capacità ed affidabilità). S

Il Titolare del trattamento dei dati deve informare ciascun Responsabile, così come individuato dal presente Regolamento, delle responsabilità che gli sono affidate in relazione a quanto disposto dalle normative vigenti. I responsabili del trattamento rispondono al Titolare di ogni violazione o mancata attivazione di quanto dettato dalla normativa vigente.

In ottemperanza all'articolo 28 del Regolamento Europeo 2016/679, i Responsabili esterni hanno l'obbligo di:

- trattare i dati in modo lecito, secondo correttezza e nel pieno rispetto della vigente normativa (nazionale ed europea) in materia di privacy;

- trattare i dati personali, anche di natura sensibile e giudiziaria, degli ospiti (o di altri interessati) esclusivamente per le finalità previste dal contratto sottoscritto con la Francesco

Pisani & Figli spa e ottemperando ai principi generali di necessità, pertinenza e non eccedenza;

- rispettare i principi in materia di sicurezza dettati dalla normativa vigente (nazionale ed europea) in materia di privacy, idonei a prevenire e/o evitare operazioni di comunicazione o diffusione dei dati non consentite, il rischio di distruzione o perdita, anche accidentale, il rischio di accesso non autorizzato o di trattamento non autorizzato o non conforme alle finalità della raccolta;

- adottare, secondo la propria organizzazione interna, misure tecniche ed organizzative idonee a garantire un livello di sicurezza adeguato al rischio, nei termini di cui all'articolo 32 del Regolamento Europeo 2016/679 rubricato "Sicurezza del trattamento" che possono anche essere definite dal Titolare del Trattamento;

- nominare, al loro interno, i soggetti autorizzati / incaricati del trattamento, impartendo loro tutte le necessarie istruzioni finalizzate a garantire, da parte degli stessi, un adeguato obbligo legale di riservatezza;

- attenersi alle disposizioni impartite dal Titolare del trattamento, anche nell'eventuale caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, nei termini di cui all'articolo 28, comma 3, lettera a) del Regolamento Europeo;

- specificare, su richiesta del Titolare, i luoghi dove fisicamente avviene il trattamento dei dati e su quali supporti e le misure minime di sicurezza adottate per garantire la riservatezza e la protezione dei dati personali trattati.

- assistere, per quanto di competenza e nella misura in cui ciò sia possibile, il Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del Regolamento Europeo (sicurezza del trattamento dei dati personali, notifica di una violazione dei dati personali all'autorità di controllo, comunicazione di una violazione dei dati personali all'interessato, valutazione di impatto sulla protezione dei dati), tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;

- su scelta del Titolare del trattamento, cancellare o restituire al medesimo tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancellare le copie esistenti, salvo che il diritto dell'Unione o dello Stato membro preveda la conservazione dei dati;

- mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'articolo 28 del Regolamento Europeo e consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzate dal Titolare del trattamento o da un altro soggetto da questi incaricato.

Nel caso di mancato rispetto delle predette disposizioni e in caso di mancata nomina dei soggetti incaricati al trattamento dei dati i **Responsabili esterni ne rispondono direttamente verso il Titolare del Trattamento.**

La designazione del Responsabile viene effettuata mediante "**accordo di nomina**" sottoscritto da parte del Titolare del trattamento e controfirmato per accettazione da parte del Responsabile esterno: il documento deve essere richiamato dagli accordi, convenzioni o contratti che prevedono l'affidamento di trattamenti di dati personali esternamente all'Azienda. L'accettazione della nomina e l'impegno a rispettare le disposizioni del presente Regolamento è condizione necessaria per l'instaurarsi del rapporto giuridico fra le Parti.

21. L'INCARICATO AL TRATTAMENTO DEI DATI

Il Regolamento Europeo non fornisce rilievo autonomo alla figura dell'incaricato al trattamento dei dati, non distingue fra designati, autorizzati e incaricati ma opera secondo diversi livelli di delega che conferiscono spazi di autonomia più ampi o più ristretti. Così le aziende, in continuità con il modello precedente al Regolamento, chiamano solitamente designati o autorizzati le figure con livelli di delega più alti ed incaricati i soggetti con pochi margini di operatività sul trattamento dei dati, sempre dietro le direttive del Titolare o del Responsabile del trattamento.

Al momento dell'ingresso in servizio è fornita, a cura dell'Ufficio Gestione Risorse Umane, per competenza, ad ogni dipendente (oltre che ad ogni collaboratore, consulente o titolare di borsa di studio) una specifica comunicazione in materia di privacy, con apposita clausola inserita nel contratto di lavoro (o nella lettera di incarico per i summenzionati soggetti non dipendenti), con la quale detti soggetti (dipendenti e non dipendenti) vengono nominati quali " incaricati al trattamento dei dati" ai sensi del Regolamento UE 2016/679.

Qualora il Titolare non nomini Incaricati gli addetti a cui permette il trattamento dei dati personali raccolti per suo conto, si instaura, non tanto un divieto assoluto di trattare i dati, ma il rigoroso regime della "comunicazione" a terzi. In altri termini in mancanza delle nomine degli Incaricati, qualsiasi operazione avente ad oggetto dati personali svolta dai dipendenti o collaboratori del Titolare non può essere considerata come utilizzo interno di dati ma, viceversa, sarà qualificata come attività svolta da un soggetto esterno senza il consenso dell'interessato. Ed in pratica è come se il Titolare avesse comunicato a terzi, estranei e qualsiasi, i dati senza avere preventivamente raccolto il relativo consenso espresso dell'interessato. Rammentiamo che il trattamento illecito dei dati costituisce un reato. Appare chiaro, sulla scorta di tali considerazioni, che la circostanza che le operazioni di trattamento siano effettuate da soggetti nominati Incaricati del trattamento, se non è - in termini assoluti - obbligatoria, è assolutamente opportuna.

Contestualmente alla nomina dovrà essere data copia del presente Manuale o, in alternative, indicazioni per poterla scaricare dal sito internet aziendale o intranet. Il Manuale contiene infatti tutti i principi fondamentali della materia, esposti in maniera semplice, chiara e puntuale e il dipendente (o il non dipendente nei termini di cui si è detto sopra), nel sottoscrivere il contratto di lavoro (o la lettera di autorizzato), è reso edotto dell'esistenza dell'anzidetto vademecum e delle modalità di consultazione del medesimo.

Ogni dipendente e/o collaboratore viene così informato sulle modalità di trattamento dei dati, sulle modalità di accesso ed utilizzo dei dati informatici, sui limiti all'utilizzo dei computer aziendali, gestione delle password e gestione di tutti gli altri beni aziendali

Analoghe considerazioni valgono per la figura dell'autorizzato "esterno": tutti coloro che svolgono un'attività di trattamento dei dati nell'ambito di questa Società, pur non essendo dipendenti e neppure

titolari di incarichi conferiti dalla medesima Azienda (quali consulenze, collaborazioni o borse di studio), devono essere designati da parte del Titolare tramite una lettera (o una nota) di nomina come incaricato. Nel caso di tali incaricati "esterni", l'accesso ai dati deve essere limitato, con particolare rigore, ai soli dati personali la cui conoscenza sia strettamente necessaria per l'adempimento dei compiti assegnati e connessi all'espletamento dell'attività.

22. RESPONSABILE DELLA PROTEZIONE DEI DATI

Il Regolamento Europeo impone la nomina del Data Protection Officer (DPO) nei termini di cui all'articolo 37, 38 e 39 del Regolamento medesimo.

La nomina del DPO è obbligatoria in tutte le organizzazioni, anche pubbliche, che trattano come attività principali i dati sensibili su larga scala, come ospedali, assicurazioni e istituti di credito. Chi svolge la funzione di DPO, quindi, deve presentare caratteristiche di indipendenza ed autorevolezza, oltre che competenze manageriali. Non deve, inoltre, essere in conflitto di interessi in quanto il Regolamento UE vieta di nominare RDP anche chi, solo in astratto, possa potenzialmente trovarsi in conflitto di interessi. Si tratta di una figura dirigenziale, di alta professionalità, a metà tra il consulente ed il revisore e non dovrebbe ricoprire ruoli gestionali rispetto all'attività dell'azienda.

Questa Società – al momento – ha deciso di non procedere alla nomina di un DPO in quanto la Francesco Pisani & Figli spa non svolge attività che consistono in un trattamento di dati che per la loro natura, oggetto o finalità, richiedono il controllo regolare e sistematico degli interessati su larga scala.

Si ritiene comunque che, per come strutturata l'organizzazione aziendale in ambito privacy, attraverso diverse figure di Responsabili esterni al trattamento, Designati al trattamento ed incaricati si possa ragionevolmente garantire la sicurezza ed il trattamento dei dati degli interessati secondo le prescrizioni del GDPR.

PARTE QUINTA: SICUREZZA DEI DATI PERSONALI - MISURE DI CARATTERE INFORMATICO E TECNOLOGICO

23. PROGETTAZIONE E PROTEZIONE DEI DATI PER IMPOSTAZIONE PREDEFINITA

L'articolo n. 25 del Regolamento Europeo n. 2016/679 introduce il criterio del "***data protection by default and by design***", ossia della 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.

Prima di procedere al trattamento dei dati vero e proprio ("sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso", secondo quanto afferma l'art. 25, paragrafo 1 del Regolamento UE) viene richiesta al Titolare del Trattamento un'analisi preventiva ed un impegno applicativo che deve sostanziarsi in una serie di attività specifiche e dimostrabili.

L'obbligo di ***data protection by design*** è basato sulla **valutazione del rischio** che deve essere fatta al momento della progettazione del sistema, quindi prima che il trattamento inizi. Chiaramente si dovrà

tenere conto anche del tipo di dati trattati, per cui in presenza di un trattamento che coinvolge dati di minori gli obblighi dovranno essere più stringenti, in considerazione del fatto che il rischio è maggiore.
L'approccio basato sul rischio comporta che si deve tenere conto dello stato della tecnologia, per cui il trattamento va adattato e modulato nel corso del tempo.

Data protection by default:

Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento.

Dunque **per impostazione predefinita le imprese devono trattare solo i dati personali nella misura necessaria e sufficiente per le finalità previste e per il periodo strettamente necessario**. Occorre, quindi, **progettare il sistema di trattamento di dati garantendo la non eccessività dei dati raccolti**.

Questa Società si sta impegnando per attuare un sistema che appunto secondo i principi della privacy by design e by default possa pienamente applicare gli strumenti e le corrette impostazioni a tutela dei dati personali.

24. REGISTRO ELETTRONICO DELLE ATTIVITA' DI TRATTAMENTO

Questa Società, in attuazione dell'articolo 30, del Regolamento UE, detiene un Registro delle operazioni di trattamento i cui contenuti sono indicati dal medesimo Regolamento. Si tratta di uno strumento fondamentale non soltanto ai fini dell'eventuale supervisione da parte del Garante, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda o di un soggetto pubblico, indispensabile per ogni valutazione e analisi del rischio.

Il Registro, in virtù delle caratteristiche questa Società, ha forma elettronica, e deve essere esibito su richiesta del Garante.

La tenuta del registro elettronico dei trattamenti non costituisce un adempimento formale bensì parte integrante di un sistema tecnologico di corretta gestione dei dati personali.

Il Registro è aggiornato e custodito dal Titolare del trattamento

25. NOTIFICA DI UNA VIOLAZIONE DEI DATI PERSONALI ALL'AUTORITA'DI CONTROLLO

A partire dal 25 maggio 2018, tutti i titolari dovranno notificare all'Autorità di controllo le violazioni di dati personali di cui vengano a conoscenza, entro 72 ore e comunque "senza ingiustificato ritardo", ma soltanto se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati (si veda considerando 85 del Regolamento UE); questa procedura va sotto il nome di "Data Breach". Pertanto, la notifica all'Autorità dell'avvenuta violazione non è obbligatoria, essendo subordinata alla valutazione del rischio per gli interessati che spetta, ancora una volta, al Titolare. Se la probabilità di tale rischio è elevata, si dovrà informare della violazione anche gli interessati, sempre "senza ingiustificato ritardo"; fanno eccezione le circostanze indicate al paragrafo 3 dell'articolo 34 del Regolamento UE. I

26. VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

Quando un trattamento dei dati può comportare un rischio elevato per i diritti e le libertà delle persone interessate (a causa del monitoraggio sistematico dei loro comportamenti, o per il gran numero dei soggetti interessati di cui sono magari trattati dati sensibili, o anche per una combinazione di questi e altri fattori), il Regolamento 2016/679 obbliga il Titolare a svolgere una **valutazione di impatto** (DPIA) prima di darvi inizio, consultando l´autorità di controllo in caso le misure tecniche e organizzative da loro stessi individuate per mitigare l´impatto del trattamento non siano ritenute sufficienti - cioè, quando il rischio residuale per i diritti e le libertà degli interessati resti elevato.

La DPIA- Data Protection Impact Assessment - è una procedura finalizzata a descrivere il trattamento per valutarne la necessità e la proporzionalità e facilitare la gestione dei rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamenti dei loro dati personali (Linee Guida WP29 4 aprile 2017)

Le Linee Guida WP29 stabiliscono i seguenti 9 criteri da seguire per distinguere i casi in cui la DPIA è necessaria

a) Trattamenti valutativi o di scoring (profilazione)
b) Decisioni automatizzate che producono effetti significativi
c) Monitoraggio sistematico
d) Dati sensibili o supersensibili
e) Trattamento dati su larga scala
f) combinazione o raffronto di dati personali
g) Dati relativi a interessati vulnerabili
h) Utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative
i) Trattamenti che impediscono di esercitare un diritto o di avvalersi di un servizio o contratto

Secondo le Linee guida WP29 (*che era il gruppo costituito dalle Autorità di controllo presenti in ogni stato membro, oggi sostituito dal Comitato europeo per la protezione dei dati (EDPB) ai sensi del GDPR*), la DPIA non è necessaria per i trattamenti che:

j) non presentano rischio elevato per diritti e libertà delle persone fisiche;
k) hanno natura, ambito, contesto e finalità molto simili a quelli di un trattamento per cui è già stata condotta una DPIA;
l) sono stati già sottoposti a verifica da parte di un'Autorità di controllo prima del maggio 2018 e le cui condizioni (es: oggetto, finalità, ecc.) non hanno subito modifiche;
m) sono compresi nell'elenco facoltativo dei trattamenti per i quali non è necessario procedere alla DPIA;
n) fanno riferimento a norme e regolamenti, Ue o di uno stato membro, per la cui definizione è stata condotta una DPIA.

L'iniziativa per lo svolgimento di una DPIA spetta al Titolare che può anche essere affiancato dal Responsabile del Trattamento o da terzi. In questi casi, però, il Titolare monitora lo svolgimento della valutazione consultandosi con il responsabile della protezione dei dati (DPO) e acquisendo - se

i trattamenti lo richiedono - il parere di esperti di settore, del responsabile della sicurezza dei sistemi informativi (Chief Information Security Officer, CISO) e del responsabile IT.

27. GESTIONE TRATTAMENTI AFFIDATI ALL'ESTERNO

Di seguito sono specificate le attività esternalizzate della nostra Società la cui esecuzione comporta trattamento di dati personali.

La nostra azienda affida a terzi le seguenti attività:

a) Gestione contabilità

b) Medicina del lavoro

c) Manutenzione e assistenza su sistemi hardware e software

d) Gestione delle vendite

Tali attività prevedono il trattamento del seguenti dati

- Dati personali, anche sensibili, di addetti e collaboratori
- Dati personali di clienti e fornitori.

La gestione della contabilità è stata affidata allo Studio Miacci-Papetti "Dottori Commercialisti Associati", che pertanto è stato nominato Responsabile esterno al trattamento dei dati tramite specifico contratto

Le attività di medicina del lavoro, le quali comportano la gestione dei dati sanitari del personale dipendente, sono affidate al Dr. Elvio Quaglieri il quale è stato nominato Responsabile esterno al trattamento dei dati tramite specifico contratto.

Anche tutti i fornitori di servizi di manutenzione e assistenza hardware c/a software, comportando la loro attività la possibilità di accesso a dati personali di cui è in possesso la nostra azienda, sono stati nominati responsabili esterni al trattamento del dati:

- INAZ
- RTS
- Arnet Solution

Altra categoria di responsabili esterni del trattamento dei dati sono i nostri agenti di vendita i quali, trattando dati sulla clientela, sono stati nominati responsabili esterni.

Affinchè sia garantito un adeguato trattamento dei dati, i responsabili indicati hanno rilasciato specifiche dichiarazioni assumendo precisi impegni in riferimento:

- Trattamento di dati ai soli fini dell’espletamento dell’incarico ricevuto;
- Adempimento degli obblighi previsti dal Codice per la protezione dei dati personali

- Rispetto delle istruzioni specifiche eventualmente ricevute per il trattamento dei dati;
- Impegno a relazionare periodicamente sulle misure di sicurezza adottate;
- Nominare e formare i propri eventuali incaricati;
- Informare il titolare del trattamento in caso di situazioni anomale a di emergenze;
- Garantire i diritti dell'interessato come previsto dal codice in materia di protezione dei dati.

28. FORMAZIONE DEL PERSONALE

Nel seguito si descrivono gli interventi formativi previsti dalla nostra Società al fine di aggiornare il personale interessato all'attuazione del sistema di tutela e sicurezza dei dati in merito a modalità operative, innovazioni tecnologiche, cambiamenti organizzativi ed evoluzione degli obblighi di legge.

A tale scopo i Responsabili del trattamento hanno la responsabilità di pianificare ed eseguire le attività di formazione necessarie ad informare ed istruire gli autorizzati e gli incaricati interni. Potranno avvalersi, se ritenuto necessario, di consulenti o società specializzate

In particolare, dovrà essere eseguita adeguata formazione nei casi di:

- Assunzione di nuovo personale incaricato al trattamento
- Cambiamento di mansioni degli incaricati
- introduzione di nuovi elaboratori
- Introduzione di nuovi programmi e sistemi informatici.

Le attività di formazione potranno avere per oggetto una o più dei seguenti argomenti:

a) Obblighi e prescrizioni di legge in materia di tutela della sicurezza dei dati personali;
b) Principi di sicurezza logica e fisica dei sistemi informativi;
c) Misure di prevenzione e di contenimento del danno;
d) Strumenti di protezione hardware e software
e) Conservazione del supporti informatici
f) Selezione, installazione e manutenzione di sistemi:
g) Procedure di creazione, gestione, conservazione e trasporto di copie di back-up
h) I piani e modalità di ripristino
i) II controllo dell'accesso fisico;
j) Sistemi di autenticazione e di autorizzazione:
k) Particolari precauzioni nel trattamento di dati sensibili

Ogni attività di formazione eseguita deve essere documentata tramite resoconto indicante: i partecipanti, la durata, i contenuti e gli obiettivi perseguiti.

Alle attività di formazione il Responsabile al Trattamento è tenuto ad eseguire attività di verifica finalizzata ad accertare la corretta applicazione delle prescrizioni di legge in materia di tutela e sicurezza dei dati.

Tali attività di verifica e di costante aggiornamento deve essere svolta con cadenza almeno semestrale nonché deve essere documentata tramite i dettagli degli accertamenti eseguiti e degli esiti conseguiti

ALLEGATI AL MANUALE

A) REGOLE PER L'ADOZIONE DELLE MISURE DI SICUREZZA

La valutazione delle misure di sicurezza da adottare deve essere vista nel contesto del rischio a cui è rivolta. Pertanto le misure di sicurezza vanno viste nel loro senso più ampio del termine partendo dal principio che l'art. 32 del Regolamento EU recita "*Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio*".

Di seguito vengono riportate ad esempio alcune regole e principi di base per diverse misure di sicurezza che verranno implementate nel tempo.

MISURE	**REGOLE/PRINCIPI DA OSSERVARE**
Presenza di un sistema di allarme	E' importante che la si doti di **impianto d'antifurto** a tutela del patrimonio delle informazioni contenute al suo interno
Custodia dei dati	E' importante che gli uffici che trattano dati sensibili e giudiziari archivino in modo consono tali informazioni
Sistemi UPS e Generatori di corrente che garantiscano la continuità elettrica	Fondamentale a tutela delle attività soprattutto per gli strumenti elettronici. Da adottare necessariamente per tutti i server e per quei pc locali che non archiviano le informazioni sul server. Infatti questi ultimi non hanno delle procedure pianificate di backup e quindi è importante ridurre al minimo i rischi che gli sbalzi di tensione possono provocare sugli hard disk.
Digitazione password all'accensione del PC	**Tutti i PC devono avere la password di Windows all'accensione del terminale, questo non vale solo come regola ma viene considerata una misura base di sicurezza**
Manutenzione programmata degli strumenti	Come tutte le macchine che si rispettano anche il sistema informativo va manutenzionato periodicamente sia attraverso l'aggiornamento

	dei suoi componenti sia con la pulizia periodica delle macchine stesse
Utilizzo di un sistema firewall	**Obbligatorio** viste le forme di attacco sempre più intelligenti.
Presenza di un sistema di autenticazione delle credenziali per tutti gli accessi agli archivi elettronici	Si intende con questa misura l'adozione di un server di dominio che consenta l'autenticazione dell'utente
Disattivazione delle credenziali di autenticazione nel caso di inutilizzo per 6 mesi	Spetta all'incaricato della custodia delle password disattivare le credenziali che hanno perso efficacia
Controllo degli accessi a siti internet non sicuri Protezione della posta elettronica	E' importante la conoscenza da parte degli operatori della navigazione in internet e dell'uso della posta elettronica. A questo proposito è stato introdotto **il Disciplinare per l'uso degli strumenti informatici**
Utilizzo di un filtro anti-spam	All'interno dello spam (posta indesiderata) si annidano spesso dei fenomeni di illegalità informatica. E' importante dotare la Società di tale strumento
Utilizzo di un antivirus	Per quanto precedentemente detto, è importante la presenza di un **antivirus** in ogni posto di lavoro, considerato che si tratta di misura di sicurezza, ovviamente sempre aggiornata
Aggiornamento periodico di programmi per il controllo della vulnerabilità	E' importante che ogni pc sia periodicamente aggiornato sulle proprie vulnerabilità con gli appositi software
Istruzioni in merito alla protezione dello strumento elettronico in caso di assenza temporanea durante le sessioni di lavoro	E' importante che l'operatore conosca il Manuale per quanto concerne l'assenza dal posto di lavoro con il PC acceso
Disattivazione delle credenziali di autenticazione in caso di perdita di qualità dell'incarico	Spetta all'incaricato della custodia delle password disattivare le credenziali che hanno perso efficacia
Aggiornamento periodico, con cadenza almeno annuale, della lista degli incaricati e dei profili di autorizzazione	Tutte le persone che operano all'interno degli uffici devono essere autorizzate dal Titolare
Istruzioni in merito alla segretezza e alla custodia delle credenziali di autenticazione	Rientra nel concetto della formazione del personale
Aggiornamento periodico delle credenziali di autenticazione	Spetta all'incaricato della custodia delle password disattivare le credenziali che hanno perso efficacia
Procedure di verifica sull'operato degli incaricati	E' un compito ispettivo che il Responsabile della sicurezza dei dati personali può demandare anche a società esterne
Formazione sugli aspetti principali della disciplina della privacy al momento dell'ingresso in servizio	Rientra nel concetto della formazione del personale
Formazione, periodica e in occasione di cambiamenti di mansioni o di introduzione di nuovi strumenti per il trattamento dei dati e la loro protezione	Rientra nel concetto della formazione del personal

Istruzioni finalizzate al controllo e alla custodia dei documenti contenenti dati personali per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento	Rientra nel concetto della formazione del personale
Adozione di procedure per le copie di sicurezza, la loro custodia ed il ripristino della disponibilità dei dati	**Il backup deve essere metodico, non affidato alle singole volontà. E' per questo importante nominare l'Incaricato delle copie di sicurezza delle banche dati**
Definizioni di responsabilità e sanzioni disciplinare	Rientra nel concetto della formazione del personale nonché è prevedere sanzioni disciplinari nei casi in cui ci sia un comportamento difforme da quando indicato dal presente Manuale
Formazione del personale	Rientra nel concetto della formazione del personale
Distruzione del cartaceo	E' importante nel limite del possibile incentivare la distruzione del cartaceo rendendolo illeggibile usando dei comodi **distruggi documenti**
Per accedere sono attive le credenziali di autenticazione	Si intende con questa misura l'adozione di un server di dominio che consenta l'autenticazione dell'utente
Definizione di procedure per le copie di sicurezza, la loro custodia e il ripristino dei dati	**Il salvataggio dei dati è fondamentale in qualsiasi organizzazione**
I dati cartacei devono essere chiusi in un armadio	Ogni documento deve essere possibilmente chiuso in un armadio e sicuramente devono essere chiusi i dati sensibili e quelli giudiziari

B) DISCIPLINARE PER L'UTILIZZO DELLA RETE INFORMATICA

Di seguito sono indicate le modalità operative e tecniche che devono essere attuate dal nostro personale, al fine di assicurare l'integrità e la protezione dei dati gestiti con strumenti elettronici.

L'utilizzo di Internet da parte dei lavoratori può infatti formare oggetto di analisi, profilazione e integrale ricostruzione mediante elaborazione di log file della navigazione web ottenuti, ad esempio, da un proxy server o da un altro strumento di registrazione delle informazioni.

E' necessaria pertanto la conoscenza del presente Disciplinare per il corretto utilizzo di qualsiasi sistema informatico, che si trovi all'interno dell'azienda, collegato o meno alla rete locale, o che custodisce qualsiasi dato personale di competenza dell'azienda e non destinato alla diffusione.

Alla data di emissione del presente Manuale, la nostra azienda effettua il trattamento con ausilio di strumenti elettronici dei dati relativi alle seguenti categorie di titolari:

- Personale dipendente e collaboratori
- Clienti
- Fornitori

La raccolta dei dati deve essere eseguita solo a seguito di informative comunicate al titolare.

Tali dati sono gestiti attraverso le seguenti banche dati e archivi informatici:

- Software RTS

- Software INAZ

Sono autorizzati ad accedere ai dati, esclusivamente, i Designati o autorizzati al trattamento e gli Incaricati interni al trattamento.

Ogni singolo incaricato, quindi, ha diritto ad accedere ed effettuare, in modo esclusivo, il trattamento dei dati e per le finalità riportate nella propria lettera di nomina.

Utilizzo dei Personal Computer.

Il Personal Computer affidato al dipendente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza, pertanto è vietato.

In particolare:

a. **E' vietato l'uso di propri personal computar portatili di proprietà dell'incaricato sia per lavorare in azienda che da remoto** a meno che non intervenga autorizzazione preventiva del Titolare e del Responsabile insieme all'Amministratore di Sistema;

b. **L'accesso all'elaboratore deve essere protetto da password che deve essere custodita dall'autorizzato con la massima diligenza e non divulgata**. La password deve essere attivata per l'accesso alla rete, per lo screensaver e per il software applicativo. Non è consentita l'attivazione della password di accensione (BIOS), senza preventiva autorizzazione da parte dell'Amministratore di Sistema;

c. **L'Amministratore di Sistema**, nell'espletamento delle sue funzioni legate alla sicurezza e alla manutenzione informatica, **avrà la facoltà di accedere in qualunque momento anche**

da remoto (dopo aver richiesto l'autorizzazione all'utente interessato) al personal computer di ciascuno

d. **Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio**. Lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. Deve essere attivato su tutti i Personal Computer lo screen saver e la relativa password

e. **L'accesso ai dati presenti nel personal computer potrà avvenire quando si rende indispensabile ed indifferibile l'intervento**, ad esempio in caso di prolungata assenza od impedimento dell'incaricato, informando tempestivamente l'incaricato dell'intervento di accesso realizzato**.**

f. **È vietato installare autonomamente programmi informatici salvo autorizzazione esplicita dell'Amministratore di Sistema**, in quanto sussiste il grave pericolo di portare Virus informatici o di alterare la stabilità delle applicazioni dell'elaboratore. L'inosservanza di questa disposizione, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre la struttura a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore.

g. **È vietato modificare le caratteristiche impostate sul proprio PC**, salvo con autorizzazione esplicita dell'Amministratore di Sistema.

h. **È vietato inserire password locali alle risorse informatiche assegnate** (come ad esempio password che non rendano accessibile il computer agli amministratori di rete), se non espressamente autorizzati e dovutamente comunicate all'Amministratore di Sistema.

i. **È vietata l'installazione sul proprio PC di dispositivi di memorizzazione, comunicazione o altro** (come ad esempio masterizzatori, modem, pen drive, dischi esterni, i-pod, telefoni, ecc.), se non con l'autorizzazione espressa dell'Amministratore di Sistema. Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente l'Amministratore di Sistema nel caso in cui vengano rilevati virus o eventuali malfunzionamenti.

Utilizzo della rete informatica

Le unità di rete sono aree di condivisione di informazioni strettamente professionali sulle quali vengono svolte regolari attività di controllo, amministrazione e backup e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato in queste unità, nemmeno per brevi periodi.

L'amministratore di Sistema può in qualunque momento procedere alla rimozione di ogni file o applicazione che ritenga essere pericolosi per la Sicurezza o in violazione del presente regolamento sia sui PC degli incaricati sia sulle unità di rete.

Le password d'ingresso alla rete ed ai programmi sono segrete e non vanno comunicate a terzi. Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È infatti assolutamente da evitare un'archiviazione ridondante.

E' importante togliere tutte le condivisioni dei dischi o di altri supporti configurate nel Personal Computer se non strettamente necessarie (e per breve tempo) allo scambio dei files con altri colleghi.

Sarà compito dell'Amministratore di Sistema provvedere alla creazione di un'area condivisa sul server per lo scambio dei dati tra i vari utenti.

Nell'utilizzo della rete informatica è fatto divieto di:

j. **Utilizzare la Rete in modo difforme da quanto previsto dal presente regolamento**

k. **Conseguire l'accesso non autorizzato a risorse di rete interne ed esterne alla Rete dell'Ente.**

l. **Agire deliberatamente con attività che influenzino negativamente la regolare operatività della Rete e ne restringano l'utilizzabilità e le prestazioni per altri utenti**.

m. **Effettuare trasferimenti non autorizzati di informazioni (software, dati, ecc).**

n. **Installare componenti hardware non compatibili con l'attività istituzionale**

o. **Rimuovere, danneggiare o asportare componenti hardware**;

p. **Utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività di altri utenti, per leggere, copiare o cancellare files e software di altri utenti**;

q. Utilizzare software visualizzatori di pacchetti TCP/IP (sniffer), software di intercettazione di tastiera (keygrabber), software di decodifica password (cracker) e più in generale software rivolti alla violazione della sicurezza del sistema e della privacy

r. **Usare l'anonimato o servirsi di risorse che consentano di restare anonimi;**

<u>Autenticazione e autorizzazione</u>

L'autenticazione configura il primo livello di controllo e consente l'accesso allo strumento informatico (hardware) utilizzando determinate credenziali.

A tale scopo, ogni Incaricato dispone uno specifico "profilo di autenticazione" costituito da:

- Codice identificativo personale (User ID);
- Una o più chiavi d'accesso (Password).

L'autorizzazione configura il secondo livello di contratto; il trattamento può essere limitato alla sola consultazione di tutti i dati o di singole categorie, oppure anche al loro aggiornamento, modificazione etc.

A tale scopo, ogni incaricato dispone di uno specifico "profilo di autorizzazione" costituito da uno a più chiavi d'accesso (passwords) per ogni singolo software, data base, etc. a cui l'Incaricato deve accedere per svolgere il proprio lavoro.

A seguito dell'assegnazione da parte del Responsabile al trattamento delle passwords, ogni incaricato al prime accesso sia agli hardware che ai software è tenuto a provvedere alla sostituzione delle passwords assegnate con altre passwords scelte personalmente.

Per questa ragione tutti gli Incaricati, ai quali viene attribuito un profilo di autorizzazione, sono direttamente responsabili della sicurezza delle parole chiave.

A seguito della definizione delle proprie passwords, dopo il primo accesso, è fatto obbligo all'Incaricato di trascrivere la propria parola chiave sul "Profilo di autenticazione" e inserire tale documento in una busta debitamente sigillata e controfirmata; tale busta deve essere consegnata al Responsabile o all'Incaricato adibito a tale funzione.

Tutte le parole chiave attribuite ai singoli Incaricati per accedere alla posta elettronica, al proprio computer, ad internet, eccetera, devono essere cambiate almeno ogni sei mesi.

Non utilizzare la stessa parola chiave per sistemi di autenticazione interni all'azienda e per sistemi di autenticazione esterni, come ad esempio l'accesso al proprio conto corrente bancario ed altre attività, non legate all'attività aziendale.

In particolare, nella nostra Società deve essere scelta una parola chiave per l'accesso al Software RTS ed una parola chiave separata per l'accesso al software INAZ.

Tutte le parole chiavi che sono state generate da un Incaricato devono essere trattate come informazione strettamente riservate e non vanno condivise

Non archiviate la parole chiave in un qualsiasi tipo di sistema di elaborazione, incluso un telefono cellulare, un computer palmare o simile.

Se avete anche solo il minimo sospetto che la vostra parole chiave sia stata in qualche modo compromessa o venuta a conoscenza di terzi, provvedete immediatamente alla sostituzione della parola chiave e riferite l'accaduto al Titolare a al diretto Responsabile del trattamento.

Ulteriori precauzioni devono essere utilizzate ai fini di una corretta custodia e gestione del supporti removibili: cd-rom, memorie di mosso, etc.

Utilizzo di internet

I Personal Computer, qualora abilitati alla navigazione in Internet, costituiscono uno strumento necessario allo svolgimento della propria attività lavorativa. Nell'uso di Internet e della Posta Elettronica **non sono consentite le seguenti attività:**

s. **L'uso di Internet per motivi personali**

t. **L'accesso a siti inappropriati (esempio siti pornografici, di intrattenimento, ecc.)**

u. **Lo scaricamento (download) di software e di file non necessari all'attività istituzionale**

v. **Utilizzare programmi per la condivisione e lo scambio di file in modalità peer to peer (Napster, Emule, Winmx, e-Donkey, ecc.)**

w. **Accedere a flussi in streaming audio/video da Internet per scopi non istituzionali (ad esempio ascoltare la radio o guardare video o filmati utilizzando le risorse Internet)**

x. **Un uso che possa in qualche modo recare qualsiasi danno all'Ente o a terzi**

Utilizzo della posta elettronica

La casella di posta, assegnata dalla Società è uno strumento di lavoro. **Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.**

È fatto divieto di utilizzare le caselle di posta elettronica della struttura per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mailing-list salvo diversa ed esplicita autorizzazione.

È buona norma evitare messaggi completamente estranei al rapporto di lavoro o alle relazioni tra colleghi. **La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti**. **Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali con la Società ricevuta da personale non autorizzato, deve essere visionata ed inoltrata al Responsabile d'Ufficio, o in ogni modo è opportuno fare riferimento alle procedure in essere per la corrispondenza ordinaria.**

La documentazione elettronica che viene contraddistinta da diciture od avvertenze dirette ad evidenziarne il carattere riservato o segreto, non può essere comunicata all'esterno senza preventiva autorizzazione del Titolare del trattamento. È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario. Per la trasmissione di file all'interno della struttura è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati (ad esempio per dimensioni superiori a 2 Mbyte è preferibile utilizzare le cartelle di rete condivise).

È obbligatorio controllare i file Attachments di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web, HTTP o FTP non conosciuti) e accertarsi dell'identità del mittente.

Tutti coloro provvisti di indirizzo individuale, devono indicare il tutor del proprio account ossia la persona autorizzata ad aprire la posta del soggetto assente o quantomeno la persona che riceverà la posta del lavoratore assente. Dopo tre mesi di assenza, l'account verrà disattivato e con esso la posta sarà trasferita ad un nuovo utente.

Per motivi di sicurezza la struttura non consente in alcun modo l'utilizzo di posta personale né attraverso l'uso di un webmail né utilizzando un client di posta.

In particolare nell'uso della Posta Elettronica non sono consentite le seguenti attività:

- **La trasmissione a mezzo di posta elettronica di dati sensibili, confidenziali e personali di alcun genere**, salvo i casi espressamente previsti dalla normativa vigente in materia di protezione dei dati personali

- **L’apertura di allegati ai messaggi di posta elettronica senza il previo accertamento dell’identità del mittente**
- **Inviare tramite posta elettronica user-id, password, configurazioni della rete interna, indirizzi e nomi dei sistemi informatici**
- **Inoltrare “catene” di posta elettronica (**catene di S. Antonio e simili), anche se afferenti a presunti problemi di sicurezza

Gestione dei dati cartacei

Di seguito sono indicate le modalità operative e tecniche, che devono essere attuate in modo tassativo dal nostro personale, al fine di assicurare l'integrità e la protezione dei dati personali gestiti su supporto cartaceo.

In particolare, alla data odierna, la Società è impegnata nel ridurre al minimo indispensabile il ricorso al cartaceo per il trattamento dei dati personali. In ogni caso, alla data di emissione del presente manuale, la nostra azienda effettua il trattamento cartaceo dei dati relativi alle seguenti categorie di titolari:

a) Personate dipendente e collaboratori

b) Clienti

c) Fornitori

Tali dati sono gestiti attraverso documenti archiviati in armadi, scaffali e schedari all'interno dei quali i documenti sono ordinati per tipologia e titolare dei dati medesimi.

Ogni archivio predisposto costituisce l'unico luogo sicuro per la tutela e garanzia di riservatezza dei dati e deve essere tenuto al riparo da accessi non autorizzati.

A tale scopo l'archivio generale destinato ad accogliere tutta la documentazione commerciale e cantabile prodotta nel tempo è protetto tramite porta chiusa a chiave.

Sono autorizzati ad accedere a tali documenti solo ed esclusivamente i Responsabili, i designati e gli Incaricati al trattamento che dispongono della chiave di accesso.

Precauzioni ancora più rigorose sono, inoltre, applicate nel caso dei documenti inerenti i dati sanitari dei dipendenti aziendali (certificati medici; copie cartacee Green Pass etc…).

In particolare**, tutta la documentazione sanitaria è custodita presso la sala medica ed è tenuta in armadi chiusi a chiave la cui responsabilità è delegata al Designato/Incaricato al trattamento dei dati**

Ogni Incaricato, inoltre, può accedere ed effettuare, esclusivamente, il trattamento dei dati cartacei per le finalità riportate nella propria lettera di nomina e nel rispetto delle seguenti indicazioni:

- **I documenti contenenti dati personali possono essere asportati dagli archivi in cui sono custoditi solo per il tempo strettamente necessario ad effettuare le operazioni di trattamento e non interi faldoni o pratiche**.
- **Per tutto il tempo in cui il documento è fuori dall’archivio l'incaricato deve adempiere a precisi obblighi di custodia** che diano sufficiente garanzie di protezione da accessi non

autorizzati (armadio chiuso a chiave, cassette chiuso a chiave, una cassaforte, classificatore chiuso a chiave).

- **Documenti contenenti dati sensibili o dati** che, per una qualunque ragione, siano stati indicati dal Responsabile come meritevoli di particolare aftenzione, in fase di affidamento, **devono essere custoditi con misure più rigide** e comunque specificate, di volta in vette, dello stesso Responsabile.
- **Eventuali fotocopie non riuscite bene debbono essere distrutte in un apposito distruggi documenti, se disponibile, oppure devono essere strappate** in pezzi talmente piccoli, da non consentire in alcun modo a ricostruzione del contenuto, che deve essere comunque illeggibile.
- **E' tassativamente proibito utilizzare le fotocopie non riuscite come carta per appunti in quanto, anche**
- E' parimenti tassativamente proibito trasportare all'esterno del pasto di lavoro fotocopie non riuscite o da utilizzare altrove come carta per appunti.
- **Quando i documenti devono essere trasportati all'esterno del luogo di lavoro, l'Incaricato deve tenere applicare le cautele più rigorose per la sicurezza del documento**
- Si faccia molta attenzione all'utilizzo di macchine fotocopiatrici di ultimo generazione, che possono catturare l'immagine del documento, memorizzarla e successivamente stamparla, talvolta conservando file elettronico del documento; in questo caso la fotocopiatrice non va classificata come strumento non elettronico, ma come strumento elettronico, ad a tutti gli effetti devono essere applicate le cautele previste per questa tipologia di strumenti nella precedente sezione del manuale.

In caso di dubbio sulle modalità di applicazione di quanta sopra illustrato, o per chiedere ulteriori chiarimenti in merito, l'Incaricato deve rivolgersi **al Responsabile del Trattamento**

Gestione aree locali

Di seguito sono riportati i criteri tecnici ed organizzativi per la protezione delle aree e dei locali interessati alle misure di sicurezza nonché le procedure per controllare l'accesso delle persone ai locali medesimi

La nostra azienda si estende su un'area di circa 48.000 mq di cui la metà coperta è destinata agli impianti di produzione ed uffici amministrativi

L'intero stabile è circoscritto da una recinzione, il cui accesso è protetto tramite cancello. Gli uffici, entro i quali si esegue il trattamento dei dati, si sviluppano su circa 400 mq. **L'accesso nei diversi uffici e presidiato e controllato dal personale interno**

I locali destinati ad archivio sia cartaceo che informatico (archivio generale - sala CED - sala medica) sono tenuti chiusi a chiave.

Tutti coloro che dispongono delle chiavi per accedere allo stabilimento e/o agli archivi sono tenuti al rispetto delle seguenti regole comportamentali:

- Applicare ogni misura necessaria per evitarne lo smarrimento;
- Conservare, sempre, le chiavi con i propri effetti personali (borsa, tasche, ecc.);
- Non consegnare le chiavi ad altre persone (colleghi, amici, ecc);
- Non lasciare mai le chiavi incustodite.

Nelle ore di apertura dei nostri uffici, l'accesso alla sede della Società di persone estranee all'azienda è consentito soltanto previo riconoscimento e autorizzazione da parte del personale amministrativo.

La sede dispone di un **servizio di vigilanza (Securpol di Frosinone**); tale sistema garantisce la necessaria protezione dei locali contro furti violazioni e accessi negli orari extra -lavorativi.

Videosorveglianza

Il trattamento dei dati personali effettuato con impianti di videosorveglianza e di videocontrollo installati presso gli immobili e le aree di pertinenza in cui si svolge l'attività della Francesco Pisani & Figli spa risponde a tutte le prescrizioni dettate dal Regolamento (UE) 2016/679, dal D.Lgs. n. 196/2003, così come modificato dal D.Lgs. n. 101/2018 nonché dal Provvedimento in materia di videosorveglianza - 8 aprile 2010 del Garante per la Protezione dei dati personali.

Nell'attivazione e nell'utilizzo degli impianti sono rispettate altresì le garanzie e le procedure di cui all'art. 4 della Legge del 20 maggio 1970, n. 300.

La sicurezza aziendale della Francesco Pisani & Figli S.p.a. è garantita da un sistema di videosorveglianza (h 24).

Le aree aziendali sottoposte a videosorveglianza sono:

- L'Ingresso
- Il parcheggio automezzi trasportatori
- Parcheggio autovetture dipendenti
- Depuratore industriale.

Gli interessati devono sempre essere informati, tramite apposita informativa, che stanno per accedere ad una zona videosorvegliata.

Gli interessati vengono, infatti, portati a conoscenza dell'installazione degli impianti di videosorveglianza tramite **cartelli informativi (il cartello "Area videosorvegliata)** da collocare prima del raggio di azione della videocamera ed in una posizione chiaramente visibile).

La Società mette inoltre a disposizione degli interessati, nel sito internet aziendale e attraverso affissione, l'informativa estesa, contenente tutti gli elementi definiti dalla normativa vigente in materia di protezione dei dati personali, come da indicazione del Garante:

- i **dati di contatto del Titolare del trattamento, quelli del Responsabile della Protezione dei Dati (DPO), se presente;**
- **le finalità del trattamento, la base giuridica che generalmente risiede nell'interesse legittimo del titolare *ex* art. 6, comma 1, lett. f) del GDPR;**
- **i destinatari del trattamento;**
- **l'eventuale trasferimento degli stessi all'estero;**
- **i diritti dell'interessato ex artt. 15, 16, 17, 18 e 21.**

I dati raccolti mediante i sistemi di videosorveglianza non possono essere utilizzati per finalità diverse o ulteriori rispetto a quelle sopra elencate e non possono essere diffusi o comunicati salvo essere trasferiti a soggetti legittimati a richiederli come l'Autorità Giudiziaria e/o di Pubblica Sicurezza.

Si precisa che il Referente Privacy di competenza, qualora registri l'assenza dell'informativa semplificata o di una delle sue caratteristiche, è tenuto a comunicarlo tempestivamente al Responsabile della videosorveglianza aziendale per le opportune azioni da intraprendere.

L'attività di videosorveglianza attivata presso la Francesco Pisani & Figli spa rispecchia le regole di legge e del Regolamento UE, ed in particolare:

- è attivata esclusivamente presso zone soggette a concreti pericoli o per le quali ricorra un'effettiva esigenza di deterrenza e solo nel caso in cui altre misure (es. sistemi di allarme, controlli fisici o logistici, misure di protezione agli ingressi) non sono sufficienti, non sono attuabili o non sono parimenti efficaci;
- la scelta delle modalità di ripresa e dislocazione degli impianti, viene effettuata nel rispetto del principio di proporzionalità in modo da comportare comunque un trattamento di dati pertinenti e non eccedenti rispetto alle finalità perseguite;
- si svolge nel rispetto dei diritti e delle libertà fondamentali nonché della dignità dell'interessato.

Inoltre la Società effettua attività di videosorveglianza esclusivamente per le seguenti **finalità istituzionali**:

- **garantire la sicurezza dei dipendenti e collaboratori**;
- **tutelare il patrimonio aziendale**;
- **tutelare i beni privati e le persone presenti nelle aree esterne da possibili atti illeciti, danneggiamenti, atti di vandalismo o furti**;
- tutelare le ulteriori finalità di sicurezza nei luoghi di lavoro

L'installazione di sistemi di videosorveglianza deve avvenire nel rispetto dei seguenti limiti:

- **l'attività considerata non può costituire forma di controllo a distanza dei lavoratori, in quanto vietata dall'art. 4, comma 1 della Legge del 20 maggio 1970, n. 300** (c.d. Statuto dei lavoratori),
- **non è ammessa l'installazione di apparecchiature di videocontrollo o di videosorveglianza in luoghi riservati esclusivamente ai lavoratori o non destinati all'attività lavorativa** (ad esempio bagni, docce, spogliatoi, armadietti e spazi ricreativi);
- **la presenza dell'impianto di videocontrollo o di videosorveglianza deve essere resa nota mediante esposizione, nel luogo in cui l'impianto è ubicato, di apposite informative**.

Considerata l'esigenza di uniformare a livello aziendale la procedura di gestione dei dati trattati mediante videosorveglianza, **il periodo di conservazione è di 72 ore dalla registrazione**. Tale

limite potrà essere superato solo in relazione a richieste investigative dell'Autorità Giudiziaria e della Polizia Giudiziaria. Inoltre, in casi eccezionali, in relazione a particolari esigenze tecniche o situazioni di grave rischiosità, è ammesso un tempo più ampio di conservazione dei dati che non può comunque superare i tre giorni, salvo diverse indicazioni scritte da parte dell'Autorità Giudiziaria e delle Forze dell'Ordine.

Il Titolare del trattamento dei dati raccolti con il sistema di videosorveglianza è la Francesco Pisani & Figli S.p.a. La responsabilità della corretta applicazione della procedura in tema di videocontrollo/monitoraggio è del Referente privacy per la videosorveglianza.

La sicurezza aziendale è inoltre garantita anche da un sistema antincendio realizzato in piena conformità alle norme e prescrizioni di legge in materia di sicurezza sul lavoro.

I locali adibiti ad ufficio sono, infine, dotati di gruppi di continuità e/o batterie atti ad evitare improvvise interruzioni di energia elettrica the potrebbero arrecare danni ai dati infornatici.

Nelle ore e nei giorni di chiusura dei nostri uffici l'accesso è consentito, previa autorizzazione, ai soli autorizzati.

C) PROCEDURA PER LA GESTIONE DELLE VIOLAZIONI – DATA BREACH

Il GDPR disciplina i Data Breach, ovvero **le procedure che un'organizzazione pubblica o privata deve adottare in caso di incidente di sicurezza in cui dati sensibili, protetti o riservati vengono consultati, copiati, trasmessi, rubati o utilizzati da un soggetto non autorizzato**.

Si verifica, pertanto, un caso di data breach se una divulgazione o un accesso non autorizzato o accidentale causa un'alterazione o la perdita, l'impossibilità di accesso o la distruzione, accidentale o non autorizzata, di dati personali. Ovviamente in questi casi non rientra solamente il furto o il danno provocato da soggetti terzi malintenzionati, ma anche la perdita accidentale, quindi la cancellazione di dati per un errore umano o di sistema, o semplicemente l'impossibilità di accesso al dato, per esempio la perdita della password di accesso ad un archivio protetto, o la criptazione provocata da un'infezione da ramsonware.

L'autorità di controllo a cui segnalare il Data Breach è il **Garante della Privacy**, come definito dall'articolo 55 del General Data Protection Regulation.

Il **registro dei data breach** è una documentazione che, ai sensi dell'art. 33 del GDPR, il Titolare del trattamento è tenuto a conservare per tenere traccia di tutti i data breach avvenuti.

Il registro dei data breach deve contenere le seguenti informazioni:

- i dettagli relativi al data breach, ovvero informazioni inerenti le cause della violazione, il luogo nel quale essa è avvenuta e la tipologia dei dati personali violati;
- gli effetti e le conseguenze della violazione;
- il piano di intervento predisposto dal titolare;
- la motivazione delle decisioni assunte a seguito del data breach nei casi in cui: o il titolare ha deciso di non procedere alla notifica o il titolare ha ritardato nella procedura di notifica o il titolare ha deciso di non notificare il data breach agli interessati

Il registro dei data breach deve essere continuamente aggiornato e messo a disposizione del Garante qualora l'Autorità chieda di accedervi.

Il titolare del trattamento dovrà registrare nel registro il data breach che ha coinvolto la Struttura contestualmente alla comunicazione al Garante, avendo cura di inserire tempestivamente gli elementi che dovessero emergere all'esito di ulteriori verifiche.

Il registro dovrà inoltre essere strutturato in modo da garantire l'integrità e l'immodificabilità delle registrazioni in esso contenute.

Assenza di rischi

In caso non ci fosse alcun rischio connesso all'attacco verso i dati personali immagazzinati, è necessario registrare la violazione e successivamente conservare il Registro. **La notifica al Garante della Privacy non è obbligatoria** ed è comunque necessario comprovare l'assenza dei rischi**.**

Presenza di rischi

In presenza di rischi per gli interessati è necessaria **la notifica entro 72 ore al Garante della Privacy**, il quale rilascia un apposito modulo (Modello di segnalazione Data Breach).

La procedura da seguire è:

- Raccogliere tutte le informazioni inerenti al Data Breach per la notifica al Garante della Privacy;
- Inviare la notifica al Garante della Privacy
- Registrare la violazione
- Conservare il registro delle violazioni

Presenza di un elevato rischio

La procedura da seguire è:

- Raccogliere tutte le informazioni inerenti al Data Breach per la notifica al Garante della Privacy e ai diretti interessati del trattamento
- Inviare la notifica al Garante della Privacy e agli interessati
- Gestione dei riscontri da parte degli interessati
- Registrare la violazione
- Conservare il registro delle violazioni

Per un **rischio elevato** si intende per esempio una **violazione che interessa un rilevante quantitativo di dati personali e/o di soggetti interessati,** piuttosto che un data breach che impatta su soggetti vulnerabili per le loro condizioni o categorie particolari di dati personali.

Inoltre, **ogni Interessato può segnalare, anche solo in caso di sospetto, che i propri Dati Personali siano stati utilizzati abusivamente o fraudolentemente da un terzo;** in tal caso, l'Interessato può richiedere all'azienda la verifica dell'eventuale violazione.

Per la **segnalazione è necessario compilare la Scheda Evento, allegata alla presente procedura,** contenente tutte le informazioni raccolte:

- Data evento anomalo;
- Data presunta di avvenuta violazione;
- Data e ora in cui si è avuto conoscenza della violazione;
- Fonte segnalazione;
- Tipologia violazione e di informazioni coinvolte;
- Descrizione evento anomalo;
- Numero Interessati coinvolti;
- Numerosità di Dati Personali di cui si presume una violazione;
- Indicazione del luogo in cui è avvenuta la violazione dei dati, specificando altresì se essa sia avvenuta a seguito di smarrimento di Device Mobili;
- Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione.

La Scheda Evento viene consegnata dall'interessato al Titolare che può farsene carico o designare un delegato.

La presa in carico di tutte le segnalazioni è di responsabilità del Responsabile del Trattamento che provvederà a gestirle coinvolgendo le altre funzioni interessate secondo quanto specificato nella presente procedura.

Casi particolari che possono verificarsi nel corso del Data Breach sono i seguenti:

Approssimazione: il titolare che non sia ancora in grado di conoscere con certezza il numero di persone e di dati personali interessati dalla violazione può comunicarne in prima battuta un ammontare approssimativo, provvedendo a specificare il numero esatto a seguito di accertamenti.

Notificazione in fasi: in questo caso il titolare, per la complessità o estensione della violazione, potrebbe non essere in grado di fornire con immediatezza all'autorità tutte le informazioni necessarie. Potrà allora ottemperare agli obblighi di notifica comunicando, dopo una prima e rapida notifica di alert, tutte le informazioni per fasi successive, aggiornando di volta in volta l'autorità sui nuovi riscontri.

Notifica differita: dopo le 72 ore previste dall'art. 33. È il caso in cui, per esempio, un'impresa subisca violazioni ripetute, ravvicinate e di simile natura che interessino un numero elevato di soggetti. Al fine di evitare un aggravio di oneri in capo al titolare e l'invio scaglionato di un numero elevato di notificazioni tra loro identiche, il titolare è autorizzato ad eseguire un'unica "notifica aggregata" di tutte le violazioni occorse nel breve periodo di tempo (anche se superi le 72 ore), purché la notifica motivi le ragioni del ritardo.

Anche il responsabile del trattamento potrà notificare la violazione per conto del titolare, anche se a lui restano le responsabilità a essa collegate.

Analizzare la violazione e valutarne i rischi connessi

L'analisi consente al titolare di individuare con prontezza adeguate misure per arginare o eliminare l'intrusione e di valutare la necessità di attivare le procedure di comunicazione e di notifica (che si ricorda si attivano solo al superamento di determinate soglie di rischio).

Obiettivo dell'analisi di primo livello è quella di verificare che la segnalazione non si tratti di un cd. "falso positivo".

Nel caso la violazione su dati personali venga accertata il Titolare o il suo delegato recupera le informazioni di dettaglio sull'evento necessarie alle analisi di secondo livello, e le riporta nella Scheda Evento.

Nel caso in cui l'evento segnalato risulti essere un falso positivo, si chiude l'incidente e la funzione IT/Security si attiva per effettuare un raffinamento delle regole di rilevazione dei falsi positivi, comunicando via e-mail l'esito dell'analisi al Titolare. L'evento viene comunque inserito a cura del Titolare o del suo delegato nel Registro dei Data Breach nella apposita sezione dedicata agli "eventi falsi positivi". Per l'analisi di secondo livello vengono analizzate congiuntamente tutte le informazioni raccolte e redige una Scheda Violazione Dati per le conseguenti valutazioni.

L'evento viene classificato tra i seguenti casi:

a. ***violazione di riservatezza,*** ovvero quando si verifica una divulgazione o un accesso a dati personali non autorizzato o accidentale.
b. ***Violazione di integrità***, ovvero quando si verifica un'alterazione di dati personali non autorizzata o accidentale.
c. ***Violazione di disponibilità,*** ovvero quando si verifica perdita, inaccessibilità, o distruzione, accidentale o non autorizzata, di dati personali. In particolari circostanze le violazioni potrebbero essere combinate tra loro.

La violazione deve essere valutata secondo i livelli di rischio:

- **NULLO**
- **BASSO**
- **MEDIO**
- **ALTO**

Il rischio va riferito alla probabilità che si verifichi una delle seguenti condizioni a danno di persone fisiche anche diverse dall'Interessato a cui si riferiscono i dati, a causa della violazione dei Dati Personali:

a) discriminazioni
b) furto o usurpazione d'identità
c) perdite finanziarie
d) pregiudizio alla reputazione
e) perdita di riservatezza dei dati personali protetti da segreto professionale
f) decifratura non autorizzata della pseudonimizzazione
g) danno economico o sociale significativo
h) privazione o limitazione di diritti o libertà
i) impedito controllo sui dati personali all'interessato
j) danni fisici, materiali o immateriali alle persone fisiche.

Saranno inoltre valutate, come variabili qualitative dell'impatto temuto, le seguenti eventuali condizioni:

k) che si tratti di dati idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché di dati genetici, dati relativi alla salute o dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza;

l) che si tratti di dati relativi a **valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personal**i;

m) che si tratti di dati di persone fisiche vulnerabili, in particolare minori;

n) che il trattamento riguardi una notevole quantità di Dati Personali;

o) che il trattamento riguardi un vasto numero di Interessati. Il Titolare deve provvedere affinché vengano tempestivamente adottate misure che consentano di minimizzare le conseguenze negative della violazione.

<u>Contenuto della notifica al Garante (Art. 33, p.3 GDPR</u>*)*

La Comunicazione al Garante della violazione dei dati deve avere questi contenuti:

- Descrizione della natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione, nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione.
- Il nome e i dati di contatto del Responsabile della Protezione dei Dati o di altro punto di contatto presso cui ottenere più informazioni.
- Descrizione delle probabili conseguenze della violazione dei dati personali.
- Descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuare i possibili effetti negativi.

Contenuto della Comunicazione agli interessati (Art. 34 p.3 GDPR)

In primo luogo il GDPR determina l'essenzialità della **notifica della violazione** dei dati all'autorità e della **comunicazione** ai soggetti interessati quando il data breach mette a rischio **le libertà e i diritti** di un individuo quali:

- Danni fisici, materiali o morali
- Danni economici o sociali
- Perdita del controllo dei dati
- Limitazione dei diritti
- Discriminazione
- Furto o usurpazione d'identità
- Perdite finanziarie
- Decifratura non autorizzata della Pseudoanimizzazione
- Pregiudizio alla reputazione
- Perdita di riservatezza dei dati protetti da segreto professionale (sanitari, giudiziari) Mentre per far scattare l'obbligo di notifica è sufficiente che sussista una violazione di dati personali che presenti un rischio per i diritti e le libertà delle persone fisiche, per la comunicazione occorre che tale rischio sia indicato come ALTO nella Scheda Violazione Dati.

La comunicazione all'interessato non è tuttavia richiesta se si ravvisano una serie di circostanze specifiche:

• quando il titolare del trattamento ha messo in atto, e applicato ai dati che sono stati oggetto di violazione, tutte le necessarie misure tecniche e organizzative di protezione, comprese quelle destinate a rendere i dati personali incomprensibili ai soggetti non autorizzati (come, ad esempio, la cifratura delle informazioni).

• quando il titolare del trattamento abbia successivamente adottato misure per scongiurare il verificarsi di un rischio elevato per i diritti e le libertà degli interessati.

• quando la comunicazione stessa richiederebbe sforzi sproporzionati e, in tal caso, si può procedere a una comunicazione pubblica o ad altra soluzione analoga, così da informare gli interessati in maniera ugualmente efficace. In sostanza, dunque, è opportuno procedere a un duplice controllo: da un lato, occorre verificare che siano state adottate le misure di protezione adeguate, così da poter stabilire se c'è stata violazione dei dati personali e informare, di conseguenza, l'autorità di controllo e gli interessati. Dall'altro, si deve stabilire se la notifica è stata trasmessa senza ingiustificato ritardo, tenendo conto, in particolare, della natura e della gravità della violazione, nonché delle sue conseguenze ed effetti negativi per l'interessato.

Devono sempre essere **privilegiate modalità di comunicazione diretta con i soggetti interessati (quali email, SMS o messaggi diretti)**. Il messaggio dovrebbe essere comunicato in maniera evidente e trasparente, evitando quindi di inviare le informazioni nel contesto di update generali o newsletter, che potrebbero essere facilmente fraintesi dai lettori. Inoltre, dovrebbe tenere conto di possibili formati alternativi di visualizzazione del messaggio e delle diversità linguistiche dei soggetti riceventi (es. l'utilizzo della lingua madre dei soggetti riceventi rende il messaggio immediatamente comprensibile).

Anche in questo caso, il Regolamento è attento a non gravare i titolari di oneri eccessivi prevedendo che, nel caso la segnalazione diretta richieda sforzi sproporzionati, questa possa essere effettuata attraverso una comunicazione pubblica. Si sottolinea però che anche questo tipo di comunicazione deve mantenere lo stesso grado di efficacia conoscitiva del contatto diretto con l'interessato. Così, mentre può ritenersi adeguata la comunicazione fornita attraverso evidenti banner o notifiche disposte sui siti web, non lo sarà se questa sia limitata all'inserimento della notizia in un blog o in una rassegna stampa.

La comunicazione agli interessati deve avere questi contenuti:

- Descrizione con un linguaggio semplice e chiaro della natura della violazione dei dati personali.
- Data e ora della violazione, anche solo presunta, e data e ora in cui si è avuto conoscenza della stessa;
- Il nome e i dati di contatto del Responsabile della Protezione dei Dati o di altro punto di contatto presso cui ottenere più informazioni.
- Descrizione delle probabili conseguenze della violazione dei dati personali.
- Descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuare i possibili effetti negativi.