ORDINE DEGLI INGEGNERI DI CUNEO
Via V.Allione, 4 - 12100 – Cuneo (CN)
Codice fiscale: 80019740044

PROCEDURE INTERNE DI SISTEMA

ai sensi del Regolamento UE n. 2016/679 - relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e del Principio di Accountability

Testo approvato dal PRESIDENTE DELL'ORDINE

IL PRESIDENTE DELL'ORDINE
(Dott. Ing. Sergio Sordo)

Firma _____

Testo adottato dall'ORDINE DEGLI INGEGNERI

IL PRESIDENTE DELL'ORDINE
(Dott. Ing. Sergio Sordo)

Firma _____

Data	Revisione	Descrizione
22/05/2019	00	Prima emissione
07/07/2020	01	Prima revisione
20/09/2021	02	Aggiornamento

Procedura interna di sistema - PRO 1.0.

GESTIONE STRUMENTI ELETTRONICI DI TRATTAMENTO

Ai sensi del Regolamento UE n. 2016/679 - relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e del Principio di Accountability

1. GESTIONE DEGLI STRUMENTI ELETTRONICI

Ciascun autorizzato è responsabile del corretto utilizzo e della custodia degli strumenti elettronici in dotazione (a titolo esemplificativo personal computer, periferiche, lettori di smart card) ed è tenuto a custodirli con diligenza sia nel corso degli spostamenti che durante l'utilizzo nel luogo di lavoro. È necessario che egli adotti misure di sicurezza adeguate alla tutela della riservatezza, onde evitare l'accesso ai dati da parte di soggetti estranei all'organizzazione o non specificamente autorizzati.

Le regole di seguito riportate si adottano sia in caso di utilizzo di pc fisso che in caso di eventuale utilizzo di un portatile:

- in caso di assenza momentanea dalla propria postazione, l'autorizzato in quanto utente del computer, deve accertarsi che l'eventuale sessione di lavoro aperta non sia accessibile da altri soggetti. Pertanto deve chiudere la sessione di lavoro sul PC facendo Logout, oppure deve attivare un salvaschermo (screen- saver) protetto dalle credenziali di autenticazione personali;

- al termine delle ore di lavoro, l'autorizzato deve provvedere a spegnere il proprio PC, a meno che non stia svolgendo elaborazioni particolari. In tale ultimo caso gli uffici devono tassativamente essere chiusi a chiave.

- relativamente all'utilizzo dello screen-saver sul PC, occorre osservare le seguenti prescrizioni:
    - non deve mai essere disattivato;
    - il suo avvio automatico deve essere previsto non oltre i primi 10 minuti di inattività del PC;
    - deve essere messo in funzione manualmente ogni volta che si lascia il PC incustodito ed acceso.

Qualora si utilizzino PC portatili valgono le seguenti ulteriori raccomandazioni:

- prima della riconsegna, l'autorizzato deve rimuovere eventuali file ivi elaborati;
- quando il PC portatile è nei locali dell'Ordine, deve evitare di lasciarlo incustodito; in caso di brevi assenze è necessario che egli si assicuri di avere attive misure di protezione adeguate al fine di evitare l'accesso al PC da parte di soggetti non autorizzati, e ove possibile è consigliato chiudere a chiave la porta dell'ufficio;
- quando il PC portatile è all'esterno dei suddetti locali, non deve mai lasciarlo incustodito;
- in caso di furto di un portatile deve avvertire tempestivamente l'Amministratore di sistema, onde prevenire possibili intrusioni ai sistemi;
- deve eseguire periodicamente salvataggi dei dati e non tenere tali backup insieme al PC portatile;
- nell'eventualità in cui venisse a mancare la fornitura di energia elettrica, si consiglia all'autorizzato, trascorsi cinque minuti dall'interruzione dell'erogazione, di provvedere alla chiusura di tutti gli applicativi utilizzati al fine di salvaguardare l'integrità dei dati elaborati e procedere allo spegnimento del PC.

Inoltre quando l'autorizzato esegue la stampa di un documento contenente dati personali, in particolare su una stampante condivisa, deve ritirare tempestivamente i documenti stampati per evitare l'accesso a soggetti non abilitati al trattamento.

La composizione informatica dell'Ordine degli Ingegneri è stata riassunta nella seguente tabella

NR	COLLOCAZIONE	PC		COLLEGAMENTO		Proprietà/ noleggio	ACCESSIBILE AL PUBBLICO		SISTEMA OPERATIVO USATO	ANTIVIRUS	
		FISSO	PORTATILE	INTERNET	RETE LOCALE		SI	NO		VERSIONE	FREQUENZA AGGIORNAMENTO
1	UFF. SEGRETERIA FERRARA PATRIZIA	X		X	X	NOLEGGIO		X	WINDOWS 10	BITDEFENDER	CONTINUA
2	UFF. SEGGRETERIA BERTACCINI CHIARA	X		X	X	NOLEGGIO		X	WINDOWS 10	BITDEFENDER	CONTINUA
3	PC-SALA RIUNIONI		x			PROPRIETA'		X	WINDOWS 10	BITDEFENDER	CONTINUA

SERVER UTILIZZATO DALL'ORDINE					
MARCA	MODELLO	SISTEMA OPERATIVO	COLLOCAZIONE	ACCESSIBILE AL PUBBLICO	ANTIVIRUS
DELL	**PowerEdge T440**	**Windows Server 2019**	**Sede Ordine**	**NO**	**PRESENTE ED AGGIORNATO**

Il sistema informatico dell'Ordine degli Ingegneri presenta un'architettura Client-server. L'organizzazione ha deciso di dotarsi di un server in cloud. Inoltre al fine di impedire intrusioni informatiche nei sistemi, a protezione degli strumenti elettronici è stato adottato un sistema FIREWALL, il quale presenta le seguenti caratteristiche tecniche:

MARCA E MODELLO	PFSENSE 2.5 - COMPACT SMALL UTM
FUNZIONE	FIREWALL PER LA RETE, NAT VERSO L'ESTERNO, CONNESSIONE VPN DA REMOTO.

2. GESTIONE PROTEZIONE DAI VIRUS INFORMATICI

Per prevenire eventuali danneggiamenti al software causati dalla presenza o dall'azione di programmi virus informatici, su ogni elaboratore è installato un software antivirus che si aggiorna automaticamente all'ultima versione disponibile, così come si evince dalla tabella di cui al capitolo precedente. L'antivirus non deve mai essere disattivato o sostituito con altro antivirus non ufficialmente fornito.

Nel caso il programma antivirus installato sul proprio PC riscontri la presenza di un virus, oppure si sospetti la presenza di un virus non rilevato dal programma antivirus è necessario darne immediatamente segnalazione al responsabile del Servizio Informatico.

Si raccomanda di non scaricare e né tantomeno aprire file provenienti via e-mail da mittenti sconosciuti. Tali file, potrebbero essere portatori di virus e compromettere la funzionalità del PC, l'integrità dei dati in esso contenuti e soprattutto l'integrità dei sistemi collegati al PC stesso.

3. GESTIONE DELLE USERNAME E PASSWORD

All'interno dell'Organizzazione l'accesso alle procedure informatiche che comportano il trattamento di dati personali e/o particolari è consentito agli autorizzati al trattamento in possesso di credenziali di autenticazione. Queste ultime permettano infatti il superamento di una procedura di autenticazione e di autorizzazione. Nello specifico, le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato (user-id o username) associato ad una parola chiave riservata (password).

La password dovrà rispondere ai seguenti requisiti minimi di sicurezza:
- deve essere costituita da una sequenza di minimo otto caratteri alfanumerici, oppure, nel caso che lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito;
- non deve essere facilmente individuabile;
- non deve contenere riferimenti riconducibili all'autorizzato (es.: cognome, nome, codice di accesso, etc.);
- non deve contenere la username;
- non deve essere simile alla password precedente.

Gli autorizzati al trattamento sono responsabili della custodia, dell'utilizzo delle proprie credenziali di autenticazione e di ogni utilizzo indebito o non consentito, pertanto devono utilizzarle e gestirle attenendosi alle seguenti istruzioni:

- la parola chiave assegnata dall'informatico, deve essere prontamente sostituita dall'autorizzato al primo utilizzo;
- laddove non prevista la forma di sostituzione automatica, la password deve essere modificata ogni 6 mesi, ogni 3 mesi in caso di trattamenti di dati particolari;
- la parola chiave deve essere custodita con la massima attenzione e segretezza, non deve essere divulgata e non deve essere scritta su nessun tipo di supporto (cartaceo/elettronico);
- nel caso in cui l'autorizzato dimentichi la propria password, dovrà provvedere immediatamente cambiandola;
- se l'autorizzato ha il sospetto di una perdita di qualità delle proprie credenziali è tenuto immediatamente a darne notizia all'Amministratore di sistema e contestualmente procedere al cambio della password;
- il Titolare ha facoltà di disattivare immediatamente le credenziali delle risorse umane che cessano la propria collaborazione con l'Organizzazione. Dopo trenta giorni l'utente, se non vi sono necessità specifiche (derivanti da richieste scritte), viene cancellato definitamente.

4. GESTIONE DELLA POSTA ELETTRONICA INTERNA

Il servizio di posta elettronica viene fornito per permettere la comunicazione con soggetti terzi interni ed esterni per le finalità dell'Organizzazione e in stretta connessione con l'effettiva attività e mansioni dell'autorizzato che utilizza tale funzionalità.
Al fine di non compromettere la sicurezza della struttura e di prevenire conseguenze legali a carico della stessa, è necessario adottare le seguenti norme comportamentali:

- se si ricevono mail da destinatari sconosciuti contenenti file di qualsiasi tipo, procedere alla loro immediata eliminazione;

- nell'invio di allegati (contenenti dati personali) mediante email, prestare attenzione nell'individuazione del destinatario e nella correttezza dei documenti, in modo da non divulgare eventuali dati a soggetti non interessati o non autorizzati alla conoscenza degli stessi;
- la casella di posta elettronica assegnata deve essere mantenuta in ordine;
- è fatto divieto di utilizzare le caselle di posta elettronica per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail list, salvo diversa ed esplicita autorizzazione;

- nell'ipotesi in cui la email debba essere utilizzata per la trasmissione di dati particolari si raccomanda di prestare attenzione a che:
    - l'indirizzo del destinatario sia stato correttamente digitato,
    - l'oggetto del messaggio non contenga direttamente il riferimento a stati, fatti o qualità idonei a rivelare dati di natura sensibile;
    - nel corpo del messaggio sia presente un'intestazione standardizzata in cui si avverta della confidenzialità/riservatezza del messaggio.

La normativa, ed in i provvedimenti adottati dal Garante della privacy, ritiene che il contenuto dei messaggi di posta elettronica (compresi i file allegati) riguardano forme di corrispondenza assistite da garanzie di segretezza, e che ciò, trasposto in ambito lavorativo, comporta la possibilità che il lavoratore possa vantare una legittima aspettativa di riservatezza su talune forme di comunicazione durante l'attività lavorativa ed anche nell'ipotesi in cui venga a cessare il rapporto di lavoro tra le parti. Come suggerito dal Garante, è buona norma rendere disponibili prima di tutto indirizzi di posta elettronica condivisi tra più lavoratori ed in tale ottica si è infatti adoperato il Titolare del trattamento.

Tuttavia il Titolare del trattamento, in caso di cessazione del rapporto di lavoro con un autorizzato, rimuoverà eventuali account di posta elettronica dell'Organizzazione riconducibili alla persona identificata o identificabile, previa disattivazione degli stessi e contestuale adozione di sistemi automatici volti ad informarne i terzi fornendo a questi ultimi indirizzi alternativi e si provvederà ad ad impedire la visualizzazione dei messaggi in arrivo durante il periodo in cui tale sistema automatico sarà in funzione.

6. UTILIZZO DELLA RETE

Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto non si deve salvare in queste unità, nemmeno per brevi periodi, alcun file che non sia legato all'attività lavorativa.

Sulle unità di rete devono essere svolte regolari attività di controllo, amministrazione e backup da parte del tecnico informatico. In caso vengano trovati file non direttamente conducibili all'attività lavorativa, questi vengono eliminati.

Nel caso in cui il tecnico informatico ritenga alcuni file o applicazioni pericolosi per la sicurezza dei Personal Computer degli autorizzati o per le unità di rete, può in qualunque momento procedere alla rimozione.

Qualora la cartella di salvataggio delle scansioni effettuate sia in rete, e quindi visibile a tutti gli operatori, sarà necessario che ciascuno di essi abbia cura di cancellare immediatamente dalla cartella condivisa i file scansionati contenenti dati personali e di procedere al salvataggio degli stessi in una cartella locale non visibile ad altri utenti.

7. UTILIZZO DI COLLEGAMENTI INTERNET

Sono vietati i collegamenti ad Internet per usi non strettamente connessi al lavoro da svolgere e devono essere evitate tutte le attività non strettamente necessarie (come ad esempio l'utilizzo di siti Internet per ascoltare radio, download di film, canzoni, ecc.).
Non è ammesso l'utilizzo di collegamenti per servizi o scopi personali. (quali servizi di Borsa, prenotazione viaggi, ecc..).

8. INSTALLAZIONE DI HARDWARE E SOFTWARE

L'installazione di hardware e software, nonché la modifica dei parametri di configurazione, possono essere eseguite dal tecnico informatico competente.

Pertanto si raccomanda agli utenti dei PC di rispettare i seguenti divieti:
- non utilizzare sul PC dispositivi personali, o comunque non aziendali, quali lettori dispositivi di memorizzazione dei dati;
- non installare sistemi per connessione esterne (es: modem, wifi); tali connessioni, aggirando i sistemi preposti alla sicurezza della rete aziendale, aumentano sensibilmente i rischi di intrusioni e di attacchi dall'esterno;
- non installare programmi, anche in versione demo. In particolare, è vietata l'installazione di giochi, programmi in prova (shareware), programmi gratuiti (freeware), programmi pirata, e in generale tutti i software non autorizzati dal Servizio Informatico;

- non modificare i parametri di configurazione del proprio PC senza espressa autorizzazione e senza il supporto di personale tecnico qualificato.

9. GESTIONE DEI SUPPORTI RIMOVIBILI

I supporti rimovibili, come ad esempio dischi magnetici esterni, penne USB o CD riscrivibili, quando contengono dati personali devono essere custoditi in luogo protetto e non accessibile (cassaforte, armadio chiuso a chiave, ecc..). Quando non sono più utilizzati devono essere distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri soggetti non autorizzati al trattamento degli stessi dati, soltanto dopo essere stati formattati.

Il trasferimento di file contenenti dati personali, dati particolari su supporti rimovibili è da eseguire unicamente in via transitoria, ponendo la massima attenzione alla destinazione di trasferimento e cancellando i file appena possibile.
Gli autorizzati al trattamento dei dati personali hanno la responsabilità di:

- segnalare la necessità di un'eventuale riparazione degli hard disk;
- segnalare la necessità di un eventuale riutilizzo degli hard disk.

10. LIMITAZIONI O ESCLUSIONE DI ATTIVITÀ NELL'USO DELLE RISORSE INFORMATICHE

Per effettuare i trattamenti previsti dalla mansione, ad ogni utente viene concesso l'utilizzo di alcune risorse informatiche (sistemi hardware, programmi e applicazioni software, apparati di rete, risorse di stampa), le quali costituiscono strumenti di esecuzione delle normali prestazioni di lavoro.

Il loro uso deve sempre essere improntato al principio di comune buon senso e di civiltà. Pertanto, al fine di garantire la funzionalità, la sicurezza ed il corretto impiego degli strumenti elettronici e, al tempo stesso, garantire un elevato livello di sicurezza dei trattamenti e assicurare la protezione della riservatezza di dipendenti e collaboratori, alcuni comportamenti (indicati di seguito) sono vietati.

Comportamenti vietati rispetto all'utilizzo del Personal Computer

È fatto espresso divieto di:

- accedere e utilizzare le risorse ed i servizi per motivi non lavorativi o non di servizio;
- usare le risorse o i servizi in violazione di normative comunitarie, leggi, regolamenti, provvedimenti, prescrizioni, o commettere attività illecite o discriminanti;
- modificare le configurazioni impostate;
- installare e utilizzare prodotti software che non siano stati autorizzati;
- installare e utilizzare software che consentano di intercettare il traffico o violare le password;
- usare le risorse o i servizi per scopi commerciali, promozionali, pubblicitari;
- utilizzare eccessivo spazio disco o assorbire capacità di banda nei sistemi di telecomunicazione, attraverso la generazione o l'invio di mail non strettamente correlate all'attività lavorativa, o in generale, attraverso il trasferimento di file o messaggi di dimensioni eccessive;
- inviare o depositare sui computer materiale di natura illegale o discriminante;
- mascherare la propria identità all'interno dei sistemi informatici;
- utilizzare le credenziali di autenticazione di altri utenti, per qualsivoglia ragione;
- tentare di violare password, sistemi di protezione, restrizioni imposte dal sistema;
- riprodurre o distribuire materiale in formato digitale senza autorizzazione;
- copiare o modificare files, redatti da altri utenti, senza autorizzazione;
- alterare i dati, introdurre o diffondere virus, trojan, backdoor, dataminer o altri codici malefici;
- interferire con il corretto funzionamento o danneggiare le attrezzature di rete;
- intercettare o alterare qualunque tipo di dato o di comunicazione digitale.

Comportamenti vietati rispetto all'utilizzo di internet

È fatto espresso divieto di:

- navigare su siti non correlati con la prestazione lavorativa;
- effettuare download di programmi e files estranei al lavoro;
- partecipare a forum, accedere e utilizzare chat line, partecipare ad aste on-line;
- scaricare, copiare, conservare, diffondere file a contenuto offensivo, discriminatorio, pedofilo, o di altro contenuto illecito penalmente o civilmente;
- accedere a siti di gioco, pornografici o con finalità ludiche;
- attivare strumenti di videochiamata (es.: skype).

Comportamenti vietati rispetto all'utilizzo della posta elettronica

È fatto espresso divieto di:

- utilizzare la posta elettronica per ragioni non attinenti ai compiti affidati;
- inviare, stampare, conservare messaggi offensivi o discriminatori;
- comunicare indirizzi di posta riconducibili al Titolare per partecipare a dibattiti, forum o mailing list di contenuto non pertinente con lo svolgimento delle mansioni affidate;
- creare cartelle segrete o nascoste per la conservazione dei messaggi.

11. GESTIONE DEI LOCALI ADIBITI AD ARCHIVIO DEI DOCUMENTI/DATI ELETTRONICI

È necessario che le banche dati su PC, server, hard disk od altri supporti siano custodite in armadi chiusi a chiave o, in mancanza di serratura, è opportuno che venga chiuso il locale stesso che è stato adibito ad archivio.

Il Personal Computer, su cui sono memorizzate le banche dati, dovrà essere spento e, nel caso non sia prevista una password di accesso al programma, dovrà essere chiuso a chiave il locale ove esso è ubicato. Le chiavi degli armadi e dei locali in cui sono custodite le banche dati devono essere depositate in luogo sicuro e conservate con l'ordinaria dirigenza.

In particolare, i locali dell'Ordine, adibiti ad archivio della documentazione cartacea od elettronica, sono inaccessibili a soggetti estranei all'Organizzazione, in quanto rimangono chiusi a chiave negli orari di chiusura delle attività lavorative.

I locali sono inoltre sorvegliati nelle ore di apertura dal personale in esso presente, che controlla gli ingressi rendendo di fatto improbabile l'accesso da parte di soggetti estranei e non autorizzati.

12. NON OSSERVANZA DELLA NORMATIVA INTERNA

Il mancato rispetto o la violazione delle regole contenute nella presente procedura è perseguibile da parte del Titolare del trattamento con provvedimenti disciplinari.

Procedura interna di sistema - PRO 2.0.

GESTIONE STRUMENTI NON ELETTRONICI DI TRATTAMENTO

Ai sensi del Regolamento UE n. 2016/679 - relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e del Principio di Accountability

Vengono riportate di seguito le norme che gli autorizzati al trattamento dei dati personali devono applicare e rispettare quando trattano documenti cartacei contenenti dati personali e particolari.

In particolare, gli autorizzati hanno l'obbligo, durante lo svolgimento dell'attività di trattamento dei documenti, di applicare le norme riportate di seguito e le direttive emanate dal Titolare del trattamento.

1. COSA SI INTENDE PER STRUMENTO "NON ELETTRONICO"

Per "non elettronici" si intendono sia documenti cartacei sia documenti di altro tipo come ad esempio microfilm, microfiches e lucidi. I documenti di questo tipo contenenti dati particolari devono essere protetti in appositi armadi dotati di chiavi. Tutti i documenti contenenti dati particolari che si ritiene debbano essere eliminati devono essere distrutti e non gettati nei cestini.

È opportuno evitare il deposito di documenti di qualsiasi genere negli ambienti di transito o pubblici (corridoi o sale riunioni), come pure l'abbandono in vista sulle scrivanie quando ci si debba assentare dal proprio posto di lavoro. Nel caso di dati particolari, il rispetto di queste norme è obbligatorio.

Gli autorizzati devono operare in modo da consentire l'accesso esclusivamente:

- all'interessato a cui tali dati si riferiscono;
- al responsabile del trattamento di quella tipologia di dato;
- agli autorizzati a trattare quella tipologia di dato.

2. ARCHIVIAZIONE DEI DOCUMENTI CARTACEI

Per quanto riguarda l'archiviazione dei documenti cartacei, è necessario che essi siano tenuti in archivi adeguatamente protetti, per evitarne la lettura e/o il prelievo non autorizzato e per garantire, quindi, la riservatezza e l'integrità dei dati in essi contenuti.

Al termine della giornata lavorativa, gli archivi dovranno essere chiusi a chiave e le chiavi dovranno essere riposte in luogo sicuro e non lasciate nelle serrature stesse.

La consultazione dei documenti contenenti dati personali e/o particolari, deve avvenire esclusivamente da parte degli Autorizzati al trattamento, solo quando operativamente necessario e, quando possibile, in loco.

Tutti i documenti cartacei decorsi i termini di conservazione previsti dalla legge e/o dal Titolare devono essere distrutti attraverso opportuni strumenti che rendano impossibile la ricostruzione del documento.

3. DISTRUZIONE DELLE COPIE CARTACEE

Coloro che procedono alla duplicazione di documentazione (con stampanti, fotocopiatrici o altre periferiche) ovvero utilizzino strumenti per la riproduzione cartacea di documenti digitali sono tenuti alla distruzione del relativo supporto qualora si verifichino errori o la riproduzione non sia corretta. È inoltre opportuno evitare di riutilizzare fogli contenenti dati personali.

4. MISURE DI SICUREZZA

Il trattamento sicuro e adeguato dei documenti contenenti dati personali richiede l'adozione di alcune misure di sicurezza con le quali l'autorizzato possa interagire ed una serie di accorgimenti direttamente gestibili dall'autorizzato stesso.

In particolare, i locali dell'Ordine degli Ingegneri, adibiti ad archivio della documentazione cartacea, sono inaccessibili a soggetti estranei all'Organizzazione, in quanto rimangono chiusi a chiave negli orari di chiusura delle attività lavorative.

I locali sono inoltre sorvegliati nelle ore di apertura dal personale in esso presente, che controlla gli ingressi rendendo di fatto improbabile l'accesso da parte di soggetti estranei e non autorizzati.

I dati particolari presenti nei locali (dati contenuti nelle Buste Paga, nei curriculum vitae ed eventuali dati particolari degli iscritti) sono conservati in un armadio chiuso a chiave. La visione ed il trattamento dei dati in questione è consentita al solo personale espressamente autorizzato mediante apposita lettera di autorizzazione.

5.PRESCRIZIONI PER GLI AUTORIZZATI

Gli autorizzati al trattamento qualora trattino documenti cartacei contenenti dati personali e/o sensibili e/o giudiziari sono tenuti ad attenersi alle seguenti prescrizioni:

- è severamente vietato l'accesso a documenti contenenti dati personali per esigenze non strettamente lavorative, connesse ai trattamenti dichiarati, autorizzati e tutelati dal Titolare;
- la documentazione contenente dati personali che, per ragioni di praticità operativa, risiede sulle scrivanie degli autorizzati deve essere rimossa al termine dell'orario di lavoro;
- l'accesso ai supporti deve essere limitato al tempo necessario a svolgere i Trattamenti previsti e gli stessi devono essere archiviati in ambiente ad accesso controllato;

- è vietato lasciare incustoditi in ambienti non controllati documenti contenenti dati personali (ad es. a seguito di stampa su stampante di rete);
- la distruzione dei documenti contenenti dati personali deve essere operata, ove possibile, direttamente dal personale autorizzato. È inoltre severamente vietato utilizzare documenti contenenti dati personali, dati particolari come carta da riciclo o da appunti;
- ove non siano disponibili strumenti per la distruzione dei documenti (trita documenti), o il volume di questi sia tale da imporre il ricorso al servizio di macero, il personale autorizzato che avvia al macero la documentazione è tenuto a confezionare tale documentazione in modo che il pacco risulti anonimo e solido;
- gli atti e i documenti contenenti dati personali, dati particolari (ex dati sensibili) o giudiziari affidati agli autorizzati per lo svolgimento dei relativi compiti devono essere controllati e custoditi dagli autorizzati stessi fino alla restituzione, in modo tale che ad essi non possano accedervi persone prive di autorizzazione, e devono essere restituiti al termine delle operazioni affidate;
- l'accesso agli archivi contenenti dati particolari deve essere controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di autorizzati alla vigilanza, le persone che vi accedono devono essere preventivamente autorizzate;
- i documenti (o copia degli stessi) non possono, senza specifica autorizzazione, essere portati fuori dai luoghi di lavoro, salvo i casi di comunicazione dei dati a terzi preventivamente autorizzati in via generale dall'Ordine.

6. NON OSSERVANZA DELLA NORMATIVA INTERNA

Il mancato rispetto o la violazione delle regole contenute nella presente procedura è perseguibile da parte del Titolare del trattamento con provvedimenti disciplinari.

Procedura interna di sistema - PRO 3.0.

ISTRUZIONI DI BACKUP - RESTORE

Ai sensi del Regolamento UE n. 2016/679 - relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e del Principio di Accountability

Il backup nell'informatica indica un'importante operazione tesa a duplicare su differenti supporti di memoria le informazioni (dati o programmi) presenti sui dischi di una stazione di lavoro o di un server.

La procedura di backup è un aspetto fondamentale nella gestione dell'attività lavorativa aziendale: in caso di guasti o manomissioni, il backup consente infatti di recuperare i dati dell'utente o degli utenti che utilizzano la singola postazione e in caso di perdita di database o dati su server può essere essenziale per l'intera attività condotta dal Titolare del trattamento.

I supporti su cui viene effettuato il backup normalmente devono essere di tipo e marca adeguati, devono essere conservati in posizioni fisicamente distinte e separate dai sistemi in uso, per evitare che in caso di furto, incendio, alluvione o altro evento catastrofico le copie vadano perse insieme agli originali e devono essere periodicamente verificati e sostituiti.

Il ripristino della disponibilità dei dati (restore) in seguito a distruzione o danneggiamento avverrà con l'intervento della società appositamente incaricata.

Supporto di Back-up	Periodicità	N. copie effettuate	N. supporti
NAS	CONTINUA	1 COPIA CONTINUA	2 HARD DISK

Supporto numero	Luogo di conservazione
1	NAS LOCALE
Operazione	**Istruzioni**
Backup	Il backup viene effettuato in maniera automatica, attraverso la copia dei contenuti presenti sui pc interni.
Ripristino	Qualora i dati - personali e particolari - trattati elettronicamente, contenuti sui PC, andassero persi o distrutti da eventi di portata straordinaria potrebbero essere recuperati dalle copie di backup. Il backup del server (programmi gestionali) viene fatto sul NAS locale, il ripristino dei dati può essere fatto dal backup giornaliero delle macchine virtuali. La copia dei dati è solo interna all'ufficio, essendo fatta sul NAS di rete. I tempi di ripristino dei dati sono di un paio d'ore da inizio intervento.

In aggiunta, backup viene effettuato anche in remoto su cloud (all'interno dell'unione europea). Il software per il backup è Nakivo. I tempi di ripristino sono gli stessi per i backup locali, per i ripristini da remoto servono almeno 1-2 giorni lavorativi.

In merito alla gestione della posta elettronica dell'Ordine si precisa quanto segue.
La posta elettronica ordinaria dell'indirizzo email info@ording.cuneo.it è gestita tramite servizio cloud di AWS (Amazon Web Services). Tale servizio è completamente gestito dall'infrastruttura Amazon. I relativi back-up sono periodi, anch'essi su S3 e sono sia incrementali che a snapshot completo. Nello specifico, gli incrementali avvengono ogni due giorni, lo snapshot settimanalmente. I dati sono tutti contenuti in server o NAS nell'Unione Europea (server farm di Francoforte e Mialno). In caso di perdita di dati si possono ripristinare in modo automatico completo oppure scaricare in modo mirato e puntuale. Il tempo di recupero è di 8 ore lavorative.

Procedura interna di sistema - PRO 4.0.

GESTIONE DEI CURRICULA

Ai sensi del Regolamento UE n. 2016/679 - relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e del Principio di Accountability

Per la gestione dei curricula ricevuti, sia cartacei che in formato elettronico, è opportuno procedere seguendo le istruzioni sotto riportate:

1) Ai sensi dell'art. 13 del GDPR, i curriculum vitae inviati spontaneamente dai candidati o inoltrati in risposta ad un annuncio di lavoro non devono contenere nessuna espressa menzione di "autorizzazione al trattamento";
2) Il Titolare del trattamento consegna l'informativa privacy ai potenziali candidati al momento del primo contatto con gli stessi, ossia in caso di invio spontaneo del curriculum vitae, l'informativa privacy dovrà essere fornita in sede di colloquio;
3) tutti i curricula che giungono presso l'Organizzazione in formato cartaceo vengono conservati in armadi o cassetti dotati di serratura adeguata, mentre quelli pervenuti in formato elettronico vengono archiviati in apposita cartella cui può accedervi soltanto il personale autorizzato;
4) i curricula ricevuti presso l'Ordine secondo i modi predetti, tanto in formato elettronico quanto in formato cartaceo, saranno conservati non oltre 24 mesi dalla data di ricezione; dopodiché i primi dovranno essere cancellati dal personale dipendente avente accesso alla cartella di archiviazione, mentre i secondi andranno distrutti per mezzo di triturazione meccanica con l'utilizzo di apposito dispositivo.

Procedura interna di sistema - PRO 5.0.

ISTRUZIONI OPERATIVE IN CASO DI VIOLAZIONE DEI DATI PERSONALI

Ai sensi del Regolamento UE n. 2016/679 - relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e del Principio di Accountability

1. DEFINIZIONE DI "VIOLAZIONE DI DATI PERSONALI"

Per **"Violazione di dati"** (Data Breach) si intende 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 (art. 4 del GDPR). Qualora si verifichi un incidente di sicurezza il Titolare non risulta essere in grado di garantire il rispetto dei principi prescritti dall'art. 5 del GDPR per il trattamento dei dati personali.

L'obbligo di notifica scatta se la violazione ragionevolmente comporta un rischio per i diritti e le libertà delle persone fisiche; qualora il rischio fosse elevato oltre alla notifica il Titolare è tenuto a darne anche comunicazione all'interessato.

2. TIPOLOGIE DI VIOLAZIONE DEI DATI

Si possono distinguere tre tipi di violazioni:

1. violazione di riservatezza, ovvero quando si verifica una divulgazione o un accesso a dati personali non autorizzato o accidentale;
2. violazione di integrità, ovvero quando si verifica un'alterazione di dati personali non autorizzata o accidentale;
3. violazione di disponibilità, ovvero quando si verifica perdita, inaccessibilità, o distruzione accidentale o non autorizzata di dati personali.

Una singola violazione potrebbe comprendere una o più tipologie.

3. TIPOLOGIE DI RISCHIO A SEGUITO DI VIOLAZIONE DEI DATI

Per comprendere quando notificare la violazione è opportuno effettuare una valutazione dell'entità dei rischi che possono derivarne:

- rischio assente: la notifica al Garante non è obbligatoria;
- rischio presente: la notifica al Garante è necessaria;
- rischio elevato: la notifica al Garante è necessaria in concomitanza alla comunicazione della violazione ai soggetti interessati. Nel momento in cui il Titolare del trattamento ha adottato sistemi di crittografia dei dati e la violazione non ha comportato l'acquisizione della chiave di decrittografia, la comunicazione ai soggetti interessati non è un obbligo.

I rischi per i diritti e le libertà degli interessati possono essere considerati "elevati" quando la violazione può, a titolo di esempio:

- coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;
- riguardare categorie particolari di dati personali;
- comprendere dati che possono accrescere ulteriormente i potenziali rischi (es. dati di localizzazione, finanziari, relativi alle abitudini e preferenze);
- comportare rischi imminenti e con un'elevata probabilità di accadimento (es. rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito);
- impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (es. pazienti, minori, soggetti indagati).

4. PROCEDURA DA SEGUIRE IN CASO DI VIOLAZIONE DEI DATI

La scoperta di un incidente di sicurezza può derivare da diversi soggetti coinvolti, interni e/o esterni all'organizzazione:

- dagli autorizzati;
- da parte dei Responsabili esterni del trattamento;
- da parte del DPO designato;
- da parte degli organi Pubblici (Agid, Polizia, altre Forze dell'Ordine, ecc);
- dai sistemi di monitoraggio automatici dei sistemi informatici;
- dagli interessati e da terzi.

Qualora uno degli attori sopra menzionati dovesse rilevare e/o venire a conoscenza di un episodio di violazione ovvero che vi è un rischio serio ed imminente di violazione dei dati personali detenuti, deve procedere ad informare, senza ingiustificato ritardo, il Titolare del trattamento (art. 33 GDPR) e il Responsabile della Protezione dei Dati (o DPO - Data Protection Officer) inviando opportuna segnalazione tramite messaggio di posta elettronica e/o attraverso i canali comunicativi a tal fine individuati.

Il Titolare del trattamento deve identificare l'incidente di sicurezza, quindi, comprendere che impatto ha sulle informazioni ed infine se tra le informazioni coinvolte dall'incidente vi siano dati personali. Pertanto, se l'incidente di sicurezza ha un impatto (a qualunque livello) su informazioni (documenti, file, strumenti, servizi, ecc.) contenenti dati personali allora si tratta di una violazione di dati e va valutata la tipologia e la quantità dei dati personali oggetto del data breach, nonché vanno individuate le contromisure tecniche correttive e preventive; altrimenti l'incidente non deve essere preso in considerazione ai fini della presente procedura.

Contestualmente alla qualificazione occorre continuare a perseguire le misure per bloccare e contenere le conseguenze dannose dell'incidente, iniziate nella fase di scoperta, coinvolgendo eventuali altri soggetti (es. informatici ed amministratori di sistema). Inoltre nel determinare l'obbligo di notificazione e di successiva comunicazione occorre valutare la possibilità che la violazione possa causare danni fisici, materiali o immateriali alla persona fisica, quali ad esempio (Considerando 85 GDPR):

- perdita del controllo dei dati personali degli interessati;
- limitazione dei diritti;
- discriminazione;
- furto o usurpazione di identità;
- perdite finanziarie;
- decifratura non autorizzata della pseudonimizzazione;

- pregiudizio alla reputazione;
- perdita di riservatezza dei dati personali protetti da segreto professionale, o qualsiasi altro danno economico o sociale significativo per la persona interessata.

Il termine per adempiere alla notifica è di 72 ore dal momento in cui il Titolare ne viene a conoscenza, mentre, l'eventuale comunicazione agli interessati deve essere fatta senza indugio.

E' importante che sia dimostrabile il momento della scoperta dell'incidente, poiché da quel momento decorrono le 72 ore per la notifica.

L'eventuale ritardo nella notificazione deve essere giustificato; il mancato rispetto dell'obbligo di notifica, invece, pone l'Autorità di controllo nella condizione di applicare le misure correttive a sua disposizione ovvero: l'esercizio dei poteri previsti dall'art. 58 GDPR (avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti al trattamento, ordine di rettifica, revoca di certificazioni, ordine di sospendere flussi di dati) e l'imposizione di sanzioni amministrative secondo l'art. 83 GDPR.

La notifica di una violazione di dati personali deve essere inviata al Garante tramite un'apposita procedura telematica, resa disponibile nel portale dei servizi online dell'Autorità, e raggiungibile all'indirizzo **https://servizi.gpdp.it/databreach/s/** (Si veda Provvedimento del Garante della privacy del 27 maggio 2021).

Procedura interna di sistema - PRO 6.0.

ESSERCIZIO DEI DIRITTI DEGLI INTERESSATI

Ai sensi del Regolamento UE n. 2016/679 - relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e del Principio di Accountability

1. MODALITA' PER L'ESERCIZIO DEI DIRITTI

Laddove il Titolare elabori dati personali su individui (clienti, lavoratori, fornitori, etc.) questi è tenuto a rispettare il diritto sulla protezione dei dati sancito dal Regolamento Ue 2016/679. L'interessato può esercitare i diritti riconosciuti dal GDPR presentando una richiesta al Titolare del trattamento. Gli artt. 11 e 12 del Regolamento disciplinano in linea generale le modalità per l'esercizio di tutti i diritti sorgenti in capo all'interessato.

I diritti che gli interessati possono esercitare (descritti più dettagliatamente al punto 2 di seguito) includono:

- Diritto di accesso a copia dei dati conservati dal Titolare (art. 15);
- Diritto di rettifica dei dati conservati dal Titolare (art. 16);
- Diritto alla cancellazione ("diritto all'oblio") dei dati conservati dal Titolare (art. 17);
- Diritto alla limitazione delle attività di trattamento da parte del Titolare (art. 18);
- Diritto alla portabilità dei dati dal Titolare ad un'altra entità (art. 20);
- Diritto di opposizione al trattamento effettuato dal Titolare (art. 21);
- Diritto di opposizione al processo decisionale automatizzato effettuato dal Titolare (art. 22).

I dettagli descritti di seguito descrivono in che modo il Titolare del trattamento, risponderà a qualsiasi richiesta di trattamento dei dati.

Il Titolare del trattamento dei dati è il principale responsabile autorizzato a rispondere ad una richiesta di trattamento dei dati e per agevolare il richiedente (l'interessato) a esercitare i propri diritti secondo le norme previste dal Regolamento. Se il Titolare condivide i dati con terze parti (eventuali responsabili esterni del trattamento dei dati), spetta al Titolare la responsabilità di informare tali terze parti di qualsiasi richiesta di trattamento (rettifica, cancellazione, limitazione) presentata dall'interessato.

Se richiesto, il Titolare deve fornire i dettagli di quelle terze parti (che concorrono al trattamento) a cui sono stati divulgati i dati dell'interessato richiedente.

Come esercitare i diritti sui dati
L'interessato, al fine di far valere i propri diritti, può contattare il Titolare del trattamento al seguente indirizzo **info@ording.cuneo.it**, utilizzando il modulo **MOD_Esercizio diritti in materia di protezione dei dati personali,** specificando l'oggetto della sua richiesta, il diritto che intende esercitare e allegando fotocopia di un documento di identità che attesti la legittimità della richiesta.

Se un lavoratore alle dipendenze del Titolare riceve una richiesta di esercizio di un diritto da parte di un lavoratore/cliente/fornitore o altri, la richiesta deve essere immediatamente inviata al Titolare del Trattamento all'indirizzo sopra specificato, insieme all'indicazione della data di ricezione della richiesta e ogni altro dettaglio fornito dal richiedente.

Processo di verifica
Il Titolare del trattamento deve agevolare l'esercizio dei diritti (artt. 15-22) da parte dell'interessato adottando ogni misura (tecnica e organizzativa) a ciò idonea.

Il Titolare effettuerà una valutazione iniziale su qualsiasi richiesta pervenuta per valutare se tale richiesta è valida. Qualsiasi richiesta di trattamento dei dati deve essere effettuata dall'individuo a cui possono essere richiesti i dati personali e la verifica dell'identità (dal diretto interessato).

Il riscontro all'interessato (per confermare la ricezione della richiesta e chiedere conferma dell'identità, se non già convalidata) avverrà in forma scritta, anche attraverso strumenti elettronici che ne favoriscano l'accessibilità; il Titolare potrà rispondere oralmente solo se così richiede l'interessato stesso. La risposta fornita all'interessato non dovrà essere solo "intelligibile", ma anche concisa, trasparente e facilmente accessibile, oltre ad utilizzare un linguaggio semplice e chiaro.

Esenzioni a una richiesta di diritti sui dati
Il Titolare può rifiutarsi di agire su una richiesta di trattamento dei dati se la richiesta sia eccessiva e/o manifestatamente infondata (ad esempio a causa di richieste ripetute per gli stessi dati). Laddove il Titolare sia autorizzato a rifiutare la richiesta, quest'ultimo dovrà essere in grado di dimostrare che la richiesta sia effettivamente eccessiva e/o manifestatamente infondata. L'esercizio dei diritti è, in linea di principio, gratuito per l'interessato, ma possono esservi delle eccezioni; se il Titolare accetta di rispondere a richieste eccessive e/o manifestatamente infondate, potrà essere addebitata una commissione ragionevole in base ai costi amministrativi relativi alla fornitura delle informazioni o all'azione richiesta.

Tempi per rispondere alle richieste di diritti sui dati
La richiesta dell'interessato deve essere di norma soddisfatta senza indebito ritardo e non oltre 1 mese dal ricevimento della richiesta. Laddove la richiesta sia particolarmente complessa, tale limite temporale sarà estendibile fino a 3 mesi ma, il Titolare dovrà comunque dare un riscontro all'interessato mediante notifica entro il termine originale (1 mese), anche in caso di diniego.

2. ESERCIZIO DEI DIRITTI SUI DATI

Diritto di accesso

Diritto di un individuo di ottenere la conferma che il Titolare del trattamento elabora dati su di lui e, in caso affermativo, di fornire dettagli dei dati trattati e aspetti specifici delle attività di trattamento relative a tali dati e per ricevere una copia di tali dettagli.

L'interessato ha il diritto di richiedere una copia dei dati che lo/la riguardano detenuti e trattati dal Titolare. Tali dati devono essere forniti in forma intelligibile.
Le informazioni fornite in risposta ad una richiesta devono includere:

a. Una descrizione dei dati personali e delle categorie di dati interessati;
b. Il periodo stimato per il quale i dati saranno archiviati;
c. Le finalità per le quali i dati sono detenuti e trattati;
d. I destinatari o i tipi di destinatari a cui i dati sono, o potrebbero essere, divulgati dal Titolare del trattamento;
e. Conferma del diritto dell'individuo di chiedere la rettifica o la cancellazione dei dati o di limitare o opporsi al trattamento;
f. Conferma del diritto dell'individuo di presentare un reclamo presso l'autorità competente per la protezione dei dati;
g. Dettagli sulla fonte dei dati personali se non sono stati raccolti dall'individuo;
h. Dettagli in merito al fatto che i dati siano soggetti a processi decisionali automatizzati (profilazione);
i. Laddove i dati siano trasferiti in paesi europeo o paesi extra europei, le opportune misure di sicurezza adottate dal Titolare in conformità con le leggi applicabili in materia di protezione dei dati.

La richiesta di accesso non richiede alcun formato particolare per qualificarsi come una richiesta valida, sebbene ciò possa essere utile per identificare il tipo di richiesta. Non deve necessariamente essere presentata per iscritto, ma è utile per scopi di archiviazione e per chiarire la richiesta. Se fatto per iscritto, il richiedente deve fornire un indirizzo e-mail e la conferma del fatto che i dati richiesti possano essere inviati via e-mail (o altrimenti specificare i mezzi preferiti con i quali i dati possono essere ricevuti).

Il Titolare non può rifiutarsi di soddisfare una richiesta di accesso a meno che non dimostri di non essere in grado di identificare il richiedente o che sia altrimenti esentato dai suoi obblighi di conformità

Diritto di rettifica
Diritto di un individuo di ottenere la rettifica, senza indebito ritardo, di dati personali inesatti che un Titolare può elaborare su di lui.

Rettifica da parte del Titolare: Se il Titolare detiene dei dati inesatti o incompleti su un individuo, questi ha il diritto di richiedere che i dati vengano modificati/corretti.
Rettifica da parte di terzi: Se il Titolare rettifica i dati di un individuo in risposta a una richiesta, il Titolare sarà tenuto ad informare terze parti con cui ha condiviso questi dati (es: responsabili esterni che concorrono al trattamento).

Diritto alla cancellazione ("diritto all'oblio")
Diritto di un individuo di richiedere al Titolare del trattamento di cancellare i dati che lo riguardano per motivi specifici – ad esempio, quando i dati personali non sono più necessari per soddisfare gli scopi per cui sono stati raccolti.

Una persona fisica può richiedere al Titolare del trattamento di eliminare i propri dati nelle seguenti circostanze:

a. I dati personali non sono più necessari per gli scopi per cui sono stati raccolti, utilizzati o altrimenti trattati;
b. I dati personali sono stati trattati illecitamente dal Titolare del trattamento;
c. Il trattamento è avvenuto sulla base del consenso dell'interessato che è stato successivamente revocato, se non esiste altro motivo legittimo per il trattamento;
d. L'interessato si oppone al trattamento e non sussiste alcun ulteriore motivo legittimo per procedere al trattamento;
e. I dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il Titolare del trattamento;
f. I dati personali sono stati raccolti in relazione ai servizi offerti sul sito web del Titolare del trattamento.

Il Titolare del trattamento nei casi indicati è obbligato a procedere alla cancellazione dei dati e ad adottare le misure ragionevoli per informare altri Titolari che stanno trattando i dati (compreso "*qualsiasi link, copia o riproduzione*") di procedere alla loro cancellazione.

Tuttavia il Titolare può continuare ad elaborare i dati se questi sono necessari per gli scopi per i quali sono stati raccolti; pertanto, sarà esente dall'obbligo di cancellare i dati quando il trattamento è necessario:

a. Per l'esercizio del diritto alla libertà di espressione e di informazione;
b. Per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
c. Per motivi di interesse pubblico nel settore della sanità pubblica;
d. A fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, nella misura in cui la cancellazione rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento;
e. Per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Diritto alla limitazione

Diritto di ogni individuo di richiedere al Titolare di limitare il trattamento dei dati personali che lo riguardano per motivi specifici.

L'interessato ha diritto di pretendere una limitazione dell'uso che il Titolare fa dei propri dati. Una simile richiesta trova fondamento al ricorrere di determinate condizioni; nello specifico:

a. Qualora l'interessato contesti l'esattezza dei dati personali, per il periodo necessario al fine di verificarne l'esattezza (ovvero il trattamento è "congelato" nel tempo tecnico richiesto per verificare se i dati siano esatti o meno, dopodiché si agirà di conseguenza, correggendo o integrando i dati);
b. Quando il trattamento dei dati sia illecito e l'interessato si opponga alla loro cancellazione, preferendo che ne sia disposta una limitazione d'utilizzo;
c. Quando il Titolare non abbia più bisogno di conservare i dati ai fini del trattamento, ma essi sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
d. Quando l'interessato si sia opposto al trattamento nell'attesa delle necessarie verifiche sulla prevalenza dei motivi legittimi del Titolare del trattamento rispetto a quelli dell'interessato.

In queste ipotesi i dati non vengono cancellati, ma ne viene ridotto l'utilizzo consentito da parte del Titolare. I dati potranno essere trattati solo ai fini della loro conservazione, a meno che vi sia il consenso dell'interessato o il trattamento sia necessario per l'esercizio o la difesa di un diritto in sede giudiziaria, per la tutela dei diritti di un'altra persona o per ragioni di interesse pubblico rilevante. La limitazione potrà essere in seguito revocata e in questo caso, prima che ciò avvenga, il Titolare del trattamento dovrà informare specificamente l'interessato.
Il Titolare, ricevuta una richiesta di limitazione del trattamento sarà tenuto a trasferire temporaneamente i dati oggetto della richiesta verso un altro sistema di trattamento, oppure rimuovere provvisoriamente i dati pubblicati dal sito web per renderli inaccessibili agli utenti.

Nel caso in cui sia fatto valere il diritto di limitazione del trattamento dei dati personali il Titolare del trattamento dovrà comunicare le eventuali correzioni o limitazioni del trattamento ai destinatari cui i dati siano stati trasmessi, a meno che risulti essere impossibile o implichi uno sforzo sproporzionato.

Diritto alla portabilità

Diritto di un individuo di ricevere i propri dati personali da un Titolare in un formato strutturato, comunemente usato e leggibile da un dispositivo automatico per trasferire tali dati ad un altro Titolare, il cui trattamento è lecito in base al consenso dell'interessato ed è effettuato con mezzi non automatizzati.

L'interessato ha il diritto di ottenere la trasmissione dei dati personali da un Titolare ad un altro "*senza ostacoli*", se è tecnicamente fattibile. Il Titolare del trattamento può adeguarsi alla norma fornendo uno strumento per il download dei dati, oppure garantendo la trasmissione diretta dei dati ad altro fornitore. Anche il Titolare ricevente i dati è soggetto a specifici obblighi, in particolare diventa il nuovo Titolare e quindi deve garantire che i dati non siano eccessivi rispetto al servizio che fornisce. Ad esempio, potrebbe essere necessario non elaborare parte dei dati perchè non necessari per fornire il servizio.
Il diritto alla portabilità dei dati non implica alcun obbligo di conservare i dati oltre il periodo stabilito dalle norme al solo fine di garantire l'esercizio della portabilità.
L'esercizio di tale diritto non deve ledere i diritti e le libertà altrui, come ad esempio se la fornitura lede i diritti di proprietà intellettuale del titolare oppure espone segreti commerciali.

La portabilità dei dati deve essere garantita quando:
- Il trattamento dei dati è basato sul consenso dell'interessato oppure su un contratto;
- Il trattamento è basato esclusivamente su elaborazione elettronica (non cartacea quindi).
In tutti gli altri casi non si può esercitare tale diritto, come ad esempio per i trattamenti basati sui legittimi interessi.

Diritto di opposizione

Diritto di un individuo di opporsi, per motivi connessi alla sua particolare situazione, al trattamento da parte del Titolare del trattamento dei dati personali che lo riguardano, se l'elaborazione è basata sugli interessi legittimi del Titolare.

Se il Titolare si basa sul fatto che l'utilizzo, la conservazione o l'elaborazione dei dati personali sono nel suo legittimo interesse, un individuo può opporsi a tale elaborazione.

Conseguenza dell'esercizio di tale diritto è l'obbligo, in capo al Titolare, di astenersi dal trattamento dei dati.

Il Titolare può tuttavia continuare ad elaborare i dati se:

a. Il Titolare può dimostrare convincenti interessi legittimi per il trattamento che prevalgono sugli interessi, i diritti e le libertà dell'individuo;
b. Il trattamento è necessario per stabilire, esercitare o difendere un obbligo legale;
c. Il trattamento è effettuato per scopi scientifici, storici o statistici realizzati nell'interesse pubblico.

Nel caso in cui i dati personali siano trattati con finalità di marketing diretto, l'interessato ha il diritto di opporsi in qualsiasi momento e gratuitamente al trattamento, anche (e soprattutto) nel caso in cui questo avvenga mediante attività di profilazione. In tale circostanza, il Titolare è tenuto ad interrompere l'uso di dati personali per il marketing diretto se riceve tale richiesta da parte di clienti/partner e altri.

Diritto di opposizione al processo decisionale automatizzato

Diritto di un individuo 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.

Il Titolare è esente quando:

a. Il trattamento automatizzato sia necessario per la conclusione o l'esecuzione di un contratto tra l'interessato e il Titolare del trattamento;
b. Il trattamento automatizzato sia autorizzato 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 e dei legittimi interessi dell'interessato;
c. Il trattamento automatizzato si basi sul consenso esplicito dell'interessato.

Nei casi di cui al paragrafo 2, lettere a) e c), il Titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, nonché il diritto di ottenere l'intervento umano da parte del Titolare del trattamento, di esprimere la propria opinione e di contestare la decisione.