CGC S.R.L.
CORPORATE GENERAL CONSULTING

PRIVACY POLICY

Politica generale sulla protezione dei dati personali
per l'attuazione del Regolamento UE 2016/679 (GDPR) relativo
alla protezione delle persone fisiche con riguardo al trattamento dei dati personali

(art. 24 par. 2 Regolamento UE 2016/679)

****

DEFINIZIONI

(ai soli fini della presente policy, e conformi alle definizioni di cui all'art. 4, co.1 del GDPR e del D.lgs. 196/2003 e ss.mm.ii.)

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.

Autorità di controllo: autorità pubbliche indipendenti incaricate di controllare l'applicazione del Regolamento UE al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento e di agevolare la libera circolazione dei dati personali all'interno dell'Unione.

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.

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.

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.

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.

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.

Dati giudiziari: i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.

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.

Interessato: la persona fisica a cui si riferiscono i dati personali oggetto di trattamento.

Autorizzati al trattamento (i.e. "incaricati"): le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare o dal Responsabile del trattamento.

Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento.

Titolare del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.

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.

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.

Violazione dei dati personali ("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;

PREMESSA

Questa Società denominata CGC s.r.l. con sede legale in Agrigento (di seguito anche "Organizzazione" o "Società") per l'espletamento delle proprie funzioni istituzionali tratta numerose informazioni personali, per tali intendendosi ai sensi del Regolamento UE 2016/679 ("GDPR) tutti i dati riferibili "*a persona fisica identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale*".
Sotto il profilo qualitativo, oltre a dati cd. "comuni", la società effettua il trattamento di informazioni di carattere specifico (già denominati dati "sensibili", oggi "categorie particolari di dati personali"), che costituiscono dati personali idonei a rivelare l'origine razziale o etnica, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché i dati biometrici intesi a identificare in modo univoco una persona fisica, dati personali idonei a rivelare lo stato di salute o l'orientamento sessuale (c.d. "categorie particolari di dati" ex art.9 GDPR), nonché dati personali idonei a rivelare provvedimenti giudiziari.
La società, per il trattamento dei dati personali, utilizza sia strumenti informatici (elaboratori) sia supporti cartacei o altri supporti di memorizzazione.

1. Obiettivo del documento

Il presente documento (d'ora in avanti "Politica" o "Regolamento" o "Policy") ha per oggetto misure procedimentali e regole di dettaglio ai fini della migliore funzionalità ed efficacia dell'attuazione del Regolamento europeo (General Data Protection Regulation del 27 aprile 2016 n. 679, di seguito indicato con "GDPR"), relativo alla protezione delle persone fisiche con riguardo ai trattamenti dei dati personali, nonché alla libera circolazione di tali dati, all'interno dell'Organizzazione.
Il presente documento descrive in linea generale i ruoli, le responsabilità, le modalità di governo e di gestione operativa in materia di trattamento di dati personali adottati dall'Organizzazione in qualità di Titolare del trattamento (nel seguito anche "Titolare") in ottemperanza al Regolamento (UE) 2016/679 (GDPR).

2. Ambito di applicazione

L'ambito di applicazione del presente documento riguarda l'intera Organizzazione, che effettua il trattamento di dati personali sul territorio dello Stato italiano, anche in caso di trasferimento di dati personali da e verso l'estero (Paesi extra UE).
Destinatario del presente Regolamento è tutto il Personale di ogni ordine e grado dell'Organizzazione, comprese le persone autorizzate al trattamento, con riguardo alla gestione interna ed esterna dei dati personali relativi a clienti, dipendenti, fornitori, visitatori e ogni altro soggetto interessato al trattamento, nonché i responsabili del trattamento nominati dal Titolare, ed i contitolari, in base allo specifico accordo di volta in volta stipulato.

3. Principi generali

I principi applicabili alla protezione dei dati personali delineano le responsabilità delle organizzazioni nella gestione dei dati personali. Il Titolare è competente per il rispetto dei principi definiti dal Regolamento UE 2016/679 e deve essere in grado di comprovarlo.
Tutto il personale che svolge attività di trattamento dei dati personali sotto l'autorità del Titolare è tenuto ad attivarsi per far sì che i seguenti principi vengano rispettati. Parimenti i responsabili di trattamento nominati dal titolare sono tenuti a rispettare i principi generali di cui alla presente policy.

3.1 Liceità, correttezza e trasparenza

I dati personali devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato.
Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

a) L'interessato ha espresso il consenso per una o più specifiche finalità.
b) Il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte.
c) Il trattamento è necessario per adempiere un obbligo legale del titolare del trattamento.
d) Il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato.
e) Il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio dei poteri di cui è investito il titolare del trattamento.
f) Il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento.

3.2 Limitazione delle finalità

I dati personali devono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità.

3.3 Minimizzazione dei dati

I dati personali devono essere adeguati, pertinenti e limitati a quanto necessario in relazione alle finalità per cui sono trattati. L'Organizzazione deve applicare l'anonimizzazione o la pseudonimizzazione ai dati personali, se possibile, per ridurre il rischio per gli interessati.

3.4 Esattezza ed aggiornamento

I dati personali devono essere esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati.

3.5 Limitazione del periodo di conservazione

I dati devono essere conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati.

3.6 Integrità e riservatezza

Tenendo conto delle tecnologie e di altre misure di sicurezza disponibili, dei costi di attuazione e la probabilità e gravità dei rischi per i dati personali, l'Organizzazione ha messo

in atto misure tecniche e organizzative per garantire un livello di sicurezza adeguato per i dati personali, inclusa la protezione dalla distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati.

3.7 Responsabilizzazione *("accountability")*

Il Titolare del trattamento dei dati è competente per il rispetto dei principi sopra descritti e attraverso la corretta applicazione ed osservazione della presente politica è in grado di comprovarlo.

4. Ruoli e responsabilità

Le norme sulla protezione dei dati personali individuano alcune figure organizzative obbligatorie:

4.1 Titolare del trattamento

L'Organizzazione come sopra denominata, quale persona giuridica, è il Titolare del trattamento dei dati personali raccolti o meno in banche dati, automatizzate o cartacee (di seguito indicato con "Titolare"). Il rappresentante legale *pro tempore* è abilitato a rappresentare - ai fini previsti dal GDPR – il Titolare, con i relativi poteri di firma e di delega, ferma restando la responsabilità della persona giuridica a tutti gli effetti e per i fini previsti dal GDPR.

Il Titolare è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 GDPR: liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza.

Il Titolare mette in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento di dati personali è effettuato in modo conforme al GDPR.

Le misure sono definite fin dalla fase di progettazione e messe in atto per applicare in modo efficace i principi di protezione dei dati e per agevolare l'esercizio dei diritti dell'interessato stabiliti dagli articoli 15-22 GDPR, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio.

Il Titolare adotta misure appropriate per fornire all'interessato:

- le informazioni indicate dall'art. 13 GDPR, qualora i dati personali siano raccolti presso lo stesso interessato;
- le informazioni indicate dall'art. 14 GDPR, qualora i dati personali non stati ottenuti presso lo stesso interessato.

Il Titolare del trattamento provvede a:

a) designare eventuali Responsabili del trattamento i soggetti pubblici o privati affidatari di attività e servizi per conto dell'Organizzazione, relativamente alle banche dati gestite da soggetti esterni all'Organizzazione in virtù di convenzioni, di contratti di fornitura, di incarichi professionali o altri strumenti giuridici consentiti dalla legge, per la realizzazione di attività connesse alle attività aziendali;

b) nominare il Responsabile della Protezione dei Dati - Data Protection Officer (DPO), ove ritenuto necessario ai sensi della normativa vigente;
c) decidere, in piena autonomia, in ordine alle finalità e alle modalità dei trattamenti dei dati personali, nonché agli strumenti utilizzati e al profilo della sicurezza;
d) nominare il personale "Autorizzati/Incaricati/designati del/al trattamento", quali soggetti interni che materialmente effettuano le operazioni di trattamento nello svolgimento delle loro attività per l'Organizzazione.

L'Organizzazione favorisce l'adesione a eventuali codici di condotta elaborati dalle associazioni e dagli organismi di categoria rappresentativi, ovvero a meccanismi di certificazione della protezione dei dati approvati, per contribuire alla corretta applicazione del GDPR e per dimostrarne il concreto rispetto da parte del Titolare e dei Responsabili del trattamento.

4.2 Responsabile del trattamento

4.2.1 *Nomina dei responsabili*

Nei casi in cui un soggetto terzo, esterno alla società, effettua trattamenti di dati personali per conto dell'Organizzazione e non può essere considerato come autonomo Titolare o come soggetto autorizzato del trattamento, questi è nominato come Responsabile trattamento dati ai sensi dell'art. 28 del Regolamento UE 2016/679.
In tale contesto, relativamente alla formalizzazione della nomina conseguente a tutte le tipologie di accordi/contratti, il Personale deve garantire che tutti i contratti aventi per oggetto in via diretta o indiretta un trattamento dei dati in nome e per conto dell'Organizzazione incorporino una specifica clausola, in cui si prevede la nomina della controparte a Responsabile esterno del trattamento oggetto del contratto o, in alternativa – laddove già sottoscritto - il contratto dovrà essere integrato tale specifica clausola

4.2.2 *Elenco responsabili del trattamento*

Per consentire agli Interessati di poter chiedere o inviare informazioni sui trattamenti che li riguardano, l'Ufficio *compliance* deve gestire, aggiornare e mantenere l'elenco di tutti i Responsabili del trattamento esterni, che dovrà essere reso disponibile a richiesta degli interessati.
Il Responsabile di Settore che provvede alla esecuzione di contratti che includano la nomina a Responsabile esterno del trattamento dei dati personali verifica, con frequenza perlomeno annuale, eventuali contratti scaduti o decaduti, al fine di aggiornare la lista in oggetto, tracciando in questa la data di revoca della nomina a Responsabile esterno per i trattamenti legati ad incarico terminato, dandone comunicazione all'Ufficio compliance.

4.3 Soggetto autorizzato del trattamento (i.e."incaricato")

L'Organizzazione designa come "Soggetto autorizzato del trattamento" tutto il proprio personale e/o collaboratore che tratta o può trattare dati personali. Il Titolare fornisce

l'informativa e l'atto di nomina a "Soggetto autorizzato del trattamento" al personale/collaboratore, di norma contestualmente all'assunzione/contratto o, se già avvenuta/o, successivamente.
Ogni soggetto autorizzato deve attenersi alle istruzioni ricevute dal Titolare.

4.4 Amministratori di sistema

Laddove presente tale/i figura/e, l'Organizzazione adotta le misure di sicurezza idonee, tenendo presente le misure definite in materia dal Garante per la protezione dei dati personali nel tempo [1]. Provvedimento "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" - 27 novembre 2008.
L'Organizzazione definisce specifiche procedure operative per disciplinare i seguenti aspetti:

- selezione e nomina degli Amministratori di Sistema (sia per il personale interno che per i consulenti), attribuzione privilegi, aggiornamento dell'elenco degli amministratori di sistema e relativa formazione obbligatoria;
- modifica e revoca delle nomine degli Amministratori di Sistema e dei relativi privilegi prevedendo il successivo aggiornamento del suddetto elenco;
- verifica dell'attività degli Amministratori di Sistema
- gestione dei contratti di outsourcing e introduzione in questi ultimi delle opportune clausole per gli adempimenti in materia di protezione dei dati un capo agli Amministratori di Sistema;
- gestione delle richieste da parte degli interessati di consultazione dell'elenco degli Amministratori di Sistema.

Nell'ambito dell'Organizzazione, il Titolare del trattamento o un soggetto dallo stesso delegato provvede alla verifica almeno annuale delle attività svolte dall'amministratore di sistema in modo da controllare la rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

5. Riservatezza dei dati

Il Personale deve sempre usare la massima discrezione sui dati personali di cui sia a conoscenza, curando attentamente la loro protezione.
Per assicurare tale discrezione è importante che gli spazi operativi destinati al ricevimento degli utenti, alla raccolta dei documenti ed alla loro conservazione siano opportunamente delimitati, per evitare il fortuito accesso da parte di terzi o di personale non interessato.
Anche le comunicazioni tra colleghi di dati personali di terzi deve limitarsi a quanto necessario per l'espletamento del servizio.

[1] Provvedimento "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" - 27 novembre 2008 e succ. modifiche introdotte con provvedimento del 25 giugno 2009

È vietata ogni comunicazione di dati all'esterno del perimetro dell'Organizzazione, salvo il caso in cui ciò sia necessario per lo svolgimento degli incarichi affidati. Ogni informazione, sia che si tratti di attività attuali sia che si tratti di attività future, ed ogni altro materiale utilizzato o prodotto dai prestatori d'opera (dipendenti, consulenti o incaricati di ditte esterne) in relazione al proprio impiego/attività, è di proprietà dell'Organizzazione.
È vietato copiare, diffondere, pubblicare, inviare notizie e/o informazioni tecniche che in qualche modo possano ridurre la sicurezza di funzionamento d'impianti o reti o che in qualche modo possano permettere di arrecare danni, anche di immagine, alla struttura del Titolare.
È fatto divieto ad ogni dipendente o collaboratore del Titolare, salvo espressa autorizzazione, rilasciare comunicazioni o interviste in nome e per conto della società.

6. <u>Sicurezza del trattamento</u>

Il Titolare e ciascun Responsabile del trattamento mettono in atto misure tecniche ed organizzative adeguate a garantire un livello di sicurezza adeguato al rischio, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, 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.
Le misure tecniche ed organizzative di sicurezza da mettere in atto per ridurre i rischi del trattamento ricomprendono:

- la pseudonimizzazione;
- la minimizzazione;
- la cifratura dei dati personali;
- la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico;
- una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Costituiscono misure tecniche ed organizzative che possono essere adottate dall'Organizzazione:

- sistemi di autenticazione; sistemi di autorizzazione; sistemi di protezione (antivirus; firewall; antintrusione; altro);
- misure antincendio; sistemi di rilevazione di intrusione; sistemi di sorveglianza; sistemi di protezione con videosorveglianza; registrazione accessi; porte, armadi e contenitori dotati di serrature e ignifughi; sistemi di copiatura e conservazione di archivi elettronici;
- altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico.

La conformità del trattamento dei dati al GDPR in materia di protezione dei dati personali è dimostrata attraverso l'adozione delle misure di sicurezza o l'adesione a codici di condotta approvati o ad un meccanismo di certificazione approvato.
Il Titolare e ciascun Responsabile del trattamento si obbligano ad impartire adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per loro conto ed abbia accesso a dati personali.

7. Registro delle attività di trattamento

Il Registro delle attività di trattamento sui dati personale è tenuto dal Titolare ovvero dal soggetto dallo stesso delegato, sempre sotto la responsabilità del Titolare, presso gli uffici della struttura organizzativa in forma telematica.
Il Registro delle attività di trattamento svolte dal Titolare del trattamento reca almeno le seguenti informazioni:

- il nome ed i dati di contatto dell'Organizzazione e degli eventuali Contitolari del trattamento, del RPD;
- le finalità del trattamento;
- la sintetica descrizione delle categorie di interessati, nonché le categorie di dati personali;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
- l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;
- ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate.

8. Valutazioni d'impatto sulla protezione dei dati (DPIA)

Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare, prima di effettuare il trattamento, deve attuare una Valutazione d'impatto sulla protezione dei dati personali (DPIA) ai sensi dell'art. 35 GDPR, considerati la natura, l'oggetto, il contesto e le finalità del trattamento stesso.
La DPIA è una procedura che permette di realizzare e dimostrare la conformità delle misure di sicurezza predisposte al rischio associato al trattamento individuato.
La DPIA è effettuata in presenza di un rischio elevato per i diritti e le libertà delle persone fisiche. Fermo restando quanto indicato dall'art. 35, par. 3, GDPR, i criteri in base ai quali sono evidenziati i trattamenti determinanti un rischio intrinsecamente elevato, sono i seguenti:

- trattamenti valutativi o di *scoring*, compresa la profilazione e attività predittive, concernenti 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 dell'interessato;
- decisioni automatizzate che producono significativi effetti giuridici o di analoga natura, ossia trattamenti finalizzati ad assumere decisioni su interessati che producano effetti

giuridici sulla persona fisica ovvero che incidono in modo analogo significativamente su dette persone fisiche;
- monitoraggio sistematico, ossia trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o la sorveglianza sistematica di un'area accessibile al pubblico;
- trattamenti di dati sensibili o dati di natura estremamente personale, ossia le categorie particolari di dati personali di cui all'art. 9, GDPR;
- trattamenti di dati su larga scala, tenendo conto: del numero di numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento; volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento; durata o persistenza dell'attività di trattamento; ambito geografico dell'attività di trattamento;
- combinazione o raffronto di insiemi di dati, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato;
- dati relativi a interessati vulnerabili, ossia ogni interessato particolarmente vulnerabile e meritevole di specifica tutela per il quale si possa identificare una situazione di disequilibrio nel rapporto con il Titolare del trattamento, come i dipendenti dell'Organizzazione, soggetti con patologie psichiatriche, richiedenti asilo, pazienti, anziani e minori;
- utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;
- tutti quei trattamenti che, di per sé, impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.

Nel caso in cui un trattamento soddisfi almeno due dei criteri sopra indicati occorre, in via generale, condurre una DPIA, salvo che il Titolare ritenga motivatamente che non può presentare un rischio elevato; il Titolare può motivatamente ritenere che per un trattamento che soddisfa solo uno dei criteri di cui sopra occorra comunque la conduzione di una DPIA.
Il Titolare si consulta con il DPO, ove nominato, anche per assumere la decisione di effettuare o meno la DPIA; tale consultazione e le conseguenti decisioni assunte dal Titolare devono essere documentate nell'ambito della DPIA.
Il DPO monitora lo svolgimento della valutazione d'impatto e fornisce – se richiesto - consulenza a riguardo.

9. Violazione dei dati personali (*data breach*)

Per violazione dei dati personali (in seguito "*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 non autorizzato ai dati personali trasmessi, conservati o comunque trattati dall'Organizzazione.
Il personale addetto al trattamento qualora venga a conoscenza, nell'espletamento delle attività di competenza o indirettamente nello svolgimento delle stesse, del verificarsi di eventuali violazioni dei dati personali o di incidenti di sicurezza che possano esporre a rischio di violazione dei dati ("*data breach"*) deve tempestivamente informare il Titolare.

Il Titolare, ove ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, provvede alla notifica della violazione al Garante per la protezione dei dati personali. La notifica dovrà avvenire entro 72 ore e comunque senza ingiustificato ritardo, utilizzando la procedura operativa predisposta.
Il Responsabile del trattamento, ove designato, è obbligato ad informare il Titolare, senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione entro 24 ore.
I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al considerando 75 del RGPD, sono i seguenti:

- danni fisici, materiali o immateriali alle persone fisiche;
- perdita del controllo dei dati personali;
- limitazione dei diritti, discriminazione;
- furto o usurpazione d'identità;
- perdite finanziarie, danno economico o sociale.
- decifratura non autorizzata della pseudonimizzazione;
- pregiudizio alla reputazione;
- perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari).

Se il Titolare ritiene che il rischio per i diritti e le libertà degli interessati conseguente alla violazione rilevata è elevato, allora deve informare questi ultimi, senza ingiustificato ritardo, con un linguaggio semplice e chiaro al fine di fare comprendere loro la natura della violazione dei dati personali verificatesi.
Per ogni altra informazione sugli step operativi da seguire in caso di violazione, si rimanda alla "Procedura per la gestione delle violazioni dei dati personali ("Data Breach") "predisposta dall'Organizzazione e messa a disposizione del Personale autorizzato al trattamento.

10. Riscontro alle richieste di esercizio dei diritti degli interessati

Ciascun Responsabile di Settore ha la responsabilità di gestire le richieste da parte degli interessati pervenute all'Ente relativamente alle casistiche identificate dall'art. 15 e seguenti del Regolamento UE 2016/679. Ciascun Responsabile di Settore deve assicurare che l'interessato riceva riscontro alla sua richiesta entro 30 giorni.
A tal fine il Responsabile di Settore è supportato:

- dal settore/ufficio competente;
- dagli esperti legali per definire il testo della risposta;
- dagli outsourcer per raccogliere i dati personali, eventualmente trattati dai sistemi informatici, necessari a fornire il riscontro richiesto.

Per ogni altra informazione sulla corretta gestione dei diritti degli interessati, si rinvia alla politica di dettaglio adottata dall'Organizzazione e portata a conoscenza di ogni soggetto autorizzato al trattamento di dati personali.
Laddove la richiesta presenti particolare complessità può essere richiesto il parere del DPO.

11. Comunicazione e diffusione dei dati

Una specifica attenzione va dedicata alle ipotesi di comunicazione o diffusione dei dati. In altri termini, ogni qual volta si prospetti l'eventualità di divulgare (in qualsiasi forma o modo) dati personali, è necessario procedere alle seguenti verifiche, specie se a riguardo di dati sensibili:

- verifica della legittimità della divulgazione alla luce della informativa fornita all'interessato;
- verifica di eventuali normative e regolamenti che consentano/rendano obbligatoria la divulgazione.

12. Misure di sicurezza per il trattamento

12.1 Trattamento effettuato senza l'utilizzo di strumenti elettronici

In particolare, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento effettuate senza l'ausilio di strumenti elettronici, i soggetti autorizzati al trattamento devono conservare gli atti, i documenti e ogni altro supporto contenente dati personali in ambienti controllati (ad esempio, locali, armadi o cassetti muniti di serratura), prelevandoli per il solo tempo necessario al loro utilizzo e restituendoli a chi ne ha la responsabilità e l'autorizzazione alla conservazione, al termine delle operazioni affidate.

Nel dettaglio:

- il materiale cartaceo contenente dati personali deve essere controllato e custodito con diligenza in modo da impedire che durante le quotidiane operazioni di lavoro terzi non autorizzati possano prenderne visione e, se il materiale contiene dati sensibili o giudiziari, esso dovrà essere conservato, sino alla restituzione, in contenitori muniti di serratura. Al termine del lavoro tutto il materiale dovrà essere riposto in armadi, cassetti o altri contenitori muniti di serratura, in maniera che ad essi non accedano persone prive di autorizzazione;
- l'accesso agli archivi contenenti dati particolari ("sensibili" o giudiziari) deve essere controllato;
- gli atti ed i documenti contenenti dati personali particolari ("sensibili" o giudiziari) sono affidati agli Autorizzati al trattamento esclusivamente per lo svolgimento dei relativi compiti assegnati in forma scritta: i medesimi atti e documenti sono controllati e custoditi dai predetti incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate;
- gli autorizzati ammessi, a qualunque titolo, agli archivi contenenti dati sensibili o giudiziari, dopo l'orario di chiusura, sono identificati e registrati: quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono devono essere preventivamente autorizzate;
- è obbligatorio distruggere o rendere inutilizzabili i documenti cartacei ed i supporti rimovibili, magnetici o ottici dismessi in modo da garantire che i dati ivi contenuti non

possano più essere ricostruiti e/o utilizzati (anche parzialmente) da parte di terzi non autorizzati al trattamento; anche il materiale destinato al macero ed i supporti magnetici o ottici da eliminare devono essere trattati in modo che risulti tecnicamente impossibile recuperare, anche parzialmente, i dati contenuti negli stessi. Pertanto, occorre prevederne la distruzione (se disponibili, con le apposite macchine "distruggi documenti/supporti" o con tecnologie similari) in modo da garantire che i dati in essi contenuti non possano essere ricostruiti, anche parzialmente, o utilizzati;

- tutte le stampe effettuate, contenenti dati personali, dovranno essere trattate in modo da evitare che terzi non autorizzati possano prenderne visione oppure accedervi e/o produrne copie.

Il Responsabile di ogni settore/ufficio verifica la corretta applicazione da parte degli autorizzati di tutte le procedure previste in materia di trattamenti effettuati senza l'ausilio di strumenti elettronici finalizzate ad evitare accessi non autorizzati ai dati personali, anche se sensibili o giudiziari o trattamenti non consentiti.
Il Responsabile suddetto verifica in particolare che l'accesso agli archivi cartacei sia consentito al solo personale autorizzato e che la distruzione dei supporti cartacei che contengono dati personali venga effettuato in conformità alla normativa vigente, utilizzando ove possibile e se disponibili, le apposite apparecchiature "distruggi documenti".

12.2 Trattamento effettuato con strumenti elettronici

Il Titolare e gli autorizzati al trattamento dei dati personali, qualora durante lo svolgimento della loro attività lavorativa utilizzino strumenti informatici sono tenuti al rispetto di quanto previsto dal "Regolamento per l'utilizzo degli strumenti informatici e telematici".

13. Smaltimento delle apparecchiature elettriche ed elettroniche

Ciascun Responsabile di Settore è responsabile dell'adozione di opportune misure di sicurezza, anche con l'ausilio o conferendo incarico a terzi tecnicamente qualificati, per garantire l'inesistenza o la non intelligibilità di dati personali sui supporti di memorizzazione destinati al reimpiego, al riciclaggio o allo smaltimento.

14. Trasferimento dei dati personali a Paesi extra UE

Qualora i Suoi dati personali siano oggetto di trasferimento al di fuori dell'Unione Europea, il Titolare si assicura di avere preso adeguate misure per proteggerli prima del trasferimento. Il Titolare trasferisce i dati solo quando ciò sia giustificato dalla necessità di adempiere ad obbligazioni contrattuali o a disposizioni legali, o per giustificate esigenze tecniche/tecnologiche e siano state implementate delle salvaguardie per assicurare che i dati continuino a essere protetti almeno allo stesso livello di tutela richiesto nella giurisdizione di origine. Per assicurare tale livello di protezione per le informazioni personali, il Titolare può usare un Accordo sul trasferimento dei dati con la terza parte ricevente basato sulle clausole contrattuali tipo approvate dalla Commissione Europea o assicurare che il trasferimento sia verso una giurisdizione soggetta a una decisione di adeguatezza da parte della Commissione Europea.

Qualsiasi trasferimento di dati verso organizzazioni internazionali e/o Paesi non appartenenti allo Spazio Economico Europeo avverrà conformemente alle modalità permesse dalla corrente legislazione.

15. Verifiche periodiche

Oltre alla normale verifica delle attività operative in capo al Responsabile di Settore, sono previste verifiche periodiche in accordo con la normativa vigente al fine di verificare il rispetto della presente Politica.
L'Organizzazione si riserva comunque le facoltà previste dalla normativa vigente di effettuare specifici controlli ad hoc nel caso di segnalazioni di attività che hanno causato danno, che ledono diritti di terzi o che, comunque, risultino illegittime.
Le attività di valutazione delle misure organizzative, procedurali e tecniche sono in carico a ciascun Responsabile di Settore, che si coordinerà con gli altri Responsabili di Settore, con il supporto e la collaborazione fondamentali del Responsabile della Protezione dei Dati (DPO), ove nominato, o professionisti esterni.
Riguardo a tali controlli il presente Regolamento costituisce preventiva e completa informativa nei confronti dei Dipendenti e collaboratori del Titolare.

16. Sanzioni

È fatto obbligo a tutti i Dipendenti e collaboratori dell'Organizzazione di osservare le disposizioni portate a conoscenza con le presenti Istruzioni Operative. Il mancato rispetto o la violazione delle regole sopra ricordate é perseguibile con provvedimenti disciplinari e/o sanzionatori previsti dalla vigente normativa, nonché con tutte le azioni civili e penali consentite. Essendo le presenti istruzioni operative ispirate ai valori etici generali contenuti nel codice etico, il mancato rispetto delle stesse costituisce violazione del codice etico aziendale, e quindi rende applicabile la clausola risolutiva espressa contrattualmente inserita ai fini scriminanti di cui all'art. 6 del D.lgs. 231/01.

17. Aggiornamento e revisione

La presente Politica è stata redatta tenendo conto della normativa vigente e dei Provvedimenti generali emanati dal Garante della protezione dei dati personali. Per qualsiasi eventuale ulteriore indicazione, valgono oltre alla presente politica le disposizioni della normativa vigente e le indicazioni emanate dal Garante privacy.
Tutti i Dipendenti e collaboratori possono proporre, quando ritenuto necessario, integrazioni al presente documento. Le proposte vanno esaminate dal Titolare tramite il Responsabile di Settore competente per materia.
La presente Politica è soggetta a revisione con frequenza periodica o qualora se ne ravveda la necessità. Copia del presente documento verrà messo a disposizione sul sito web aziendale.

Tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi sostituite dalle presenti.

18. <u>Rinvio</u>

Per tutto quanto non espressamente disciplinato con le presenti disposizioni, si applicano le disposizioni del Regolamento UE 2016/679 (GDPR) e della normativa nazionale vigente in materia di protezione dei dati personali.

Data di ultima revisione

02/01/2024

Il Titolare del trattamento

Amministratore Unico