Manuale sulla Protezione dei dati personali

CONSIGLIO DI PRESIDENZA
della GIUSTIZIA TRIBUTARIA

Roma - Via Solferino, 15 - 00185 Telefono: +39 06.9383065 Fax: 06.4440729
Mail: UfficioSegreteriaCPGT@finanze.it **Pec:** UfficioSegreteriaCPGT@pce.finanze.it

ULTIMA REVISIONE del 03/12/2024

Redatto	**Verificato**	**Approvato**

CONSIGLIO DI PRESIDENZA della GIUSTIZIA TRIBUTARIA
Roma - Via Solferino, 15 - 00185 Telefono: +39 06.9383065 Fax: 06.4440729
Mail: UfficioSegreteriaCPGT@finanze.it Pec: UfficioSegreteriaCPGT@pce.finanze.it

SOMMARIO

N.	Titolo	Pagina
1	Revisione	04
2	Scopo	04
3	Campo di applicazione	04
4	Rinvio	04
5	Periodicità di revisione del presente documento	04
6	Riferimenti normativi principali	04
7	Definizioni	05
8	Ruoli, compiti e nomina delle figure previste per la sicurezza dei dati personali	06
8.1	Titolare del trattamento dei dati personali	06
8.2	Delega alla gestione del trattamento dei dati personali	06
8.3	Responsabile Protezione Dati Personali	06
8.4	Persone autorizzate al trattamento	07
8.4.1	Autorizzazione generale al trattamento	07
8.4.2	Istruzioni generali per il trattamento dei dati personali	07
8.4.3	Modalità di acquisizione e accesso ai dati	07
8.4.4	Modalità di trattamento di dati personali effettuato con l'ausilio di strumenti elettronici	08
8.4.5	Trattamento di dati personali effettuato senza l’ausilio di strumenti elettronici	08
8.5	Responsabili del trattamento esterni	08
9	Regole generali sul trattamento dei dati personali	09
9.1	Trattamento legale, equo e trasparente	09
9.2	Finalità legittime	09
9.3	Minimizzazione dei dati	10
9.4	Accuratezza	10
9.5	Archiviazione / rimozione	10
9.6	Sicurezza	11
9.7	Violazione	11
9.8	Gestione informazioni su siti internet	12
10	Regole generali per l’utilizzo dei sistemi informatici del CPGT	12
10.1	Utilizzo del Personal Computer	12
10.2	Utilizzo di internet	13
10.3	Utilizzo del servizio di posta elettronica	14
11	Registro del Trattamento	15
11.1	Contenuti del Registro	15

N.	Titolo	Pagina
11.2	Modalità di aggiornamento e verifica	15
11.3	Accesso e consultazione	16
11.4	Formazione e sensibilizzazione	16
11.5	Monitoraggio e audit	16
12	Gestione violazioni dati personali (data breach)	16
12.1	Procedura da seguire in caso di violazione dei dati personali	16
12.2	Contenuto delle notifiche al garante e agli interessati	17
12.3	Registro delle violazioni	18
13	Diritti dell'interessato	18
13.1	Diritto di accesso dell’interessato	18
13.2	Rettifica e cancellazione	19
13.3	Diritto alla cancellazione («diritto all’oblio»)	19
13.4	Diritto di limitazione di trattamento	19
13.5	Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento	20
13.6	Diritto alla portabilità dei dati	20
13.7	Diritto di opposizione e processo decisionale automatizzato relativo alle persone fisiche	20
13.8	Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione	21
13.9	Limitazioni	21
13.10	Procedura di gestione richieste di esercizio del diritto da parte degli interessati	22

Roma - Via Solferino, 15 - 00185 Telefono: +39 06.9383065 Fax: 06.4440729
Mail: UfficioSegreteriaCPGT@finanze.it **Pec:** UfficioSegreteriaCPGT@pce.finanze.it

1. Revisione

Storico delle revisioni

Rev.	Data	Descrizione
0	03/12/2024	Prima emissione

2. Scopo

Il presente Manuale è redatto al fine di individuare le norme comportamentali e le procedure tecnico-organizzative da rispettare in materia di trattamento dei dati personali e di sicurezza nello svolgimento di tutte le attività istituzionali del Consiglio di Presidenza della Giustizia Tributaria (di seguito anche "CPGT").
In particolare, si ritiene necessario definire una chiara disciplina interna affinchè il trattamento dei dati personali svolto nell'ambito delle mansioni lavorative rispetti i diritti e le libertà fondamentali, nonché la dignità degli interessati, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

3. Campo di applicazione

Il regolamento si applica alle attività che comportano il trattamento dei dati personali di titolarità del CPGT.

4. Rinvio

Per quanto non espressamente disciplinato in questa sede, si rinvia ai Provvedimenti Generali, alle Autorizzazioni Generali e alle Linee Guida emanate dall'Autorità Garante per la Protezione dei dati personali e, più in generale, alla normativa vigente in materia di protezione di dati personali, che qui deve intendersi integralmente richiamata.

5. Periodicità di revisione del presente documento

Il presente documento rimane in vigore fino a eventuali variazioni organizzative, procedurali, strutturali, legislative che possano influenzare il corretto svolgimento delle attività per la protezione dei dati e che risultino in contrasto con quanto riportato nel presente documento.

6. Riferimenti normativi principali

1. **Regolamento (UE) 2016/679** del Parlamento Europeo e del Consiglio, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati);
2. **Decreto Legislativo 30 giugno 2003, n.196** recante il "Codice in materia di protezione dei dati personali", emendato dal Decreto Legislativo 10 agosto 2018, n. 101, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali,

nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)" (in G.U. 4 settembre 2018 n.205)

7. Definizioni

a) «**dato personale**»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
b) «**trattamento**»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
c) «**limitazione di trattamento**»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
d) «**pseudonimizzazione**»: il trattamento dei dati personali effettuato in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
e) «**archivio**»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
f) «**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;
g) «**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;
h) «**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.
i) «**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;
j) «**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, affinchè i dati personali che lo riguardano siano oggetto di trattamento;
k) «**violazione dei dati personali**»: 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;
l) «**dati biometrici**»: i dati personali ottenuti da un trattamento tecnico specifico, e 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;
m) «**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;

n) «**autorità di controllo**»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51.

8. Ruoli, compiti e nomina delle figure previste per la sicurezza dei dati personali

8.1. Titolare del trattamento dei dati personali

Il Titolare del trattamento ai sensi dell'art. 28 del Codice Privacy, è il Consiglio di Presidenza della Giustizia Tributaria nel suo complesso.

8.2. Delega alla gestione del trattamento dei dati personali

Il CPGT ha individuato la Presidente Carolina Lussana come rappresentante del Titolare del Trattamento per l'organizzazione interna della tutela della protezione dei dati personali, con la facoltà per la stessa:

- di attribuire, ai sensi dell'art. 2-quaterdecies del D.lgs. 196/2003 e s.m.i. a uno o più soggetti espressamente designati specifici compiti e funzioni connessi al trattamento di dati personali;
- di approvare la documentazione eventualmente predisposta ad evidenza e governo dell'organizzazione interna per il rispetto della normativa sulla protezione dei dati personali in vigore.

8.3. Responsabile per la protezione dei dati personali

Ai sensi dell'art. 37 del Reg. UE 679/16, il "Rappresentante del titolare" ha individuato come Responsabile per la protezione dei dati personali la dott.sa Manuela Bianchi (C.F. BNCMNL75L68H501C – P.IVA 16830811002), già nominata con Delibera n. 110/2023 del Comitato di Presidenza del Consiglio di Presidenza della Giustizia Tributaria.

Il predetto "Rappresentante del titolare", nel rispetto di quanto previsto dall'art. 39, par. 1, del Reg. UE 679/16 è incaricato di svolgere, in **piena autonomia e indipendenza**, i seguenti compiti e funzioni:

a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento, nonché ai Consiglieri e ai dipendenti che eseguono il trattamento, in merito agli obblighi derivanti dal Reg. UE 679/16, nonché da altre disposizioni nazionali o dell'Unione relative alla protezione dei dati;
b) sorvegliare l'osservanza del Reg. UE 679/16, di altre disposizioni nazionali o dell'Unione relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi:
   - l'attribuzione delle responsabilità,
   - la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del Reg. UE 679/16;
d) cooperare con il Garante per la protezione dei dati personali;
e) fungere da punto di contatto con il Garante per la protezione dei dati personali per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione;
f) tenere il registro delle attività di trattamento sotto la responsabilità del titolare.

I compiti del Responsabile della Protezione dei Dati personali attengono all'insieme dei trattamenti di dati effettuati dal CPGT.

Il Titolare si impegna a:

a) mettere a disposizione del Responsabile Protezione Dati le risorse necessarie al fine di consentire l'ottimale svolgimento dei compiti e delle funzioni assegnate;
b) non penalizzare il Responsabile Protezione Dati in ragione dell'adempimento dei compiti affidati nell'esercizio delle sue funzioni;
c) garantire che il Responsabile Protezione Dati eserciti le proprie funzioni in autonomia e indipendenza.

I dati di contatto del Responsabile Protezione Dati sono i seguenti, e sono altresì resi disponibili nelle informative pubblicate dal CPGT, oltre che comunicati al Garante per la protezione dei dati personali:

Dott.ssa Manuela Bianchi
+39 340 5954349
manuela.bianchi.privacy@gmail.com

8.4. Persone autorizzate al trattamento

8.4.1. Autorizzazione generale al trattamento

Tutti i Consiglieri e i dipendenti, nell'ambito di appartenenza e di collegamento ai diversi uffici del CPGT, sono autorizzati al trattamento specifico per ufficio, secondo quanto riportato nel registro delle attività di trattamento pubblicato sul sito istituzionale.
Specifiche differenziazioni di autorizzazione possono essere comunicate ai Consiglieri e ai dipendenti attraverso i canali di comunicazione interna, da parte del Rappresentante del Titolare.

8.4.2. Istruzioni generali per il trattamento dei dati personali

Si forniscono le seguenti istruzioni sulle modalità di trattamento dei dati personali/sensibili ex artt. 29 e 32 c.4 del Regolamento Europeo sulla Protezione dei Dati (2016/679), in relazione alle operazioni di trattamento di dati cui il personale autorizzato ha accesso nell'ambito delle attività effettivamente svolte nel CPGT, che ogni persona autorizzata è tenuta a rispettare.
L'ambito del trattamento consentito è quello relativo alla sua funzione e può essere di volta in volta modificato secondo quanto previsto dall'organizzazione dell'area secondo le indicazioni del Dirigente o Responsabile superiore di riferimento.
Le tipologie di trattamento possono essere le seguenti: raccolta, registrazione, organizzazione, conservazione, consultazione, comunicazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione.
Le categorie di dati personali a cui la persona autorizzata avrà accesso saranno quelle definite per la specifica area a cui appartiene nell'ambito del registro delle attività del trattamento predisposto dal Titolare.

8.4.3 Modalità di acquisizione e accesso ai dati

- Se nelle attività assegnate il personale autorizzato acquisisce presso l'interessato dati personali si deve accertare che il soggetto abbia ricevuto l'informativa nella forma prevista dal Titolare o Responsabile dell'area di riferimento e abbia accettato (ove previsto il consenso) il trattamento dei dati;
- Nell'acquisizione dei dati il personale autorizzato deve acquisire dati limitati a quelli necessari per l'espletamento delle attività istituzionali, senza integrarli con dati aggiuntivi non necessari, in generale attenendosi ai format di compilazione eventualmente predisposti.

8.4.4 Modalità di trattamento di dati personali effettuato con l'ausilio di strumenti elettronici

Il personale autorizzato deve:

- effettuare esclusivamente i trattamenti di dati personali che rientrano nell'ambito di trattamento definito nel registro delle attività di trattamento specifico dell'area di appartenenza, per le relative finalità dichiarate e secondo le ulteriori eventuali istruzioni impartite anche verbalmente dal Responsabile superiore;
- segnalare al Responsabile superiore le necessità di trattamento diverse da quelle definite ai fini di valutarne l'idoneità ed eventualmente renderle attive;
- prestare particolare attenzione all'esattezza dei dati trattati e, se sono inesatti o incompleti, deve provvedere ad aggiornarli tempestivamente quando applicabile;
- osservare tutte le misure di protezione e sicurezza atte a evitare rischi di distruzione o perdita anche accidentale dei dati, accesso non autorizzato, trattamento non consentito o non conforme alle finalità della raccolta, sia imposte come configurazioni tecniche sia dettate in regolamenti, linee guida, codici di condotta, policy di sicurezza emanate dal CPGT anche successivamente alla formalizzazione del presente documento;
- nel caso abbia ricevuto le credenziali di autenticazione per il trattamento dei dati personali deve conservare con la massima segretezza le componenti riservate delle credenziali di autenticazione (parole chiave/password) e i dispositivi di autenticazione in proprio possesso e uso esclusivo;
- non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento dei dati personali.

8.4.5 Trattamenti di dati personali effettuato senza l'ausilio di strumenti elettronici

Altre regole di comportamento cui deve attenersi il personale autorizzato sono le seguenti:

- i documenti non devono essere portati al di fuori dei locali individuati per la loro conservazione se non ove espressamente autorizzato dal titolare;
- quando i documenti devono essere portati al di fuori dei locali individuati per la loro conservazione o addirittura all'esterno del luogo di lavoro, tenere sempre con sé la cartella o la borsa, nella quale i documenti sono contenuti;
- controllare che i documenti siano sempre completi e integri;
- ai termine dell'orario di lavoro riporre tutti i documenti nei locali individuati per la loro conservazione;
- i documenti non devono essere mai lasciati incustoditi sul tavolo durante l'orario di lavoro;
- si deve adottare ogni cautela affinché le persone non autorizzate, non possano accedere ai documenti;
- limitare l'utilizzo di copie fotostatiche;
- è proibito utilizzare copie fotostatiche di documenti (anche se non perfettamente riuscite) all'esterno del posto di lavoro, né tanto meno si possono utilizzare come carta per appunti;
- è proibito discutere, comunicare o comunque trattare dati personali per telefono, se non si è certi che il destinatario sia un incaricato autorizzato a potere trattare i dati in questione;
- si raccomanda vivamente di non parlare mai ad alta voce, trattando dati personali per telefono, soprattutto utilizzando apparati cellulari, in presenza di terzi non autorizzati, per evitare che i dati personali possano essere conosciuti da terzi non autorizzati, anche accidentalmente.

8.5. Responsabili del trattamento esterni

Ai sensi dell'Art. 28 del Reg. UE 679/16, i soggetti esterni che, in qualità di fornitori, consulenti o comunque contraenti, per esigenze organizzative del CPGT, gestiscono specifici servizi o svolgono attività connesse, strumentali o di supporto a quelle del CPGT, che prevedano il trattamento di dati personali di titolarità del CPGT (ad es.: fornitura di prestazioni professionali o di prestazioni e servizi anche in convenzione quali consulenti, fornitori di servizi cloud,

fornitori di software SaaS, ecc.), sono individuati in qualità di Responsabili del trattamento.
Ogni Responsabile di Ufficio è tenuto quindi, per ogni nuovo fornitore che tratti dati personali per conto del CPGT, a verificare la capacità del fornitore di rispettare i requisiti regolamentatori in termini di protezione dei dati personali, e a interfacciarsi con l'Ufficio "Economato" per interessare/informare i soggetti competenti a ufficializzare la nomina/accordo di Responsabile Trattamento esterno, per conto del CPGT.

9. Regole Generali sul trattamento dei dati personali

Il CPGT si impegna a elaborare i dati in conformità al Regolamento sulla Protezione dei dati 679/16 UE (di seguito RGPD).
Di conseguenza, in base all'articolo 5 del RGPD si impegna a far sì che all'interno del CPGT, i dati personali siano:

a) trattati in modo lecito, equo e trasparente nei confronti delle persone interessat. L'ulteriore elaborazione a fini di archiviazione nell'interesse pubblico, a fini di ricerca scientifica o storica o a fini statistici non è considerata incompatibile con le finalità iniziali;
b) raccolti per scopi determinati, espliciti e legittimi e non ulteriormente trattati in modo incompatibile con tali scopi;
c) adeguati, pertinenti e limitati a quanto necessario in relazione alle finalità per le quali sono trattati;
d) accurati e, se necessario, aggiornati. Deve essere adottato ogni ragionevole sforzo per garantire che i dati personali che sono inaccurati, in relazione agli scopi per cui sono trattati, siano cancellati o rettificati senza indugio;
e) tenuti in una forma che consenta l'identificazione degli interessati per un periodo non superiore a quello necessario agli scopi per i quali i dati personali sono trattati e alla necessità del CPGT di tutela giuridica e di mantenimento del know-how, ferma restando l'implementazione delle idonee misure tecniche e organizzative richieste dal RGPD al fine di salvaguardare i diritti e le libertà delle persone;
f) elaborati in modo tale da garantire un'adeguata sicurezza dei dati personali, compresa la protezione contro l'elaborazione non autorizzata o illecita e contro la perdita accidentale, la distruzione o il danneggiamento, ricorrendo a misure tecniche o organizzative appropriate.

Pertanto il CPGT impartisce le seguenti regole generali, cui devono attenersi tutti i Consiglieri e i dipendenti che vi operano all'interno.

9.1. Trattamento legale, equo e trasparente

a) per garantire che il trattamento dei dati sia lecito, equo e trasparente, è necessario mantenere un registro dei trattamenti;
b) il registro dei trattamenti deve essere riesaminato almeno una volta all'anno;
c) le persone interessate hanno il diritto di essere sempre informate in modo chiaro, preciso e completo sul trattamento dei loro dati personali;
d) le persone interessate hanno il diritto di accedere ai propri dati personali e qualsiasi richiesta di questo tipo fatta al CPGT deve essere trattata tempestivamente da qualsiasi dipendente che la riceve.

9.2. Finalità legittime

a) tutti i dati trattati dal CPGT devono essere eseguiti su una delle seguenti basi legali: consenso, contratto, obbligo legale, interessi vitali, incarichi pubblici o interessi legittimi (rispettando le direttive e le linee guida del Garante per la Protezione dei dati per maggiori informazioni);
b) il CPGT annota la base legale appropriata nel registro dei trattamenti;

c) laddove il consenso sia considerato una base legale per il trattamento dei dati, le prove del consenso devono essere conservate insieme ai dati personali;
d) laddove le comunicazioni siano inviate alle persone in base al loro consenso, l'opzione per la persona di revocare il proprio consenso deve essere chiaramente disponibile e devono essere predisposti sistemi per garantire che tale revoca sia rispettata con adeguata tempestività e precisione nei sistemi di trattamento del CPGT.

9.3. Minimizzazione dei dati

a) il CPGT garantirà che i dati personali siano adeguati, pertinenti e limitati a quanto necessario in relazione agli scopi per cui sono trattati;
b) tutte le persone operanti all'interno del CPGT, prima del trattamento di dati personali dovranno interfacciarsi con il Titolare o suo delegato all'interno del CPGT per verificare il rispetto di tale principio;
c) la progettazione o acquisizione di nuovi sistemi di trattamento dei dati dovrà rispettare tale principio.

9.4. Accuratezza

a) il CPGT adotterà ragionevoli misure per garantire che i dati personali siano accurati e, ove necessario, aggiornati in modo tempestivo. A tal fine, ogni responsabile di trattamento deve effettuare verifiche periodiche della correttezza dei dati registrati;
b) laddove necessario per la base legale su cui i dati sono trattati, devono essere predisposti provvedimenti per garantire che i dati personali siano mantenuti aggiornati. Questi meccanismi devono prevedere audit periodici e procedure di verifica che consentano l'identificazione e la correzione di eventuali inesattezze;
c) ogni sistema di trattamento dei dati deve essere progettato o acquisito in modo tale da consentire facilmente l'aggiornamento e la rettifica dei dati personali. Le specifiche tecniche devono includere funzionalità che permettano la registrazione di modifiche ai dati e la tracciatura delle attività di aggiornamento per garantire trasparenza e integrità;
d) in caso di segnalazioni da parte degli interessati relative a inesattezze dei propri dati personali, il CPGT deve attivare una procedura di verifica e, se del caso, di correzione dei dati entro un termine congruo, specificato dal Responsabile Protezione Dati, per evitare danni agli interessati;
e) il Responsabile Protezione Dati deve stabilire e monitorare una cadenza regolare di audit per la verifica dell'accuratezza dei dati in tutti i sistemi di archiviazione, con l'implementazione di misure correttive immediate in caso di rilevazione di dati non accurati;
f) la collaborazione con terze parti che trattano dati per conto del CPGT deve prevedere clausole contrattuali che richiedano l'adozione di misure per garantire l'accuratezza e l'aggiornamento dei dati personali da parte delle stesse;
g) gli interessati devono essere informati della possibilità di richiedere la rettifica dei propri dati personali e dei processi messi in atto dal CPGT per rispondere a tali richieste in conformità agli articoli 16 e 19 del GDPR.

9.5. Archiviazione / rimozione

a) per garantire che i dati personali siano conservati per un periodo non più lungo del necessario, il CPGT deve attuare una politica di archiviazione per ogni area in cui i dati personali vengono elaborati e rivedere questo processo ogni anno;
b) la politica di archiviazione deve considerare quali dati devono essere conservati, per quanto tempo e perché.

9.6. Sicurezza

a) **Protezione dei Dati Personali**: il CPGT deve garantire che i dati personali siano archiviati e trattati in modo sicuro, adottando misure tecniche e organizzative adeguate per proteggere i dati da accessi non autorizzati, perdite accidentali, distruzioni o alterazioni. Queste misure devono includere l'uso di sistemi e software aggiornati e il monitoraggio regolare per rilevare e prevenire eventuali vulnerabilità;
b) **Limitazione dell'Accesso**: l'accesso ai dati personali deve essere limitato esclusivamente al personale autorizzato che ha effettiva necessità di trattarli per motivi professionali. Devono essere implementati meccanismi di autenticazione a più fattori e policy di gestione delle password per garantire un accesso sicuro e controllato;
c) **Cancellazione Sicura dei Dati**: quando i dati personali devono essere eliminati, devono essere predisposte procedure che ne assicurino la cancellazione sicura e irreversibile, garantendo che i dati non possano essere recuperati. Questo processo deve essere conforme agli standard di sicurezza riconosciuti e documentato per garantire la tracciabilità;
d) **Back-up e Disaster Recovery**: il CPGT deve predisporre e mantenere adeguate soluzioni di back-up dei dati personali per proteggere contro la perdita di dati in caso di incidenti tecnici o altri eventi straordinari. Queste soluzioni devono essere accompagnate da un piano di disaster recovery che preveda procedure dettagliate per il ripristino tempestivo delle operazioni in caso di interruzione;
e) **Formazione e Consapevolezza**: tutti i membri del personale devono ricevere una formazione periodica sulle best practice di sicurezza informatica e sulla protezione dei dati personali. La formazione deve includere informazioni sull'importanza della sicurezza, sulla gestione delle credenziali e sul riconoscimento di minacce come phishing e malware;
f) **Monitoraggio e Audit di Sicurezza**: devono essere effettuati controlli e audit regolari per monitorare l'efficacia delle misure di sicurezza adottate e per identificare eventuali debolezze o non conformità. Questi audit devono essere documentati e devono prevedere l'adozione di misure correttive quando necessario;
g) **Registrazione degli Accessi**: il sistema informatico deve includere un registro delle attività di accesso e modifica dei dati personali, garantendo la tracciabilità e la verifica delle operazioni effettuate. Tali registri devono essere periodicamente esaminati dal Responsabile Protezione Dati per individuare accessi o attività sospette;
h) **Gestione delle Violazioni di Sicurezza**: devono essere predisposte procedure operative per la gestione immediata delle violazioni di sicurezza (data breach). Queste procedure devono includere: la notifica al Responsabile Protezione Dati, la valutazione dei rischi connessi alla violazione, la documentazione dell'evento e, se necessario, la segnalazione al Garante della Privacy entro 72 ore dalla scoperta;
i) **Protezione dei Sistemi Informatici**: il CPGT deve adottare strumenti di protezione (come firewall, software antivirus e sistemi di rilevamento delle intrusioni) per proteggere i dati da minacce esterne. Devono essere implementati aggiornamenti regolari per mantenere i sistemi sicuri e conformi alle best practices attuali;
j) **Contratti con Terze Parti**: qualora i dati personali siano trattati da terzi per conto del CPGT, devono essere stipulati contratti che impongano l'adozione di misure di sicurezza equivalenti a quelle utilizzate dal CPGT. I contratti devono specificare le responsabilità e le misure di sicurezza richieste per garantire la protezione dei dati.

9.7. Violazione

In caso di violazione della sicurezza che porti alla distruzione accidentale o illecita, alla perdita, alterazione, furto, alla divulgazione non autorizzata di dati personali o all'accesso a tali dati, il CPGT dovrà prontamente valutare il rischio per i diritti e le libertà delle persone e, ove risultasse probabile che la violazione dei dati personali comporti un rischio per i diritti e le libertà delle persone fisiche, segnalare, entro e non oltre 72 ore dalla scoperta, tale violazione

all' Autorità Garante per la Protezione dei dati.

9.8. Gestione informazioni su siti internet

I siti web del CPGT devono essere dotati delle misure di sicurezza adeguate alle best practices attualmente in uso.
Per ogni sito deve essere presente e facilmente accessibile una privacy policy che contempli il trattamento sia dei dati forniti volontariamente dagli utenti sia acquisiti automaticamente (es. cookies).
Quando non necessari per le funzionalità e le finalità del sito web, i dati degli utenti possono essere trattati solo su consenso dell'interessato.

10. Regole generali per l'utilizzo dei sistemi informatici del CPGT

Il personal computer (fisso o mobile) ed i relativi programmi e/o applicazioni affidati al personale sono, come è noto, strumenti di lavoro, pertanto:

- vanno custoditi in modo appropriato e possono essere utilizzati solo per fini professionali (in relazione, ovviamente alle mansioni assegnate) e non per scopi personali, tanto meno per scopi illeciti;
- debbono essere prontamente segnalati al CPGT il furto, danneggiamento o smarrimento di tali strumenti;

Poiché in caso di violazioni contrattuali e giuridiche, sia il CPGT che il singolo Consigliere o dipendente sono potenzialmente perseguibili con sanzioni disciplinari, il CPGT verificherà, nei limiti consentiti dalle norme legali e contrattuali: il rispetto delle regole, l'integrità del proprio sistema informatico e la coerenza delle sue configurazioni e dei suoi archivi con le finalità del CPGT.
In questo contesto il CPGT potrà, per necessità di sicurezza del CPGT o per esigenze di continuità della normale attività lavorativa, accedere agli archivi di corrispondenza elettronica o ai file di log riservati alla tracciatura degli eventi di connessione.

10.1. Utilizzo del Personal Computer

I personal computer (fissi e mobili) e i relativi programmi e applicazioni forniti al personale del CPGT sono considerati strumenti di lavoro e devono essere utilizzati esclusivamente per scopi professionali. Pertanto, il personale è tenuto a rispettare le seguenti regole e procedure per garantire un uso appropriato e sicuro di tali strumenti:

a) **Utilizzo Professionale**: i personal computer devono essere utilizzati solo per finalità lavorative correlate alle mansioni assegnate. Qualsiasi uso personale è vietato, e non è consentito utilizzare i computer per attività illecite o che possano compromettere la sicurezza dei dati e delle informazioni;
b) **Custodia dei Dispositivi**: è responsabilità del personale custodire i dispositivi in modo appropriato per prevenire furti, danneggiamenti o smarrimenti. I computer devono essere sempre bloccati quando non sono in uso e non devono essere lasciati incustoditi in luoghi pubblici;
c) **Segnalazione di Incidenti**: il personale deve segnalare immediatamente al CPGT qualsiasi furto, danneggiamento o smarrimento dei dispositivi informatici. La segnalazione deve essere effettuata attraverso i canali ufficiali e in modo tempestivo per attivare le procedure di sicurezza necessarie;
d) **Installazione di Software**: è consentito installare programmi provenienti dall'esterno solo previa autorizzazione esplicita da parte del Titolare o del referente designato. Qualsiasi software installato deve essere conforme alle normative vigenti in materia di copyright e licenze;
e) **Download di File**: non è consentito scaricare file dalla rete o da supporti esterni che non siano direttamente pertinenti alle attività lavorative. I file devono essere verificati per

garantire che non contengano virus o malware;

f) **Utilizzo di Software di Intercettazione**: non è permesso utilizzare strumenti software o hardware atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici. È vietata l'installazione di qualsiasi strumento di comunicazione personale sui dispositivi aziendali;
g) **Condivisione di Risorse**: non è consentito condividere file, cartelle, hard disk o parti di questi con altre persone per accedere a servizi non autorizzati di peer-to-peer al fine di scaricare materiale protetto dalle normative sul diritto d'autore (software, file audio, film, ecc.) ;
h) **Conservazione di Dati Personali**: è vietato conservare all'interno dei personal computer del CPGT foto, video, messaggi personali non collegati alle attività lavorative, e qualsiasi altro dato personale non pertinente alle mansioni lavorative e comunque non rientrante nell'ambito del trattamento autorizzato;
i) **Uso di Dispositivi "Stand Alone"**: i personal computer "stand alone" o in rete sono destinati esclusivamente alla condivisione di informazioni strettamente professionali. Qualsiasi file che non sia direttamente collegato all'attività lavorativa non può essere archiviato su questi dispositivi;
j) **Rimozione di File**: il CPGT si riserva il diritto di rimuovere ogni file o applicazione ritenuti pericolosi per la sicurezza del sistema o installati in violazione delle presenti istruzioni.

Queste regole sono fondamentali per garantire un ambiente di lavoro sicuro e produttivo, e sono previste al fine di proteggere sia i dati aziendali che la privacy delle informazioni personali. Il rispetto di queste norme è essenziale per prevenire incidenti di sicurezza e garantire la conformità alle leggi e alle normative vigenti.

10.2. Utilizzo di Internet

L'accesso a Internet tramite i personal computer e i dispositivi mobili forniti dal CPGT è un privilegio che deve essere utilizzato in modo responsabile e professionale. Pertanto, il personale è tenuto a rispettare le seguenti linee guida per garantire un utilizzo appropriato e sicuro della rete:

a) **Navigazione Professionale**: è consentito navigare in Internet solo per attività strettamente attinenti allo svolgimento delle mansioni lavorative. L'accesso a siti non pertinenti al lavoro deve essere evitato, e il personale è tenuto a limitare la navigazione a risorse utili per le proprie attività;
b) **Contenuti Inappropriati**: non è consentito navigare su siti che contengano contenuti contrari alla morale e alle normative vigenti, inclusi, ma non limitati a, contenuti pornografici, violenti o di incitamento all'odio. La navigazione su tali siti è considerata una violazione delle norme aziendali e può comportare sanzioni disciplinari;
c) **Profilazione e Raccolta Dati**: è vietato visitare siti che possano raccogliere informazioni personali per scopi di profilazione. In particolare, la navigazione su siti che richiedono l'immissione di dati personali sensibili (come opinioni politiche, religione, orientamento sessuale, ecc.) deve essere evitata, salvo che tale attività sia autorizzata per scopi lavorativi e necessaria per il raggiungimento delle finalità istituzionali;
d) **Transazioni Finanziarie**: non è consentito effettuare operazioni di transazioni finanziarie, comprese le operazioni di remote banking e acquisti online, salvo specifiche autorizzazioni scritte dal Titolare e nel rispetto delle normali procedure di acquisto. Ogni operazione deve essere documentata e approvata secondo le linee guida interne;
e) **Scarico di Software**: non è permesso scaricare software gratuiti, trial, freeware e shareware da siti Internet non ufficiali, a meno che non sia espressamente autorizzato dal Titolare o dal Responsabile. Tale attività deve essere effettuata con cautela, garantendo la provenienza legittima e la sicurezza dei file scaricati;
f) **Partecipazione a Forum e Giochi Online**: la partecipazione a forum, giochi online e simili per motivi non professionali è vietata. Qualsiasi richiesta di partecipazione a tali attività

deve essere autorizzata dal referente o dal Titolare e deve essere giustificata da motivazioni lavorative;

g) **Registrazione a Siti**: non è consentito registrarsi a siti web i cui contenuti non siano direttamente legati all'attività lavorativa. Qualsiasi registrazione deve essere approvata dal Titolare e deve rispettare le normative sulla protezione dei dati personali;
h) **Monitoraggio e Sicurezza**: il CPGT si riserva il diritto di monitorare l'uso di Internet per garantire il rispetto di queste linee guida e per prevenire attività dannose per l'ente. Eventuali violazioni delle politiche di utilizzo di Internet possono comportare azioni disciplinari e sanzioni secondo la normativa vigente;
i) **Consapevolezza della Sicurezza**: è responsabilità del personale mantenere un comportamento sicuro durante la navigazione. Ciò include il non cliccare su link sospetti, l'evitare di fornire informazioni personali a siti non affidabili e l'utilizzo di password sicure per accedere a servizi online.

10.3. Utilizzo del Servizio di Posta Elettronica

La posta elettronica (e-mail) è uno strumento di lavoro fondamentale per la comunicazione all'interno del CPGT e con soggetti esterni. Pertanto, è importante che il personale utilizzi il servizio di posta elettronica in modo appropriato e professionale, seguendo le seguenti linee guida:

a) **Utilizzo Professionale**: è consentito utilizzare la posta elettronica esclusivamente per motivi lavorativi e per comunicazioni attinenti alle mansioni assegnate. L'uso della posta elettronica per scopi personali è severamente vietato;
b) **Contenuti Inappropriati**: non è permesso inviare o memorizzare messaggi (interni ed esterni) che contengano contenuti offensivi, discriminatori o inappropriati in relazione a sesso, lingua, religione, razza, origine etnica, opinioni politiche, appartenenza sindacale o qualsiasi altra caratteristica personale. Tali comportamenti possono essere soggetti a sanzioni disciplinari;
c) **Riservatezza delle Informazioni**: la posta elettronica inviata al di fuori della rete informatica del CPGT può essere intercettata da terzi. Pertanto, non deve essere utilizzata per inviare informazioni, dati o documenti di lavoro che siano considerati "strettamente riservati". È importante utilizzare canali di comunicazione sicuri per la trasmissione di tali informazioni;
d) **Partecipazione a Dibattiti e Forum**: non è consentito utilizzare l'indirizzo di posta elettronica del CPGT per partecipare a dibattiti, forum o mailing list non autorizzati. La partecipazione a tali attività può avvenire solo previa autorizzazione scritta da parte del referente o del Titolare, in conformità alle procedure del CPGT;
e) **Allegati e Link**: è responsabilità del personale prestare attenzione agli allegati e ai link inclusi nelle e-mail ricevute. Non si devono aprire allegati o cliccare su link provenienti da fonti non verificate o sospette, in quanto potrebbero contenere virus o malware;
f) **Archiviazione e Cancellazione**: è importante gestire la propria casella di posta elettronica in modo efficiente, archiviando i messaggi pertinenti e cancellando regolarmente quelli non necessari. L'archiviazione dei messaggi deve essere effettuata in conformità con le politiche di conservazione dei documenti del CPGT;
g) **Risposta e Comunicazione**: quando si inviano e-mail, il personale deve garantire una comunicazione chiara e professionale, utilizzando un linguaggio appropriato ed evitando abbreviazioni o gergo informale. È consigliabile rispondere tempestivamente alle e-mail ricevute, rispettando i tempi di risposta stabiliti per le comunicazioni interne;
h) **Formazione e Aggiornamento**: il personale è tenuto a partecipare a corsi di formazione sulla sicurezza informatica e sull'uso appropriato della posta elettronica, per garantire la protezione dei dati e la conformità alle normative vigenti;
i) **Monitoraggio e Sanzioni**: il CPGT si riserva il diritto di monitorare l'uso della posta elettronica per garantire il rispetto di queste linee guida. Le violazioni delle politiche di

utilizzo della posta elettronica possono comportare azioni disciplinari, in conformità con la normativa vigente e le politiche interne.

11. Registro del Trattamento

Il CPGT ha istituito un Registro del Trattamento dei dati personali, che è uno strumento fondamentale per garantire la trasparenza e la responsabilità nella gestione dei dati. Questo registro è suddiviso per Trattamento/Ufficio di pertinenza e deve essere mantenuto aggiornato per riflettere accuratamente tutte le attività di trattamento effettuate dall'istituzione. Di seguito sono elencate le informazioni che devono essere incluse nel Registro.

11.1 Contenuti del Registro

Il Registro del Trattamento deve contenere almeno le seguenti informazioni:

a) **Identità del Titolare**: nome e dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
b) **Finalità del Trattamento**: descrizione chiara delle finalità per cui i dati personali vengono trattati, specificando il motivo giuridico che giustifica il trattamento;
c) **Categorie di Interessati**: una descrizione delle categorie di interessati i cui dati personali sono oggetto di trattamento (es. dipendenti, utenti, fornitori, etc.);
d) **Categorie di Dati Personali**: un elenco delle categorie di dati personali trattati (es. dati identificativi, dati di contatto, dati relativi alla salute, ecc.);
e) **Categorie di Destinatari**: indicazione delle categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi o organizzazioni internazionali;
f) **Trasferimenti di Dati**: dove applicabile, informazioni sui trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti basati sull'articolo 49 del GDPR, la documentazione delle garanzie adeguate;
g) **Tempi di Conservazione**: se possibile, indicazione dei termini previsti per la cancellazione delle diverse categorie di dati;
h) **Misure di Sicurezza**: descrizione generale delle misure di sicurezza tecniche e organizzative adottate per proteggere i dati personali in conformità con l'articolo 32 del GDPR.

11.2 Modalità di Aggiornamento e Verifica

Il Registro del Trattamento deve essere aggiornato regolarmente e secondo necessità. Le modalità di gestione del Registro includono:

a) **Redazione e Aggiornamento**: a cura del Responsabile della Protezione Dati, con la collaborazione dei responsabili di ufficio. Ogni ufficio è tenuto a comunicare tempestivamente eventuali modifiche ai trattamenti effettuati;
b) **Verifica di Completezza**: a cura del Rappresentante del Titolare, che deve assicurarsi che tutte le informazioni siano complete e aggiornate;
c) **Approvazione**: a cura del Rappresentante del Titolare, che approva le modifiche apportate al Registro;
d) **Conservazione**: il Registro deve essere conservato in formato elettronico presso il sito

istituzionale del CPGT, in modo da garantire accessibilità e trasparenza.

11.3 Accesso e Consultazione

Il Registro del Trattamento deve essere reso disponibile agli interessati, a richiesta, per garantire la trasparenza sul trattamento dei dati personali. Le informazioni devono essere presentate in modo comprensibile e accessibile.

11.4 Formazione e Sensibilizzazione

Il personale del CPGT deve essere formato sull'importanza del Registro del Trattamento e sui requisiti normativi associati. I corsi di formazione devono includere informazioni su come mantenere il Registro aggiornato e su come identificare i trattamenti che richiedono registrazione.

11.5 Monitoraggio e Audit

Il Responsabile della Protezione Dati dovrà effettuare controlli periodici per garantire la conformità al GDPR e alle politiche interne del CPGT relative al trattamento dei dati. I risultati di tali audit dovranno essere documentati e utilizzati per migliorare continuamente le pratiche di gestione dei dati personali.

12. Gestione Violazioni dati personali (Data Breach)

Il presente paragrafo descrive le modalità da adottare per tutto il personale CPGT che tratta i dati personali, per la gestione delle violazioni dei dati personali (data breach) intesa come la divulgazione (intenzionale o meno), la distruzione, la perdita, la modifica o l'accesso non autorizzato ai dati trattati (art. 4, comma 2 del Regolamento UE 679/2016, d'ora in poi RGPD).

12.1. Procedura da seguire in caso di violazione dei dati personali

Ogni persona che tratta dati personali che si accorga o rilevi (cd. "scoperta") che si è verificato un evento tra quelli prima descritti ne dà immediata comunicazione via mail al Responsabile Protezione Dati e per conoscenza al Rappresentante del Titolare, indicando i dati coinvolti e descrivendo l'evento secondo la seguente tipologia:

a) Violazione di riservatezza, ovvero quando si verifica una divulgazione o un accesso a dati personali non autorizzato o accidentale;
b) Violazione di integrità, ovvero quando si verifica un'alterazione di dati personali non autorizzata o accidentale;
c) Violazione di disponibilità, ovvero quando si verifica perdita, inaccessibilità, o distruzione, accidentale o non autorizzata, di dati personali.

La comunicazione deve altresì descrivere la natura della violazione dei dati personali indicando, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione.

I predetti soggetti devono altresì:

a) comunicare, ove ne siano a conoscenza, il nome e i dati di contatto del responsabile del

trattamento o di chiunque altro possa fornire elementi utili alla valutazione;
b) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Il Responsabile Protezione Dati organizza un gruppo di lavoro con cui valutare le conseguenze dell'evento sulla tutela dei diritti e delle libertà delle persone alle quali i dati appartengono.

Entro 72 ore dalla scoperta dell'evento, il Responsabile Protezione Dati e il gruppo di lavoro possono:
a) Decidere l'archiviazione della segnalazione, dandone contezza in ogni caso in un registro delle violazioni, se ritenuto che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche coinvolte; oppure
b) chiedere al Rappresentante del Titolare di notificare al Garante privacy l'avvenuta violazione di dati personali (art. 33 GDPR). Nel caso in cui la violazione venga qualificata dal Responsabile Protezione Dati come suscettibile di produrre un rischio elevato per i diritti e le libertà delle persone, ne viene data contestuale "comunicazione" agli interessati nelle forme di comunicazione stabilite dal Rappresentante del titolare, al fine di consentire a questi ultimi l'adozione di ogni precauzione per ridurre al minimo il potenziale danno derivante dalla violazione dei dati (art. 34 del GDPR).

Tutti gli incaricati del trattamento devono provvedere con la massima sollecitudine alla comunicazione al Responsabile Protezione Dati dell'evento dal momento che, qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore dalla scoperta dell'evento, dovranno essere esplicitati i motivi del ritardo, anche al fine di non incorrere nelle sanzioni previste dal GDPR.

12.2. Contenuto delle notifiche al Garante e agli interessati

La notifica al Garante Privacy deve contenere, ai sensi dell'art. 33 del GDPR:
a) la descrizione della natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione, nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
b) la comunicazione del nome e dei dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
c) la descrizione delle probabili conseguenze della violazione dei dati personali;
d) la descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne possibili effetti negativi.

La comunicazione agli interessati, ai sensi dell'art. 34 del GDPR, contiene le seguenti informazioni:
a) il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
b) la descrizione delle probabili conseguenze della violazione dei dati personali;
c) la descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Non è richiesta la comunicazione all'interessato se:
a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;

b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui sopra;
c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

12.3. Registro delle Violazioni

All'atto della prima violazione segnalata verrà istituito il registro dei "data breach" nel quale verranno documentate le violazioni di dati personali eventualmente verificatesi, anche se non comunicate alle autorità di controllo, l'esito delle ulteriori verifiche nonché le conseguenze e i provvedimenti adottati. Nel registro verranno documentate anche le ragioni delle decisioni assunte, al fine di poterle produrre, su richiesta al Garante, nei casi in cui non si sia proceduto alla notifica, oppure nei casi in cui la stessa sia stata ritardata e nei casi in cui non si sia ritenuta necessaria la comunicazione della violazione agli interessati.

La tenuta del registro dei data breach, così come quella del registro dei trattamenti, è a cura del Responsabile Protezione Dati del CPGT.

13. Diritti dell'interessato

Di seguito si riportano i diritti degli interessati, da rispettare per il personale che tratta i dati personali, nonché la procedura da rispettare per l'esercizio dei diritti degli interessati.

13.1. Diritto di accesso dell'interessato

(Rif art 15 Reg. UE 679/16)

L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:

a) le finalità del trattamento;
b) le categorie di dati personali in questione;
c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
f) il diritto di proporre reclamo a un'autorità di controllo;
g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22 del Reg. UE 2016/679 paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

- Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate relative al trasferimento, ai sensi dell'articolo 46.
- Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le

informazioni sono fornite in un formato elettronico di uso comune.
- Il diritto di ottenere una copia non deve ledere i diritti e le libertà altrui.

13.2. Rettifica e cancellazione

(Rif art 16 Reg. UE 679/16)
L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

13.3. Diritto alla cancellazione («diritto all'oblio»)

(Rif art 17 Reg. UE 679/16)
1. L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:

a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento;
c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2;
d) i dati personali sono stati trattati illecitamente;
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 relativamente all'offerta di servizi del CPGT dell'informazione di cui all'articolo 8, paragrafo 1.

2. Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, ai sensi del paragrafo 1, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.
3. I paragrafi 1 e 2 non si applicano nella misura in cui il trattamento sia 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 in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3;
d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; o
e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

13.4. Diritto di limitazione di trattamento

(Rif art 18 Reg. UE 679/16)
1. L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento quando ricorre una delle seguenti ipotesi:
a) l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del

trattamento per verificare l'esattezza di tali dati personali;
b) il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;
c) benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
d) l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

2. Se il trattamento è limitato a norma del paragrafo 1, tali dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.

3. L'interessato che ha ottenuto la limitazione del trattamento a norma del paragrafo 1 è informato dal titolare del trattamento prima che detta limitazione sia revocata.

13.5. Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento

(Rif art 19 Reg. UE 679/16)
Il titolare del trattamento comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche o cancellazioni o limitazioni del trattamento effettuate a norma dell'articolo 16, dell'articolo 17, paragrafo 1, e dell'articolo 18, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Il titolare del trattamento comunica all'interessato tali destinatari qualora l'interessato lo richieda.

13.6. Diritto alla portabilità dei dati

(Rif art 20 Reg. UE 679/16)
1. L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora:
a) il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o dell'articolo 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b); e
b) il trattamento sia effettuato con mezzi automatizzati.

2. Nell'esercitare i propri diritti relativamente alla portabilità dei dati a norma del paragrafo 1, l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile.
3. L'esercizio del diritto di cui al paragrafo 1 del presente articolo lascia impregiudicato l'articolo 17. Tale diritto non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento. 4. Il diritto di cui al paragrafo 1 non deve ledere i diritti e le libertà altrui.

13.7. Diritto di opposizione e processo decisionale automatizzato relativo alle persone fisiche

(Rif art 21 Reg. UE 679/16)
1. L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f), compresa la profilazione sulla base di tali disposizioni. Il titolare

del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.
2. Qualora i dati personali siano trattati per finalità di marketing diretto, l'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali finalità, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto.
3. Qualora l'interessato si opponga al trattamento per finalità di marketing diretto, i dati personali non sono più oggetto di trattamento per tali finalità.
4. Il diritto di cui ai paragrafi 1 e 2 è esplicitamente portato all'attenzione dell'interessato ed è presentato chiaramente e separatamente da qualsiasi altra informazione al più tardi al momento della prima comunicazione con l'interessato.
5. Nel contesto dell'utilizzo di servizi del CPGT dell'informazione e fatta salva la direttiva 2002/58/CE, l'interessato può esercitare il proprio diritto di opposizione con mezzi automatizzati che utilizzano specifiche tecniche.

6. Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici a norma dell'articolo 89, paragrafo 1, l'interessato, per motivi connessi alla sua situazione particolare, ha il diritto di opporsi al trattamento di dati personali che lo riguarda, salvo se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico.

13.8. Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione

(Rif art 22 Reg. UE 679/16)
1. L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.
2. Il paragrafo 1 non si applica nel caso in cui la decisione:
a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;
b) sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato;
c) si basi sul consenso esplicito dell'interessato.
3. 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, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione.
4. Le decisioni di cui al paragrafo 2 non si basano sulle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, a meno che non sia d'applicazione l'articolo 9, paragrafo 2, lettere a) o g), e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato.

13.9. Limitazioni

(Rif art 23 Reg. UE 679/16)
1. Il diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o il responsabile del trattamento può limitare, mediante misure legislative, la portata degli obblighi e dei diritti di cui agli articoli da 12 a 22 e 34, nonché all'articolo 5, nella misura in cui le disposizioni ivi contenute corrispondano ai diritti e agli obblighi di cui agli articoli da 12 a 22, qualora tale limitazione rispetti l'essenza dei diritti e delle libertà fondamentali e sia una misura necessaria e proporzionata in una società democratica per salvaguardare:

a) la sicurezza nazionale;
b) la difesa;
c) la sicurezza pubblica;
d) la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica;
e) altri importanti obiettivi di interesse pubblico generale dell'Unione o di uno Stato membro, in particolare un rilevante interesse economico o finanziario dell'Unione o di uno Stato membro, anche in materia monetaria, di bilancio e tributaria, di sanità pubblica e sicurezza sociale;
f) la salvaguardia dell'indipendenza della magistratura e dei procedimenti giudiziari;
g) le attività volte a prevenire, indagare, accertare e perseguire violazioni della deontologia delle professioni regolamentate;
h) una funzione di controllo, d'ispezione o di regolamentazione connessa, anche occasionalmente, all'esercizio di pubblici poteri nei casi di cui alle lettere da a), a e) e g);
i) la tutela dell'interessato o dei diritti e delle libertà altrui;
j) l'esecuzione delle azioni civili.

2. In particolare qualsiasi misura legislativa di cui al paragrafo 1 contiene disposizioni specifiche riguardanti almeno, se del caso:
a) le finalità del trattamento o le categorie di trattamento;
b) le categorie di dati personali;
c) la portata delle limitazioni introdotte;
d) le garanzie per prevenire abusi o l'accesso o il trasferimento illeciti;
e) l'indicazione precisa del titolare del trattamento o delle categorie di titolari;
f) i periodi di conservazione e le garanzie applicabili tenuto conto della natura, dell'ambito di applicazione e delle finalità del trattamento o delle categorie di trattamento;
g) i rischi per i diritti e le libertà degli interessati; e
h) il diritto degli interessati di essere informati della limitazione, a meno che ciò possa compromettere la finalità della stessa.

13.10. Procedura di gestione richieste di esercizio del diritto da parte degli interessati

I diritti dell'interessato possono essere esercitati a mezzo mail, pec, lettera raccomandata a/r. Per facilitare l'esercizio di tali diritti, nelle informative predisposte si indicano i recapiti a cui inviare le richieste, generalmente il recapito del Responsabile Protezione dati.

Il Responsabile Protezione dati provvederà a coinvolgere un gruppo di lavoro, composto dai Responsabili di ufficio interessati per la gestione della richiesta.

Il Responsabile Protezione dati comunicherà, direttamente o per il tramite di un suo incaricato, all'interessato le informazioni relative alla richiesta presentata dall'interessato senza ingiustificato ritardo e, comunque, entro 30 gg dal ricevimento della richiesta stessa.

Tale termine può essere prorogato di ulteriori 60 gg, se necessario, tenuto conto della complessità e del numero delle richieste. Il titolare del trattamento informa l'interessato di tale proroga e dei motivi del ritardo, entro 30 gg dal ricevimento della richiesta. Se l'interessato presenta la richiesta mediante mezzi elettronici, le informazioni sono fornite, ove possibile, con mezzi elettronici salvo diversa indicazione dell'interessato.

Il gruppo di lavoro se del caso, sottopone la richiesta all'autorizzazione del Rappresentante del Titolare, in qualità di Titolare del Trattamento.

Se il Titolare del Trattamento decide di non ottemperare alla richiesta dell'interessato, lo stesso o un suo incaricato informa l'interessato senza ritardo, e al più tardi entro 30 gg dal ricevimento della richiesta, dei motivi dell'inottemperanza e della possibilità di proporre reclamo a

Roma - Via Solferino, 15 - 00185 Telefono: +39 06.9383065 Fax: 06.4440729
Mail: UfficioSegreteriaCPGT@finanze.it **Pec:** UfficioSegreteriaCPGT@pce.finanze.it

un'autorità di controllo e di proporre ricorso giurisdizionale.

Le informazioni fornite all'interessato ed eventuali comunicazioni e azioni intraprese sono gratuite.

Se le richieste dell'interessato sono manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo, il titolare del trattamento può:

a) addebitare un contributo spese ragionevole tenendo conto dei costi amministrativi sostenuti per fornire le informazioni o la comunicazione o intraprendere l'azione richiesta; oppure
b) rifiutare di soddisfare la richiesta.

Incombe al titolare del trattamento l'onere di dimostrare il carattere manifestamente infondato o eccessivo della richiesta.

Qualora il titolare del trattamento nutra ragionevoli dubbi circa l'identità della persona fisica che presenta la richiesta di cui agli articoli da 15 a 21 del Reg UE 2016/679, può richiedere ulteriori informazioni necessarie per confermare l'identità dell'interessato.