Comune di Chialamberto

Via Roma, 2 – 10070 Chialamberto

Regolamento Comunale per l'attuazione del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali

Redatto a
Chialamberto
Data come da certificato di data certa allegato

Documento certificato tramite
TIME STAMP DATA di Aruba Pec

File salvato nell'archivio
informatico aziendale

Il Titolare del trattamento:
Comune di Chialamberto

Articolo 1 - Oggetto del Regolamento Comunale

Il Regolamento Comunale è redatto in conformità al Regolamento Europeo per la protezione dei dati personali n. 2016/679 (di seguito definito anche solo come "GDPR") e disciplina le modalità del trattamento dei dati personali effettuato dal Comune di Chialamberto.

Il Regolamento Comunale contiene le procedure e le regole di trattamento adottate dal Comune di Chialamberto ed è redatto altresì:

in conformità all'art. 25 - **Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita** - poiché riporta le misure tecniche e organizzative adeguate messe in atto dal Titolare volte ad attuare in modo efficace i principi di protezione dei dati e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del regolamento 679 e tutelare i diritti degli interessati;

in conformità all'art. 30 – **Registro delle attività di trattamento** - in quanto contiene tutte le informazioni richieste dal paragrafo 1 del citato articolo, ovvero:

a) il nome e i 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) le finalità del trattamento;
c) una descrizione delle categorie di interessati e delle categorie di dati personali;
d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
e) ove applicabile, i 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 di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

Lo sviluppo ed il costante aggiornamento di questo documento, anche mediante un'attività di audit periodico, rappresenta uno strumento atto a soddisfare le appropriate e proporzionali misure tecniche e organizzative di protezione dei dati personali, previste dall'articolo 24 comma 1.

Articolo 2 - Responsabilizzazione

2.1 - Soggetti che trattano dati personali

Ciascun Ente che tratta dati personali è qualificato dall'articolo 4 comma 7 del GDPR come **Titolare del trattamento**.

Il **Titolare del trattamento** deve identificare correttamente le varie figure coinvolte nel processo di trattamento dei dati e assegnare loro direttive e responsabilità.

Articolo 4, comma 7 Definizioni

*«**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;*

Oltre al Titolare sono coinvolte nel trattamento le seguenti figure:

- Titolare del trattamento;
- *Data Protection Team*, composto da:
  - Soggetto autorizzato al trattamento dei dati personali con funzioni di sorveglianza, c.d. "Responsabile interno al trattamento" o "Delegato al trattamento";
  - Soggetto autorizzato al trattamento dei dati personali, c.d. "Incaricato del trattamento";
- Data Processor o responsabile esterno del trattamento;
- Amministratore di sistema (come indicato da "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008*" G.U. n. 300 del 24 dicembre 2008, modificato in base al provvedimento del 25 giugno 2009);
- Responsabile della protezione dei dati o DPO (*Data Protection Officer*).

Tali soggetti trattano dati acquisiti direttamente dall'Ente mediante contatto diretto con gli interessati nonché dati raccolti da soggetti terzi quali, ad esempio, appaltatori o consulenti.

Il Comune di Chialamberto non tratta dati personali destinati ad esser trasferiti verso Paesi extra UE fatto salvo il caso di specifica richiesta dell'interessato.

2.2 Rischi potenziali

La mancanza di una chiara politica di responsabilizzazione può essere causa di una scorretta gestione dei dati degli interessati. Tale situazione può determinare conseguenze pregiudizievoli quali, esemplificativamente e non esaustivamente:

- perdita di fiducia nei confronti dell'Ente
- rivelazione non autorizzata di dati personali
- trattamenti non consentiti o proibiti

Tali illeciti possono danneggiare l'immagine dell'Ente e far sorgere richieste risarcitorie nei confronti dello stesso.
Inoltre, l'errato trattamento può avere un impatto negativo sull'obbligatoria revisione periodica delle procedure di gestione dei dati personali trattati ed archiviati dell'Ente.

2.3 Azioni intraprese

Sulla base di quanto enunciato in precedenza il Titolare ha provveduto ad una mappatura riguardante:

- Soggetti che trattano dati (personale interno ed esterno);
- Dati raccolti;
- Finalità del trattamento.

Nella tabella sottostante si riportano i risultati ottenuti.

(Tab 1)

SOGGETTI INTERNI ALL'ENTE			
NOMINATIVO	**INCARICO**	**DATI TRATTATI**	**FINALITÀ**
Comune di Chialamberto	Titolare del trattamento	**Cittadini:** anagrafica; dati di contatto; dati economici; dati fiscali; dati relativi a convinzioni religiose; dati relativi a ideologie politiche; dati inerenti alla salute; dati biometrici; dati giudiziari; dati sull'orientamento e la vita sessuale; dati sull'origine razziale o etnica; Immagini. **Terzi:** anagrafica; dati di contatto; dati fiscali; dati relativi a convinzioni religiose; dati relativi ad ideologie politiche; dati inerenti alla salute; Immagini. **Dipendenti:** anagrafica; dati di contatto; dati economici; dati fiscali; dati relativi a convinzioni religiose; dati relativi ad ideologie politiche;	Esecuzione obblighi di legge; Censimento della popolazione; Gestione amministrativa; Fornitura erogazione di servizi e agevolazioni ai cittadini; Gestione tasse e tributi; Esercizio diritti civili; Vigilanza e controllo del territorio; Attività di pubblica sicurezza; Salvaguardia del territorio; Promozione del territorio; Salvaguardia della salute pubblica; Gestione dei rapporti di lavoro subordinato.

SOGGETTI INTERNI ALL'ENTE			
NOMINATIVO	**INCARICO**	**DATI TRATTATI**	**FINALITÀ**
		dati inerenti alla salute; Immagini **Fornitori ed altri professionisti:** anagrafica; dati di contatto; dati economici; dati fiscali.	
Come da allegati "Scheda Ufficio"	Soggetto autorizzato al trattamento dati personali con funzioni di sorveglianza c.d. Responsabile del trattamento	L'allegato "Scheda Ufficio", redatto specificamente per le varie divisioni interne dell'Ente, riporta l'elenco dei dati trattati divisi per le singole categorie di soggetti	L'allegato "Scheda Ufficio", redatto specificamente per le varie divisioni interne dell'Ente, riporta l'elenco delle finalità perseguite dall'ufficio e dal personale autorizzato
Come da allegati "Scheda Ufficio"	Soggetto autorizzato al trattamento dei dati personali c.d. Incaricato del trattamento	L'allegato "Scheda Ufficio", redatto specificamente per le varie divisioni interne dell'Ente, riporta l'elenco dei dati trattati divisi per le singole categorie di soggetti	L'allegato "Scheda Ufficio", redatto specificamente per le varie divisioni interne dell'Ente, riporta l'elenco delle finalità perseguite dall'ufficio e dal personale autorizzato

Viene reso possibile per gli interessati comunicare con il titolare ed il Data Protection Officer mediante i seguenti canali:

(Tab 2)

Titolare del trattamento	
Denominazione	Comune di Chialamberto
Indirizzo	Via Roma, 2 - 10070 Chialamberto (TO)
P.IVA	02214960011
Codice Fiscale	83002850010
N. telefono	0123.506701
E-mail	info@comune.chialamberto.to.it
Domicilio digitale (PEC o altro)	comchialamberto@pec.it
Responsabile della Protezione dei Dati	
Data Protection Officer	Avv. Luisa Di Giacomo
E-mail	digiacomo@studiofbeassociati.it
Domicilio digitale (PEC o altro)	luisaannamariadigiacomo@pec.ordineavvocatitorino.it

(Tab 3)

SOGGETTI ESTERNI ALL'ENTE			
NOMINATIVO	**INCARICO**	**DATI TRATTATI**	**FINALITÀ**
Come da allegati "Responsabile esterno"	*Data processor*	L'allegato "Responsabile esterno", redatto specificamente per i singoli data processor, ovvero i soggetti esterni all'organizzazione che trattano dati per conto del Titolare, riporta l'elenco dei dati trattati divisi per le singole categorie di soggetti	L'allegato "Responsabile Esterno", redatto specificamente per i singoli data processor, riporta l'elenco delle finalità perseguite dal Data Processor

Il Titolare del trattamento ha provveduto alla redazione di politiche e procedure specifiche per la protezione dei dati personali, in accordo con quanto enunciato dal Regolamento Europeo, dalla normativa Nazionale (D.L.gs., 196/03 come modificato dal D.Lgs. 101/08) e basandosi su buone prassi, norme ISO, UNI e, qualora applicabili, codici di condotta. Tali policy sono soggette a revisione periodica al fine di mantenerle coerenti con l'evoluzione tecnica ed il tipo di attività svolto dal Comune di Chialamberto.

Articolo 28 comma 1:

"Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato."

Il concetto di responsabilizzazione non è rivolto solo al personale interno del Comune, ma anche a tutti i soggetti terzi che con esso collaborano e, così facendo, trattano dati per conto dal Comune di Chialamberto. Il Titolare del Trattamento ha provveduto ad informare tali soggetti esterni (*Data Processor-Responsabile esterno del trattamento*) circa la *policy* del Comune di Chialamberto in materia di dati personali ed essi hanno assicurato di rispettare i requisiti di sicurezza e attenzione nei confronti dei dati previsti dall'articolo 28, comma 1 del GDPR.
Al momento dell'avvio della collaborazione con un soggetto esterno, il Titolare del Trattamento provvederà a nominarlo Responsabile Esterno del Trattamento, tramite lettera di incarico scritta.
Assumendo l'incarico, l'*Outsourcer* accetterà anche tutti gli obblighi in materia di protezione dei dati connessi al suo incarico e si attiverà al fine di adottare le misure di sicurezza richieste dall'articolo 32 del Regolamento Europeo, come indicato nell'articolo 28, comma 3, lettera c).

2.4 Piano interno di formazione

Articolo 29

"Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri."

Il Comune procede alla formazione del personale nel più breve tempo possibile, compatibilmente agli impegni dell'Ente ed alla disponibilità del soggetto formatore.
I dipendenti assunti di recente che hanno la possibilità di entrare in contatto con dati personali vengono informati, all'atto della presa di servizio da parte del Titolare o da personale apposito da esso incaricato sulle procedure organizzative e di *data governance* in atto presso il Comune di Chialamberto.

Il Regolamento Comunale, insieme alle *slide* utilizzate durante le attività formative, costituiscono materiale didattico da utilizzarsi in occasione di questi primi incontri.

Il personale deputato al trattamento dei dati personali del Comune di Chialamberto riceve formazione adeguata e commisurata alla funzione svolta all'interno del *Data Protection Team*, all'esito della quale è messo nelle condizioni di operare in sicurezza.
Il Titolare del trattamento non permette a personale non formato di effettuare trattamenti sui dati, come indicato all'articolo 29 del GDPR.
La formazione dei **soggetti autorizzati al trattamento dei dati,** indipendentemente dall'esecuzione di funzioni di sorveglianza o meno (identificati quali Delegati del trattamento), viene attuata mediante corso della durata di 4 ore.
Gli allegati "Scheda Ufficio" riportano i nomi dei soggetti autorizzati al trattamento dati personali.

La formazione impartita ha come programma:

- Regolamento Europeo e Codice *Privacy*: le normative in vigore;
- Novità e modifiche introdotte dal Regolamento 2016/679 UE;
- Definizioni;
- Figure coinvolte nella gestione privacy e loro doveri, nomine e lettere di incarico;
- Informativa e Consenso;
- Valutazione del rischio;
- Valutazione d'impatto;
- Registro delle attività di trattamento;
- *Data Breach* e gestione degli eventi avversi;
- Videosorveglianza;
- Siti internet e *cookie policy*;
- Diritti dell'interessato;
- Sanzioni amministrative e penali.

Gli attestati ottenuti all'esito dei programmi di formazione vengono allegati alla documentazione del Comune di Chialamberto relativa al trattamento dei dati personali.

Il titolare del trattamento provvede, in collaborazione con il *Data Protection Officer*, alla rivalutazione con cadenza annuale dell'attuale piano e qualora le misure in essere non risultassero pienamente efficaci o eccessive provvederà a modificare o rielaborare il presente documento.

Articolo 3 - Identificazione delle finalità del trattamento

3.1

Il Titolare del trattamento ha provveduto all'identificazione ed alla classificazione delle tipologie di dati che devono essere raccolti per il soddisfacimento delle legittime e trasparenti finalità di trattamento.

L'identificazione delle tipologie di dati raccolti permette al Titolare di ottenere unicamente le informazioni delle quali necessita, limitando i dati raccolti e trattati, nell'ottica di una politica di *Privacy by default* rispondente al principio di minimizzazione dei dati, previsto all'articolo 5, comma 1, lettera c), del GDPR.

Articolo 5 - **Principi applicabili al trattamento di dati personali**

1. *I dati personali sono:*

a) *trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);*

b) *raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);*

c) *adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);*

d) *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 («esattezza»);*

e) *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; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);*

f) *trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).*

2. *Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»).*

Le informazioni devono essere raccolte per finalità specifiche, esplicite, legittime e non devono essere assoggettate ad ulteriori trattamenti che siano con queste incompatibili.

Vi deve inoltre essere congruità tra la natura, la quantità dei dati trattati e le finalità del trattamento, che devono essere coerenti e compatibili con l'attività svolta dal titolare.

Inoltre, è importante che nel definire le finalità non si utilizzino espressioni talmente generiche da renderle incomprensibili all'interessato del quale si vogliono raccogliere i dati.

Nel definire le finalità dei trattamenti svolti dal titolare (riportati nella Tabella 1) viene applicato il seguente schema di riferimento:

(Tab 4)

FASE	PUNTI SALIENTI
Raccolta dei dati	Analisi e classificazione dei dati raccolti, acquisiti od ottenuti da soggetti terzi; Metodi di acquisizione; Motivo della raccolta.
Trattamento	Analisi delle modalità con le quali i dati vengono trattati dal Titolare.
Comunicazione	Analisi delle tempistiche, delle motivazioni e dei destinatari ai quali i dati vengono comunicati.

In caso di una non corretta valutazione delle finalità di raccolta dei dati, i rischi che ne possono derivare sono suddivisibili in 4 categorie:

- economici;
- legali;
- di immagine;
- organizzativi.

Economici in quanto il trattamento di grandi masse di dati comporta l'utilizzo di rilevanti risorse, a livello tecnico e di personale, con conseguente aumento dei costi.
Legali poiché una raccolta non controllata di dati può comportare sanzioni pecuniarie fino ad un massimo di 20 milioni di euro o pari al 4% del fatturato annuo mondiale, riferito all'anno precedente.
Di immagine in quanto la perdita dei dati o il loro trattamento illecito potrebbero determinare la perdita di fiducia nei confronti dell'Ente.
Organizzativi poiché una grossa massa di dati è oggettivamente di più difficile gestione rispetto ad una inferiore.

3.2 Azioni intraprese per l'identificazione delle finalità del trattamento

Il Comune di Chialamberto ha identificato le finalità di trattamento, incrociandole con i dati raccolti.

La *tabella 1* inserita nell'articolo 2 riporta le finalità dei trattamenti effettuati dal Comune di Chialamberto.

Le finalità indicate sono riportate integralmente sull'informativa fornita all'interessato, attraverso metodi e supporti differenti a seconda delle situazioni:

- verbale;
- consegna informativa cartacea;
- esposizione dell'informativa in area facilmente visibile;
- caricamento dell'informativa sul sito web del Comune;
- invio, su richiesta dell'Interessato, a mezzo posta elettronica.

Il consenso al trattamento dei dati personali da parte dell'interessato, qualora necessario, può essere raccolto con modalità differenti ma preferibilmente in forma scritta con apposizione di data e firma autografa.

Dall'analisi svolta risulta che le finalità alla base dei trattamenti effettuati dal Comune di Chialamberto sono **specifiche, esplicite e legittime**, così come previsto dall'articolo 5 del GDPR.

Questa analisi è stata eseguita posteriormente alla raccolta dei dati ed al loro trattamento, poiché l'Ente ha iniziato la sua attività ben prima dell'entrata in vigore del GDPR.
Attesa l'obbligatorietà dei trattamenti effettuati dalle pubbliche amministrazioni e la necessità di assicurare la continuità dei servizi ai cittadini, non era inoltre ipotizzabile limitare il trattamento nel periodo necessario ad effettuare l'analisi.

Questa analisi è stata effettuata preventivamente alla raccolta dei dati ed al loro trattamento.

Il Regolamento Comunale, insieme al verbale di riunione del *Data Protection Team* che vede la partecipazione non solo del Titolare, ma anche dei soggetti autorizzati al trattamento, costituisce elemento di prova attiva della diffusione dei concetti di *protection by default* e *by design* all'interno dell'Ente.

Tutti gli attori del *Data Protection Team* sono quindi in grado di spiegare all'interessato le finalità della raccolta e del trattamento o lo sanno indirizzare verso i contatti necessari per interagire con il titolare del trattamento.

3.4 Introduzione di nuove finalità
Qualora per obblighi di legge, motivi organizzativi, commerciali o di altra natura sia necessaria la raccolta di ulteriori dati o il loro trattamento con modalità e finalità differenti rispetto a quelle indicate nell'informativa consegnata agli interessati, il Titolare fornisce loro le nuove informazioni e richiede un nuovo consenso esplicito ed informato. Tale consenso potrà essere verbale, anche se le politiche interne di gestione della privacy prediligono un consenso scritto, in modo da poter disporre di una prova evidente in caso di contestazione o esercizio dei diritti dell'interessato.

3.5 Codifica dei dati
Nel caso in cui sia tecnicamente ed economicamente possibile, il Titolare del trattamento provvede a rendere i dati non identificabili, mediante procedure di:

- codifica;
- anonimizzazione;
- pseudonimizzazione;
- aggregazione;
- cifratura.

In questi casi viene redatto un registro di correlazione e la sua tenuta verrà affidata direttamente al Titolare o ad uno dei responsabili interni, che ne proteggerà il contenuto.

Articolo 4 - Modalità di messa a disposizione dell'informativa

4.1 Obiettivi

In questo articolo vengono analizzate le metodologie utilizzate dal Comune di Chialamberto per fornire agli interessati l'informativa sui dati raccolti, i trattamenti effettuati, le finalità del trattamento, etc., in accordo con gli articoli 13 e 14 del GDPR, a seconda che i dati vengano raccolti presso l'interessato stesso o presso un soggetto terzo.

4.2 Analisi dei rischi potenziali

L'utilizzo di un'informativa non corretta può essere fonte di diversi problemi per il Titolare del trattamento, quali ad esempio:

- aver raccolto dati che non possono essere utilizzati in quanto sull'informativa non erano specificate le finalità;
- dover giustificare come mai si abbia accesso ai dati non indicati sull'informativa ed a quale scopo;
- far si che un interessato si rivolga direttamente all'autorità di controllo in quanto sull'informativa non sono presenti i dati di contatto del titolare del trattamento.

Il Titolare del trattamento deve fornire agli interessati tutte le informazioni relative al trattamento svolto mediante un documento di facile comprensione, sintetico e che tenga conto, tra le altre cose, del livello culturale medio degli interessati, della loro età e capacità di comprensione o meno della lingua scritta.

4.3 Verifica delle modalità di messa a disposizione dell'informativa

Nessun dato viene acquisito dal personale del Comune di Chialamberto se prima non è stata fornita all'interessato un'informativa, anche sintetica, sui dati raccolti, le finalità, i trattamenti in essere, etc., come indicato dagli articoli 13 e 14 del GDPR.
L'unica eccezione è data dall'invio diretto dei CV, per i quali la consegna dell'informativa avviene alla prima occasione utile, solitamente in caso di colloquio.
In questa situazione i dati possono essere trattati in quanto liberamente forniti dall'interessato.

L'informativa viene consegnata sempre in maniera gratuita, anche nei casi in cui risulti su supporto cartaceo.
Le modalità con le quali il Titolare fornisce una prima informativa sono differenti:

- consegna cartacea;
- esposizione dell'informativa cartacea;
- pubblicazione su di una pagina web.

Per rendere facilmente intelligibili le informative presentate in formato elettronico, il Comune di Chialamberto ha provveduto a formattarle nel modo più corretto, permettendo il *reflow* del testo e la modifica dei caratteri visualizzati dai più comuni browser.
Copia delle informative utilizzate sono allegate al Regolamento Comunale (vedi art. 19).

4.4 Aggiornamento delle informative

Il Titolare monitora gli aggiornamenti normativi e adegua le procedure di trattamento dei dati personali degli interessati.

Articolo 5 - Raccolta del consenso

L'ottenimento del consenso informato da parte dell'interessato rappresenta un aspetto fondamentale per la raccolta, il trattamento e la comunicazione di dati personali, salvo casi specifici per i quali il GDPR prevede un'eccezione, come nel caso dell'esecuzione di un contratto, di rapporti precontrattuali, quando il titolare agisce sulla base del proprio legittimo interesse o su quello dell'interessato oppure per ottemperare ad obblighi di legge.
L'argomento è trattato nell'articolo 7 del GDPR.

Articolo 7 - Condizioni per il consenso

"1. Qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali.
2. Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante.
3. L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato.
4. Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto."

Il Titolare non svolge alcun trattamento senza che l'interessato abbia espresso il proprio consenso o sia presente un'adeguata base giuridica.

Affinché il consenso possa mantenere le proprie caratteristiche (essere libero e informato), è necessario che venga preceduto da una fase nella quale all'interessato vengono spiegati quali tipologie di dati verranno richiesti, come saranno trattati, etc. La consegna di un'informativa correttamente stilata permette di gestire a pieno questa necessità.

Le modalità di raccolta del consenso, per quanto differenti tra loro possano apparire, rientrano in due macro categorie:

- consensi espliciti
- consensi obbligatori

Si hanno **consensi espliciti in** tutti quei casi nei quali l'interessato esprime direttamente il proprio assenso al trattamento, mediante un atto diretto ed inequivocabile, come l'apposizione di una firma autografa o la registrazione della propria voce.

Si hanno **consensi impliciti/obbligatori in** tutti quei casi nei quali non è richiesta un'azione specifica o un atto diretto per manifestare il proprio consenso.

Un trattamento svolto in assenza di consenso da parte dell'interessato può comportare una serie di danni economici e di immagine ed esporre al rischio di pesanti sanzioni, soprattutto laddove l'obbligo di raccoglierlo sia richiesto da specifiche disposizioni di legge o codici di autoregolamentazione.

Articolo 6 - Azioni intraprese per la valutazione delle modalità di raccolta del consenso

6.1 - Modalità di raccolta del consenso

Le modalità di raccolta dei consensi da parte dell'Ente sono adeguate alle circostanze, al tipo di dato raccolto ed ai tipi di trattamento, e comprendono:

(Tab 5)

Tipo di consenso	Caso di applicazione
Consenso obbligatorio (finalità primarie)	Adempimento obblighi di legge; Esecuzione di un contratto; Riprese per attività di videosorveglianza.
Consenso esplicito (finalità secondarie)	Trattamento su dati raccolti presso gli interessati; Attività divulgative

Il consenso fornito per le finalità primarie non implica automaticamente che lo stesso venga assegnato per finalità secondarie, come quelle di promozione o divulgazione delle attività svolte dal Titolare.

La modulistica, sia analogica che digitale, utilizzata dal Comune di Chialamberto permette la distinzione tra i due tipi di consenso ed evita che il consenso secondario possa essere dato in maniera automatica.

6.2 - Importanza della formazione nella raccolta del consenso

La raccolta diretta del consenso da parte dei dipendenti del Comune è possibile solo in seguito a formazione, nel corso della quale vengono fornite le nozioni necessarie per far fronte ad eventuali domande degli interessati. Gli stessi soggetti autorizzati ad operare sui dati possono spiegare agli interessati la possibilità di revoca del consenso ed il fatto che tale revoca non pregiudica la liceità del trattamento basato sul consenso precedentemente prestato.

La formazione impartita consente che i soggetti autorizzati ad operare sui dati non utilizzino nessun dato in assenza di consenso e che, in caso di raccolta di dati contrattuali, non richiedano informazioni eccedenti quelle strettamente necessarie all'adempimento del contratto

6.3 - Azioni da intraprendere in caso di revoca del consenso

Il Titolare del trattamento mette a disposizione degli interessati che abbiano necessità di inviare segnalazioni circa il trattamento effettuato i contatti riportati nell'informativa, ai quali è possibile ricorrere per esercitare i diritti previsti dal GDPR. Tale segnalazione può avvenire in forma semplificata ed informale, anche mediante una semplice telefonata.

In caso di richiesta di revoca del consenso da parte dell'Interessato il Titolare adotta la seguente procedura:

Delegato al trattamento dati	Incaricato del trattamento dati
Identifica l'interessato; Comunica all'interessato di aver preso in carico la sua richiesta; Identifica i trattamenti svolti sui dati dell'interessato;	Comunica la situazione al Titolare o al Responsabile del trattamento; Analizza la richiesta di revoca e della motivazione insieme al resto del *Data Protection Team*.

Delegato al trattamento dati	Incaricato del trattamento dati
Identifica i trattamenti non sottoposti ad un obbligo di legge; Blocca tutti i trattamenti non sottoposti ad un obbligo legale; Per i trattamenti sottoposti ad obbligo, limita i trattamenti alla persona del Delegato al trattamento; Richiede all'interessato il motivo che ha portato alla decisione di revocare il consenso al trattamento, al fine di poter evitare il ripetersi di una condizione simile; Comunica all'interessato l'adempimento svolto; Analizza la richiesta di revoca e della motivazione insieme al resto del *Data Protection Team*.	

Articolo 7 - Protezione dei dati "by default"

7.1 - Obiettivi

Il principio della protezione "*by default*" impone che i dati personali debbano essere protetti in ogni attività di trattamento.
Tale necessità viene soddisfatta al momento della richiesta dei dati, limitandone la raccolta alla minor quantità necessaria, anche in caso di dati reperiti presso qualsiasi fonte diversa dall'interessato, come ad esempio soggetti terzi.
Devono quindi essere raccolti solamente i dati strettamente necessari per adempiere alle finalità espresse nell'informativa (c.d. "principio di minimizzazione").
A tal fine la raccolta del consenso è effettuata in modo da permettere all'interessato di poter esprimere il consenso su alcuni trattamenti e non su altri.

7.2 - Rischi potenziali

L'eccessiva raccolta di dati aumenta i rischi connessi al loro trattamento ed alla loro conservazione aumentando altresì i costi di gestione.

La limitazione dei dati trattati dall'Ente ha quindi anche lo scopo di ridurre i possibili errori e l'impatto che questi possono avere sull'interessato.

Le modalità operative di raccolta si applicano ai dati ottenuti per via cartacea nonché a quelli di origine informatica come, ad esempio, i *cookie* ricavati durante una sessione di navigazione.

7.3 - Azioni intraprese

Il Titolare ha adottato policy di limitazione dei dati trattati che vengono raccolti in conformità con le finalità espresse nell'informativa rilasciata all'interessato.

La *policy* dell'Ente è soggetta a controllo annuale in occasione degli audit svolti dal *Data Protection Officer*.

In alcuni casi l'Ente può utilizzare dati raccolti presso soggetti terzi. Sarà cura, in fase di selezione dei partner, richiedere quali siano le loro policy di gestione dei dati e se rispettino o meno le indicazioni del GDPR.

I partner selezionati ed incaricati quali *Data Processor* (Responsabili esterni al trattamento) potranno essere oggetto di audit da parte del Titolare del trattamento o da personale da esso incaricato.

7.4 - Gestione *cookie*

Sulla base del principio di minimizzazione l'Ente ha ridotto l'utilizzo dei *cookie* al quantitativo minimo necessario allo svolgimento delle proprie attività (Allegato al presente documento sono riportati i cookie utilizzati in un'ordinaria sessione di navigazione).
Il Titolare provvede a fornire agli interessati un'informativa alla prima connessione al sito www.comune.chialamberto.to.it.

Poiché nel sito dell'Ente sono presenti anche *cookie* in grado di raccogliere informazioni sulle attività di navigazione, in occasione della prima connessione è richiesto il consenso all'utente. L'espressione di tale consenso è data dall'accettazione dell'informativa breve proposta come *banner*.

Articolo 8 - Il diritto di limitazione del trattamento

8.1 - Limitazione del trattamento

Al fine di limitare a singoli incaricati o a gruppi ristretti l'accesso a particolari dati o trattamenti, il Titolare ha implementato procedure interne relative all'utilizzo di strumenti tecnologici e loro settaggi nonché alla formazione del personale.
Mediante l'informativa l'interessato è messo a conoscenza del proprio diritto di limitare il trattamento effettuato dall'Ente.
Sono messi a disposizione dell'interessato anche un indirizzo mail ed un numero di telefono al quale rivolgersi per l'esercizio del diritto di limitazione.
Nel caso in cui fosse necessario per l'Ente effettuare trattamenti ulteriori, con finalità o metodi diversi, verrà consegnata all'interessato una nuova informativa e si provvederà alla raccolta di un nuovo consenso.

La procedura di gestione delle richieste di limitazione prevede:

Operazioni svolte dal Titolare del trattamento	**Operazioni svolte dal soggetto autorizzato al trattamento**
Identificazione dell'interessato; Comunicazione all'interessato di aver preso in carico la sua richiesta; Mappatura dei dati dell'interessato trattati all'interno dell'Ente; Identificazione dei soggetti interni all'Ente che possono entrare in contatto con i dati dell'interessato; Decisione su come applicare la limitazione per i dati cartacei e informatici: • Dati cartacei: spostamento della documentazione dell'interessato in un settore diverso da quello dove vengono trattati i dati degli altri interessati OPPURE identificazione delle informazioni associandole all'identificativo dell'incaricato al trattamento; • Dati informatici: Limitazione dell'accesso a determinate cartelle OPPURE ai singoli file mediante *password*; Comunicazione della procedura selezionata a tutti i soggetti deputati ad operare su dati; Comunicazione all'interessato delle procedure messe in atto.	Comunicazione della richiesta al titolare attraverso i canali di comunicazione interni; Messa in atto della procedura individuata dal Titolare per la limitazione dei dati cartacei e informatici.

Articolo 9 - Diritto di opposizione al trattamento

L'Ente adotta procedure interne finalizzate a consentire all'interessato di esercitare il diritto di **opposizione** al trattamento dei dati personali che lo riguardano se:

- il trattamento è 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;
- il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore;
- il trattamento è effettuato per finalità di marketing diretto e/o prevede la profilazione dell'interessato.

Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che possa dimostrare 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.

La procedura di gestione delle richieste di opposizione ~~limitazione~~ prevede:

Titolare del trattamento dati
Identificazione dell'interessato;
Comunicazione all'interessato di aver preso in carico la sua richiesta;
Mappatura dei dati dell'interessato trattati all'interno dell'Ente;
Valutazione della richiesta e verifica dell'eventuale sussistenza di motivi legittimi cogenti che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato, e impongono di procedere comunque al trattamento;
Limitazione del trattamento per tutto il periodo della verifica;
Identificazione i dati che devono essere mantenuti in caso di interesse legittimo prevalente, o per far fronte ad un obbligo legale o per la difesa di un diritto in sede giudiziaria e tempo rimanente per la loro conservazione;
Eliminazione i dati non necessari;
Pianificazione della cancellazione o anonimizzazione dei dati dell'interessato al termine del periodo di conservazione obbligatorio;
Comunicazione all'interessato dell'esito della valutazione e delle procedure messe in atto.

Articolo 10- Comunicazione dei dati

I dati trattati dal Comune di Chialamberto non sono comunicati a soggetti terzi a meno che ciò non sia necessario allo svolgimento dei trattamenti o sia imposto da leggi.

Tali comunicazioni avvengono soltanto tra il Titolare e soggetti che garantiscono la conformità, anche mediante autocertificazione, al Regolamento. Al fine di garantire questa rispondenza, il Titolare nomina tali soggetti Responsabili del trattamento ai sensi dell'articolo 28 comma 1 del GDPR.

Art.28 comma 1

Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.

Le nomine dei responsabili al trattamento avvengono in forma scritta, con sottoscrizione per accettazione da parte del ricevente.

Articolo 11 - Periodo di conservazione

Il Titolare conserva i dati in proprio possesso per il tempo minimo necessario allo svolgimento dei trattamenti previsti salvo differenti obblighi di legge che impongano maggiori tempi di conservazione.
I termini di conservazione dei dati, o i criteri utilizzati per determinare tale periodo, sono riportati sull'informativa fornita agli interessati.
Al termine del periodo di conservazione stabilito, il Titolare provvederà alla distruzione dei dati, sia cartacei che digitali (anche su supporti di memoria) in accordo alle indicazioni della UNI EN 15713:2009.
Il personale incaricato al trattamento è stato informato sulle tempistiche di conservazione.

RISCHI POTENZIALI
Una gestione non corretta di questi diritti può comportare conseguenze legali gravose, e per tale motivo il Titolare ha stabilito una tabella di tempi massimi di conservazione dei dati.
Nella tabella sottostante sono riportati i tipi di dati oggetto del trattamento, la metodologia utilizzata per l'archiviazione degli stessi (Analogica, Digitale o Mista) e le tempistiche massime di conservazione (**data retention**).

(Tab 8)

Tipologia di dato	Metodologia di archiviazione	Tempo massimo di conservazione
Cittadini: • Anagrafica; • Dati di contatto; • Dati economici; • Dati fiscali; • Dati giudiziari; • Convinzioni religiose; • Ideologie politiche; • Dati inerenti la salute; • Immagini.	Mista	10 anni dal termine del trattamento attivo o per differente termine imposto da obblighi di legge. Al termine del periodo indicato i dati saranno conservati presso l'archivio storico per finalità storico-statistiche
Terzi: • Anagrafica; • Dati di contatto; • Dati economici; • Dati fiscali; • Dati giudiziari; • Convinzioni religiose; • Ideologie politiche; • Dati inerenti la salute; • Immagini.	Mista	10 anni dal termine del trattamento attivo o per differente termine imposto da obblighi di legge

Tipologia di dato	Metodologia di archiviazione	Tempo massimo di conservazione
Dipendenti: • Anagrafica; • Dati di contatto; • Dati economici; • Dati fiscali; • Appartenenza sindacale; • Convinzioni religiose; • Dati inerenti la salute; • Opinioni politiche; • Immagini.	Mista	Successivamente all'esaurimento del contratto i dati saranno conservati per un periodo di 10 anni o per un periodo maggiore qualora previsto da disposizioni legislative (ad es. in materia pensionistica). Le cartelle sanitarie saranno conservate per dieci anni qualora non siano stati segnalati dal Medico Competente profili di rischio che richiedono un diverso temine anche maggiore (vedi art. 25 co. 1 lett. e D.lgs 81/08)
Terzi: • Anagrafica; • Dati di contatto; • Dati economici; • Dati fiscali; • Dati giudiziari; • Convinzioni religiose; • Ideologie politiche; • Dati inerenti la salute; • Immagini.	Mista	10 anni dal termine del trattamento attivo o per differente termine imposto da obblighi di legge
Fornitori ed altri professionisti: • Anagrafica; • Dati di contatto; • Dati economici; • Dati fiscali.	Mista	10 anni dal termine del rapporto commerciale o per differente termine imposto da obblighi di legge

Articolo 12 – L'accuratezza dei dati raccolti

L'Ente si impegna a raccogliere e trattare dati accurati, completi ed aggiornati.
Gli interessati devono essere informati circa la necessità di comunicare tempestivamente eventuali variazioni dei dati che li riguardano.
Al fine di mantenere aggiornati i dati in proprio possesso il Comune di Chialamberto provvede, con cadenza periodica o in occasione di contatto con l'interessato, al controllo delle informazioni possedute.

Devono essere verificati per lo meno i seguenti dati:

- Anagrafica interessato;
- Dati di contatto;
- Dati di fatturazione.

Articolo 13 - Procedure e tecnologie di security applicate al trattamento

Al fine di definire le procedure necessarie a regolamentare l'utilizzo di dispositivi tecnologici (*hardware e software*) e analogici all'interno del Comune di Chialamberto, il Titolare si avvale della collaborazione di consulenti esterni incaricati di analizzare gli strumenti informatici utilizzati.

Il Titolare adotta procedure e tecnologie di sicurezza analogiche e digitali appropriate e proporzionali alla criticità dei dati trattati.

Allegato al presente documento vengono riportate le attività di messa in sicurezza adottate dal Comune con l'approvazione del Regolamento comunale

CONTROLLI PERIODICI

Con cadenza almeno annuale vengono riviste le procedure di sicurezza e protezione dei dati personali mediante attività di audit svolta dal *Data Protection Officer*. Al termine delle attività viene rilasciato un verbale di audit che sarà allegato al presente documento.

DIFFUSIONE DELLE PROCEDURE OPERATIVE

Il *Data Protection Team* del Comune di Chialamberto è a conoscenza delle misure messe in atto per proteggere i dati personali in quanto ha programmato un apposito corso di formazione e partecipato ad una riunione formativa.

Articolo 14 - La trasparenza del trattamento

Con l'espressione "trasparenza del trattamento" si intende la possibilità di fornire all'interessato tutte le informazioni richieste sui dati trattati dall'Ente e sui trattamenti attuati, nonché sulle politiche adottate in materia di protezione dei dati personali.

In ottemperanza al "principio di *accountability*" l'Ente rende note le modalità di trattamento adottate, fra cui:

- metodiche di accesso ai dati personali trattati dell'Ente;
- tipologia dei dati trattati dell'Ente;
- metodiche di utilizzo dei dati personali, raccolti in fase di informativa e consenso;
- comunicazione dei dati: verso quali soggetti avviene;
- politiche di acquisizione e trattamento dei dati personali;
- codici etici di riferimento.

Il titolare ha attivato e reso disponibili agli interessati una serie di canali attraverso i quali interagire, richiedere informazioni ed esercitare i propri diritti. Tali canali di contatto sono indicati nell'articolo 2.

I canali di contatto sono resi noti agli interessati mediante un'informativa redatta in maniera semplice e con un linguaggio agevolmente comprensibile da tutti gli utenti.
Le procedure per ottenere informazioni sulle politiche adottate nella protezione dei dati personali sono semplici e dirette.
È possibile per l'interessato contattare l'Ente mediante l'invio di mail ordinaria o mediante contatto telefonico.
Il personale deputato alla ricezione di queste richieste è formato ed è in grado di fornire risposte.
Qualora le richieste fossero particolarmente articolate o complesse la richiesta di informazioni deve essere inoltrata dall'Ente al Responsabile della protezione dei dati (DPO).

Articolo 15 - Gestione sito web

Il Comune di Chialamberto mantiene attiva la propria presenza sul web grazie al sito internet www.comune.chialamberto.to.it.

Gli esiti dell'audit svolto sul sito internet dell'Ente sono parte del *framework privacy*.

Articolo 16 – Valutazione del rischio

Il Titolare del trattamento adotta politiche di valutazione del rischio finalizzate all'individuazione delle modalità di trattamento più sicure e meno invasive.
Gli esiti della valutazione vengono indicati nel documento di Valutazione del Rischio.

Articolo 17 – Gestione del *data breach*

Il Comune di Chialamberto ha provveduto all'implementazione di procedure atte a ridurre al minimo possibile i rischi per le informazioni in proprio possesso.

L'accesso a tutte le macchine è protetto da combinazione USER-Password conosciuta esclusivamente da ogni singolo utente: qualora la macchina venisse resettata da remoto o segnalasse errori verrà avvisato immediatamente il responsabile al trattamento, in modo da ridurre al minimo i tempi di intervento.

Il Titolare del trattamento provvede alla tenuta di un registro digitale o analogico delle violazioni subite nel quale sono riportate anche le misure messe in atto per evitare il ripetersi di tali violazioni.

Nel caso in cui la violazione abbia compromesso categorie particolari di dati personali, il Comune di Chialamberto provvede altresì a darne celermente comunicazione agli interessati mediante canali d'informazione ritenuti più opportuni.

Articolo 18 – Il diritto di accesso dell'interessato

In ottemperanza al dettato del GDPR il Titolare ha messo in atto procedure che consentono agli interessati il pieno e liberto esercizio dei propri diritti relativi al trattamento dei dati personali.

L'interessato può contattare il titolare in maniera semplice ed immediata, senza necessità di particolari formalità mediante i riferimenti di cui all'articolo 2.
Gli Incaricati al trattamento sono stati formati ed informati su come rispondere ai quesiti dell'interessato e, in caso di domande particolarmente complesse, l'Ente trasmette le richieste al DPO.

In caso di domanda di trasferimento di informazioni tra due *data controller* (diritto alla portabilità), il Titolare del trattamento si coordinerà con il ricevente al fine di predisporre l'invio dei dati in maniera sicura, sia per quanto riguarda la trasmissione che per la quantità di dati inviati.

In caso di richiesta di accesso ai dati da parte degli interessati, verranno indicati anche tutti i soggetti terzi ai quali i dati sono stati comunicati.
Gli stessi soggetti terzi verranno informati qualora l'interessato chiedesse di modificare i dati personali trattati dell'Ente.

Articolo 19 – Allegati

La modifica degli allegati non comporterà la necessaria modifica del presente Regolamento e non dovrà essere adottata mediante delibera del Consiglio Comunale.

Articolo 20 – Definizioni

Accountability (o responsabilizzazione): capacità di dimostrare la conformità al GDPR. Il Regolamento stabilisce esplicitamente che questa sia a carico dell'organizzazione. Per dimostrare la conformità è necessario implementare adeguate misure tecniche e organizzative.

Anonimizzazione: modalità di trattamento dei dati personali che non consente l'identificazione di uno specifico interessato.

Categorie particolari di dati personali: sono le categorie di dati che includono l'origine razziale o etnica, le opinioni politiche, le opinioni religiose o filosofiche, l'appartenenza sindacale, l'orientamento sessuale e i dati sanitari, genetici e biometrici elaborati per identificare un individuo in modo univoco.

Consenso: Il consenso è qualsiasi "manifestazione di volontà libera, specifica, informata e inequivocabile" dell'interessato, con la quale lo stesso acconsente, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento per uno o più scopi specifici.

Cookie: Sono file salvati sul computer del visitatore di un sito web da parte di applicazioni presenti nelle pagine del sito stesso con lo scopo di immagazzinare informazioni.

Sono "tecnici" quando salvano informazioni anonime, ma utili, come, per esempio, i prodotti messi nel carrello di un e-commerce o la lingua selezionata quando si visita un sito la prima volta. Sono di "profilazione" quando servono ad esempio a rendere identificabile la persona che sta navigando nel sito o a salvare la cronologia delle azioni fatte e delle pagine viste.

Contitolare del trattamento: quando due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal regolamento 2016/679, con particolare riguardo all'esercizio dei diritti dell'interessato.

Compliance: conformità alle regole e disposizioni del GDPR e alle normative cogenti.

Data breach: violazione di sicurezza nella quale i dati, protetti o riservati, vengono consultati, copiati, trasmessi, rubati, persi, distrutti o utilizzati da un soggetto non autorizzato.

Può essere volontaria o involontaria, a seguito di attacchi informatici, accessi abusivi, incidenti o eventi avversi, come incendi o altre calamità.

Data Processor (Responsabile esterno del trattamento): persona fisica o giuridica esterna all'organizzazione del Titolare che, nello svolgimento delle proprie mansioni, tratta dati che vengono forniti dal Titolare.

Data Protection by Default: principio tramite il quale si configura il trattamento dei dati personali attivando in maniera predefinita livelli di sicurezza tali da ridurre al minimo tecnicamente e organizzativamente possibile i rischi nei quali possono incorrere i dati personali.

Ciò richiede "un'analisi preventiva e un impegno applicativo da parte dei titolari che devono sostanziarsi in una serie di attività specifiche e dimostrabili".

Data Protection by Design: principio tramite il quale si configura il trattamento dei dati personali prevedendo, fin dalle fasi di progettazione, misure indispensabili per soddisfare i requisiti del regolamento e tutelare i diritti degli interessati.

Ciò richiede "un'analisi preventiva e un impegno applicativo da parte dei titolari che devono sostanziarsi in una serie di attività specifiche e dimostrabili".

Dati personali: Qualsiasi informazione relativa a un individuo identificato o identificabile, che riguardi la sua vita privata, professionale o pubblica. Può essere un nome, una foto, un indirizzo di

posta elettronica, i dati bancari, un post su siti di social networking, delle informazioni mediche, un indirizzo IP o una combinazione di dati che ne permettono direttamente o indirettamente l'identificazione.

Delegato interno del trattamento – Soggetto autorizzato al trattamento dati con funzioni di sorveglianza: Persona fisica interna all'organizzazione con il compito di coordinare i soggetti autorizzati al trattamento sulla base delle indicazioni ricevute dal Titolare del trattamento.

Double opt-in: è l'azione di consenso che deve dare l'interessato in due step divisi: prima nel form di richiesta sulla pagina di un blog o sito per accedere ad una determinata offerta, poi nella successiva mail di conferma che gli viene inviata, nella quale deve fornire nuovamente il proprio consenso al trattamento dei dati che ha condiviso con l'azienda.

D.P.O.: Data Protection Officer (di seguito DPO) è una figura introdotta dal GDPR. Il suo compito principale è quello di osservare, valutare e organizzare la gestione del trattamento di dati personali (e dunque la loro protezione) all'interno di un'organizzazione, affinché questi siano trattati nel rispetto delle normative europee e nazionali.

La nomina del DPO è obbligatoria al verificarsi delle seguenti condizioni:

- trattamento effettuato da un'autorità pubblica o da un organismo pubblico, escluse le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;
- le attività principali del Titolare del trattamento o del Responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
- le attività principali del Titolare del trattamento o del Responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali o di dati relativi a condanne penali e a reati.
- Organizzazione con al suo interno un numero di dipendenti superiore a 250.

Incaricato del trattamento: vedi "Soggetto autorizzato al trattamento dati personali";

Informativa: si tratta delle informazioni che devono essere fornite dal Titolare del trattamento ad ogni Interessato, verbalmente o per iscritto sia che i dati vengano raccolti presso l'Interessato stesso, oppure presso terzi. L'informativa deve precisare sinteticamente e in modo colloquiale quali sono gli scopi e le modalità del trattamento; se l'interessato è obbligato o no a fornire i dati; quali sono le conseguenze se i dati non vengono forniti; a chi possono essere comunicati o diffusi i dati; quali sono i diritti riconosciuti all'interessato; chi sono il titolare e l'eventuale responsabile del trattamento e dove sono raggiungibili (indirizzo, telefono, fax, ecc.).

Interessato: persona fisica identificata o identificabile cui si riferiscono i dati personali. Esempi di interessati possono essere un individuo, un cliente, un potenziale cliente, un dipendente, un referente, ecc.

Legittimo interesse: base giuridica secondo la quale il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

Privacy policy: documento presente all'interno di un sito che informa e descrive in modo dettagliato e chiaro come vengono gestiti e trattati i dati personali dei visitatori da parte del titolare.

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

Pseudonimizzazione: modalità di trattamento dei dati personali che riduce la possibilità di attribuirli ad uno specifico interessato se non attraverso l'utilizzo di informazioni aggiuntive.

Rappresentante del trattamento: Persona fisica o giuridica, stabilita nell'Unione Europea che rappresenta l'Organizzazione titolare del trattamento qualora questa abbia sede in un Paese esterno alla UE.

Registro dei trattamenti: documento contenente le informazioni relative alle operazioni di trattamento effettuate all'interno di un'organizzazione. In esso vengono indicate le finalità del trattamento, ma anche informazioni quali le modalità di conservazione, le categorie degli Interessati e dei dati personali, gli eventuali trasferimenti verso paesi terzi, eventuali misure di sicurezza applicate, etc.

Soggetto autorizzato al trattamento dati con funzioni di sorveglianza: vedi "Delegato interno del trattamento";

Soggetto autorizzato al trattamento dati personali: persona fisica che opera all'interno dell'organizzazione del Titolare che, per lo svolgimento delle proprie mansioni, tratta i dati raccolti dall'organizzazione.

Terzo: qualsiasi persona fisica o giuridica, autorità pubblica, agenzia o altro organismo diverso dall'Interessato, dal Titolare, dal Responsabile, dall'Incaricato e dal Responsabile esterno al trattamento.

Titolare del trattamento (o data controller): 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.

Trasferimento: Comunicazione digitale o invio fisico di materiale contenente dati personali dell'interessato.

Valutazione d'impatto (DPIA, *Data Protection Impact Assesment*): procedura di analisi per la valutazione dei rischi connessi al trattamento di dati, con lo scopo di identificare le misure idonee per affrontarli. Si tratta di un procedimento obbligatorio per tutti quei trattamenti che presentano rischi elevati per i diritti e le libertà delle persone fisiche.