COMUNE DI GREVE IN CHIANTI
Città Metropolitana di Firenze

Comune di
Greve in Chianti

Regolamento
sulla protezione
dei dati personali
adottato in attuazione del Regolamento (UE) 2016/679

Approvato con deliberazione Consiglio Comunale n. 4 in data 18/01/2021

SOMMARIO

DISPOSIZIONI GENERALI....4
Art. 1 Definizioni....4
Art. 2 Quadro normativo di riferimento....4
Art. 3 Oggetto....5
Art. 4 Finalità....5
CAPO II PRINCIPI 6
Art. 5 Principi e responsabilizzazione....6
Art. 6 Liceità del trattamento 6
Art. 7 Condizioni per il consenso....7
Art. 8 Informativa....8
Art. 9 Sensibilizzazione e formazione....10
CAPO III - IL TRATTAMENTO DEI DATI PERSONALI....10
Art. 10 Trattamento dei dati personali, ricognizione dei trattamenti e indice dei trattamenti....10
Art.11 Tipologie di dati trattati....11
Art. 12 Trattamento dei dati sensibili e giudiziari....11
Art.13 Trattamento dei dati sensibili relativi alla salute....11
Art. 14 Trattamento dei dati del personale 11
Art. 15 Registro delle attività di trattamento e delle categorie di trattamento....12
CAPO IV - DIRITTI DEGLI INTERESSATI....12
Art. 16 Pubblicità e diffusione di dati personali contenuti in atti e provvedimenti amministrativi 12
Art. 17 Diritti dell'interessato....13
Art. 18 Diritto di accesso....13
Art. 19 Diritto alla rettifica e cancellazione....14
Art. 20 Diritto alla limitazione....15
Art. 21 Diritto alla portabilità....16
Art. 22 Diritto di opposizione e processo decisionale automatizzato relativo alle persone 16
Art. 23 Modalità di esercizio dei diritti dell'interessato....16
Art. 24 Indagini difensive....18
CAPO V - SOGGETTI....19
Art. 25 Titolare e contitolari....19
Art. 26 Responsabili del trattamento e sub responsabili....20
Art. 27 Incaricati del trattamento dipendenti del titolare....20
Art. 28 Incaricati del trattamento non dipendenti del titolare....21
Art. 29 Amministratore di sistema....21
Art. 30 Responsabile della protezione dei dati personali (RPD) 21
CAPO VI - SICUREZZA DEI DATI PERSONALI....23

Art. 31 Misure di sicurezza.....23
Art. 32 Valutazione d'impatto sulla protezione dei dati- DPIA 23
Art. 33 Consultazione preventiva.....24
Art. 34 Modulistica e procedure.....25
Art. 35 Notificazione di una violazione dei dati personali.....25
Art. 36 Comunicazione di una violazione dei dati personali.....26
Art. 37 Disposizioni finali.....26

CAPO I - DISPOSIZIONI GENERALI

Art. 1 Definizioni

Il presente regolamento di avvale delle seguenti definizioni:

- **Codice**: D.Lgs. n. 196/2003, come modificato dal D.Lgs 101/2018;
- **GDPR:** il 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 (GDPR generale sulla protezione dei dati);
- **Regolamento:** il presente Regolamento;
- **Titolare:** il Comune o l'Amministrazione che adotta il presente regolamento, Comune di Greve in Chianti, con sede in Piazza Matteotti 8, Greve in Chianti (FI)
- **Responsabili del trattamento**: i soggetti che esercitano i poteri delegati dal titolare o che sono nominati dal titolare per esercitare tali poteri.
- **Incaricati del trattamento:** i soggetti designati da ciascun Responsabile incaricati di svolgere le operazioni di trattamento dei dati personali di competenza con l'indicazione specifica dei compiti, dell'ambito di trattamento consentito e delle modalità.
- **Dati sensibili**: tutte le categorie particolari di dati indicati dall'art 9 del GDPR

Il presente regolamento recepisce le definizioni del D.Lgs. n. 196/2003 come modificato dal D. Lgs. 101/2018 e del GDPR, fermo restando che, in caso di discordanza, prevalgono le definizioni contenute nei rispettivi testi normativi

Art. 2 Quadro normativo di riferimento

Il presente Regolamento tiene conto dei seguenti documenti:

- Codice in materia di dati personali recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016 (D.Lgs. n.196/2003, come modificato dal D.Lgs 101/2018);
- Linee guida e raccomandazioni del Garante;
- GDPR UE 679/2016 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;
- Legge 25 ottobre 2017, n. 163 (art.13), recante la delega per l'adeguamento della normativa nazionale alle disposizioni del GDPR (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;
- D.Lgs. n. 101/2018 di adeguamento della normativa interna al GDPR;
- Dichiarazioni del gruppo di lavoro articolo 29 sulla protezione dei dati (WP29) - 14/EN;
- Linee-guida sui responsabili della protezione dei dati (RPD) - WP243 Adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
- Linee-guida sul diritto alla portabilità dei dati - WP242 Adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
- Linee-guida per l'individuazione dell'autorità di controllo capofila in rapporto a uno

specifico Titolare o Responsabile del trattamento - WP244 adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;

- Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento possa presentare un rischio elevato ai sensi del regolamento 2016/679 - WP248 adottate dal Gruppo di lavoro Art. 29 il 4 aprile 2017;
- Linee guida elaborate dal Gruppo Art. 29 in materia di applicazione e definizione delle sanzioni amministrative - WP253 adottate dal Gruppo di lavoro Art. 29 il 3 ottobre 2017;
- Linee guida elaborate dal Gruppo Art. 29 in materia di processi decisionali automatizzati e prolazione - WP251 Adottate dal Gruppo di lavoro Art. 29 il 6 febbraio 2018;
- Linee guida elaborate dal Gruppo Art. 29 in materia di notifica delle violazioni di dati personali (*data breach notification*) - WP250 Adottate dal Gruppo di lavoro Art. 29 il 6 febbraio 2018;
- Parere del WP29 sulla limitazione della finalità - 13/EN WP 203;
- Allegato 1 al provvedimento n. 467 del 11 ottobre 2018 *Elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione di impatto*;
- Norme internazionali;
- Regolamenti interni, approvati dai titolari e/o dai responsabili.

Art. 3 Oggetto

Il presente Regolamento ha per oggetto la protezione dei diritti e delle libertà delle persone fisiche in ordine al trattamento dei dati personali effettuato dal titolare, nel rispetto di quanto previsto dal GDPR.

Il presente Regolamento sostituisce integralmente il Regolamento sui dati sensibili, approvato con deliberazione C.C. n. 125 in data 21.12.2005, ferme restando le operazioni eseguibili in riferimento alle specifiche finalità di rilevante interesse pubblico perseguite nei singoli casi ed espressamente elencate dalla legge.

Art. 4 Finalità

Il titolare garantisce che il trattamento dei dati che gestisce nell'esercizio delle sue funzioni, a tutela delle persone fisiche, si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali, a prescindere dalla loro nazionalità o della loro residenza.

Il titolare, nell'ambito delle sue funzioni, gestisce gli archivi e le banche dati rispettando i diritti, le libertà fondamentali e la dignità delle persone, con particolare riferimento alla riservatezza e all'identità personale.

Ai fini della tutela dei diritti e delle libertà delle persone fisiche in ordine al trattamento dei dati personali, tutti i processi, inclusi i procedimenti amministrativi di competenza del titolare, vanno gestiti conformemente alle disposizioni del Codice, del GDPR, e del presente Regolamento.

CAPO II - PRINCIPI

Art. 5 Principi e responsabilizzazione

Vengono integralmente recepiti, nell'ordinamento interno del titolare, i principi del GDPR, per effetto dei quali dati personali sono:

- trattati in modo lecito, corretto e trasparente nei confronti dell'interessato (liceità, correttezza e trasparenza);
- 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 considerato incompatibile con le finalità iniziali (limitazione della finalità);
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati in base del principio di minimizzazione dei dati;
- 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 in base del principio di esattezza
- 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, GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato in base al principio di limitazione della conservazione;
- 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 in base ai principi di integrità e riservatezza;
- configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità possano essere perseguite mediante dati anonimi o con l'uso di opportune modalità che permettono di identificare l'interessato solo un caso di necessità *(principio di necessità*).

Il titolare è competente per il rispetto dei principi sopra declinati, ed è in grado di comprovarlo in base al principio di responsabilizzazione.

Art. 6 Liceità del trattamento

Vengono integralmente recepiti, nell'ordinamento interno del titolare, le disposizioni del GDPR in ordine alla liceità del trattamento e, per l'effetto, il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

- l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità ;
- il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;

- il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il Titolare del trattamento;
- il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
- 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.

L'ultimo punto non si applica al trattamento di dati effettuato dal titolare nell'esecuzione dei propri compiti e funzioni.

Laddove il trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti non sia basato sul consenso dell'interessato o su un atto legislativo dell'Unione o degli Stati membri che costituisca una misura necessaria e proporzionata per la salvaguardia degli obiettivi di cui all'articolo 23, paragrafo 1 GDPR, al fine di verificare se il trattamento per un'altra finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il Titolare tiene conto, tra l'altro:

1. di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto;
2. del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il Titolare del trattamento;
3. della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'art. 9 del GDPR, oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell'articolo 10 del medesimo GDPR;
4. delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati;
5. dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione.

Art. 7 Condizioni per il consenso

Fermi restando i casi, disciplinati dall'art. 6 del GDPR e dagli artt. 2-ter e 2-sexies del Codice, nei quali può essere legittimamente effettuato il trattamento senza consenso, nei casi in cui il trattamento dei dati personali, per una o più specifiche finalità, è subordinato al consenso dell'interessato, si applica la disciplina del GDPR la quale prevede che:

- 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;
- 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;
- 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;

- 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.
- per i dati sensibili il consenso deve essere esplicito e in forma scritta; lo stesso dicasi per il consenso a decisioni basate su trattamenti automatizzati, compresa la profilazione;
- il consenso dei minori è valido a partire dai 16 anni, fermo restando il diverso limite di età, comunque non inferiore a 13 anni, previsto dalla normativa nazionale; prima del limite di età previsto dalla normativa nazionale occorre raccogliere il consenso dei genitori o di chi ne fa le veci;
- deve essere, in tutti i casi, libero e autonomo, specifico, informato e inequivocabile e non è ammesso il consenso tacito o presunto (no a caselle prespuntate su un modulo);
- deve essere manifestato attraverso dichiarazione o azione positiva inequivocabile.

Se il consenso dell'interessato al trattamento dei propri dati personali 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 GDPR e del presente Regolamento, è vincolante.

In caso di impossibilità fisica, incapacità di agire o incapacità di intendere e di volere dell'interessato, emergenza sanitaria o di igiene pubblica, rischio grave e imminente per la salute dell'interessato, il consenso può intervenire senza ritardo, anche successivamente alla prestazione, da parte di chi esercita legalmente la potestà , ovvero da un prossimo congiunto, da un familiare, da un convivente.

Qualora il trattamento sia basato sul consenso, il consenso deve essere reso, da parte dell'interessato, attraverso la compilazione di apposita modulistica, predisposta dal titolare, previa consegna e presa d'atto dell'informativa.

Il titolare adotta misure organizzative adeguate a facilitare l'espressione del consenso da parte dell'interessato.

La manifestazione del consenso, ad opera dell'interessato, va resa al momento del primo accesso alle prestazioni, ed è valido ed efficace fino alla revoca della stessa o, per i minorenni, fino al compimento del diciottesimo anno di età .

Art. 8 Informativa

Il titolare, al momento della raccolta dei dati personali, è tenuto a fornire all'interessato, anche avvalendosi del personale incaricato, apposita informativa secondo le modalità previste dal GDPR, in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori.

L'informativa è data, in linea di principio, per iscritto e preferibilmente in formato elettronico, soprattutto nel contesto di servizi online, anche se sono ammessi altri mezzi, potendo essere fornita anche oralmente, ma nel rispetto delle caratteristiche di cui sopra.

L'informativa è fornita, mediante idonei strumenti:

- attraverso appositi moduli da consegnare agli interessati. Nel modulo sono indicati i soggetti a cui l'utente può rivolgersi per ottenere maggiori informazioni ed esercitare i

propri diritti, anche al fine di consultare l'elenco aggiornato dei responsabili;

- avvisi agevolmente visibili dal pubblico, posti nei locali di accesso delle strutture del titolare, nelle sale d'attesa e in altri locali in cui ha accesso l'utenza o diffusi nell'ambito di pubblicazioni istituzionali e mediante il sito internet del titolare;
- apposita avvertenza inserita nei contratti ovvero nelle lettere di affidamento di incarichi del personale dipendente, dei soggetti con i quali vengono instaurati rapporti di collaborazione o libero-professionali, dei tirocinanti, dei volontari, degli stagisti ed altri soggetti che entrano in rapporto con il titolare.;
- resa in sede di pubblicazione dei bandi, avvisi, lettere d'invito, con l'indicazione dell'incaricato del trattamento dei dati relativi alle procedure.

L'informativa contiene il seguente contenuto minimo:

- l'identità e dati di contatto del titolare e, ove presente, del suo rappresentante;
- i dati di contatto del RPD;
- le finalità del trattamento;
- i destinatari dei dati;
- la base giuridica del trattamento;
- l' interesse legittimo del titolare se quest'ultimo costituisce la base giuridica del trattamento;
- se il titolare trasferisce i dati personali in Paesi terzi e, in caso affermativo, attraverso quali strumenti;
- il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione;
- il diritto dell'interessato di chiedere al titolare l'accesso, la rettifica, la cancellazione dei dati, la limitazione del trattamento che lo riguarda, il diritto di opporsi al trattamento e il diritto alla portabilità dei dati;
- il diritto di presentare un reclamo all'autorità di controllo;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione, e le informazioni significative sulla logica utilizzata nonché l'importanza e le conseguenze di tale trattamento per l'interessato.

Nel caso di dati personali non raccolti direttamente presso l'interessato (diritto all'informazione):
a) il titolare deve informare l'interessato in merito a:

- le categorie di dati personali trattati;
- la fonte da cui hanno origine i dati personali e l'eventualità che i dati provengano da fonti accessibili al pubblico.

b) l'informativa deve essere fornita entro un termine ragionevole che non può superare 1 mese dalla raccolta, oppure dal momento della comunicazione (e non della registrazione) dei dati a terzi o all'interessato.
Apposite informative devono essere inserite nei bandi e nella documentazione di affidamento dei contratti pubblici, nei contratti, accordi o convenzioni, nei bandi di concorso pubblico, nelle segnalazioni di disservizio e, più in generale, in ogni altro documento contenente dati personali.
Nel fornire l'informativa, il titolare fa espresso riferimento alla normativa che prevede gli obblighi o i compiti in base alla quale e' effettuato il trattamento dei dati sensibili e giudiziari.

L'Ente ha predisposto una Informativa generale, nel rispetto di quanto previsto dagli artt. 13 e 14 del Regolamento UE 679/2016, relativa alle informazioni da fornire all'interessato in merito al trattamento dei propri dati personali.
Nell'informativa sono indicati:
- l'identità e i dati di contatto del Titolare del trattamento;
- i dati di contatto del responsabile della protezione dei dati;
- le finalità del trattamento e la sua base giuridica;
- le modalità di comunicazione e gestione dei dati
- i diritti dell'interessato.
Tale informativa è stata pubblicata sul sito web del Comune nell'apposita sezione Privacy

Art. 9 Sensibilizzazione e formazione
Ai fini della corretta e puntuale applicazione della disciplina relativa ai principi, alla liceità del trattamento, al consenso, all'informativa e, più in generale, alla protezione dei dati personali, il titolare sostiene e promuove, all'interno della propria struttura organizzativa, ogni strumento di sensibilizzazione che possa consolidare la consapevolezza del valore della riservatezza dei dati, e migliorare la qualità del servizio.
A tale riguardo, il presente regolamento riconosce che uno degli strumenti essenziali di sensibilizzazione è l'attività formativa del personale del titolare e l'attività informativa diretta a tutti coloro che hanno rapporti con il titolare.

CAPO III - IL TRATTAMENTO DEI DATI PERSONALI

Art. 10 Trattamento dei dati personali, ricognizione dei trattamenti e indice dei trattamenti
Il titolare tratta i dati personali per lo svolgimento delle proprie finalità istituzionali, come identificate da disposizioni di legge, statutarie e regolamentari, e nei limiti imposti dal Codice, dal GDPR e dalle Linee guida e dai provvedimenti del Garante.
Il titolare effettua i trattamenti di dati personali, previsti da disposizioni legislative e regolamentari.
Il trattamento dei dati personali è esercitabile, all'interno della struttura organizzativa del titolare, solo da parte dei soggetti appositamente autorizzati:

- titolare
- Responsabili di Settore nominati Responsabili del Trattamento, in qualità di soggetti che esercitano i poteri delegati dal titolare o in qualità di soggetti nominati dal titolare per l'esercizio di tali poteri
- dipendenti, in qualità di incaricati del trattamento.

Non è consentito il trattamento da parte di persone non autorizzate.
Ai fini del trattamento, il titolare provvede, in collaborazione con i Responsabili di Settore nominati Responsabili del Trattamento, alla integrale ricognizione e all'aggiornamento di tutti i trattamenti di dati personali effettuati nell'ambito dei processi e procedimenti del titolare medesimo, funzionali alla formazione dell'indice dei trattamenti.
E' compito delle posizione organizzative, Responsabili del Trattamento, effettuare e documentare l'aggiornamento periodico, almeno annuale, della ricognizione dei trattamenti e del relativo indice, e la valutazione periodica, almeno annuale, del rispetto dei principi di cui all'art. 5 del presente Regolamento con riferimento a tutti i trattamenti.
Il titolare, le posizioni organizzative Responsabili del Trattamento e gli incaricati si attengono alle

modalità di trattamento indicate nel Codice, nel GDPR, nonché nelle disposizioni attuative e nelle Linee guida del Garante per la protezione dei dati personali, in particolare con riferimento all'Allegato 1 al provvedimento n. 467 del 11 ottobre 2018 Elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione di impatto.

Art.11 Tipologie di dati trattati

Nell'ambito dei trattamenti inclusi nell'indice dei trattamenti, il titolare, nell'esercizio delle sue funzioni istituzionali, tratta in modo anche automatizzato, totalmente o parzialmente, le seguenti tipologie di dati:

- dati comuni identificativi
- categorie particolari di dati personali di cui all'art 9 del GDPR

Art. 12 Trattamento dei dati sensibili e giudiziari

Il titolare conforma il trattamento dei dati sensibili e giudiziari secondo modalità volte a prevenire la violazione dei diritti, delle libertà fondamentali e della dignità dell'interessato.

A tale fine, il titolare applica i principi degli articoli 9 paragrafo 1 del GDPR e l'art. 2-sexies del Codice e si conforma alle Linee Guida del Garante in materia.

Il titolare sensibilizza, forma e aggiorna i dipendenti in ordine al trattamento dei dati sensibili e giudiziari.

Art.13 Trattamento dei dati sensibili relativi alla salute

Il Titolare si conforma all'art. 2-septies del Codice nonché alle Linee Guida del Garante in materia di trattamento dei dati personali sensibili relativi allo stato di salute.

I dati idonei a rivelare lo stato di salute e la vita sessuale sono trattati da soggetti adeguatamente formati e sono conservati separatamente da ogni altro dato personale trattato per finalità che non richiedono il loro utilizzo.

Art. 14 Trattamento dei dati del personale

Il titolare tratta i dati, anche di natura sensibile o giudiziaria, dei propri dipendenti per le finalità, considerate di rilevante interesse pubblico, di instaurazione e di gestione di rapporti di lavoro di qualunque tipo.

Secondo la normativa vigente, il titolare adotta le massime cautele nel trattamento di informazioni personali del proprio personale dipendente che siano idonee a rivelare lo stato di salute, le abitudini sessuali, le convinzioni politiche, sindacali, religiose filosofiche o d'altro genere e l'origine razziale ed etnica.

Il trattamento dei dati sensibili del dipendente, da parte del datore di lavoro, deve avvenire secondo i principi di necessità e di indispensabilità che impongono di ridurre al minimo l'utilizzo dei dati personali, e quando non si possa prescindere dall'utilizzo dei dati giudiziari e sensibili, di trattare solo le informazioni che si rivelino indispensabili per la gestione del rapporto di lavoro.

Il titolare, nel trattamento dei dati sensibili relativi alla salute dei propri dipendenti, deve rispettare i principi di necessità e indispensabilità.

Il titolare si conforma alle Linee Guida del Garante in materia di trattamento dei dati personali dei lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico.

Art. 15 Registro delle attività di trattamento e delle categorie di trattamento

Il titolare del trattamento istituisce un registro, in forma scritta, delle attività di trattamento e delle categorie di trattamenti svolte sotto la propria responsabilità. Il registro del titolare e dei responsabili del trattamento è unico.

Il registro digitale, in formato excel, è conservato su apposito spazio di rete, accessibile soltanto ai soggetti nominati responsabili del trattamento e al titolare, e le azioni di modifica/aggiornamento sono annotate sul registro denominato Accountability.

Il registro deve essere continuamente aggiornato dai Responsabili del Trattamento, e messo a disposizione delle autorità di controllo.

Tale registro contiene le seguenti informazioni:

- il nome e i dati di contatto del Titolare del trattamento, del Responsabile per la protezione dei dati, dei responsabili del trattamento e degli incaricati;
- le finalità del trattamento;
- una descrizione delle categorie di interessati e delle categorie dei dati personali;
- le categorie dei trattamenti effettuati per conto del titolare del trattamento;
- la categorie di destinatari, a cui i dati personali sono o saranno comunicati;
- un'eventuale possibilità di trasferimenti di dati all'estero, 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 GDPR la documentazione delle garanzie adeguate;
- una descrizione generale delle misure di sicurezza, generiche e specifiche, così come disciplinate dalla normativa vigente in tema di sicurezza dei dati personali e delle misure tecniche e organizzative di cui all'art 32 paragrafo 1 GDPR
- indicazione dei termini ultimi previsti per la cancellazione delle diverse categorie di dati trattati.

CAPO IV - DIRITTI DEGLI INTERESSATI

Art. 16 Pubblicità e diffusione di dati personali contenuti in atti e provvedimenti amministrativi

Il Titolare, in sede di pubblicazione e diffusione, tramite l'albo pretorio informatico e la rete civica, di dati personali contenuti in atti e provvedimenti amministrativi, assicura, mediante l'implementazione delle necessarie misure tecniche ed organizzative, il rispetto dei seguenti principi:

- sicurezza
- completezza
- esattezza
- accessibilità
- legittimità e conformità ai principi di pertinenza, non eccedenza, temporaneità ed indispensabilità rispetto alle finalità perseguite.

Salva diversa disposizione di legge, il titolare garantisce la riservatezza dei dati in sede di pubblicazione all'Albo on line o sulla rete civica, mediante la non identificabilità dei soggetti cui tali dati si riferiscono, adottando gli opportuni accorgimenti in sede di predisposizione degli atti stessi e dei relativi allegati. A tal fine, il titolare adotta e implementa adeguate misure organizzative,

di gestione documentale e di formazione.
Il titolare si conforma alle Linee guida del Garante in materia di pubblicazione e diffusione di dati personali contenuti in atti e provvedimenti amministrativi.

Art. 17 Diritti dell'interessato

Il titolare attua e implementa le misure organizzative, gestionali, procedurali e documentali necessarie a facilitare l'esercizio dei diritti dell'interessato, di seguito elencati, in conformità alla disciplina contenuta nel GDPR e nel Codice:

– diritto di accesso
– diritto alla rettifica e cancellazione
– diritto alla limitazione e obbligo di notifica di cui all'art 19 del GDPR
– diritto alla portabilità
– diritto di opposizione e processo decisionale automatizzato relativo alle persone

Durante l'espletamento delle attività che prevedono il trattamento dei dati personali da parte del Titolare, l'Interessato può chiedere informazioni circa le modalità di trattamento e l'esercizio dei propri diritti dell'interessato, anche in forma scritta al titolare e ai Responsabili del Trattamento

Art. 18 Diritto di accesso

Il presente Regolamento tiene conto della disciplina del GDPR in tema di diritto di accesso secondo la quale 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:

- le finalità del trattamento;
- le categorie di dati personali in questione;
- 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;
- quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- 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;
- il diritto di proporre reclamo a un'autorità di controllo;
- qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4 GDPR, 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.
Il diritto di ottenere una copia non deve ledere i diritti e le libertà altrui.
L'esercizio del diritto di accesso ai dati personali di cui al presente articolo non riguarda i seguenti casi:
– dati personali sottoposti a contitolarità per i quali l'Ente non ha competenza;

– dati personali di qualsiasi tipologia non più disponibili presso l'Ente a seguito di:

- cessazione dei termini di custodia/archiviazione;
- cessazione di utilità ai fini dei trattamenti in essere;
- anonimizzazione dei riferimenti direttamente o indirettamente volti a rilevare l'identità dell'interessato;

– dati personali per i quali non è esercitabile il diritto di accesso, in base a specifiche norme di legge (es. dati riconducibili ai rapporti tra l'Ente e le Autorità Giudiziarie o di Polizia).

Art. 19 Diritto alla rettifica e cancellazione

Il presente Regolamento tiene conto della disciplina del GDPR in tema di diritto di rettifica e cancellazione (diritto all'oblio), di seguito indicata.

Quanto al diritto di rettifica, 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.

Il titolare comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato.

Quanto al diritto all'oblio, consistente nel diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo, lo stesso non si applica nella misura in cui il trattamento sia necessario:

- per l'esercizio del diritto alla libertà di espressione e di informazione;
- 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;
- 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 GDPR;
- a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1 GDPR, nella misura in cui il diritto all'oblio rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento;
- per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

L'esercizio del diritto alla cancellazione ai dati personali di cui al presente articolo non riguarda i seguenti casi:

– dati personali sottoposti a contitolarità per i quali l'Ente non ha competenza;

– dati personali di qualsiasi tipologia non più disponibili presso l'Ente a seguito di:

- cessazione dei termini di custodia/archiviazione;
- cessazione di utilità ai fini dei trattamenti in essere;
- anonimizzazione dei riferimenti direttamente o indirettamente volti a rilevare l'identità dell'interessato;

– dati personali per i quali non è esercitabile il diritto di accesso, in base a specifiche norme di legge (es. dati riconducibili ai rapporti tra l'Ente e le Autorità Giudiziarie o di Polizia).

L’esercizio del diritto di rettifica/integrazione di dati personali di cui al presente articolo non riguarda i seguenti casi:

- Dati anagrafici identificativi e di recapito acquisiti da fonti autoritative (es. anagrafe tributaria SOGEI);
- Dati della banca dati dell'anagrafe, di stato civile ed elettorale, per le quali si rinvia alla normativa in materia vigente
- Dati personali non più disponibili presso l'Ente a seguito di:

- cessazione dei termini di custodia/archiviazione;
- cessazione di utilità ai fini dei trattamenti in essere;
- anonimizzazione dei riferimenti direttamente o indirettamente volti a rilevare l’identità dell’interessato.

Art. 20 Diritto alla limitazione

Il presente Regolamento tiene conto della disciplina del GDPR in tema di diritto alla limitazione, e di seguito indicata.

L'interessato ha il diritto di ottenere dal titolare la limitazione del trattamento quando ricorre una delle seguenti condizioni:

- l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare per verificare l'esattezza di tali dati personali;
- il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;
- benchè 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;
- l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1 GDPR, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del Titolare del trattamento rispetto a quelli dell'interessato.

Se il trattamento è limitato a norma del paragrafo 1 dell'art. 18 GDPR, 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.

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

Il titolare del trattamento comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali limitazioni del trattamento 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.

Art. 21 Diritto alla portabilità

Il presente Regolamento tiene conto della circostanza che, in forza della disciplina del GDPR, il diritto alla portabilità dei dati 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. L'Interessato, nell'esercizio di tale diritto chiede al Titolare di ricevere i dati personali

che sta trattando in un formato strutturato, di uso comune e leggibile da dispositivo automatico, oppure di trasmetterli, in tutto o in parte direttamente ad altro titolare del trattamento.

Art. 22 Diritto di opposizione e processo decisionale automatizzato relativo alle persone

L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f) del GDPR, 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. Il diritto di cui ai paragrafi 1 e 2 dell'art. 21 GDPR 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.

Art. 23 Procedura per la gestione delle richieste di esercizio dei diritti dell'interessato

Per l'esercizio dei diritti dell'interessato, in ordine all'accesso ed al trattamento dei suoi dati personali, si applicano le disposizioni del GDPR, del Codice e del presente Regolamento.
Il titolare si conforma alle Linee guida del Garante in tema di esercizio dei diritti dell'interessato.
E' definita la presente procedura per le richieste formali per assicurare il rispetto dei seguenti parametri qualitativi:

• Acquisizione delle richieste in data certa;
• Identificazione dell'Interessato richiedente;
• Tracciamento dei tempi di risposta da parte dell'Ente;
• Verifica del destinatario della documentazione prodotta in adempimento alle richieste.

L'interessato utilizzando il modello reso disponibile sul sito del comune può inviare le richieste formali di esercizio dei propri diritti oppure segnalazione di presunte inottemperanze o violazioni tramite i canali di comunicazione cartacea ovvero elettronica descritti nel seguito:

a) richieste formali di esercizio dei diritti da parte dell'Interessato, indirizzate al Comune di Greve in Chianti, in qualità di Titolare del trattamento, da trasmettere a mezzo pec all'indirizzo comune.greve-inchianti@postacert.toscana.it o per posta ordinaria al Comune di Greve in Chianti piazza Matteotti 8, Greve in Chianti;

b) segnalazioni formali, in caso di presunta violazione dei dati o di immotivata ottemperanza alle richieste di esercizio dei diritti, da inviare tramite pec al Responsabile della Protezione dei Dati all'indirizzo *dpo@comune.greve-in-chianti.fi.it*, e per conoscenza al Titolare del Trattamento.

La richiesta per l'esercizio dei diritti può essere fatta pervenire:

- direttamente dall'interessato, anche facendosi assistere da una persona di fiducia, con l'esibizione di un documento personale di riconoscimento o allegandone copia o anche con altre adeguate modalità o in presenza di circostanze atte a dimostrare l'identità personale dell'interessato stesso, come ad esempio, la conoscenza personale;
- tramite altra persona fisica o associazione, a cui abbia conferito per iscritto delega o procura; in tal caso, la persona che agisce su incarico dell'interessato deve consegnare copia della procura o della delega, nonché copia fotostatica non autenticata di un documento di riconoscimento del sottoscrittore;

- tramite chi esercita la potestà o la tutela, per i minori e gli incapaci;
- in caso di persone decedute, da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione;
- dalla persona fisica legittimata in base ai relativi statuti od ordinamenti, se l'interessato è una persona giuridica, un ente o un'associazione.

La richiesta, per l'esercizio dei diritti di accesso ai dati personali, può essere esercitata dall'interessato solo in riferimento alle informazioni che lo riguardano e non ai dati personali relativi ai terzi, eventualmente presenti all'interno dei documenti che lo riguardano.
Di seguito sono elencati i compiti dei vari attori che agiscono nella procedura, nel rispetto di quanto previsto dal GDPR.

Il Segretario Generale:

- riceve ed identifica univocamente la richiesta di esercizio dei diritti, verifica la completezza della richiesta e la presenza di idoneo documento identificativo dell'Interessato;
- valuta in maniera preliminare la congruità e la ricusabilità della richiesta, eventualmente chiedendo il parere di competenza al Responsabile Protezione Dati;
- nel caso la richiesta di esercizio sia da ritenersi "ricusabile", fornisce tempestiva comunicazione all'Interessato ai riferimenti indicati nella richiesta;
- nel caso in cui la richiesta di esercizio sia da ritenersi "non ricusabile", smista la richiesta al Responsabile di Settore competente, in qualità di Responsabile "interno" del trattamento, per ottemperare a quanto richiesto dall'Interessato indicando i tempi massimi di risposta;
- riceve la comunicazione di adempimento da parte del Responsabile interno nei termini previsti;
- comunica all'Interessato le informazioni relative alla richiesta entro 30 giorni dal ricevimento della richiesta stessa;
- comunica all'Interessato le motivazioni dell'eventuale inottemperanza, nel caso il Responsabile interno segnalasse l'impossibilità ad adempiere alla richiesta;
- comunica al Titolare e al Responsabile Protezione Dati ogni eventuale criticità rilevata nello svolgimento delle attività, segnalando eventuali violazioni dei dati riscontrate, per consentire il rapido espletamento degli obblighi di comunicazione al Garante per la tutela dei dati personali.

Il Responsabile della Protezione Dati:

- riceve ed identifica univocamente le segnalazioni formali di presunta violazione dei dati o di immotivata ottemperanza alle richieste di esercizio dei diritti;
- effettua l'istruttoria e la verifica di sussistenza delle segnalazioni e predispone il riscontro all'Interessato e al Titolare del trattamento;
- nel caso vengano riscontrate delle non conformità nel trattamento o una immotivata inottemperanza delle richieste di esercizio dei diritti, comunica al Titolare del trattamento le azioni correttive/migliorative da adottare (e la relativa tempistica) per assicurare la tutela de diritti dell'Interessato;
- nel caso venga riscontrata una violazione dei dati, predispone le azioni individuate nella procedura "Data Breach" nella tempistica prevista dal GDPR;
- esprime parere di competenza sulla "ricusabilità" delle richieste di esercizio dei diritti dell'Interessato;

- fornisce consulenza ai Responsabili "interni" per le attività necessarie ad adempiere alle richieste di esercizio dei diritti;
- coopera con il Segretario Generale per la revisione, adeguamento, miglioramento dei processi e delle attività afferenti alla tutela dei diritti dell'Interessato.

Il Responsabile del trattamento:

- riceve le richieste di esercizio dei diritti, pervenute dal Segretario Generale e ritenute "non ricusabili";
- analizza le richieste e mette in atto tutte le azioni necessarie a ottemperare alle stesse nelle tempistiche indicate dal Segretario Generale e comunque non oltre 30 gg;
- nel caso nell'esecuzione delle attività richieste riscontrasse la necessità di supporto circa le indicazioni del GDPR, inoltra richiesta di consulenza al Responsabile Protezione Dati;
- nel caso in cui riscontri l'impossibilità oggettiva ad ottemperare alla richiesta o la necessità di tempi di risoluzione maggiori, comunica le motivazioni e le eventuali tempistiche al Segretario Generale che provvederà ad informare l'Interessato;
- segnala al Titolare e al Responsabile Protezione Dati ogni eventuale criticità rilevata nello svolgimento delle attività, segnalando eventuali violazioni dei dati riscontrate, per consentire il rapido espletamento degli obblighi di comunicazione al Garante per la tutela dei dati personali.

Il termine per ottemperare alla richiesta dell'Interessato è di 30 giorni e può essere prorogato di ulteriori 60 giorni, se necessario, tenuto conto della complessità e del numero delle richieste. In tal caso il Titolare del Trattamento informa l'interessato di tale proroga e dei motivi del ritardo, entro 30 giorni dal ricevimento della richiesta.
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.
L'accesso dell'interessato ai propri dati personali può essere differito limitatamente al periodo strettamente necessario durante il quale i dati stessi sono trattati esclusivamente per lo svolgimento di indagini difensive o per salvaguardare esigenze di riservatezza del titolare. L'accesso è tuttavia consentito agli altri dati personali dell'interessato che non incidono sulle ragioni di tutela a base del differimento.

Art. 24 Indagini difensive

Ai fini delle indagini svolte nel corso di un procedimento penale, il difensore, ai sensi della Legge 7 dicembre 2000, n. 397 e dell'art. 391-quater del Codice di procedura penale, può chiedere documenti in possesso del titolare, e può estrarne copia, anche se contengono dati personali di un terzo interessato.
Il rilascio è subordinato alla verifica che il diritto difeso sia di rango almeno pari a quello dell'interessato, e cioè consistente in un diritto della personalità o in un altro diritto o libertà fondamentale ed inviolabile rinviando, per ogni altro e ulteriore aspetto, alla relativa disciplina al Regolamento del titolare sul diritto di accesso.
Il titolare si conforma alle Linee guida del Garante in tema di indagini difensive.

CAPO V - SOGGETTI

Art. 25 Titolare e contitolari

Il titolare del trattamento è il Comune di Greve in Chianti, rappresentato dal Sindaco pro tempore, in qualità di legale rappresentante del titolare, con sede in Piazza Matteotti 8 Greve in Chianti.
Il titolare provvede:

- a definire gli obiettivi strategici per la protezione dei dati personali in ordine al trattamento, provvedendo all'inserimento di tali obiettivi strategici nel DUP e negli altri documenti di programmazione e pianificazione del titolare;
- a mettere in atto misure tecniche e organizzative adeguate per garantire che il trattamento sia effettuato conformemente al Codice, al GDPR e al presente Regolamento;
- a delegare ovvero a nominare, con proprio atto, i Responsabili di Settore, responsabili del trattamento per i compiti, le funzioni e i poteri in ordine ai processi, procedimenti, e adempimenti relativi al trattamento dei dati personali, alla sicurezza e alla formazione, impartendo ad essi, le necessarie istruzioni, in relazione all'informativa agli interessati, alla tipologia dei dati da trattare, alle condizioni normative previste per il trattamento dei dati, alle modalità di raccolta, comunicazione e diffusione dei dati, all'esercizio dei diritti dell'interessato, all'adozione delle misure di sicurezza per la conservazione, protezione e sicurezza dei dati, all'eventuale uso di apparecchiature di videosorveglianza;
- a formare e aggiornare l'elenco dei Responsabili di Settore, responsabili del trattamento, delegati o nominati, e a pubblicarlo sul sito web istituzionale del titolare;
- a designare, con proprio atto, il Responsabile per la protezione dei dati personali;
- a disporre periodiche verifiche sul rispetto delle istruzioni impartite, anche con riguardo agli aspetti relativi alla sicurezza dei dati e alla formazione dei dipendenti;
- a favorire l'adesione a codici di condotta elaborati dalle associazioni e dagli organismi di categoria rappresentativi;
- a favorire l'adesione a meccanismi di certificazione;
- ad assolvere agli obblighi nei confronti del Garante nei casi previsti dalla vigente normativa;

Il titolare si trova in rapporto di contitolarità con altri titolari quando determinano congiuntamente le finalità e i mezzi del trattamento.
I contitolari sono tenuti a determinare, in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal GDPR e dal presente Regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14 GDPR, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. Tale accordo può designare un punto di contatto per gli interessati. L'accordo interno deve riflettere adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.
Indipendentemente dalle disposizioni dell'accordo interno, l'interessato può esercitare i propri diritti ai sensi del presente regolamento nei confronti di e contro ciascun titolare del trattamento.

Art. 26 Responsabili del trattamento

Il Responsabile è il soggetto che agisce per conto del titolare.

I Responsabili del trattamento interni sono i Responsabili del Settore, titolari di posizione organizzativa

Il titolare può avvalersi, per il trattamento di dati, anche sensibili, di soggetti pubblici o privati che per esperienza, capacità ed affidabilità forniscano le garanzie del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. A tale scopo il titolare autorizza i Responsabili interni all'individuazione e nomina mediante atto scritto di tali soggetti.

Gli obblighi dei Responsabili del trattamento sono tutti quelli previsti dall'art.28 del GDPR

Nel caso di mancato rispetto delle predette disposizioni, e in caso di mancata comunicazione al titolare dell'atto di nomina dei soggetti incaricati al trattamento dei dati e dei responsabili esterni ne risponde direttamente, verso il titolare, il Responsabile del trattamento.

L'accettazione della nomina e l'impegno a rispettare le disposizioni del Codice, del GDPR e del presente Regolamento è condizione necessaria per l'instaurarsi del rapporto giuridico fra le parti.

All'atto di designazione del Responsabile esterno vengono consegnate la procedura per la gestione delle richieste di esercizio dei diritti dell'interessato di cui all'art 23 del presente Regolamento e il registro per la notifica delle violazioni di cui all'art 35, e copia del presente regolamento

Art. 27 Incaricati del trattamento dipendenti del titolare

Gli incaricati del trattamento sono le persone fisiche, dipendenti del titolare, designati da ciascun Responsabile del Trattamento, incaricati di svolgere le operazioni di trattamento dei dati personali di competenza con l'indicazione specifica dei compiti, dell'ambito di trattamento consentito, e delle modalità .

La designazione dell'incaricato al trattamento dei dati personali è di competenza del Responsabile di Settore; la nomina è effettuata per iscritto e individua specificatamente i compiti spettanti all'incaricato e le modalità cui deve attenersi per l'espletamento degli stessi e l'ambito del trattamento consentito.

A prescindere dalla nomina, si considera tale anche la documentata preposizione della persona fisica ad un'unità per la quale risulti individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima. Per effetto di tale disposizione, ogni dipendente preposto ad un determinato ufficio/settore, tenuto ad effettuare operazioni di trattamento nell'ambito di tale settore, è da considerare, incaricato ai sensi dell'art. 2-quater decies del Codice nonché ai sensi degli artt. 4 comma 10 e art. 29 del GDPR.

Gli incaricati devono comunque ricevere idonee ed analitiche istruzioni, anche per gruppi omogenei di funzioni, riguardo le attività sui dati affidate e gli adempimenti a cui sono tenuti.

Gli incaricati collaborano con il titolare ed il Responsabile del Trattamento segnalando eventuali situazioni di rischio nel trattamento dei dati e fornendo ogni informazione necessaria per l'espletamento delle funzioni di controllo.

In particolare, gli incaricati devono assicurare che, nel corso del trattamento, i dati siano:

- trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
- raccolti e registrati per scopi determinati, espliciti e legittimi, e successivamente trattati in modo compatibile con tali finalità;
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono

trattati;

- 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;
- conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore a quello necessario per il conseguimento delle finalità per le quali i dati sono trattati;
- trattati in modo tale che venga ad essere garantita un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure organizzative e tecniche adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentale.

Gli incaricati sono tenuti alla completa riservatezza sui dati di cui siano venuti a conoscenza in occasione dell'espletamento della propri attività, impegnandosi a comunicare i dati esclusivamente ai soggetti indicati dal titolare e dal Responsabile del Trattamento, nei soli casi previsti dalla legge, nello svolgimento dell'attività istituzionale del titolare.
Gli incaricati dipendenti del titolare sono destinatari degli interventi di formazione di aggiornamento.

Art. 28 Incaricati del trattamento non dipendenti del titolare

Tutti i soggetti che svolgono un'attività di trattamento dei dati, e che non sono dipendenti del titolare, quali a titolo meramente esemplificativo i tirocinanti, i volontari e i soggetti che operano temporaneamente all'interno della struttura organizzativa del titolare o incaricati nominati dal Responsabile esterno, devono essere incaricati del trattamento tramite atto scritto di nomina.
Questi ultimi sono soggetti agli stessi obblighi cui sono sottoposti tutti gli incaricati dipendenti del titolare, in modo da garantire il pieno rispetto della tutela della riservatezza dei dati.
Gli incaricati non dipendenti dal titolare sono destinatari degli interventi di formazione di aggiornamento.

Art. 29 Amministratore di sistema

L'amministratore di sistema, individuato nel Responsabile del Centro Elaborazione Dati, sovraintende alla gestione e alla manutenzione delle banche dati e, nel suo complesso, al sistema informatico di cui è dotata l'Amministrazione.
La nomina dell'amministratore di sistema deve avvenire previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati e in tema di sicurezza. La designazione dell'amministratore di sistema è individuale e deve recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.
L'amministratore di sistema svolge attività, quali il salvataggio dei dati, l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e la manutenzione hardware e propone al Titolare del trattamento un documento di valutazione del rischio informatico.
Nel rispetto della normativa in materia di protezione dei dati e della sicurezza, l'amministratore di sistema deve adottare sistemi idonei alla registrazione degli accessi logici ai sistemi di elaborazione e agli archivi elettronici.
Le registrazioni (access log) devono essere complete, inalterabili, verificabili nella loro integrità, e adeguate al raggiungimento dello scopo di verifica per cui sono richieste.
Le registrazioni devono comprendere il riferimento temporale e la descrizione dell'evento che le ha

generate e devono essere conservate per un periodo congruo, non inferiore ai sei mesi.
Secondo la normativa vigente, l'operato dell'amministratore di sistema deve essere verificato, con cadenza annuale, da parte del Titolare del trattamento, in modo da controllare la rispondenza alle misure tecnico-organizzative e di sicurezza attivate rispetto all'attività di trattamento dei dati personali.
Il titolare di sistema applica le disposizioni impartite dal Garante in materia di misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema.
L'amministratore di sistema è destinatario degli interventi di formazione di aggiornamento.

Art. 30 Responsabile della protezione dei dati personali (RPD)

Il Titolare designa il Responsabile della protezione dei dati (RPD).
Il RPD deve essere in possesso di:

- un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali;
- deve adempiere alle sue funzioni in totale indipendenza e in assenza di conflitti di interesse;
- operare alle dipendenze del titolare del trattamento oppure sulla base di un contratto di servizio.

Il RPD è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti.
Il titolare del trattamento mette a disposizione del RPD le risorse necessarie per adempiere ai suoi compiti e accedere ai dati personali e ai trattamenti.
Il RPD svolge i seguenti compiti:

- informa e fornisce consulenze al titolare del trattamento, nonché ai dipendenti che eseguono il trattamento dei dati in merito agli obblighi vigenti relativi alla protezione dei dati;
- verifica l'attuazione e l'applicazione della normativa vigente in materia, nonché delle politiche del Titolare o del Responsabile del trattamento relative alla protezione dei dati personali, inclusi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale coinvolto nelle operazioni di trattamento, e gli audit relativi;
- fornisce, qualora venga richiesto, pareri in merito alla valutazione d'impatto sulla protezione dei dati e sorveglia i relativi adempimenti;
- funge da punto di contatto per gli interessati in merito al trattamento dei loro dati personali e all'esercizio dei diritti;
- funge da punto di contatto con il Garante per la protezione dei dati personali per questioni connesse al trattamento dei dati, tra cui la consultazione preventiva.

CAPO VI - SICUREZZA DEI DATI PERSONALI

Art. 31 Misure di sicurezza

Il titolare, nel trattamento dei dati personali, garantisce l'applicazione di adeguate misure di sicurezza che consentono di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alla finalità della raccolta.

In particolare il titolare del trattamento mette in atto misure e tecniche, organizzative, di gestione, procedurali e documentali adeguate per garantire un livello di sicurezza adeguato al rischio, conformi alle Linee Guida AGID e al GDPR nonché sostenibili dall'Ente, e riepilogate nel Registro Unico dei Trattamenti.

ART. 32 Valutazione d'impatto sulla protezione dei dati- DPIA

La valutazione d'impatto sulla protezione dei dati (di seguito solo DPIA) è un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per affrontarli.

La DPIA è uno strumento importanti per la responsabilizzazione in quanto sostiene il titolari non soltanto nel rispettare i requisiti del GDPR, ma anche nel dimostrare che sono state adottate misure appropriate per garantire il rispetto del medesimo GDPR.

La DPIA sulla protezione dei dati personali deve essere realizzata, prima di procedere al trattamento, dal titolare del trattamento quando un tipo di trattamento, considerata la natura, il contesto, le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, intendendosi per rischio uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità, e per gestione dei rischi l'insieme delle attività coordinate volte a indirizzare e controllare un'organizzazione in relazione ai rischi.

Prioritariamente alla DPIA deve:

- essere effettuata o aggiornata la ricognizione dei trattamenti.
- essere effettuata la determinazione in ordine alla possibilità che il trattamento possa determinare un rischio elevato per i diritti e le libertà degli interessati.

La decisione in ordine alla possibilità che il trattamento possa produrre un rischio elevato sulla protezione dei dati delle persone fisiche e, quindi, sulla obbligatorietà della DPIA, fermo restando l'elenco dei trattamenti per i quali la DPIA è obbligatoria e di cui all'Allegato 1 al provvedimento del Garante n. 467 del 11 ottobre 2018, viene adottata applicando i casi indicati l'art. 35, paragrafo 3 del GDPR e i criteri esplicativi contenuti nelle Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento possa presentare un rischio elevato ai fini del regolamento (UE) 2016/679 adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo Linee guida).

La DPIA non è richiesta nei seguenti casi:

- quando, sulla base di predetti criteri, risulta che il trattamento non è tale da presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
- quando la natura, l'ambito di applicazione, il contesto e le finalità del trattamento sono molto simili a un trattamento per il quale è stata svolta una valutazione d'impatto sulla protezione dei dati. In tali casi, si possono utilizzare i risultati della valutazione d'impatto

sulla protezione dei dati per un trattamento analogo;

- quando le tipologie di trattamento sono state verificate da un'autorità di controllo prima del maggio 2018 in condizioni specifiche che non sono cambiate;
- qualora un trattamento, effettuato a norma dell'articolo 6, paragrafo 1, lettere c) o e) GPDR, trovi una base giuridica nel diritto dell'Unione o nel diritto dello Stato membro, tale diritto disciplini il trattamento specifico o sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nel contesto dell'adozione di tale base giuridica (articolo 35, paragrafo 10 GPDR).

La DPIA deve contenere almeno:

- una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal Titolare del trattamento;
- una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
- una valutazione dei rischi per i diritti e le libertà degli interessati;
- le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento, il titolare del trattamento, se necessario, procede a un riesame della valutazione d'impatto sulla protezione dei dati.

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme UNI ISO (31000 e 27001) nonché degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del GDPR:

- una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal Titolare del trattamento;
- una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
- una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1, art. 35 del GDPR;
- le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Il titolare del trattamento, nello svolgere l'attività di valutazione, si consulta con il Responsabile della protezione dei dati, acquisendone il parere.

Laddove la DPIA riveli la presenza di rischi residui elevati, il titolare è tenuto a richiedere la consultazione preventiva dell'autorità di controllo in relazione al trattamento ai sensi dell' art. 36, paragrafo 1 GDPR.

Art. 33 Consultazione preventiva

Il titolare, prima di procedere al trattamento dei dati, consulta, per il tramite del RPD, il Garante qualora la valutazione d'impatto sulla protezione dei dati abbia evidenziato che il trattamento potrebbe presentare un rischio elevato in assenza di misure adottate.

Art. 34 Modulistica e procedure.

Il titolare, al fine di agevolare e semplificare la corretta e puntuale applicazione delle disposizioni del Codice, del GDPR, del presente Regolamento, e di tutte le linee guida e provvedimenti del Garante:

a) adotta e costantemente aggiorna:

- modelli uniformi di informativa;
- modelli e formule uniformi necessarie per gestire il trattamento dei dati e le misure di sicurezza;

b) elabora, approva, e costantemente aggiorna:

- adeguate procedure gestionali.

Tali procedure e i relativi modelli sono conservati su apposita porzione del Server in una cartella di lavoro accessibile al Titolare e ai Responsabili del Trattamento interni, e saranno costantemente aggiornati a loro cura. A titolo esemplificativo ma non esaustivo tale cartella comprende:

- il modello di informativa di cui all'art 8
- il modello di registro dei trattamenti di cui all'art 16
- il registro dell'Accountability
- la procedura e la modulistica per la gestione delle richieste di esercizio dei diritti dell'interessato di cui all'art 23
- il registro contenente la procedura per la notifica delle violazioni di cui all'art 35
- il modello di atto di nomina degli incaricati del trattamento
- il modello di atto di nomina dei Responsabili esterni

Art. 35 Notificazione di una violazione dei dati personali

In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione al Garante senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

Il Responsabile del Settore, responsabile del trattamento, senza giustificato ritardo, sentito il Titolare del Trattamento, il Segretario Generale e il RPD, valuta l'esistenza di una violazione ed il rischio, nonché la necessità di informare il Garante. Conseguentemente compila il registro istituito per la notifica del data breach, e conservato nella cartella di cui all'art 34, e ne informa il Titolare.

La notifica al Garante deve:

a) descrivere la 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) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;

c) descrivere le probabili conseguenze della violazione dei dati personali;

d) 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.

Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

Art. 36 Comunicazione di una violazione dei dati personali

Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.

La comunicazione all'interessato del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d) del GDPR.

Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle condizioni previste dall'art 34 paragrafo 3 del GDPR.

Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui all'art 34 paragrafo 3 è soddisfatta.

Art. 37 Disposizioni finali

Per quanto non previsto nel presente Regolamento si applicano le disposizioni del Codice, del GDPR, le Linee guida e i provvedimenti del Garante.

Il presente Regolamento è aggiornato a seguito di ulteriori modificazioni alla vigente normativa in materia di riservatezza e protezione dei dati personali.

Si intende abrogata ogni norma regolamentare vigente in contrasto con il presente regolamento**.**