MANUALE GDPR

ORDINE DEI GEOLOGI DELLA REGIONE UMBRIA

Via Martiri dei Lager 58 – 06128 Perugia

Ai sensi del codice della Privacy coordinato ed aggiornato, da ultimo, con le modifiche apportate dalla **L. 27 dicembre 2019, n. 160**, dal **D.L. 14 giugno 2019, n. 53**, dal **D.M. 15 marzo 2019** e dal **Decreto di adeguamento al GDPR (Decreto Legislativo 10 agosto 2018, n. 101)**

ELENCO DOCUMENTI

- ✓ Manuale GPDR
- ✓ Organigramma Privacy
- ✓ Contratti / Nomine GDPR
- ✓ Verbale di formazione / Informazioni
- ✓ Informative GDPR
- ✓ DPIA GDPR
- ✓ Registro del Titolare del Trattamento

MANUALE GPDR

SOMMARIO

1. PREMESSA

Dal 25 maggio 2018 è in vigore il GDPR, il **nuovo regolamento** sulla **privacy** che ha introdotto **nuovi** adempimenti e obblighi per professionisti ed imprese e un un **nuovo** sistema di sanzioni amministrative e penali generando una sorta di riforma nell'ambito delle regole sul trattamento dei dati.

a. OGGETTO E FINALITA'

Il presente manuale è redatto dal titolare de trattamento dei dati personali con l'intento di definire le azioni per il trattamento dei dati personali nel rispetto della normativa vigente, adottando le misure di sicurezza idonee e valutando i rischi eventuali dei trattamenti dei dati personali effettuati dal titolare del trattamento.

b. AMBITO DI APPLICAZIONE

Il presente manuale si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali effettuati dal titolare del trattamento.

c. REVISIONE

Questo manuale ed i documenti allegati verranno periodicamente aggiornati anche alla luce delle attività svolte e dei trattamenti dati effettuati dal titolare del trattamento.

2. RIFERIMENTI NORMATIVI

Ai sensi del codice della Privacy coordinato ed aggiornato, da ultimo, con le modifiche apportate dalla **L. 27 dicembre 2019, n. 160**, dal **D.L. 14 giugno 2019, n. 53**, dal **D.M. 15 marzo 2019** e dal **Decreto di adeguamento al GDPR (Decreto Legislativo 10 agosto 2018, n. 101)**.

3. TERMINI E DEFINIZIONI (Articolo 4 Reg. UE 679/2016)

«**dato personale**»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

«**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;

«**limitazione di trattamento**»: il contrassegno dei dati personali conservati con l'obiettivo di

limitarne il trattamento in futuro;

«**profilazione**»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali 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**»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

«**archivio**»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

«**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;

«**responsabile del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

«**destinatario**»: la persona fisica o giuridica, l'autorità pubblica, l’ente (nel caso di specie ente pubblico non economico = ordine professionale) o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

«**terzo**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

«**consenso dell'interessato**»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

«**violazione dei dati personali**»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

«**dati genetici**»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

«**dati biometrici**»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

«**dati relativi alla salute**»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

«**stabilimento principale»**: per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;
con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;

«**rappresentante**»: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;

«**impresa**»: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;

«**gruppo imprenditoriale**»: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;

«**norme vincolanti d'impresa**»: le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;

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

«**autorità di controllo interessata**»: un'autorità di controllo interessata dal trattamento di dati personali in quanto:
a) il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo;
b) gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento;
c) un reclamo è stato proposto a tale autorità di controllo;

«**trattamento transfrontaliero**»:
trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;

«**obiezione pertinente e motivata**»: un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;

«**servizio della società dell'informazione**»: il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio;

«**organizzazione internazionale**»: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

4. IL TRATTAMENTO DEI DATI PERSONALI

a. DEFINIZIONE

L'articolo 4 del Regolamento europeo definisce il **trattamento dei dati personali,** come 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.

Il concetto di trattamento ingloba tutte quelle **operazioni che implicano una conoscenza di dati personali**.

Il **trattamento di dati personali** può costituire un'ingerenza con il diritto al rispetto della vita privata.
Quest'ultimo diritto non è un diritto assoluto, ma relativo, cioè va contemperato opportunamente con gli altri diritti in gioco, sia privati sia pubblici.
Qualsiasi trattamento deve, quindi, essere svolto in maniera lecita e secondo correttezza, i dati devono essere raccolti e trattati per scopi determinati, espliciti e legittimi, e utilizzati in termini compatibili con tali scopi. Inoltre, i dati devono essere esatti e aggiornati, pertinenti, completi e non eccedenti rispetto agli scopi del trattamento. Infine, devono essere conservati per un periodo non superiore al tempo necessario per raggiungere gli scopi del trattamento, trascorso il quale i dati vanno cancellati oppure anonimizzati.
Ovviamente **i dati raccolti o trattati in modo illecito non possono essere in alcun modo utilizzati**. In caso contrario l'utilizzatore può essere soggetto a sanzioni e condannato al risarcimento dei danni causati (art. 2050 cod. civ. e art. 13 Cod. Privacy).

b. TIPI DI TRATTAMENTO

La **raccolta** dei dati è la prima operazione e generalmente rappresenta l'inizio del trattamento. Consiste nell'attività di acquisizione del dato.
La **registrazione** consiste nella memorizzazione dei dati su un qualsiasi supporto.
L'**organizzazion**e consiste nella classificazione dei dati secondo un metodo prescelto.
La **strutturazione** consiste nell'attività di distribuzione dei dati secondi schemi precisi.
La **conservazione** consiste nel mantenere memorizzate le informazioni su un qualsiasi

supporto.
La **consultazione** è la lettura dei dati personali. Anche la semplice visualizzazione dei dati è un trattamento che può rientrare nell'operazione di consultazione.
L'**elaborazione** consiste nell'attività con la quale il dato personale subisce una modifica sostanziale. La modificazione differisce dall'elaborazione in quanto può riguardare anche solo parte minima del dato personale.
La **selezione** consiste nell'individuazione di dati personali nell'ambito di gruppi di dati già memorizzati.
L'**estrazione** consiste nell'attività di estrapolazione di dati da gruppi già memorizzati.
Il **raffronto** è un'operazione di confronto tra dati, sia una conseguenza di elaborazione che di selezione o consultazione.
L'**utilizzo** è un'attività generica che ricopre qualsiasi tipo di impiego dei dati.
L'**interconnessione** consiste nell'utilizzo di più banche dati, e si riferisce all'impiego di strumenti elettronici.
Il **blocco** consiste nella conservazione con sospensione temporanea di ogni altra operazione di trattamento.
La **comunicazione** (o cessione) consiste nel dare conoscenza di dati personali ad uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati. In caso di comunicazione il dato viene trasferito a terzi, ed è quindi attività particolarmente delicata.
Per **diffusione**, invece, si intende il dare conoscenza dei dati a soggetti indeterminati, in qualunque forma anche mediante la loro messa a disposizione o consultazione. Si ha, quindi, diffusione anche quando si pubblica online, ad esempio una fotografia su un social network. In assenza di consenso tale attività deve ritenersi illecita.
La **cancellazione** consiste nell'eliminazione di dati tramite utilizzo di strumenti elettronici.
La **distruzione** è l'attività di eliminazione definitiva dei dati.

c. I PRINCIPI GENERALI DEL TRATTAMENTO DATI PERSONALI

I 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, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («**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 («**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, 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**»);

- 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 («i**ntegrità e riservatezza**»).

d. BASE GIURIDICA DEL TRATTAMENTO

Come la precedente normativa, anche il regolamento generale europeo (GDPR) stabilisce che un trattamento di dati personali deve trovare fondamento in una base giuridica.
La base giuridica è ciò che autorizza legalmente il trattamento.
In assenza di una base legale il trattamento è illecito.

Il titolare del trattamento ha l'obbligo di valutare quale sia la base giuridica più idonea rispetto al trattamento che intende porre in essere, e questo prima di iniziare il trattamento. Cioè, **non è libero di scegliere la base giuridica che preferisce**, ma deve deve rispettare le condizioni previste dal GDPR in relazione alle caratteristiche di ciascuna delle basi indicate nell'art. 6, ed essere sempre in grado di dimostrare la correttezza della scelta fatta. Ogni base giuridica, infatti, obbedisce a condizioni specifiche, e ha differenti conseguenze sui diritti delle persone. Ovviamente non esiste una gerarchia tra le diverse basi giuridiche.

La base giuridica è indicata nell'informativa rivolta agli utenti. Inoltre è utile documentare la scelta della base giuridica, e menzionare la base giuridica nel registro dei trattamenti. Per il trattamento dei dati di cui all'art. 9 (dati sensibili), oltre ad individuare una corretta base giuridica, occorre fare riferimento alle condizioni previste nell'articolo indicato.

L'articolo 6 del regolamento europeo enuncia le condizioni in base alle quali il trattamento può dirsi lecito.

- **Consenso**

Il consenso dell'interessato autorizza il trattamento dei dati. Il consenso deve essere specifico, cioè legato ad una finalità precisa. Se il trattamento è basato sul consenso il titolare del trattamento deve fornire l'informativa e garantire la portabilità dei dati.
Le autorità di protezione dei dati incoraggiano attivamente le imprese a superare l'intero processo di acquisizione del consenso per il trattamento dei dati personali. Questo perché il "consenso" non è ritenuto affidabile, nel senso che poche persone in realtà prendono una decisione "specifica, informata ed inequivocabile". Ben pochi, infatti, leggono le informative in materia. Il consenso è ritenuto, quindi, un onere per le imprese difficile da attuare per come è configurato. Le persone non vogliono essere bombardate dagli odiosi cookie banner, e comunque un banner dovrebbe contenere molte più informazioni di quante generalmente ne contiene, degradando enormemente l'esperienza di navigazione online. Ecco perchè

esistono molti casi nei quali la base giuridica del trattamento è diversa dal consenso.
Teniamo presente, inoltre, che il regolamento europeo supera la vecchia prospettiva della visione proprietaria del dato, per il cui trattamento occorre il consenso, passando ad una **prospettiva di controllo del dato**, in base alla quale l'interessato deve sapere se i suoi dati sono usati e se sono usati in modo da proteggerlo dai rischi che il trattamento può provocare.

- **Adempimento di obblighi contrattuali o misure precontrattuali**
  Il trattamento è lecito se è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso interessato. Sostanzialmente è una forma speciale di consenso. Occorre ovviamente **l'informativa**, e deve essere garantita la **portabilità dei dati**.

- **Obblighi di legge cui è soggetto il titolare del trattamento**
  L'obbligo legale deve soddisfare **quattro condizioni**:
  - deve essere definito dalla legge europea o nazionale di uno Stato membro a cui è soggetto il titolare del trattamento (in base all'art. 2-ter del Codice Privacy, solo norme di legge o, nei casi previsti dalla legge, di regolamento);
  - tali disposizioni legali devono stabilire un obbligo imperativo di trattamento dei dati personali, sufficientemente chiaro e preciso;
  - tali disposizioni devono almeno definire le finalità del trattamento in questione;
  - tale obbligo deve essere imposto al titolare del trattamento e non alle persone interessate dal trattamento.

  Nel caso di trattamento dei dati necessario per l'adempimento di obblighi derivanti da legge, regolamento o normativa comunitaria non occorre il consenso, non si deve garantire la portabilità dei dati, ma occorre fornire l'informativa, nella quale va indicata la base giuridica del trattamento. In questo caso la finalità è specificata dalla legge.

- **Interessi vitali della persona interessata o di terzi**
  Il trattamento è ammesso se è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica, come nel caso di un incidente stradale oppure se l'interessato si trova nell'incapacità fisica di prestare il consenso (una persona si sente male mentre si trova nel vostro ufficio, questa base giuridica consente di trattare i suoi dati al fine di chiamare un'ambulanza). L'interesse deve essere così importante per la vita dell'interessato che questi consentirebbe di porre in essere un determinato trattamento di dati senza ulteriori presupposti.
  Si può utilizzare come base giuridica solo se nessuna delle altre condizioni di liceità può trovare applicazione. In questo caso non occorre il consenso, non si deve garantire la portabilità dei dati, ma occorre fornire l'informativa, nella quale va indicata la base giuridica del trattamento.

- **Legittimo interesse prevalente del titolare o di terzi cui i dati vengono comunicati**
  Quando il trattamento è necessario per il perseguimento dei legittimi interessi 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. Non occorre consenso,

non si deve garantire la portabilità dei dati, ma occorre fornire l'informativa, nella quale va indicata la base giuridica del trattamento.

- **Interesse pubblico o esercizio di pubblici poteri**
  Questa base giuridica si applica in particolare per il trattamento effettuato dalle autorità pubbliche necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri (es. fini umanitari, controllo di epidemie, catastrofi naturali e umane) di cui è investito il titolare del trattamento (tramite legge statale o dell'Unione). E' la norma giuridica (legge, regolamento o decreto) che deve indicare i compiti, e quindi l'interesse pubblico. Può riguardare anche organizzazioni private che svolgono compiti di interesse pubblico.
  L'art. 2 -sexies del Codice Privacy precisa che la finalità di interesse pubblico deve essere prevista dal diritto UE ovvero, nell'ordinamento interno, da disposizioni di legge o, nei casi previsti dalla legge, di regolamento che specifichino:
  - i tipi di dati che possono essere trattati;
  - le operazioni eseguibili e il motivo di interesse pubblico rilevante;
  - le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

5. TRASPARENZA DEL TRATTAMENTO DATI

a. INFORMATIVA

L'informativa sulla privacy è il documento che il titolare (nel caso di specie l'ordine professionale) che tratta dati personali di terzi predispone. Ecco cosa deve contenere.

L'informativa sulla privacy è un documento che fa parte degli adempimenti imposti dalla disciplina in materia di protezione dei dati personali.

Con essa chi pone in essere il trattamento deve informare il titolare dei dati personali, tra le altre cose, delle modalità con le quali gli stessi saranno trattati, della finalità e dei diritti dell'interessato.

I contenuti dell'informativa sono elencati **in modo tassativo** negli articoli 13, paragrafo 1, e 14, paragrafo 1, del regolamento e in parte sono più ampi rispetto al Codice.

In particolare, il titolare **DEVE SEMPRE** specificare i **dati di contatto del RPD-DPO (Responsabile della protezione dei dati-Data Protection Officer)**, ove esistente, la **base giuridica** del trattamento, **qual è il suo interesse legittimo** se quest'ultimo costituisce la base giuridica del trattamento, nonché **se trasferisce i dati personali in Paesi terzi** e, in caso affermativo, **attraverso quali strumenti** (esempio: si tratta di un Paese terzo giudicato adeguato dalla Commissione europea; si utilizzano BCR di gruppo; sono state inserite specifiche clausole contrattuali modello, ecc.).

Il regolamento prevede anche **ulteriori informazioni** in quanto "necessarie per garantire un trattamento corretto e trasparente": in particolare, il titolare deve specificare **il periodo di conservazione dei dati** o i criteri seguiti per stabilire tale periodo di conservazione, e il diritto di **presentare un reclamo** all'autorità di controllo.

Se il trattamento comporta processi decisionali automatizzati (anche la **profilazione**), l'informativa deve specificarlo e deve indicare anche la **logica** di tali processi decisionali e le conseguenze previste per l'interessato.

Tempi dell'informativa
Nel caso di dati personali non raccolti direttamente presso l'interessato *(art. 14 del regolamento)*, l'informativa deve essere fornita **entro un termine ragionevole che non può superare 1 mese** dalla raccolta, oppure **al momento della comunicazione** (**NON** della registrazione) dei dati a terzi o all'interessato (diversamente da quanto prevede attualmente l'art. 13, comma 4, del Codice).

Modalità dell'informativa
Il regolamento specifica molto più in dettaglio rispetto al Codice le caratteristiche dell'informativa, che deve avere forma **concisa, trasparente, intelligibile per l'interessato e facilmente accessibile**; occorre utilizzare un linguaggio **chiaro e semplice**, e per i minori occorre prevedere informative idonee *(si veda anche considerando 58)*.

L'informativa è data, **in linea di principio, per iscritto** e **preferibilmente in formato elettronico** (soprattutto nel contesto di servizi online: *si vedano art. 12, paragrafo 1, e considerando 58*), anche se sono ammessi "altri mezzi", quindi può essere fornita anche oralmente, ma nel rispetto delle caratteristiche di cui sopra *(art. 12, paragrafo 1)*. Il regolamento ammette, soprattutto, l'utilizzo di **icone** per presentare i contenuti dell'informativa in forma sintetica, **ma solo "in combinazione" con l'informativa estesa** *(art. 12, paragrafo 7)*; queste icone dovranno essere identiche in tutta l'Ue e saranno definite prossimamente dalla Commissione europea.

Sono inoltre **parzialmente diversi i requisiti che il regolamento fissa per l'esonero dall'informativa** *(si veda art. 13, paragrafo 4 e art. 14, paragrafo 5 del regolamento, oltre a quanto previsto dall'articolo 23, paragrafo 1, di quest'ultimo)*, anche se occorre sottolineare che **spetta al titolare**, in caso di dati personali raccolti da fonti diverse dall'interessato, **valutare se la prestazione dell'informativa agli interessati comporti uno sforzo sproporzionato** *(si veda art. 14, paragrafo 5, lettera b)* – a differenza di quanto prevede l'art. 13, comma 5, lettera c) del Codice.

6. AMBITO DI APPLICAZIONE E SCOPO

Ambito di Applicazione

Il presente disciplinare si applica ai dati personali censiti e comunicati dagli incaricati del trattamento nonché i responsabili nelle modalità specificate dal regolamento trattati da parte dell'Ordine.
Tale documento è predisposto e tenuto aggiornato anche per definire, sulla base dell'analisi dei rischi della distribuzione dei compiti e della responsabilità, nell'ambito delle strutture preposte al trattamento dei dati:
- Criteri tecnici e organizzativi per la protezione dei dispositivi, delle aree e dei locali interessati dalle misure di sicurezza, nonché tutte le procedure per controllare l'accesso delle persone autorizzate gli stessi;
- I criteri e le procedure per assicurare l'integrità dei dati;

- I criteri e le procedure per la sicurezza della trasmissione dei dati;
- L'elaborazione di un piano di formazione verso tutti i referenti dell'organigramma della privacy al fine di renderli e dotti dei rischi individuati e dei modi per prevenire danni.

Scopo

Il presente disciplinare è redatto con l'obiettivo di garantire la conformità agli obblighi di sicurezza e di protezione dei dati personali imposti dal nuovo regolamento europeo sulla protezione dei dati.l'approccio con il quale questo disciplinare è stato redatto si ispira al principio della privacy by design che prevede di gestire la privacy a partire dalla progettazione di un processo aziendale.

Nell'ambito dei generali obblighi di sicurezza il presente disciplinare si propone di:

- Assicurare l'adozione di misure di sicurezza tali da garantire un livello di protezione dei dati personali;
- Rappresentare un valido strumento per l'adozione di idonee misure di sicurezza in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, tali da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati trattati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta di dati medesimi;
- Realizzare la protezione e la sicurezza dei dati attraverso misure di sicurezza di natura fisica, logica organizzativa adottate dal titolare del trattamento, dai responsabili esterni del trattamento.

Le conseguenza della violazione della normativa

Il GDPR ha previsto rilevanti sanzioni di natura amministrativa in caso di violazione della normativa sulla protezione dei dati personali.

In particolare, l'articolo 83 del GDPR distingue due gruppi di sanzioni amministrative:

- Nel primo gruppo rientrano le violazioni cosiddette di minore gravità per le quali sono previste le sanzioni amministrative pecuniarie fino a 10 milioni di euro o per le imprese fino al 2% del fatturato mondiale totale anno dell'esercizio precedente, sei superiore, e riguardano nello specifico le violazioni degli obblighi imposti ai seguenti soggetti:

A) Il titolare del trattamento ed il responsabile esterno del trattamento articolo otto 11 da 25 e 29 42 e 43 GDPR;

B) L'organismo di certificazione;

C) L'organismo di controllo dei codici di condotta articolo 41 GDPR.

- Nel secondo gruppo di sanzioni, più pesanti in considerazione della maggiore gravità della fattispecie a cui sono ricondotte, le sanzioni ammontano fino a 20 milioni di euro o, per le imprese fino al 4% del fatturato mondiale totale anno dell'esercizio precedente, se è superiore, e riguardano nello specifico le seguenti violazioni:

A) Dei principi di base del trattamento, comprese le condizioni relative al consenso, a norma degli articoli 5 6 7 9;

B) Dei diritti degli interessati a norma degli articoli da 10 a 22;

C) I trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale a norma degli articoli da 44 e 49;

D) qualsiasi obbligo ai sensi delle legislazioni degli Stati membri adottate a norma del capo nove;

E) L'inosservanza di un ordine, di una limitazione provvisoria o definitiva del trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo ovvero il garante privacy ai sensi dell'articolo 58 paragrafo due o in negato accesso in violazione dell'articolo 58 paragrafo 1 GDPR.

Il garante per la protezione dei dati personali è l'organo competente ad irrogare le sanzioni sopracitate ai sensi dell'articolo 15 comma tre del decreto legislativo 101 2018. Lo stesso dovrà avere cura di valutare caso per caso le violazioni affinché le sanzioni siano sempre effettive, proporzionate e dissuasive articolo 83 comma uno GDP Our tenendo in debito conto le circostanze di cui all'83 comma due GDPR ossia la natura la gravità la durata della relazione il carattere doloso colposo della stessa le categorie di dati personali interessate dalle violazioni, ecc.

Dalla violazione della normativa in materia di protezione dei dati personali possono derivare anche responsabilità penali. La materia penale è di stretta competenza nazionale e pertanto non viene disciplinata dal GDPR che si limita ad indicare che "gli Stati membri stabiliscono le norme relative alle sanzioni per le violazioni del presente regolamento in particolare per le proprie violazioni non soggetti a sanzioni amministrative pecuniarie".
Il D.Lgs. 101/2018 modifica le fattispecie penalmente rilevanti già previste dal codice privacy, introduce nuove sanzioni ed abroga la fattispecie penali relative a obblighi non più sussistenti.
In base al nuovo impianto definito dal decreto di adeguamento, sono previsti i seguenti illeciti penali ai sensi del riformato codice della privacy:
- trattamento illecito di dati articolo 167 reclusione da sei mesi a un anno e sei mesi
- comunicazione diffusione illecita di dati personali oggetto di trattamento sul larga scala articolo 167 bis reclusione da uno a sei anni
- acquisizione fraudolenta di dati personali oggetto di trattamento sul larga scala articolo 167ter reclusione da uno a 4 anni
- falsità nelle dichiarazioni al garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del garante articolo 168 reclusione da sei mesi a tre anni
- inosservanza dei provvedimenti del garante articolo 170 reclusione da tre mesi a due anni
- violazioni delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori articolo 171
La condanna per uno dei delitti previsti dal codice privacy importa la pubblicazione della sentenza.

7. PROCEDURA PER LA PROTEZIONE DEI DATI PERSONALI

Scopo
La procedura per la protezione dei dati personali prevede specifiche e requisiti generali di sicurezza e protezione dei dati personali adottati dall'ordine in adempimento di quanto richiesto nel nuovo regolamento.

Attraverso la procedura, l'ordine definisce e applica i principi obiettivi in tema di protezione dei dati:
- l'identificazione degli aspetti connessi ai rischi derivanti dal trattamento dei dati personali già in fase di definizione/progettazione/revisione dei processi;
- l'adozione di misure di sicurezza idonee a prevenire e ridurre al minimo i rischi inerenti al trattamento dei dati personali;
- l'adozione di opportuni criteri e modalità di ripristino dei dati in caso di danneggiamento perdita accidentale;
- sensibilizzazione dei dipendenti, fornitori, clienti in materia di protezione dei dati;
- motivare e formare costantemente il personale dipendente affinché venga sviluppato, ad ogni livello, il senso di responsabilità verso la tutela dei dati personali e la sicurezza delle informazioni;
- formazione del corretto trattamento dei dati personali sicurezza delle informazioni;
- evidenza della conformità legislativa attraverso un sistema di gestione per la protezione dei dati personali costantemente oggetto di analisi.

Applicabilità
Il presente documento si applica a tutte le modalità di trattamento dei dati da parte degli operatori dell'ordine e agli strumenti utilizzati e gli aspetti relativi alla sicurezza.

I principi della procedura di sicurezza e protezione dei dati:
1. Devono essere trattati in modo lecito, corretto e trasparente nei confronti degli interessati;
2. Devono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in maniera tale da non essere incompatibile con tali finalità;
3. Devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono stati trattati;
4. Debbono essere esatti e aggiornati, oltre al fatto che vanno utilizzate misure per cancellare rettificare i dati inesatti;
5. Devono essere conservati in maniera tale che possono essere identificati dagli interessati per un arco temporale legato alla finalità del loro utilizzo;
6. Debbono essere trattati in maniera da garantire sicurezza dei dati personali, compresa la protezione mediante misure tecniche organizzative adeguate.

Condizioni per il consenso
Il consenso è una delle basi giuridiche del trattamento, nell'ambito del regolamento generale per la protezione dei dati personali.

Caratteristiche
Il consenso deve essere:

inequivocabile,
Vuol dire che non è necessario che sia esplicito ma può anche essere implicito, ma non tacito, purché, nel momento in cui sia desunto dalle circostanze, non sussista alcun dubbio che col proprio comportamento l'interessato abbia voluto comunicare il proprio consenso.

libero,
L'interessato deve essere in grado di operare una scelta effettiva, senza subire intimidazioni o raggiri, ne deve subire conseguenze negative a seguito del mancato conferimento del consenso.

specifico,
Relativo alla finalità per le quali eseguito in quel trattamento.qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per ogni finalità considerando 32 GDP R quindi, i dati dovranno essere pertinenti al consenso fornito, e in caso di modifiche del trattamento occorre richiedere un nuovo consenso.

informato,
L'interessato deve essere posto in condizione di conoscere quali dati sono trattati, con che modalità e finalità e i diritti che gli sono attribuiti dalla legge. Inoltre l'interessato deve essere opportunamente informato sulle conseguenze del suo consenso attraverso l'apposita informativa. Il regolamento europeo si concreta più che sui requisiti formali del consenso, sulla necessità della validità sostanziale del consenso, per cui l'aspetto informativo è essenziale, richiedendo un linguaggio semplice e comprensibile, anche eventualmente colloquiale.

verificabile,
Il titolare del trattamento deve essere in grado di dimostrare che l'interessato lo ha conferito con riferimento a quello specifico trattamento. Il titolare dovrà essere in grado di sapere anche a quale informativa l'utente a consentito, distinguendo fra le varie versioni.

revocabile,
L'interessato deve poter revocare il proprio consenso in qualunque momento. La revoca deve essere facile e non vi è alcun obbligo di motivare la revoca, a seguito della quale il trattamento deve interrompersi. Per revocare il consenso, quindi, il titolare del trattamento dovrebbe predisporre una procedura analoga a quella offerta per concedere il consenso. In alternativa è possibile revocare il consenso inviando una comunicazione. Nel caso in cui il titolare del trattamento non ottemperi ci si può rivolgere al garante o al tribunale per la tutela dei propri diritti.

Scadenza
Occorre tenere presente che quando si raccolgono dati personali occorre informare l'interessato della durata della conservazione del dato, scaduta la quale il dato va o anonimizzato oppure cancellato. Per questo motivo in alcuni casi potrebbe essere preferibile una base giuridica diversa dal consenso, come ad esempio legittimi interessi del titolare del trattamento.

8. TRATTAMENTO DI DATI PERSONALI A MEZZO DI NUOVE TECNOLOGIE

Dati trattati

I dati che potrebbero essere trattati sia in maniera elettronica che cartacea sono classificabili in:

dati comuni
informazioni non riguardanti una persona fisica identificata o identificabile

dati personali
informazioni riguardanti una persona fisica identificata o identificabile

dati personali particolari
informazioni idonee a rilevare l'origine razziale o etnica, le opinioni politiche le convinzioni religiose o filosofiche, l'appartenenza sindacale nonché i dati genetici dati Bíometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Trattamento dei dati mediante l'utilizzo di nuove tecnologie
Il trattamento dei dati personali mediante l'utilizzo di nuove tecnologie ad esempio videosorveglianza Geolocalizzazione o attraverso Sim dell'ordine presentano un rischio elevato per i diritti e le libertà dei soggetti.
Questa tipologia di trattamento dei dati non forma oggetto di legislazione specifica, ma al riguardo si applicano le disposizioni generali in tema di protezione dei dati personali. quindi con il nuovo regolamento europeo l'attività da svolgere per essere a norma non cambiano ma diventa molto più precisa e soggetta a sanzioni.
Il trattamento dei dati personali mediante l'utilizzo di nuove tecnologie deve, in ogni caso fondarsi sui principi di seguito esplicitati:
Principio di liceità, in base al quale i dati devono essere trattati secondo le prescrizioni normative;
principio di necessità, in base al quale i sistemi informativi e i programmi informatici devono essere configurati in modo tale da ridurre al minimo l'utilizzo dei dati personali;
principio di proporzionalità in base al quale i dati personali oggetto di trattamento devono essere pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
principio di finalità, in base al quale i dati devono essere raccolti e trattati per scopi determinati, espliciti e legittimi.

Videosorveglianza

Con il termine videosorveglianza si definisce l'acquisizione in modo continuativo, di immagini, eventualmente associate a suoni, relative a persone identificabili. Spesso il rilevamento comporta anche una contestuale registrazione di una successiva conservazione dei dati. La raccolta, la registrazione, la conservazione ed in generale, l'utilizzo di immagini configura un trattamento di dati personali, come specificato in più punti, è considerato dato personale qualunque informazione relativa a una persona fisica identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione articolo quattro comma uno lett. b) Cod. privacy.

Le linee guida 3/19 sul trattamento dei dati personali attraverso dispositivi video adottati per la consultazione pubblica il 10 luglio 2019 evidenziano, innanzitutto, l'importanza del principio di minimizzazione dei dati, sottolineando che l'utilizzo di dispositivi video deve limitarsi ai soli casi in cui ci siano esigenze prevalenti ad opera del titolare del trattamento rispetto ai diritti e le libertà degli interessati e che non vi siano soluzioni alternative che consentano ed implicano un impatto minore sulla privacy di questi ultimi ad esempio, mediante l'impiego di personale addetto alla sicurezza.

Obbligo di informativa

Le nuove linee guida 3/19 sul trattamento dei dati personali, prescrivono di fornire e distribuire un'informativa su due livelli. È da tempo che la legislazione europea sulla protezione dei dati indica che gli interessati devono essere a conoscenza del fatto che la videosorveglianza è in funzione, e devono essere informati in modo dettagliato in merito ai luoghi monitorati, e nell'articolo 12 del GDPR sono stabiliti ed indicati obblighi generali di trasparenza e di informazione.

In dettaglio, un primo avviso, definito di primo livello segnale di avvertimento può contenere:
una icona grafica esplicativa sia un icona che sia facilmente visibile e comprensibile chiaramente leggibile ed implichi una panoramica significativa del trattamento previsto articolo 12 GDPR

i contatti e l'identità del titolare del trattamento previsto del DPO

i dettagli sulle finalità e sulle eventuale legittimo interesse del titolare del trattamento

i diritti dell'interessato, informazioni sui maggiori impatti del trattamento, richiamo riferimento alla seconda informativa, in particolare come tu per riferirla (preferenza di fonti digitali QR code o link web che indirizza all'informativa online.

Il formato delle informazioni deve essere adattato alla posizione individuale, praticamente deve essere posizionata ad una distanza adeguata e ragionevole dal sistema di video device in modo tale che l'interessato possa facilmente riconoscere in anticipo le circostanze della sorveglianza, prima di entrare nell'area monitorata approssimativamente all'altezza degli occhi.

Le informazioni di secondo livello, contenuto in un documento informativo completo, che può essere rappresentato da un foglio, un cartello, un poster, un link web o lo stesso QR cod, deve contenere informazioni più complete e dettagliate, collocate in un luogo facilmente accessibile e disponibile per gli interessati, ossia in una posizione centrale ad esempio ufficio informazioni Scrivanie reception. In ogni caso il titolare del trattamento, anche per il tramite di un incaricato, ove richiesto è tenuto a fornire anche oralmente l'informativa adeguata, contenente gli elementi individuati dall'articolo 13 del codice privacy.

Obbligo di verifica preliminare

Altro obbligo stabilito nel provvedimento generale del garante riguarda la verifica preliminare.

E’ ancora previsto che i trattamenti di dati personali nell’ambito di un’attività di videosorveglianza debbano essere effettuati rispettando le misure e gli accorgimenti prescritti dal garante come esito di una verifica preliminare attivata d’ufficio o a seguito di un interpello del titolare del trattamento articolo 17 del codice privacy, quando vi sono rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità degli interessati, in relazione alla natura dei dati o alle modalità di trattamento o agli effetti che può determinare.

Il garante ha individuato i casi in cui ci sono maggiori rischi:

quando i sistemi di raccolta delle immagini siano associati a dati biometrici; quando i sistemi siano dotati di software che permettono il riconoscimento della persona tramite collegamento, incrocio confronto delle immagini rilevate, con altri specifici dati personali, ovvero sulla base del confronto della stessa immagine con una campionatura di soggetti precostituita la raccolta di dati; quando si abbia che fare con con i sistemi cosiddetti intelligenti, i quali non si limitano a riprendere registrare le immagini, ma sono in grado di rilevare automaticamente comportamenti o eventi anomali, segnalarli ed eventualmente registrarli; quando si prevedono tempi di conversazione dei dati maggiori di sette giorni derivanti da speciali esigenze di ulteriore conservazione, a meno che non derivi da una specifica richiesta dell’autorità giudiziaria o di polizia giudiziaria relazione è un’attività investigativa in corso; quando i trattamenti effettuati tramite videosorveglianza hanno natura e caratteristiche tali per cui le misure e gli accorgimenti individuati nel presente provvedimento sono integralmente applicabili, in relazione alla natura dei dati o alle modalità del trattamento agli effetti che possono determinare, il titolare del trattamento è tenuto a richiedere la verifica preliminare al garante.

Tali dati possono essere conservati per un massimo di 72 ore se non in casi particolari come quelli sopra previsti.

Geolocalizzazione

Anche il fenomeno della geolocalizzazione solleva questioni in termini di privacy e nel rispetto delle sempre più stringenti norme in tema di riservatezza, in quanto i dati delle coordinate geografiche, sebbene ad un primo esame possono sembrare anonimi, in realtà in incrocio di questi con altri dati ad esempio i dati del sistema turni, consentono di risalire all’identità di un dipendente a cui sia stato assegnato uno specifico dispositivo. Molti titolari utilizzano il sistema di Geolocalizzazione GPS dei propri veicoli. Il GPS è uno strumento che permette di rilevare la posizione geografica sul veicolo sul quale è installato e grazie all’utilizzo di software dedicati gestire le vetture dell’ordine (qualora ve ne fossero) a tal proposito il garante della privacy ha affrontato tale questione e sottolineato che gli adempimenti che le imprese devono svolgere prima di installare i dispositivi ed iniziare il trattamento dei relativi dati.

Telefoni cellulari dell’Ordine (in caso ve ne fossero):

Il datore di lavoro ha il potere di controllare l'attività lavorativa svolta dei dipendenti sia conforme alle direttive da lui impartite e può farlo anche mediante Sim intestate all'Ordine inserite in telefoni cellulari dati in uso agli stessi.

L'autorità garante propende per l'ammissibilità dei controlli sulle Sim alla duplice condizione che i dati non siano utilizzati per contestazioni disciplinari e che siano conservati per un periodo massimo di sei mesi. Viene affermato un principio di necessità del trattamento in base al quale le informazioni sul traffico telefonico possono essere analizzati solo se necessarie, pertinenti e non eccedenti gli scopi dichiarati. Tali requisiti ricorrono nel caso delle chiamate in uscita ma sono dei scooter liberty per le chiamate in entrata senza specifici addebiti in caso di tariffe flat. In ogni caso poiché il sistema idoneo a realizzare un potenziale indiretto controllo a distanza sull'attività dei dipendenti dovrà comunque essere stipulato uno specifico accordo sindacale nel rispetto della disciplina di settore.

9. ORGANIZZAZIONE PERSONALE: PRINCIPALI SOGGETTI DEL TRATTAMENTO DEI DATI

Nel presente capitolo si definiscono quelli che sono i principali soggetti protagonisti del trattamento dei dati, così come descritti dal nuovo regolamento e viene definito l'organigramma del titolare rispetto all'applicazione della normativa con l'individuazione di vari figure:

Titolare del trattamento dei dati:

Definizione
È la persona fisica o giuridica l'autorità pubblica il servizio o l'ente pubblico (nel caso in oggetto ente pubblico non economico = ordine professionale) o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati. personali.
Aspetto fondamentale quindi è il potere decisionale a lui imputabile in ordine al trattamento dei dati personali.

TITOLARE: ORDINE DEI GEOLOGI DELLA REGIONE UMBRIA

Responsabilità e compiti
L'articolo 24 del regolamento stabilisce la responsabilità generale del titolare del trattamento per qualsiasi trattamento di dati personali che quest'ultimo abbia effettuato direttamente o che altri abbiano effettuato per suo conto.
Il titolare del trattamento deve essere in grado di dimostrare:
- la conformità dell'attività di trattamento con il regolamento stesso e deve mettere in atto misure adeguate di efficaci volti a garantire ciò
- tali misure dovrebbero tener conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento nonché del rischio per i diritti e le libertà delle persone fisiche
- determinare, la probabilità e la gravità del rischio per i diritti e le libertà dell'interessato, sulla base di una valutazione oggettiva, con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento

- utilizzare un possibile i codici di condotta
- adottare procedure interne e attuare misure che soddisfino i principi della protezione dei dati di default ai fini della progettazione.

Contitolari del trattamento:
Si ha contitolarità nel trattamento secondo l'articolo 26 del GDPR quando due o più titolari determinano congiuntamente le finalità e i mezzi del trattamento.
E' necessaria in questo caso una chiara ripartizione delle responsabilità che viene determinata sulla base di un accordo interno con particolare riguardo all'esercizio dei diritti dell'interessato.
Qualora vi fossero contitolari del trattamento verranno nominati con atti separati

Responsabile esterno del trattamento:
È la persona fisica, giuridica, pubblica amministrazione o ente che elabora i dati personali per conto del titolare del trattamento.

Responsabilità e compiti
L'articolo 28 del regolamento elenca i compiti del responsabile esterno del trattamento.
Egli è tenuto a prestare al titolare del trattamento la massima collaborazione ed ha una peculiare responsabilità diretta.
Egli deve possedere garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi requisiti del regolamento.
Egli ha tre obblighi fondamentali:
- obbligo di tracciabilità e trasparenza. Il rapporto fra titolare del trattamento e responsabile esterno del trattamento è disciplinato tramite la contrattualizzazione dei reciproci obblighi. In particolare, il responsabile esterno del trattamento necessita di:
- ricevere per iscritto le istruzioni in ordine ai trattamenti che effettui per conto del titolare del trattamento, da poter così dimostrare che tratta i dati personali soltanto su istruzioni documentata del titolare del trattamento;
- dovrà essere autorizzato per iscritto dal titolare del trattamento ad avvalersi dei Sab di un Sab responsabile nel caso in cui voglia designarne uno;
- dovrà mettere a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi che gli impone l'articolo 28 del regolamento e dovrà consentire e contribuire alle attività di revisione comprese le ispezioni o audit realizzati dal titolare del trattamento;
- dovrà anche tenere il registro dei trattamenti per conto dei titolari del trattamento per cui tratta i dati;
- obbligo di garantire la sicurezza dei dati
Uno specifico obbligo del responsabile esterno del trattamento è quello riferito alla sicurezza dei dati: il responsabile esterno del trattamento non è solo obbligato di adottare tutte le misure che consentano un livello di sicurezza dei dati personali che sia adeguata al rischio, ma deve anche garantire la riservatezza dei trattamenti, deve informare il titolare del trattamento di tutte le violazioni di dati di cui sia venuto a conoscenza, e, una volta terminata la prestazione di servizi, secondo le istruzioni ricevute dal titolare del trattamento, dovrà cancellare tutti i dati o restituirli al titolare del trattamento e cancellare tutte le cose esistenti.

- obbligo di avvisare assistere e consigliare il titolare del trattamento
Al responsabile esterno del trattamento sono posti in capo anche obblighi che implicano una collaborazione col titolare del trattamento che si concreta nell'avvisare, assistere e consigliare il titolare del trattamento in merito al trattamento;
egli inoltre, deve prestare assistenza al titolare del trattamento per consentirgli di evadere le richieste inerenti all'esercizio dei diritti degli interessati.
I responsabili estreni del trattamento sono nominati con separati atti approvati dal Consiglio.

Responsabile della protezione dati (RPD/DPO):
È una figura autonoma indipendente, che svolge i suoi compiti in assenza di conflitto di interesse. In tal senso non può ricoprire tale incarico un soggetto che si trova ai vertici dell'Ordine, quindi in grado di influenzare le scelte adottate in materia di trattamento dati. Il RPD/DPO è designato dal titolare del trattamento o del responsabile esterno del trattamento in base ad un contratto la designazione poi deve essere comunicata all'autorità di controllo nazionale.

Responsabilità e compiti
Informare e consigliare il titolare del trattamento o il responsabile esterno del trattamento nonché i dipendenti, sugli obblighi previsti dalle norme in materia e quindi verificarne l'attuazione e l'applicazione.
Fornire pareri ed assistere il titolare del trattamento in merito alla valutazione di impatto sulla protezione dei dati sorvegliare i relativi adempimenti;
Essere il punto di contatto non solo per il garante ma anche per gli interessati al trattamento in merito a qualunque problematica connessa ai loro dati o all'esercizio dei loro diritti;
Consultare il garante anche di propria iniziativa
Non è però personalmente responsabile dell'inosservanza degli obblighi in materia di protezione dei dati personali.
Risponde solo per lo svolgimento dei suoi obblighi considerati di consulenza e assistenza nei confronti del titolare del trattamento che è l'unico soggetto responsabile del rispetto della normativa.

L'Ordine non è tenuto alla nomina di più RPD/DPO non trattando dati su larga scala.
Il Responsabile Protezione Dati è nominato con apposite contratto approvato dal Consiglio.

Incaricati al trattamento dei dati:
Gli incaricati del trattamento dei dati sono persone autorizzate al trattamento dei dati sotto l'autorità diretta del titolare del trattamento. All'incaricato il titolare del trattamento ed il responsabile esterno del trattamento devono dare istruzioni precise su come deve agire pertanto devono fornire esplicite procedure per il trattamento dei dati personali sotto la loro diretta responsabilità e supervisione.
Sono incaricati al trattamento di dati tutti i dipendenti dell'Ordine.

10. FORMAZIONE

Il regolamento europeo prevede l'obbligo di formazione per tutte le figure che partecipano a trattamento dati. Il titolare del trattamento provvede all'apposita formazione attraverso soggetti esperti in materia.

Il mancato rispetto dell'obbligo formativo comporta la rilevante sanzione amministrativa pecuniaria fino a 10 milioni di euro o per le imprese fino al 2% del fatturato mondiale annuo dell'anno precedente se superiore.

La formazione costituisce, pertanto, una misura di sicurezza per il titolare.
Il titolare effettua formazione interna finalizzata alla conoscenza di requisiti fondamentali per il trattamento dei dati previsti nell'ambito del proprio settore di attività.

L'aggiornamento e la formazione viene posto in essere, come previsto, dal DPO/RPD che provvede sia all'aggiornamento periodico (trimestrale) che alla formazione (quadrimestrale).

11. REGISTRO DEL TRATTAMENTO DATI

Il registro del trattamento dati è uno strumento che parte integrante di quel generale sistema di corretta gestione dei dati personali che il titolare deve porre in essere. L'obbligo di tenuta del registro del trattamento, in forma scritto anche in formato elettronico, sussiste non solo per il titolare del trattamento ma anche per il responsabile esterno del trattamento.

Il registro del trattamento, ai sensi dell'articolo 30 del regolamento europeo 2016/ 279 deve contenere:

- il nome e i dati di contatto del titolare del trattamento e, se presente del contitolari del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dati;
- le finalità del trattamento;
- la descrizione delle categorie di interessati delle categorie di dati personali;
- le categorie di destinatari a cui i dati personali siano stati o saranno comunicati, compresi i destinatari di paesi terzi;
- se presenti, i trasferimenti di dati personali verso paesi terzi la loro identificazione;
- i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- una descrizione generale delle misure di sicurezza tecniche organizzative;
- modalità di trattamento;
- strumenti utilizzati.

Il titolare del trattamento ha predisposto il registro dei trattamenti dati

12. MISURE DI SICUREZZA

Il titolare del trattamento e il responsabile esterno del trattamento mettono in atto misure tecniche organizzative adeguate a garantire un livello di sicurezza adeguato al rischio che comprendono (art. 32):

La pseudominimizzazione e la cifratura dei dati personali; la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; la capacità di ripristinare tempestivamente la disponibilità all'accesso dei dati personali in caso di incidente fisico tecnico; una procedura per testare,

verificare e valutare le coralmente l'efficacia delle misure tecniche organizzative al fine di garantire la sicurezza del trattamento.

13. VALUTAZIONE D'IMPATTO

La valutazione di impatto sulla protezione dei dati è un processo che il titolare del trattamento deve effettuare quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche (art. 35).

La valutazione deve contenere almeno: una descrizione sistematica dei trattamenti previsti delle finalità del trattamento, compreso, se del caso, l'interesse legittimo perseguito dal titolare del trattamento; una valutazione della necessità e proporzionalità dei trattamenti relazione alla 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 crismi per garantire la protezione 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.

La DPIA per quanto può riguardare una sola operazione trattamento dei dati, potrebbe essere utilizzata per valutare molteplici obliterazione di trattamento che sono simili in termini di rischi presentati, purché adeguatamente considerate la specifica natura, portata, contesti e finalità del trattamento.

La valutazione di impatto è necessaria quando i rischi sugli effetti dell'interessato al trattamento sono alti, oppure si ricade nell'ambito di applicazione obbligatoria di impatto. La valutazione di impatto obbligatorio quanto un trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche articolo 35 paragrafo uno come meglio chiarito il paragrafo tre dell'articolo 35 integrato da quanto prevede al paragrafo quattro dello stesso articolo.

La predisposizione e l'espletamento della valutazione di impatto spetta al titolare del trattamento che può farsi consigliare da aiutare da soggetti interni ed esterni o rivolgersi nel caso in cui sia presente al responsabile della protezione dati.

Il titolare nello specifico non è tenuto alla valutazione di impatto in quanto non ricorrono rischi elevati per gli interessati in relazione ai trattamenti effettuati e non si ricade nel campo di applicazione spesso dell'articolo 35 del regolamento.

14. PROCEDURE

1) Gestione protezione dei dati

Lo scopo della presente procedura è quello di definire le modalità operative da adottare per garantire che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali nonché della dignità dell'interessato, con particolare di ferimento alla riservatezza, all'identità personale e al diritto di protezione dei dati personali, così come previsto dal regolamento ware 679/2016.

Il titolare applica a tutti i trattamenti dati questa procedura con le eventuali precisazioni limitazioni esclusioni definitie nella procedura stessa.

La procedura prevede:

- identificare gli interessati del trattamento e fornirgli un'adeguata informativa;

- raccogliere i relativi consensi ad esclusione dei casi in cui ciò non è richiesto;
- definire l'organizzazione per il trattamento dei dati;
- adozione delle misure di sicurezza previste;
- adempimenti periodici;
- monitoraggio e miglioramento del sistema;
- Informativa dipendenti personale interno;
- Informativa e consenso clienti;
- Informativa e consenso dei fornitori;
- Il titolare ha provveduto all'adozione delle misure di sicurezza nel trattamento dei dati;
- Il titolare del trattamento ha previsto che le password vanno modificate almeno ogni sei mesi
- ogni postazione di lavoro è adottata è dotata di adeguato antivirus
- gli antivirus installati dovranno essere aggiornati almeno mensilmente
- Nel caso in cui sia presente una rete interna con accesso di Internet, deve essere prevista la possibilità di istallare un firewall di protezione
- Viene predisposto un backup periodico dei dati
- Per quanto riguarda gli archivi cartacei debbono essere conservati in modo sicuro e, quando non più necessari, saranno distrutti in sicurezza.

2) Gestione formazione

Il titolare provvederà agli obblighi di formazione imposti dalla legge.
La formazione costituisce una misura di sicurezza per il titolare, un onere a carico dello stesso, un diritto e dovere per i dipendenti e collaboratori.
La formazione sarà posta garantita dal RPD/DPO su base periodica come verrà stabilito fra le parti con apposite contratto.

3) Gestione data breach

In caso di violazione dei dati personali il titolare deve reagire con prontezza ed informare tutti soggetti interessati.
Ogni incaricato al trattamento qualora venga a conoscenza di un potenziale caso di perdita di dati avvisa tempestivamente il responsabile esterno del trattamento.
Quest'ultimo, valutato l'evento, se confermate le valutazioni di potenziale data Breach, lo segnala tempestivamente al titolare del trattamento.
Il responsabile esterno del trattamento effettua una valutazione dell'evento sulla scorta delle determinazioni raggiunte predispone l'eventuale comunicazione all'autorità a firma del titolare del trattamento da inviare senza ingiustificato ritardo e ove possibile entro 72 ore determinarsi dal momento del verificarsi di un incidente di sicurezza che riguardi dati personali; oltre il termine 72 ore, la notifica deve essere guardata le ragioni del ritardo.
Il titolare del trattamento effettua una valutazione dell'evento per la corretta analisi della situazione.
Il titolare del trattamento predispone il modello di notifica al garante.
Nel caso in cui la perdita di dati possa causare un rischio elevato per i diritti e le libertà delle persone, anche questi devono essere informati senza ingiustificato ritardo, al fine di consentire loro di prendere i provvedimenti per proteggersi da eventuali conseguenze negative della violazione.

15. **ISTRUZIONI**

Istruzioni per il responsabile esterno del trattamento dati:
Il responsabile esterno al trattamento dei dati personali, deve scrupolosamente attenersi alle istruzioni dettate dal titolare del trattamento.
Il titolare del trattamento ha impartito regole precise al responsabile esterno del trattamento indicando espressamente I seguenti principi di ordine generale:
-principio di liceità
-principio fondamentale di correttezza
-principio di trasparenza
-principio di adeguatezza
-principio di pertinenza
-principio della limitatezza

I dati devono essere raccolti solo per:
-scopi esatti
-conservati per un periodo non superiore a quello necessario
-trattati in modo tale che venga garantita un'adeguata sicurezza
-scopi determinati
-scopi espliciti
-scopi legittimi

Ciascun trattamento deve, inoltre, avvenire nei limiti imposti dal principio fondamentale di riservatezza nel rispetto della dignità della persona dell'interessato al trattamento, ovvero deve essere effettuato eliminando ogni occasione di impropria conoscibilità dei dati da parte di terzi.

Istruzioni per gli incaricati al trattamento dati
Il titolare del trattamento ha incaricati del trattamento dati interni identificati nel/nei dipendenti ai quali ha impartito le precise istruzioni per il trattamento dei dati personali;

****

Il presente disciplinare è stato redatto dal titolare del trattamento per l'integrazione dell'adeguamento al GDPR.
Sono state redatte apposite informative ed il registro del trattamento dati con atti separati ed in possesso del titolare del trattamento.