CENTRO STUDI
CONSIGLIO NAZIONALE DEI GEOLOGI

CONSIGLIO NAZIONALE
DEI GEOLOGI

LINEE GUIDA
PER GLI ORDINI NAZIONALE E REGIONALI DEI GEOLOGI
ALL'APPLICAZIONE DEL REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI PERSONALI
(REGOLAMENTO UE N. 679/2016 - GDPR)

PARTE GENERALE

1. LE LINEE GUIDA

Il trattamento dei dati è attività centrale e cruciale per ogni ordine professionale.

Gli Ordini, sia quello Nazionale sia quelli Regionali, dei Geologi (di seguito singolarmente "**Ordine**" e cumulativamente "**Ordini**") sono, pertanto, chiamati ad uniformarsi alle prescrizioni del Regolamento Europeo n. 679/2016 in materia di protezione di dati personali (di seguito "**Regolamento**" o "**GDPR**") entro il prossimo 25 maggio 2018.

L'attività di adeguamento alle previsioni del Regolamento richiede un consistente impegno sia in termini di analisi delle previsioni applicabili sia in termini di esame delle esistenti fattispecie e condizioni di trattamento dei dati personali sia in termini di intervento di modifica e adeguamento della propria organizzazione.

Nella consapevolezza della crucialità del trattamento dei dati nell'ambito delle attività istituzionali degli Ordini e, allo stesso tempo, della complessità e gravosità delle analisi e indagini richieste, nonché dei conseguenti adempimenti, per conformarsi alla nuova normativa europea, con le presenti Linee Guida si è inteso fornire indicazioni agli Ordini medesimi al fine di agevolarne il processo di adeguamento alle disposizioni del Regolamento.

Con il preliminare chiarimento sull'obbligo per ciascun Ordine di adempiere autonomamente alle previsioni in materia di protezione dei dati personali, in quanto autonomi titolari dei trattamenti effettuati nello svolgimento delle proprie attività istituzionali, le presenti Linee Guida intendono, in particolare, fornire agli Ordini gli strumenti utili:

i) a comprendere le principali novità della nuova disciplina, riservando, però, particolare attenzione – anche nelle conclusioni dei singoli paragrafi – ai concreti impatti che le stesse hanno sul modello organizzativo dell'Ordine (nella "Parte generale");

ii) a proporre una serie di misure ed interventi concreti da adottare al fine di conformarsi al Regolamento (nella "Parte speciale"), ove occorra, mediante proposizione di appositi schemi esemplificativi (negli "Allegati").

Le misure e gli interventi proposti sono stati, in ogni caso, elaborati tenendo conto della generalità delle fattispecie di trattamenti che coinvolgono gli Ordini, che singolarmente hanno, quindi, l'onere di verificare, anche nel corso del tempo, l'adeguatezza delle proposte contenute nelle presenti Linee Guida per le eventuali peculiarità specifiche dello stesso Ordine.

2. IL REGOLAMENTO PRIVACY EUROPEO – GDPR

INTRODUZIONE

Il Regolamento disciplina la protezione delle persone fisiche, con riguardo al trattamento dei dati personali ed alla loro libera circolazione, introducendo, su questi temi, una legislazione uniforme e valida per tutta l'Europa.

Il GDPR è stato approvato dal Parlamento europeo il 14 aprile 2016 ed è, dunque, attualmente già in vigore, ma diverrà definitivamente applicabile in tutti gli Stati membri a partire dal 25 maggio 2018.

Il Regolamento nasce da precise esigenze, come indicato dalla stessa Commissione europea, di certezza giuridica, armonizzazione e maggiore semplicità delle norme riguardanti il trasferimento di dati personali dall'Unione Europea (di seguito "**UE**") verso altre parti del mondo

Il GDPR ha abrogato la direttiva 95/46/CE, ossia il Regolamento generale sulla protezione dei dati, che aveva impegnato gli Stati membri ad emanare, ciascuno, una propria legge nazionale sulla protezione dei dati personali.

L'Italia, in ottemperanza, aveva dapprima emanato la Legge 675/96, poi sostituita dal D.Lgs. 196/2003 (di seguito "**Codice della privacy**").

Il GDPR consta di 99 articoli ed è preceduto da 173 "considerando", che non hanno carattere normativo, bensì valore interpretativo del corpo del testo, laddove non apparisse chiaro o risultasse impreciso.

Trattandosi di un regolamento, non necessita di recepimento da parte degli Stati dell'Unione e verrà attuato allo stesso modo in tutti gli Stati dell'UE, senza margini di libertà nell'adattamento. Il suo scopo è, infatti, la definitiva armonizzazione della regolamentazione in materia di protezione dei dati personali all'interno dell'Unione.

Il Regolamento è direttamente applicabile senza necessità di leggi nazionali di recepimento. Entro il 25 Maggio è necessario garantire la piena conformità.

RAPPORTI CON LA LEGISLAZIONE NAZIONALE

Il Codice della privacy non risulta abrogato, ma subisce una rilettura in chiave di GDPR.

Sarà, pertanto, disapplicata la legge statale in favore del Regolamento, laddove vi sia incompatibilità tra le due norme; mentre essa rimarrà applicabile in caso di compatibilità e, soprattutto, ove il Codice della privacy disciplini in maniera più dettagliata ambiti che il Regolamento non approfondisce.

Le previsioni del Codice della privacy devono comunque essere rispettate.

AMBITO DI APPLICAZIONE

Il GDPR disciplina il trattamento dei dati personali relativi alle persone fisiche da parte di entità terze aventi o meno personalità giuridica.

Il Regolamento non si applica, quindi, al trattamento dei dati personali di persone decedute o di persone giuridiche.

Relativamente all'ambito territoriale, per mera completezza, si ricorda che l'articolo 3 del Regolamento prevede, innanzitutto, la propria operatività quando il titolare o il responsabile siano stabiliti nell'UE, a prescindere da dove avvenga il trattamento dei dati.

Sotto il profilo "passivo", il Regolamento si applica, invece, al trattamento di dati personali di interessati che si trovino nell'UE, indipendentemente da dove si trovi il titolare o il responsabile del trattamento. L'operatività della norma è, quindi, condizionata solo al fatto che le attività di trattamento riguardino l'offerta di beni o la prestazione di servizi agli interessati o il monitoraggio del loro comportamento all'interno dell'UE.

In tal modo l'applicazione del GDPR tutela tutti gli interessati che sono nel territorio dell'UE, indipendentemente da dove si attui il trattamento dei loro dati.

Chiunque tratti dati personali in "ambito" territoriale UE è sottoposto al GDPR.

COS'È UN DATO PERSONALE

Nell'articolo 4 del GDPR si definisce "**dato personale**" qualsiasi informazione riguardante una persona fisica identificata o identificabile ("**interessato**"); si considera identificabile la persona fisica che può essere individuata, 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.

Ai sensi delle definizioni presenti nel Codice della privacy:

- i dati sensibili sono quelli che possono rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, lo stato di salute e la vita sessuale;

- i dati giudiziari sono quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o, anche, di indagato.

Il GDPR non definisce più i dati sensibili, ma categorie di dati particolari, facendovi rientrare espressamente anche dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica e dati relativi all'orientamento (oltre che alla vita) sessuale.

Lo stesso Regolamento identifica i dati giudiziali con i dati personali relativi a condanne penali e reati, senza riportarne una definizione.

I dati personali sono tutte le informazioni inerenti una persona fisica ("interessato"), ivi inclusi quelli appartenenti a categorie particolari o relativi a condanne penali e reati.

COSA SI INTENDE PER TRATTAMENTO

L'articolo 4 del GDPR definisce "**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.

Per trattamento si intende qualsiasi operazione compiuta ed applicata a dati personali.

CHI È IL TITOLARE

Ai sensi dell'articolo 4 del GDPR, il "**titolare del trattamento**" è 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'UE o dei suoi Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'UE o dei suoi Stati membri.

Il titolare del trattamento è l'entità che determina le finalità e i mezzi del trattamento di dati personali.

CHI È IL RESPONSABILE

Secondo l'articolo 4 del GDPR, il "**responsabile del trattamento"** è la persona fisica o giuridica, la pubblica amministrazione oppure l'ente che elabora i dati personali per conto del titolare del trattamento.

Si tratta di un soggetto, distinto dal titolare, che deve essere in grado di fornire garanzie al fine di assicurare il pieno rispetto delle disposizioni in materia di trattamento dei dati personali, nonché di garantire la tutela dei diritti dell'interessato.

RESPONSABILE INTERNO

Vale la pena chiarire che in Italia l'applicazione della normativa in materia di privacy è stata caratterizzata negli anni anche dalla presenza della figura del responsabile interno del trattamento. A questa figura, il titolare poteva delegare una serie di responsabilità in merito al trattamento dei dati personali effettuati dalla propria organizzazione.

Il GDPR non fa alcun cenno alla figura del responsabile interno e, ai sensi della nuova disciplina europea, chiunque, all'interno di una organizzazione, effettui operazioni di trattamento è "*persona autorizzata al trattamento dei dati personali sotto l'autorità diretta del titolare*". Se ne deduce che la figura del soggetto autorizzato, di cui si dirà

meglio nel paragrafo che segue, corrisponde alla "vecchia" figura dell'incaricato del trattamento ai sensi del Codice della privacy.

Pertanto, lo svolgimento di operazioni di trattamento dei dati personali effettuate all'interno di un'organizzazione da parte di un dipendente o collaboratore della stessa rientra tra le mansioni assegnate a questi ultimi ed è, pertanto, disciplinato nell'ambito del rapporto di lavoro instaurato tra il titolare e il dipendente o collaboratore stesso.

In estrema sintesi, l'eventuale nomina di un responsabile interno non avrebbe alcuna rilevanza esterna e, comunque, non diminuirebbe in alcun modo la responsabilità del titolare.

RESPONSABILE ESTERNO

Quando il soggetto a cui è demandato in tutto o in parte il trattamento di dati personali da parte del titolare è un soggetto esterno all'organizzazione di quest'ultimo, la nomina dello stesso come responsabile del trattamento non solo è necessaria, ma deve avvenire per iscritto in virtù di apposito contratto o previsione inclusa in un contratto tra il titolare ed il responsabile stesso.

In forza del menzionato contratto, il responsabile del trattamento si obbliga a:

- trattare i dati personali solo sulla base di un'istruzione documentata del titolare del trattamento;
- garantire che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
- adottare tutte le misure richieste dall'articolo 32 del GDPR, ovvero le misure tecniche e organizzative necessarie al fine di garantire un livello di sicurezza adeguato al rischio;
- rispettare tutte le condizioni previste per l'eventuale nomina di un sub-responsabile;
- assistere il titolare del trattamento con misure tecniche e organizzative adeguate, e tenuto conto della natura del trattamento, al fine di soddisfare l'obbligo di dare seguito alle richieste per l'esercizio dei diritti dell'interessato;
- assistere il titolare del trattamento nel garantire il rispetto degli obblighi in materia di tutela della sicurezza dei dati;
- su indicazione del titolare del trattamento, cancellare o restituire tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento o dopo che è terminato il tempo di conservazione previsto dal titolare e conforme alle prescrizioni del regolamento;
- mettere a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto dei suoi obblighi;
- contribuire alle attività di revisione, comprese le ispezioni, realizzate dal titolare del trattamento o da un altro soggetto da lui incaricato;
- informare immediatamente il titolare del trattamento qualora ritenga che un'istruzione del titolare violi il Regolamento o altre disposizioni nazionali o di diritto europeo relative alla protezione dei dati.

Una novità importante rispetto alla disciplina del Codice della privacy è quella che riguarda la possibilità per il responsabile di nominare dei sub-responsabili del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare.

A questo proposito, è previsto che il responsabile del trattamento possa ricorrere ad un altro responsabile solo previa autorizzazione scritta (che può essere, però, sia specifica che generale) del titolare del trattamento.

L'eventuale nomina di uno o più sub-responsabili del trattamento (attraverso un contratto o altro atto giuridico equivalente) dovrà avvenire nel rispetto degli stessi obblighi in materia di protezione dei dati sanciti in capo al responsabile "primario" del trattamento.

Il responsabile del trattamento è l'entità che elabora i dati personali per conto del titolare del trattamento, che, con il GDPR, ove appartenente all'organizzazione di quest'ultimo, si identifica con il mero soggetto autorizzato al trattamento.

I SOGGETTI AUTORIZZATI

Il Codice della privacy prevedeva la figura degli "**incaricati**", quali persone fisiche autorizzate dal titolare o dal responsabile del trattamento a compiere operazioni di trattamento; a tale fine, l'articolo 30 del Codice della privacy prevedeva l'obbligo di nominare formalmente gli incaricati con atto scritto.

Nell'ambito del GDPR gli incaricati corrispondono alle "*persone autorizzate al trattamento*", cioè a coloro che svolgono il trattamento sotto l'autorità diretta del titolare o del responsabile.

Il Regolamento non prevede espressamente l'obbligo di nomina scritta dei soggetti autorizzati.

Pur non essendovi questo obbligo di designazione formale, la scelta del titolare che volesse mantenere le precedenti nomine degli incaricati o effettuarne di nuove, purché conformi al nuovo approccio introdotto dal GDPR, non potrebbe risultare incompatibile con le prescrizioni di quest'ultimo.

Va, tuttavia, precisato che, più dell'atto formale di nomina, come si vedrà meglio di seguito, è fondamentale "l'istruzione" di tali soggetti al rispetto delle norme in materia di protezione dei dati personali; sarà, quindi, opportuno prevedere percorsi formativi adeguati per coloro che saranno coinvolti a tale titolo nel trattamento dati.

Nel GDPR gli incaricati corrispondono alle persone autorizzate al trattamento, cioè a coloro che svolgono il trattamento sotto l'autorità diretta del titolare o del responsabile.

LE SANZIONI

L'articolo 83 del GDPR prevede che la violazione delle disposizioni del Regolamento possa comportare l'applicazione di sanzioni amministrative pecuniarie fino a 10 o 20 milioni di euro a seconda dei casi, o pari rispettivamente al 2% o al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

La decisione sull'applicazione delle sanzioni spetta all'autorità di controllo (in Italia: l'Autorità Garante per la Protezione dei Dati Personali), che, nella valutazione, tiene conto delle circostanze del singolo caso, ossia:

– della natura, gravità e durata della violazione;

– del carattere doloso o colposo della violazione;

– delle misure adottate per attenuare il danno subito dagli interessati;

– delle eventuali precedenti violazioni commesse dal titolare del trattamento;

– del grado di cooperazione con l'autorità di controllo;

– degli eventuali altri fattori aggravanti.

Sono previste sanzioni pecuniarie per le ipotesi di violazione del GDPR.

3. LE PRINCIPALI NOVITÀ DEL GDPR

Il Regolamento cambia profondamente la prospettiva in cui si colloca la protezione dei dati personali.

Il GDPR riconosce il diritto alla protezione dei dati personali come diritto fondamentale, la cui tutela si fonda non più sull'adempimento prevalentemente formale, ma su un approccio fortemente sostanziale ed incentrato

sulla responsabilità di assicurare e mantenere la conformità al Regolamento, nonché di tutelare i diritti e la dignità degli interessati.

Non è più sufficiente adeguarsi alle prescrizioni delle norme che disciplinano la tutela dei dati personali, ma diventa necessario dimostrare di avere adottato un processo complessivo di misure organizzative e tecniche per la protezione dei dati personali (principio di accountability).

È richiesta maggiore trasparenza.

È necessaria maggiore tutela nel trattamento dei dati.

Vi è un ampliamento delle garanzie e dei diritti azionabili dall'interessato per il controllo dei propri dati.

IL PRINCIPIO DI ACCOUNTABILITY

La principale novità introdotta dal Regolamento è il principio di "responsabilizzazione" (cd. *accountability*), che attribuisce direttamente al titolare del trattamento il compito di assicurare, ed essere in grado di comprovare, il rispetto dei principi applicabili al trattamento dei dati personali.

La novità introdotta si traduce in un approccio completamente diverso nel trattamento dei dati personali, che demanda al titolare il compito di decidere autonomamente le modalità ed i limiti del trattamento dei dati.

Spetta al titolare ed ai responsabili del trattamento stabilire, in autonomia, le misure tecniche ed organizzative per quest'ultimo, nonché valutarne la relativa adeguatezza, nella consapevolezza che l'Autorità Garante per la Protezione dei Dati Personali potrebbe considerare quella valutazione inadeguata o insufficiente, applicando, di conseguenza, una sanzione.

Questa è una grande novità in termini di approccio: il GDPR non contiene prescrizioni puntuali o tassative, ma demanda al titolare la dimostrazione di aver protetto in modo adeguato i dati trattati in conformità ai principi in esso contenuti.

Il Regolamento non fornisce indicazioni precise su quali siano le misure pratiche da adottare: l'approccio dovrà essere valutato caso per caso, tenendo in considerazione la natura, l'ambito di applicazione, il contesto e le finalità del trattamento.

MAGGIORE TRASPARENZA

Il GDPR introduce una generale maggiore trasparenza nella gestione dei trattamenti.

Il titolare è tenuto ad adottare misure appropriate per fornire all'interessato tutte le informazioni relative ai trattamenti gestiti dalla propria organizzazione, in forma concisa, trasparente, intelligibile e facilmente accessibile.

Il titolare è tenuto, altresì, ad agevolare l'esercizio dei diritti da parte dell'interessato e, in particolare, a fornire un riscontro alla richiesta del medesimo senza ingiustificato ritardo e, comunque, entro un mese dal ricevimento della medesima (prorogabile di due mesi ove necessario, tenuto conto della complessità e del numero delle richieste).

È, infine, necessario fornire all'interessato informazioni sul periodo di conservazione e sul diritto di reclamo all'Autorità Garante per la Protezione dei Dati Personali.

Sulla base di questo incremento degli obblighi di trasparenza e comunicativi, le informazioni all'interessato devono essere date:

- con linguaggio semplice e chiaro;

- in forma scritta.

MAGGIORE TUTELA NEL TRATTAMENTO DEI DATI

L'articolo 25 del GDPR introduce i principi di *privacy by design* e di *privacy by default*, che introducono un approccio concettuale innovativo teso alla garanzia di una tutela effettiva dei dati personali trattati.

Il principio di *privacy by design* prevede che il titolare dovrà valutare il rischio inerente alle attività di trattamento che sta per avviare. Tale valutazione andrà fatta al momento della progettazione dell'attività che comporterà il trattamento dei dati, quindi prima che il trattamento inizi. In tale valutazione si dovrà tenere conto anche del tipo di dati trattati.

Il principio di *privacy by default* stabilisce, invece, che, per impostazione predefinita, i titolari ed i responsabili devono trattare i dati personali solo nella misura strettamente necessaria e sufficiente per le finalità previste e per il periodo strettamente necessario a tali fini. Occorre, quindi, progettare il sistema di trattamento di dati garantendo la non eccessività dei dati raccolti.

MAGGIORI GARANZIE E POTERI ALL'INTERESSATO

Il GDPR individua diverse possibilità per consentire al soggetto interessato di tutelare i propri dati personali.

DIRITTO DI ACCESSO

L'articolo 15 del Regolamento prevede il diritto dell'interessato di accesso, cioè il diritto di conoscere quali dati personali il titolare sta trattando e con quali finalità, nonché di ricevere una copia (gratuita) dei dati.

I titolari possono eventualmente anche consentire un accesso diretto ai dati da remoto.

Con l'esercizio di detto diritto l'interessato può chiedere di conoscere:

- le finalità del trattamento;
- le categorie di dati personali trattate;
- i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di Paesi terzi rispetto all'UE o organizzazioni internazionali, e le garanzie applicate in caso di trasferimento dei dati verso Paesi terzi;
- 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;
- l'esistenza del 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, e informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

DIRITTO DI LIMITAZIONE DEL TRATTAMENTO

L'articolo 4 del GDPR definisce espressamente cosa si intende per "**limitazione di trattamento**", ossia il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro.

L'articolo 18 del GDPR elenca, invece, le ipotesi in cui l'interessato può esercitare il diritto di limitare l'utilizzo dei suoi dati personali al solo fine della conservazione dei medesimi; in particolare, affinché l'interessato possa esercitare tale diritto deve ricorrere almeno una delle seguenti ipotesi:

- l'interessato contesta l'esattezza dei dati personali;
- il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali;
- i dati sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria, mentre al titolare del trattamento non servono più a fini del trattamento;

- l'interessato si è opposto al trattamento e si è in attesa delle verifiche necessarie per determinare se i motivi legittimi del titolare del trattamento prevalgano su quelli dell'interessato.

DIRITTO ALLA CANCELLAZIONE (OBLIO)

Il GDPR introduce il diritto dell'interessato ad ottenere la cancellazione dei propri dati personali se non pertinenti o non più pertinenti, o se inadeguati rispetto alle finalità del trattamento, o se l'interessato abbia revocato il proprio consenso, o qualora i dati siano trattati in modo illecito.

È opportuno evidenziare che detto diritto all'oblio può essere limitato se ricorre una delle ipotesi elencate dal comma 3 dell'articolo 17 del Regolamento, tra i quali risultano di maggiore interesse la garanzia della libertà di espressione, l'adempimento di un obbligo legale, l'esecuzione di compiti svolti nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

DIRITTO ALLA PORTABILITÀ DEI DATI

Il diritto alla portabilità dei dati è un nuovo diritto previsto dal Regolamento.

Il diritto alla portabilità consente all'interessato di ricevere, in un formato strutturato, di uso comune e leggibile da dispositivo automatico, i dati personali che lo riguardano, forniti a un titolare del trattamento, e di trasmettere tali dati a un altro titolare senza impedimenti.

Affinché sia possibile esercitare il diritto alla portabilità dei dati occorre, dunque, che sussistano le seguenti condizioni:

1. trattamento effettuato con mezzi automatizzati;
2. trattamento basato sul consenso dell'interessato o contratto di cui è parte l'interessato;
3. dati personali relativi all'interessato;
4. dati forniti dall'interessato.

MODALITÀ DI ESERCIZIO DEI DIRITTI

Le modalità per l'esercizio di tutti i diritti da parte degli interessati sono stabilite, in via generale, negli articoli 11 e 12 del Regolamento.

L'interessato può rivolgersi direttamente al titolare del trattamento per l'esercizio dei suoi diritti.

Anche se è solo quest'ultimo obbligato a dare riscontro, il responsabile del trattamento è tenuto a collaborare col titolare.

In caso di mancata risposta, o di risposta inadeguata, l'interessato può rivolgersi all'Autorità Garante per la Protezione dei Dati Personali o all'autorità giudiziaria per la tutela dei suoi diritti.

Il termine per la risposta è, in ogni caso, di 1 mese.

Tale termine può essere esteso a 3 mesi in ipotesi di particolare complessità. In questo caso, il titolare del trattamento deve, comunque, avvertire l'interessato entro un mese.

L'esercizio dei diritti è in linea di massima gratuito. Spetta, comunque, al titolare valutare se la propria risposta è complessa al punto da dover chiedere un contributo all'interessato e stabilirne l'ammontare, ma ciò solo se si tratta di richieste manifestamente infondate, eccessive o ripetitive.

La risposta si deve fornire, di regola, in forma scritta, anche attraverso strumenti elettronici. Può essere orale solo se espressamente richiesta in tal senso dall'interessato.

La risposta del titolare deve essere, in ogni caso, chiara e coincisa, nonché facilmente accessibile e comprensibile.

4. IN PRATICA: I NUOVI OBBLIGHI

LA NOMINA DEL RESPONSABILE DELLA PROTEZIONE DEI DATI

L'articolo 37 del GDPR prevede che il titolare del trattamento e il responsabile del trattamento designano un responsabile della protezione dei dati (*Data Protection Officer*, di seguito "**DPO**") quando "il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali; le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala", nonché quando "le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali".

I COMPITI DEL DPO

Il DPO dovrà, in particolare:

- sorvegliare l'osservanza del Regolamento, valutando i rischi di ogni trattamento alla luce della natura, dell'ambito di applicazione, del contesto e delle finalità;
- collaborare con il titolare/responsabile, laddove necessario, nel condurre una valutazione di impatto sulla protezione dei dati;
- informare e sensibilizzare il titolare o il responsabile del trattamento, nonché i dipendenti di questi ultimi, riguardo agli obblighi derivanti dal Regolamento e da altre disposizioni in materia di protezione dei dati;
- cooperare con l'Autorità Garante per la Protezione dei Dati Personali e fungere da punto di contatto per quest'ultima su ogni questione connessa al trattamento;
- supportare il titolare o il responsabile in ogni attività connessa al trattamento di dati personali, anche con riguardo alla tenuta di un registro delle attività di trattamento.

I REQUISITI DEL DPO

Il paragrafo 5 dell'allegato A alle "*Linee guida sui responsabili della protezione dei dati*" – adottate il 13 dicembre 2016 dal Gruppo di Lavoro sulla tutela delle persone fisiche con riguardo al trattamento dei dati personali, istituito dalla direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 (di seguito "**Gruppo di Lavoro art. 29**") –, successivamente emendate in data 5 aprile 2017, chiarisce che il DPO "*è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti* [...]".

Il livello necessario di conoscenza specialistica dovrebbe essere determinato in base ai trattamenti di dati effettuati ed alla protezione richiesta per i dati personali oggetto di trattamento.

È necessaria la nomina di un *Data Protection Officer – DPO*, avente specifici requisiti e competenze, ai fini dello svolgimento di determinate funzioni di protezione dei dati.

IL REGISTRO DEI TRATTAMENTI

L'articolo 30 del GDPR prevede che sia il titolare sia il responsabile del trattamento devono tenere un registro dei trattamenti (di seguito "**Registro dei trattamenti**").

Il Registro dei trattamenti deve contenere una serie di informazioni, tra cui le finalità del trattamento, la descrizione delle categorie di interessati e di dati personali che vengono trattati, oltre che l'indicazione delle misure di sicurezza adottate.

La tenuta del Registro dei trattamenti costituisce un adempimento di fondamentale importanza nell'ottica del principio di *accountability* di cui si è detto sopra, in quanto permette di conoscere e monitorare in maniera approfondita le operazioni di trattamento all'interno dell'organizzazione.

Il Registro dei trattamenti costituisce, dunque, sia uno strumento operativo di lavoro con cui mappare in maniera ordinata tutti i trattamenti effettuati e, per l'effetto, i dati trattati, sia un vero e proprio strumento attraverso cui provare di aver adempiuto alle prescrizioni del Regolamento.

Considerata tale ulteriore finalità, può essere opportuno indicare nel Registro dei trattamenti una serie di elementi non espressamente imposti dall'articolo 30 del GDPR, ma che si riveleranno importanti per tener traccia delle operazioni di trattamento effettuate. Tra questi, ad esempio, la base giuridica del trattamento, che, di regola, deve essere obbligatoriamente citata nell'informativa.

Il titolare o il responsabile dei trattamenti istituiscono e tengono un dettagliato registro di questi ultimi.

LA VALUTAZIONE D'IMPATTO

La valutazione d'impatto sulla protezione dei dati (*Data Protection Impact Assessment*, di seguito "**DPIA**") è uno dei nuovi adempimenti previsti dal GDPR, che, all'articolo 35, prevede il suo svolgimento da parte del titolare quando un trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

L'articolo 35 del GDPR riporta un elenco, esemplificativo e non esaustivo, dei trattamenti soggetti a DPIA, prevedendone l'obbligo quando essi siano relativi:

- ad una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
- al trattamento, su larga scala, di dati sensibili (articolo 9) o di dati giudiziari (articolo 10);
- alla sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Vista la complessità e l'assoluta novità dell'adempimento introdotto, il Gruppo di Lavoro art. 29 è intervenuto sul tema, pubblicando delle apposite Linee guida, modificate da ultimo il 4 ottobre 2017. Le Linee guida offrono al titolare validi strumenti per condurre efficacemente la valutazione sull'obbligatorietà della DPIA.

Il Gruppo di Lavoro art. 29, infatti, ha individuato 9 indici di "rischiosità" del trattamento e ha chiarito che maggiore è il numero di criteri soddisfatti dal trattamento, più è probabile che sia presente un rischio elevato per i diritti e le libertà degli interessati e, di conseguenza, che sia necessario una DPIA.

Il Gruppo di Lavoro art. 29 ritiene, inoltre, che una DPIA non sia richiesta nei seguenti casi:

- quando 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 già stato svolto una DPIA;
- quando le tipologie di trattamento sono state verificate da un'autorità di controllo prima del maggio 2018 in condizioni specifiche che non hanno subito modifiche;
- qualora un trattamento trovi una base giuridica nel diritto dell'UE o di un suo Stato membro, tale diritto disciplini il trattamento specifico o sia già stata effettuata una DPIA nel contesto dell'adozione di tale base giuridica;
- qualora il trattamento sia incluso nell'elenco facoltativo (stabilito dall'autorità di controllo) delle tipologie di trattamento per le quali non è richiesta alcuna valutazione d'impatto sulla protezione dei dati.

Relativamente all'ultimo punto dell'elenco dei casi di esclusione, va precisato che ulteriori e, auspicabilmente, risolutivi chiarimenti si attendono ancora dall'elenco che l'Autorità Garante per la Protezione dei Dati Personali dovrà pubblicare ai sensi dell'articolo 35 del GDPR e che dovrà contenere, appunto, le tipologie di trattamenti da ritenersi soggetti al requisito della valutazione di impatto.

Il soggetto obbligato ad effettuare una DPIA è il titolare del trattamento con il supporto del DPO, se nominato, e del responsabile del trattamento eventualmente coinvolto.

Al titolare del trattamento spetta, quindi, di assicurare che la DPIA venga eseguita, assumendosene l'intera responsabilità. Il titolare del trattamento è tenuto, poi, a consultarsi con il DPO, qualora designato, e dovrà attenersi al parere ricevuto.

In un'ottica di efficientamento, il Gruppo di Lavoro art. 29 ha chiarito che un processo di DPIA può riguardare una singola operazione di trattamento dei dati, ma si può ricorrere ad una singola DPIA anche nel caso di trattamenti multipli simili tra loro in termini di natura, ambito di applicazione, contesto, finalità e rischi.

In ogni caso, il titolare può ritenere che un trattamento che soddisfi soltanto uno di suddetti 9 criteri individuati dal Gruppo di Lavoro art. 29 richieda lo svolgimento di una DPIA.

Così come un trattamento può corrispondere ai casi di cui ai medesimi criteri ed essere comunque considerato dal titolare tale da non "presentare un rischio elevato". In tali ipotesi il titolare del trattamento dovrà, però, necessariamente giustificare e documentare i motivi che lo hanno spinto a non effettuare una DPIA, nonché allegare il parere del DPO, se presente.

È richiesta un *Data Protection Impact Assessment - DPIA* quando un trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

LE MISURE DI SICUREZZA

L'articolo 32 del GDPR dispone, come sopra accennato, che il titolare del trattamento debba adottare delle misure tecniche ed organizzative idonee al fine di assicurare, ed essere poi in grado di dimostrare, che il trattamento dei dati personali è realizzato in modo conforme alla disciplina dettata dal Regolamento stesso.

Più nello specifico l'articolo 32 del GDPR impone ai titolari di garantire la sicurezza dei trattamenti attraverso l'adozione di una serie di procedure concrete che siano idonee ad assicurare un livello adeguato per prevenire i rischi per i dati personali determinati dagli specifici trattamenti.

Al fine di effettuare la valutazione di adeguatezza delle misure richiesta si dovrà tener conto dell'attuale stato dell'arte (della tecnologica disponibile, dei sistemi informatici, ecc.), dei costi di attuazione, della natura dei dati e dei meccanismi adottati, del campo di applicazione, del contesto e delle finalità del trattamento dei dati, oltre che del rischio per i diritti e le libertà delle persone fisiche, che può essere più o meno probabile e più o meno alto a seconda di ciascun diverso contesto.

In pratica, non esiste più un obbligo generalizzato di adozione di misure minime di sicurezza, come previsto attualmente dall'articolo 33 del Codice della privacy e dal relativo allegato tecnico che contiene le misure minime di sicurezza che tutti i titolari dovevano indistintamente adottare.

Sempre l'articolo 32 del GDPR propone una lista di possibili misure da adottare, che sono:

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

È importante, tuttavia, ribadire che la lista è meramente esemplificativa. Ciò vuol dire, in concreto, che non è possibile ritenere né sufficiente né necessaria l'adozione delle misure di sicurezza riportate all'interno dell'articolo 32 del GDPR. Spetta, infatti, al titolare e al responsabile del trattamento valutare, caso per caso, in rapporto ai rischi specificamente individuati, quali misure adottare.

LE MISURE MINIME DEL CODICE DELLA PRIVACY

Come indicato anche dall'Autorità Garante per la Protezione dei Dati Personali nella Guida all'applicazione del Regolamento in materia di protezione dei dati personali, non potranno sussistere dopo il 25 maggio 2018 obblighi generalizzati di adozione di misure "minime" di sicurezza.

Tuttavia – rileva il Garante – "*facendo anche riferimento alle prescrizioni contenute, in particolare, nell'Allegato "B" al Codice, l'Autorità potrà valutare la definizione di linee-guida o buone prassi sulla base dei risultati positivi conseguiti in questi anni*".

In concreto allora, le misure minime di sicurezza non potranno continuare a essere considerate misure obbligatorie, ma è possibile ritenere che esse rappresentino il nucleo centrale minimo per garantire la sicurezza dei dati. Spetta poi al titolare e al responsabile del trattamento, ai sensi dell'articolo 32 del GDPR, analizzando specificamente i rischi legati al trattamento dei dati, valutare, oltre a questo nucleo, se e quali misure di sicurezza tecniche e organizzative adottare.

Il titolare del trattamento deve adottare misure tecniche ed organizzative idonee al fine di assicurare, ed essere poi in grado di dimostrare, che il trattamento dei dati personali è realizzato in modo conforme alla disciplina dettata dal GDPR.

DATA BREACH

Secondo il Regolamento per "**violazione dei dati personali**" si deve intendere "*ogni violazione della 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.*"

Importante chiarire, dunque, che un *data breach* non è solo un attacco informatico, ma può essere anche un accesso abusivo, un incidente (es. un incendio), una semplice perdita di una chiavetta USB o una sottrazione di documenti con dati personali.

Una delle novità più significative introdotte dal Regolamento consiste nell'obbligo, per amministrazioni pubbliche e aziende, di comunicare all'Autorità Garante per la Protezione dei Dati Personali i casi di *data breach*, cioè tutte le violazioni della sicurezza informatica in grado di comportare la perdita, distruzione o diffusione indebita dei dati personali trattati.

Tale segnalazione all'Autorità Garante per la Protezione dei Dati Personali deve essere effettuata dal titolare del trattamento in modo chiaro e specifico.

La notifica deve avere il contenuto previsto dall'articolo 33 del GDPR:

- descrivendo la natura della violazione dei dati personali, compresi, ove possibile, le categorie ed il numero approssimativo di interessati in questione, nonché le categorie ed il numero approssimativo di registrazioni dei dati personali in questione;
- comunicando il nome e i dati di contatto del DPO o di altro punto di contatto presso cui ottenere più informazioni;
- descrivendo le probabili conseguenze della violazione dei dati personali;
- descrivendo 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.

Nei casi più gravi, 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 è obbligato a comunicare la violazione anche agli interessati a cui si riferiscono i dati, senza ingiustificato ritardo.

Vanno comunicati all'Autorità Garante per la Protezione dei Dati Personali i casi di *data breach*, cioè le violazioni della sicurezza informatica in grado di comportare la perdita, distruzione o diffusione indebita dei dati personali trattati.

5. IL PIANO DI ADEGUAMENTO

Alla luce delle novità introdotte dal GDPR, sopra sinteticamente analizzate, il processo di adeguamento al Regolamento deve necessariamente partire da una mappatura dei trattamenti effettuati e da un'analisi delle condizioni e modalità di trattamento degli stessi.

Tale attività si rivelerà prodromica per qualsiasi ulteriore attività di *compliance* con la normativa in esame, oltre che base per il compimento di specifici adempimenti.

Il successivo essenziale passo sarà lo svolgimento della *gap analysis* (analisi delle carenze), che è finalizzata all'individuazione delle possibili azioni correttive del corrente sistema privacy, richieste per adeguarsi al Regolamento.

Dalla *gap analysis*, che includerà anche una verifica dei documenti privacy fino ad ora utilizzati, verosimilmente emergerà la necessità di adeguare sia i testi delle informative sia i testi di contratti con eventuali responsabili esterni per renderli conformi alle nuove prescrizioni.

In caso di esito positivo della verifica sull'obbligatorietà della sua nomina, il titolare dovrà procedere alla selezione e designazione del DPO.

Andranno poi predisposti i nuovi documenti introdotti dal GDPR, tra cui, primo tra tutti, il Registro dei trattamenti e la DPIA, se necessaria.

Un altro passaggio fondamentale è rappresentato dalla mappatura e analisi di adeguatezza delle misure di sicurezza adottate.

Relativamente agli incrementati obblighi in materia di *data breach*, andrà predisposta una procedura per gestire le eventuali violazioni dei dati personali.

Un ulteriore importante passo sarà poi rappresentato dall'adozione di procedure interne per facilitare la gestione delle richieste dell'interessato; si tratterà di un'attività interna in cui verranno chiariti i compiti dei soggetti deputati a tali attività, nonché le modalità, le condizioni e i tempi di svolgimento delle attività stesse.

Infine, affinché l'organizzazione sia effettivamente pronta a gestire e porre in essere le attività facenti parte del processo di adeguamento, sarà essenziale che i soggetti coinvolti in tali processi siano adeguatamente formati.

È necessario un processo di adeguamento si compone delle seguenti fasi principali:

- **Mappatura;**
- ***Gap Analysis*;**
- **Nomina e comunicazione del DPO;**
- **Revisione dei testi delle informative per il trattamento di dati personali;**
- **Revisione dei testi delle nomine dei responsabili esterni;**
- **Impostazione e redazione delle nuove documentazioni obbligatorie (Registro dei trattamenti e, eventualmente, DPIA);**
- **Audit tecnologico sulle misure di sicurezza;**
- **Adozione di procedure di gestione di *data breach*;**
- **Organizzazione interna per la gestione delle richieste dell'interessato;**
- **Formazione dei soggetti autorizzati sul GDPR.**

PARTE SPECIALE

6. GLI ORDINI DEI GEOLOGI ED IL TRATTAMENTO DEI DATI

Gli Ordini sono qualificabili come enti pubblici non economici che, nello svolgimento dei compiti istituzionali, trattano su larga scala dati personali, tra cui anche dati sensibili e giudiziari.

L'analisi degli impatti del GDPR sulle attività degli Ordini non può prescindere da una breve ricognizione delle principali disposizioni normative e regolamentari, oltre che degli atti indirizzo, che disciplinano o hanno disciplinato, in ambito privacy, l'attività degli ordini professionali accompagnate da alcune conseguenziali considerazioni ritenute utili ai fini della presente analisi:

- **Art. 18 del Codice della privacy. Principi applicabili a tutti i trattamenti effettuati da soggetti pubblici:** "*2. Qualunque trattamento di dati personali da parte di soggetti pubblici è consentito soltanto per lo svolgimento delle funzioni istituzionali.*";
- **Art. 19 del Codice della privacy - Principi applicabili al trattamento di dati diversi da quelli sensibili e giudiziari**: "*2. La comunicazione da parte di un soggetto pubblico ad altri soggetti pubblici è ammessa quando è prevista da una norma di legge o di regolamento … 3. La comunicazione da parte di un soggetto pubblico a privati o a enti pubblici economici e la diffusione da parte di un soggetto pubblico sono ammesse unicamente quando sono previste da una norma di legge o di regolamento.*"
- **Art. 20 del Codice della privacy. Principi applicabili al trattamento di dati sensibili:** "*1. Il trattamento dei dati sensibili da parte di soggetti pubblici è consentito solo se autorizzato da espressa disposizione di legge nella quale sono specificati i tipi di dati che possono essere trattati e di operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite. 2. Nei casi in cui una disposizione di legge specifica la finalità di rilevante interesse pubblico, ma non i tipi di dati sensibili e di operazioni eseguibili, il trattamento è consentito solo in riferimento ai tipi di dati e di operazioni identificati e resi pubblici a cura dei soggetti che ne effettuano il trattamento, in relazione alle specifiche finalità perseguite nei singoli casi e nel rispetto dei principi di cui all'articolo 22, con atto di natura regolamentare adottato in conformità al parere espresso dal Garante ai sensi dell'articolo 154, comma 1, lettera g), anche su schemi tipo.*"
- **Art. 21 del Codice della privacy. Principi applicabili al trattamento di dati giudiziari:** "*1. Il trattamento di dati giudiziari da parte di soggetti pubblici è consentito solo se autorizzato da espressa disposizione di legge o provvedimento del Garante che specifichino le finalità di rilevante interesse pubblico del trattamento, i tipi di dati trattati e di operazioni eseguibili. 2. Le disposizioni di cui all'articolo 20, commi 2 e 4, si applicano anche al trattamento dei dati giudiziari.*"
- **Art. 22 del Codice della privacy. Principi applicabili al trattamento di dati sensibili e giudiziari:** "*1. I soggetti pubblici conformano il trattamento dei dati sensibili e giudiziari secondo modalità volte a prevenire violazioni dei diritti, delle libertà fondamentali e della dignità dell'interessato. 2. Nel fornire l'informativa di cui all'articolo 13 i soggetti pubblici fanno espresso riferimento alla normativa che prevede gli obblighi o i compiti in base alla quale è effettuato il trattamento dei dati sensibili e giudiziari. 3. I soggetti pubblici possono trattare solo i dati sensibili e giudiziari indispensabili per svolgere attività istituzionali che non possono essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa. 4. I dati sensibili e giudiziari sono raccolti, di regola, presso l'interessato. 5. In applicazione dell'articolo 11, comma 1, lettere c), d) ed e), i soggetti pubblici verificano periodicamente l'esattezza e l'aggiornamento dei dati sensibili e giudiziari, nonché la loro pertinenza, completezza, non eccedenza e indispensabilità rispetto alle finalità perseguite nei singoli casi, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa. … 6. I dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, sono trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità. 7. I dati idonei a rivelare lo stato di salute e la vita sessuale sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo. I medesimi dati sono trattati con le modalità di cui al comma 6 anche quando sono tenuti in elenchi, registri o banche di dati senza l'ausilio di strumenti elettronici. … 9. Rispetto ai dati sensibili e giudiziari indispensabili ai sensi del comma 3, i soggetti pubblici sono autorizzati ad effettuare unicamente le operazioni di trattamento indispensabili per il perseguimento delle finalità per le quali il trattamento è consentito, anche quando i dati sono raccolti nello svolgimento di compiti di vigilanza, di controllo o ispettivi.*"

- **Art. 61 del Codice della privacy. Utilizzazione di dati pubblici**: "*2. Agli effetti dell'applicazione del presente codice i dati personali diversi da quelli sensibili o giudiziari, che devono essere inseriti in un albo professionale in conformità alla legge o ad un regolamento, possono essere comunicati a soggetti pubblici e privati o diffusi, ai sensi dell'articolo 19, commi 2 e 3, anche mediante reti di comunicazione elettronica. Può essere altresì menzionata l'esistenza di provvedimenti che dispongono la sospensione o che incidono sull'esercizio della professione. 3. L'ordine o collegio professionale può, a richiesta della persona iscritta nell'albo che vi ha interesse, integrare i dati di cui al comma 2 con ulteriori dati pertinenti e non eccedenti in relazione all'attività professionale. 4. A richiesta dell'interessato l'ordine o collegio professionale può altresì fornire a terzi notizie o informazioni relative, in particolare, a speciali qualificazioni professionali non menzionate nell'albo, ovvero alla disponibilità ad assumere incarichi o a ricevere materiale informativo a carattere scientifico inerente anche a convegni o seminari.*"
- **Art. 65 del Codice della privacy. Diritti politici e pubblicità dell'attività di organi:** "*1. Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità di applicazione della disciplina in materia di: a) elettorato attivo e passivo e di esercizio di altri diritti politici, nel rispetto della segretezza del voto, nonché di esercizio del mandato degli organi rappresentativi o di tenuta degli elenchi dei giudici popolari; b) documentazione dell'attività istituzionale di organi pubblici. 2. I trattamenti dei dati sensibili e giudiziari per le finalità di cui al comma 1 sono consentiti per eseguire specifici compiti previsti da leggi o da regolamenti fra i quali, in particolare, quelli concernenti: a) lo svolgimento di consultazioni elettorali e la verifica della relativa regolarità; b) le richieste di referendum, le relative consultazioni e la verifica delle relative regolarità; c) l'accertamento delle cause di ineleggibilità, incompatibilità o di decadenza, o di rimozione o sospensione da cariche pubbliche, ovvero di sospensione o di scioglimento degli organi; d) l'esame di segnalazioni, petizioni, appelli e di proposte di legge di iniziativa popolare, l'attività di commissioni di inchiesta, il rapporto con gruppi politici; e) la designazione e la nomina di rappresentanti in commissioni, enti e uffici. 3. Ai fini del presente articolo, è consentita la diffusione dei dati sensibili e giudiziari per le finalità di cui al comma 1, lettera a), in particolare con riguardo alle sottoscrizioni di liste, alla presentazione delle candidature, agli incarichi in organizzazioni o associazioni politiche, alle cariche istituzionali e agli organi eletti. 4. Ai fini del presente articolo, in particolare, è consentito il trattamento di dati sensibili e giudiziari indispensabili: a) per la redazione di verbali e resoconti dell'attività di assemblee rappresentative, commissioni e di altri organi collegiali o assembleari; b) per l'esclusivo svolgimento di una funzione di controllo, di indirizzo politico o di sindacato ispettivo e per l'accesso a documenti riconosciuto dalla legge e dai regolamenti degli organi interessati per esclusive finalità direttamente connesse all'espletamento di un mandato elettivo. 5. I dati sensibili e giudiziari trattati per le finalità di cui al comma 1 possono essere comunicati e diffusi nelle forme previste dai rispettivi ordinamenti. Non è comunque consentita la divulgazione dei dati sensibili e giudiziari che non risultano indispensabili per assicurare il rispetto del principio di pubblicità dell'attività istituzionale, fermo restando il divieto di diffusione dei dati idonei a rivelare lo stato di salute.*"
- **Art. 66 del Codice della privacy. Materia tributaria e doganale:** "*1. Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le attività dei soggetti pubblici dirette all'applicazione, anche tramite i loro concessionari, delle disposizioni in materia di tributi, in relazione ai contribuenti, ai sostituti e ai responsabili di imposta, nonché in materia di deduzioni e detrazioni e per l'applicazione delle disposizioni la cui esecuzione è affidata alle dogane. 2. Si considerano inoltre di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le attività dirette, in materia di imposte, alla prevenzione e repressione delle violazioni degli obblighi e alla adozione dei provvedimenti previsti da leggi, regolamenti o dalla normativa comunitaria, nonché al controllo e alla esecuzione forzata dell'esatto adempimento di tali obblighi, alla effettuazione dei rimborsi, alla destinazione di quote d'imposta, e quelle dirette alla gestione ed alienazione di immobili statali, all'inventario e alla qualificazione degli immobili e alla conservazione dei registri immobiliari.*"
- **Art. 67 del Codice della privacy. Attività di controllo e ispettive**: "*1. Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità di: a) verifica della legittimità, del buon andamento, dell'imparzialità dell'attività amministrativa, nonché della rispondenza di detta attività a requisiti di razionalità, economicità, efficienza ed efficacia per le quali sono, comunque, attribuite dalla legge a soggetti pubblici funzioni di controllo, di riscontro ed ispettive nei confronti di altri soggetti; b) accertamento, nei limiti delle finalità istituzionali, con riferimento a dati sensibili e giudiziari relativi ad esposti e petizioni, ovvero ad atti di controllo o di sindacato ispettivo di cui all'articolo 65, comma 4.*"
- **Art. 68 del Codice della privacy. Benefici economici ed abilitazioni:** "*1. Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità di applicazione della disciplina in materia di concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti e abilitazioni. 2. Si intendono ricompresi fra i trattamenti regolati dal presente articolo anche quelli indispensabili in relazione: a) alle comunicazioni, certificazioni ed informazioni previste dalla normativa antimafia; b) alle elargizioni di contributi previsti dalla normativa in materia di usura e di vittime di richieste estorsive; c) alla corresponsione delle pensioni di guerra o al riconoscimento di benefici in favore di perseguitati politici e di internati in campo di sterminio e di loro congiunti; d) al*

riconoscimento di benefici connessi all'invalidità civile; e) alla concessione di contributi in materia di formazione professionale; f) alla concessione di contributi, finanziamenti, elargizioni ed altri benefici previsti dalla legge, dai regolamenti o dalla normativa comunitaria, anche in favore di associazioni, fondazioni ed enti; g) al riconoscimento di esoneri, agevolazioni o riduzioni tariffarie o economiche, franchigie, o al rilascio di concessioni anche radiotelevisive, licenze, autorizzazioni, iscrizioni ed altri titoli abilitativi previsti dalla legge, da un regolamento o dalla normativa comunitaria. 3. Il trattamento può comprendere la diffusione nei soli casi in cui ciò è indispensabile per la trasparenza delle attività indicate nel presente articolo, in conformità alle leggi, e per finalità di vigilanza e di controllo conseguenti alle attività medesime, fermo restando il divieto di diffusione dei dati idonei a rivelare lo stato di salute."

- **Art. 71 del Codice della privacy. Attività sanzionatorie e di tutela:** "*1. Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità: a) di applicazione delle norme in materia di sanzioni amministrative e ricorsi; b) volte a far valere il diritto di difesa in sede amministrativa o giudiziaria, anche da parte di un terzo, anche ai sensi dell'articolo 391-quater del codice di procedura penale, o direttamente connesse alla riparazione di un errore giudiziario o in caso di violazione del termine ragionevole del processo o di un'ingiusta restrizione della libertà personale. 2. Quando il trattamento concerne dati idonei a rivelare lo stato di salute o la vita sessuale, il trattamento è consentito se il diritto da far valere o difendere, di cui alla lettera b) del comma 1, è di rango almeno pari a quello dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile."*
- **Art. 86 del Codice della privacy. Altre finalità di rilevante interesse pubblico:** "*1. Fuori dei casi di cui agli articoli 76 e 85, si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità, perseguite mediante trattamento di dati sensibili e giudiziari, relative alle attività amministrative correlate all'applicazione della disciplina in materia di: a) tutela sociale della maternità e di interruzione volontaria della gravidanza, con particolare riferimento a quelle svolte per la gestione di consultori familiari e istituzioni analoghe, per l'informazione, la cura e la degenza delle madri, nonché per gli interventi di interruzione della gravidanza; … c) assistenza, integrazione sociale e diritti delle persone handicappate effettuati, in particolare, al fine di: 1) accertare l'handicap ed assicurare la funzionalità dei servizi terapeutici e riabilitativi, di aiuto personale e familiare, nonché interventi economici integrativi ed altre agevolazioni; 2) curare l'integrazione sociale, l'educazione, l'istruzione e l'informazione alla famiglia del portatore di handicap, nonché il collocamento obbligatorio nei casi previsti dalla legge; ...*"
- **Art. 95 del Codice della privacy. Dati sensibili e giudiziari:** "*1. Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità di istruzione e di formazione in ambito scolastico, professionale, superiore o universitario, con particolare riferimento a quelle svolte anche in forma integrata.*"
- **Art. 112 del Codice della privacy. Finalità di rilevante interesse pubblico:** "*1. Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità di instaurazione e gestione da parte di soggetti pubblici di rapporti di lavoro di qualunque tipo, dipendente o autonomo, anche non retribuito o onorario o a tempo parziale o temporaneo, e di altre forme di impiego che non comportano la costituzione di un rapporto di lavoro subordinato. 2. Tra i trattamenti effettuati per le finalità di cui al comma 1, si intendono ricompresi, in particolare, quelli effettuati al fine di: a) applicare la normativa in materia di collocamento obbligatorio e assumere personale anche appartenente a categorie protette; b) garantire le pari opportunità; c) accertare il possesso di particolari requisiti previsti per l'accesso a specifici impieghi, anche in materia di tutela delle minoranze linguistiche, ovvero la sussistenza dei presupposti per la sospensione o la cessazione dall'impiego o dal servizio, il trasferimento di sede per incompatibilità e il conferimento di speciali abilitazioni; d) adempiere ad obblighi connessi alla definizione dello stato giuridico ed economico, ivi compreso il riconoscimento della causa di servizio o dell'equo indennizzo, nonché ad obblighi retributivi, fiscali o contabili, relativamente al personale in servizio o in quiescenza, ivi compresa la corresponsione di premi e benefici assistenziali; e) adempiere a specifici obblighi o svolgere compiti previsti dalla normativa in materia di igiene e sicurezza del lavoro o di sicurezza o salute della popolazione, nonché in materia sindacale; f) applicare, anche da parte di enti previdenziali ed assistenziali, la normativa in materia di previdenza ed assistenza ivi compresa quella integrativa, anche in applicazione del decreto legislativo del Capo provvisorio dello Stato 29 luglio 1947, n. 804, riguardo alla comunicazione di dati, anche mediante reti di comunicazione elettronica, agli istituti di patronato e di assistenza sociale, alle associazioni di categoria e agli ordini professionali che abbiano ottenuto il consenso dell'interessato ai sensi dell'articolo 23 in relazione a tipi di dati individuati specificamente; g) svolgere attività dirette all'accertamento della responsabilità civile, disciplinare e contabile ed esaminare i ricorsi amministrativi in conformità alle norme che regolano le rispettive materie; h) comparire in giudizio a mezzo di propri rappresentanti o partecipare alle procedure di arbitrato o di conciliazione nei casi previsti dalla legge o dai contratti collettivi di lavoro; i) salvaguardare la vita o l'incolumità fisica dell'interessato o di terzi; l) gestire l'anagrafe dei pubblici dipendenti e applicare*

la normativa in materia di assunzione di incarichi da parte di dipendenti pubblici, collaboratori e consulenti; m) applicare la normativa in materia di incompatibilità e rapporti di lavoro a tempo parziale; n) svolgere l'attività di indagine e ispezione presso soggetti pubblici; o) valutare la qualità dei servizi resi e dei risultati conseguiti. 3. La diffusione dei dati di cui alle lettere m), n) ed o) del comma 2 è consentita in forma anonima e, comunque, tale da non consentire l'individuazione dell'interessato."

- **Parere dell'Autorità Garante per la protezione dei dati personali doc. web n. 1370395. 7 dicembre 2006. Trattamenti dei dati sensibili e giudiziari presso gli ordini professionali sottoposti alla vigilanza del Ministero della Giustizia:** Il Garante ha espresso, ai sensi dell'articolo 20, comma 2 del Codice Privacy, parere favorevole sullo schema di regolamento trattamento dei dati sensibili e giudiziari da effettuarsi presso gli Ordini professionali sottoposti alla vigilanza del Ministero della Giustizia, tra cui rientrano gli Ordini dei Geologi. Per l'effetto di tale parere i dati sensibili e giudiziari possono essere legittimamente trattati dagli Ordini qualora sia adottato previamente un atto di natura regolamentare conforme allo schema di parere su cui il garante ha espresso parere favorevole. Opportuno ricordare che resta ferma la necessità che i dati personali utilizzati e le operazioni del trattamento compiute risultino comunque indispensabili rispetto alla finalità perseguita nei singoli casi (art. 22, comma 3, del Codice).
- **Provvedimento dell'Autorità Garante per la protezione dei dati personali doc. web n. 1487903. 23 gennaio 2008. Rivelazioni biometriche per verificare la presenza a corsi di formazione:** Il Garante ha ritenuto che rientri tra le legittime facoltà di un consiglio di un ordine professionale quella di sovrintendere al regolare espletamento dei corsi di formazione dei praticanti iscritti, ma il titolare del trattamento deve rispettare i princìpi di necessità e di proporzionalità, restando impregiudicata la facoltà di adottare sistemi di controllo degli accessi che escludano l'utilizzo di dati biometrici, in grado di consentire un'efficace attività di verifica dell'identità personale degli interessati ma, al tempo stesso, più rispettosi della sfera personale degli individui, quali, ad esempio, l'utilizzo di tesserini magnetici e l'effettuazione di controlli "a vista" dei partecipanti.
- **Provvedimento dell'Autorità Garante per la protezione dei dati personali doc. web n. 7810723. 1 febbraio 2018. Invio di e-mail promozionali a indirizzi PEC raccolti da registri pubblici:** Il Garante ha espresso la necessità del previo consenso informato dell'interessato anche quando i dati personali (come, nella fattispecie, una parte degli indirizzi di posta elettronica destinatari delle comunicazioni in parola) siano rinvenibili in altri registri o elenchi pubblici (quali quelli disponibili sui siti web istituzionali degli ordini professionali), in quanto l'agevole reperibilità degli stessi non ne autorizza il trattamento per qualsiasi scopo, ma soltanto per le specifiche finalità sottese alla loro pubblicazione (principio costantemente affermato dal Garante a partire dal provvedimento 11 gennaio 2001, doc. web n. 40823 e, quindi, con il provvedimento generale sullo spamming del 29 maggio 2003, doc. web n. 29840 e Linee guida "spam", par. 2.5; v. altresì provv. 6 ottobre 2016, n. 390, doc. web n. 5834805; provv. 21 settembre n. 2017, n. 378, doc. web n. 7221917; provv. 30 novembre 2017, doc. web n. 7522090).
- **Art. 9 del GDPR. Trattamento di categorie particolari di dati personali**: "*1. È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona. 2. Il paragrafo 1 non si applica se si verifica uno dei seguenti casi: ….. il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato; ...".*
- **Art. 10 del GDPR**. **Trattamento dei dati personali relativi a condanne penali e reati**: "*Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati.*".

In riferimento agli ultimi due punti che precedono è opportuno rilevare che il GDPR non prevede, come invece faceva il Codice della privacy, una distinzione tra condizioni di liceità applicabili a titolari del trattamento che fossero soggetti privati e condizioni valide per i titolari soggetti pubblici, cosicché l'istituto del consenso non costituisce più l'elemento distintivo tra titolari privati e titolari pubblici.

Infine, per una corretta analisi dei trattamenti effettuati dagli Ordini, vale ricordare preliminarmente che tali trattamenti sono posti in essere per l'esercizio delle funzioni e dei compiti attribuiti, in via istituzionale, agli

Ordini stessi. In particolare, i trattamenti effettuati nel detto esercizio di funzioni e compiti istituzionali sono volti a verificare, nei limiti necessari e proporzionali, il regolare espletamento delle attività normative e contrattuali da parte degli interessati.

I SOGGETTI COINVOLTI

Come anticipato, ogni singolo Ordine si qualifica, ai fini privacy, come titolare del trattamento e, pertanto, ogni Ordine territoriale deve ritenersi come un autonomo centro di imputazione degli adempimenti in materia di protezione dei dati personali.

I medesimi Ordini effettuano i trattamenti dei dati più dettagliatamente indicati nella sezione "mappatura dei trattamenti dei dati" mediante le seguenti figure rilevanti.

Titolare del trattamento:

è l'Ordine che, ai fini privacy, agisce per il tramite del Consiglio, in persona del Presidente e legale rappresentante *pro tempore*.

Responsabili del trattamento:

fino ad ora, come anticipato sopra, sono stati distinti in responsabili interni, a cui il titolare ha affidato la gestione interna del trattamento dei dati personali inerenti alcune aree di attività specifiche, e responsabili esterni, a cui il titolare ha demandato, esternalizzandolo, lo svolgimento di alcune attività.

Alla luce della disciplina europea, come chiarito sopra, **il ruolo del responsabile esterno è del tutto diverso da quello di un eventuale responsabile interno**: mentre il primo è un'entità – fisica o giuridica – "altra" rispetto al titolare e da questo autonoma, il secondo ne è diretta emanazione e, in merito al trattamento dei dati personali, è una "*persona autorizzata al trattamento dei dati personali sotto l'autorità diretta del titolare*".

Pur confermando quanto affermato sopra in merito alla non necessità di procedere o mantenere le nomine dei responsabili interni, si chiarisce tuttavia che **ove l'Ordine ritenga di voler aggiornare le nomine interne attualmente esistenti può farlo**, ma deve considerarle solo un modo per trasmettere informazioni e focalizzare l'attenzione del personale sull'importanza di proteggere i dati personali oggetto di trattamento.

Soggetti autorizzati:

sono tutti i soggetti interni all'organizzazione dell'Ordine, che sono operativamente coinvolti nelle attività di trattamento. Tali soggetti andranno opportunamente preparati e sensibilizzati sulla disciplina della protezione dei dati personali ed in particolare sugli obblighi imposti all'Ordine dal Regolamento, anche mediante, ove ritenuto, corsi di formazione interni, condivisione del regolamento adottato ai sensi dell'art. 20 del Codice della privacy, pubblicazione di *FAQ* ad uso interno. Per quanto chiarito nel paragrafo che precede, i soggetti precedentemente nominati come responsabili interni sono ora qualificabili come soggetti autorizzati.

MAPPATURA DEI TRATTAMENTI DEI DATI

Come sopra meglio chiarito, l'attività di mappatura e analisi dei trattamenti effettuati è cruciale per il processo di adeguamento al Regolamento.

Nelle tabelle riassuntive che seguono si riportano le operazioni compiute dagli Ordini che implicano il trattamento di dati personali, fermo quanto sopra riportato con riferimento ai limiti delle presenti Linee Guida.

DENOMINAZIONE DEL TRATTAMENTO
ASSUNZIONE E GESTIONE DEI DIPENDENTI E COLLABORATORI.

DESCRIZIONE E SCOPO DEL TRATTAMENTO

I dati sono trattati al fine di consentire agli interessati di accedere all'impiego, accertando la sussistenza dei requisiti richiesti per l'espletamento delle mansioni.

I dati sono, inoltre, trattati per la gestione del rapporto di lavoro o di collaborazione.

In questi trattamenti rientrano quelli effettuati:

- per esigenze di verifica dell'idoneità e dell'attitudine a svolgere prestazioni;
- per adempimenti connessi all'adesione a sindacati o ad organizzazioni di carattere sindacale o similari;
- per esigenze derivanti dalle opinioni politiche, credenze religiose e dalle convinzioni filosofiche o da simili orientamenti d'altro genere;
- per adempimenti connessi all'origine etnica, ivi inclusi i benefici previsti dalla legge;
- per gestione della struttura organizzativa, dell'anagrafica del personale e registrazione degli eventi di carriera;
- per adempimenti relativi a riserve di legge e maternità o paternità;
- per rilevazione e gestione delle presenze;
- per esigenze di igiene e sicurezza sul luogo di lavoro;
- per svolgimento di pratiche assicurative, assistenziali o previdenziali, ivi incluse quelle inerenti denunce di infortuni, sinistri e/o indennizzi;
- per garantire la fruizione di particolari esenzioni o permessi lavorativi per il personale dipendente;
- per gestione della formazione;
- per erogazione della retribuzione, dei compensi e di ogni accessorio;
- per mutamenti inerenti il rapporto, tra cui mobilità e trasferimenti;
- per programmazione annuale degli obiettivi e per valutazione del personale;
- per avvio, istruttoria e chiusura di procedimenti disciplinari;
- per gestione di procedimenti amministrativi e giurisdizionali inerenti il rapporto di lavoro o collaborazione, ivi inclusi quelli di natura conciliativa.

NATURA DI DATI TRATTATI

Dati personali.

Dati sensibili e giudiziari aventi ad oggetto:

- stato di salute del dipendente o collaboratore;
- dati inerenti la salute di familiari del dipendente o collaboratore;
- origine etnica del dipendente o collaboratore;
- convinzioni politiche e sindacali, religiose, filosofiche e di altro genere equiparabile del dipendente o collaboratore;
- vita sessuale del dipendente o collaboratore, con riferimento ad una eventuale rettificazione di attribuzione di sesso;

- informazioni sul dipendente o collaboratore contenute nel casellario giudiziale e nel certificato dei carichi pendenti.

MODALITÀ DEL TRATTAMENTO

Raccolta presso gli interessati e presso terzi.

Elaborazione con documenti cartacei e con modalità informatiche.

BASE GIURIDICA DEL TRATTAMENTO

Normativa legislativa e regolamentare inerente in generale il personale assunto dell'ente pubblico non economico identificato nell'Ordine, tra cui quella in materia di:

- impiego pubblico, ivi inclusa quella disciplinare, di formazione, di occupazione, di maternità e paternità e di mobilità;
- conferimento di incarichi individuali di collaborazione, formazione, ricerca e studio;
- assicurativa, assistenziale, previdenziale e sindacale;
- sicurezza e salute sui luoghi di lavoro;
- documentazione amministrativa, ivi inclusa quella sul relativo accesso;
- anticorruzione, codice di condotta dei dipendenti pubblici e trasparenza;
- amministrazione digitale;
- amministrazione e contabilità degli enti pubblici non economici;
- procedimenti, giudiziali e stragiudiziali, di natura amministrativa, civile, contabile, penale e tributaria.

Contratto collettivo nazionale del comparto enti pubblici non economici.

Contratto individuale di lavoro subordinato, di lavoro parasubordinato o di prestazione d'opera.

INTERESSATI AL TRATTAMENTO

Dipendente o collaboratore.

Familiari del dipendente o collaboratore.

DESTINATARI DEI DATI

Amministrazioni in sede di controllo delle dichiarazioni sostitutive rese ai fini del DPR 445/2000.

Organizzazioni sindacali relativamente ai dipendenti iscritti.

Enti assistenziali, previdenziali e assicurativi e autorità legali di pubblica sicurezza ai fini assistenziali e previdenziali, nonché per rilevazione di eventuali patologie o infortuni sul lavoro.

Compagnie di assicurazioni su richiesta dell'interessato o qualora sia previsto dal contratto di assicurazione.

Presidenza del Consiglio dei Ministri in relazione alla rilevazione annuale dei permessi per cariche sindacali e funzioni pubbliche elettive.

Uffici competenti per il collocamento obbligatorio, relativamente ai dati anagrafici degli assunti appartenenti alle "categorie protette".

Enti di appartenenza dei lavoratori comandati in entrata e in uscita (per definire il trattamento retributivo del dipendente).

Ministero dell'Economia e Finanze nel caso in cui l'ente svolga funzioni di centro assistenza fiscale.

Enti competenti in materia di igiene e sicurezza nei luoghi di lavoro.

Strutture sanitarie competenti per visite fiscali e medico competente.

Soggetti pubblici e privati ai quali ai sensi delle leggi regionali/provinciali viene affidato il servizio di formazione del personale.

Autorità giudiziarie.

Collegi di conciliazione.

Ogni altra Autorità per la verifica della sussistenza di requisiti contrattuali o di legge, anche quelle di pubblica sicurezza.

RILEVANTI FINALITÀ DI INTERESSE PUBBLICO

Art. 61 del d.lgs. n. 196/2003.

Art. 68 del d.lgs. n. 196/2003.

Art. 112 del d.lgs. n. 196/2003.

CONSERVAZIONE DEI DATI

Per tutti i trattamenti, salvi quelli di seguito indicati: 10 anni decorrenti dalla data di cessazione del rapporto da cui deriva il singolo trattamento dei dati.

Per i dati trattati ai fini di pagamenti da effettuarsi periodicamente ad anno o in termini più brevi: 5 anni decorrenti dalla data di cessazione del rapporto da cui deriva il singolo trattamento dei dati.

Al termine del periodo di conservazione i dati verranno cancellati o anonimizzati.

DENOMINAZIONE DEL TRATTAMENTO

ABILITAZIONE ALLA PROFESSIONE. TENUTA E GESTIONE DELL'ALBO E DELL'ELENCO SPECIALE.

DESCRIZIONE E SCOPO DEL TRATTAMENTO

I dati sono trattati al fine di consentire agli interessati di sostenere l'esame di Stato e, in caso di esito positivo, di iscrizione all'Albo o all'Elenco speciale.

I dati sono, inoltre, trattati per la gestione e la tenuta dell'Albo e dell'Elenco speciale.

In questi trattamenti rientrano quelli effettuati:

- per l'acquisizione e verifica della domanda di ammissione all'esame di Stato;
- per garantire la partecipazione e l'espletamento delle prove previste per l'esame di Stato;
- per l'acquisizione e verifica della domanda di iscrizione, di cancellazione o di modifica di dati di cui

all'Albo o all'Elenco speciale;

- per l'iscrizione all'Albo o all'Elenco speciale;
- per la verifica della sussistenza dei presupposti per la permanenza nell'Albo o nell'Elenco speciale;
- per la cancellazione d'ufficio o la radiazione dall'Albo o dall'Elenco speciale;
- per l'annotazione di provvedimenti disciplinari, ivi inclusa la sospensione dall'esercizio della professione, nell'Albo o nell'Elenco speciale;
- per lo svolgimento di attività di vigilanza, di controllo e di monitoraggio connesse alla gestione e alla tenuta relative all'Albo e all'Elenco speciale, oltre che all'abilitazione professionale a seguito del superamento dell'esame di Stato.

NATURA DI DATI TRATTATI

Dati personali.

Dati sensibili e giudiziari aventi ad oggetto:

- stato di salute dell'iscritto (ivi incluse patologie attuali e pregresse);
- origine etnica dell'iscritto;
- vita sessuale dell'iscritto, con riferimento ad una eventuale rettificazione di attribuzione di sesso;
- informazioni sull'iscritto contenute nel casellario giudiziale e nel certificato dei carichi pendenti.

MODALITÀ DEL TRATTAMENTO

Raccolta presso gli interessati e presso terzi.

Elaborazione con documenti cartacei e con modalità informatiche.

BASE GIURIDICA DEL TRATTAMENTO

Normativa legislativa e regolamentare inerente l'esame di Stato.

Normativa legislativa e regolamentare in materia di riconoscimento di titoli di studio per l'accesso alla professione.

Normativa legislativa e regolamentare inerente l'istituzione dell'Albo e dell'Elenco speciale.

Normativa legislativa e regolamentare per la tutela del titolo e della professione, ivi inclusa quella inerente l'esercizio abusivo.

Normativa legislativa e regolamentare per la tenuta e la gestione dell'Albo e dell'Elenco speciale, a seguito di iscrizioni, modifiche di informazioni, cancellazioni e sanzioni disciplinari.

Normativa legislativa e regolamentare in materia di provvedimenti disciplinari da annotare nell'Albo o nell'Elenco speciale.

Normativa legislativa e regolamentare in materia di documentazione amministrativa, ivi inclusa quella sul relativo accesso.

Normativa legislativa e regolamentare in materia di amministrazione digitale.

Normativa legislativa e regolamentare in materia di procedimenti, giudiziali e stragiudiziali, di natura amministrativa, civile, contabile, penale e tributaria.

Normativa legislativa e regolamentare in materia di previdenza obbligatoria per gli iscritti all'Albo e all'Elenco speciale.

Domanda di iscrizione all'Albo o all'Elenco speciale e successive domande per modifica di dati o cancellazione.

INTERESSATI AL TRATTAMENTO

Iscritto all'Albo o all'Elenco speciale.

DESTINATARI DEI DATI

Organi ed organismi del sistema ordinistico, ivi inclusi i Consigli di disciplina, per i provvedimenti di competenza nei confronti dell'interessato.

Associazioni di Ordini e Ordini di altre professioni presso i quali l'interessato svolga determinate funzioni.

Enti previdenziali di iscrizione dell'interessato.

Uffici giudiziari competenti per provvedimenti coinvolgenti l'interessato.

Amministrazioni in sede di controllo delle dichiarazioni sostitutive rese ai fini del DPR 445/2000.

Compagnie di assicurazioni ove richiesto o previsto.

Enti pubblici e privati dai quali l'interessato abbia ricevuto incarichi professionali.

Ogni altra Autorità per la verifica della sussistenza di requisiti contrattuali o di legge inerenti gli iscritti all'Albo e all'Elenco speciale.

RILEVANTI FINALITÀ DI INTERESSE PUBBLICO

Art. 61 del d.lgs. n. 196/2003.

Art. 68 del d.lgs. n. 196/2003.

Art. 112 del d.lgs. n. 196/2003.

CONSERVAZIONE DEI DATI

Per tutti i trattamenti, salvi quelli di seguito indicati: 10 anni decorrenti dalla data di cessazione del rapporto da cui deriva il singolo trattamento dei dati.

Per i dati trattati ai fini di pagamenti da effettuarsi periodicamente ad anno o in termini più brevi: 5 anni decorrenti dalla data di cessazione del rapporto da cui deriva il singolo trattamento dei dati.

Al termine del periodo di conservazione i dati verranno cancellati o anonimizzati, a meno che non sia diversamente previsto da disposizioni inderogabili di legge, ivi incluse quelle in materia di documentazione avente rilevanza storica.

DENOMINAZIONE DEL TRATTAMENTO

PROCEDIMENTI AMMINISTRATIVI E DISCIPLINARI COINVOLGENTI ISCRITTI

ALL'ALBO E ALL'ELENCO SPECIALE.

DESCRIZIONE E SCOPO DEL TRATTAMENTO

I dati sono trattati al fine di avviare, istruire e chiudere procedimenti di natura amministrativa e disciplinare nei confronti di iscritti all'Albo e all'Elenco speciale.

In questi trattamenti rientrano quelli effettuati:

- per l'avvio e l'istruttoria di procedimenti relativi alla liquidazione degli onorari;
- per la riscossione di contributi, diritti, tasse, tributi e altri oneri nei confronti degli iscritti;
- per l'avvio e l'istruttoria di altri procedimenti amministrativi su istanza di parte o d'ufficio;
- per le comunicazioni di tutti i provvedimenti amministrativi;
- per l'avvio e l'istruttoria di procedimenti disciplinari su segnalazione o d'ufficio;
- per le comunicazioni di sanzioni disciplinari;
- per lo svolgimento di attività di vigilanza, di controllo e di monitoraggio sull'esercizio dell'attività professionale.

NATURA DI DATI TRATTATI

Dati personali.

Dati sensibili e giudiziari aventi ad oggetto:

- stato di salute dell'iscritto (ivi incluse patologie attuali e pregresse);
- dati inerenti la salute dei familiari dell'iscritto;
- vita sessuale dell'iscritto, con riferimento ad una eventuale rettificazione di attribuzione di sesso;
- convinzioni politiche e sindacali, religiose, filosofiche e di altro genere equiparabile dell'iscritto;
- informazioni sull'iscritto contenute nel casellario giudiziale e nel certificato dei carichi pendenti.

MODALITÀ DEL TRATTAMENTO

Raccolta presso gli interessati e presso terzi.

Elaborazione con documenti cartacei e con modalità informatiche.

BASE GIURIDICA DEL TRATTAMENTO

Normativa legislativa e regolamentare inerente i procedimenti disciplinari.

Normativa legislativa e regolamentare inerente la liquidazione degli onorari.

Normativa legislativa e regolamentare in materia di amministrazione e contabilità degli enti pubblici non economici, ivi inclusa quella relativa ai loro bilanci.

Normativa legislativa e regolamentare inerente la riscossione di contributi, diritti, tasse, tributi e altri oneri dovuti dagli iscritti.

Normativa legislativa e regolamentare per la tutela del titolo e della professione, ivi inclusa quella inerente

l'esercizio abusivo.

Normativa legislativa e regolamentare in materia di documentazione amministrativa, ivi inclusa quella sul relativo accesso.

Normativa legislativa e regolamentare in materia di amministrazione digitale.

Normativa legislativa e regolamentare in materia di procedimenti, giudiziali e stragiudiziali, di natura amministrativa, civile, contabile, penale e tributaria.

Normativa legislativa e regolamentare in materia di previdenza obbligatoria per gli iscritti all'Albo e all'Elenco speciale.

Normativa legislativa e regolamentare in materia di formazione professionale continua.

Codice deontologico.

INTERESSATI AL TRATTAMENTO

Iscritto all'Albo o all'Elenco speciale.

DESTINATARI DEI DATI

Organi ed organismi del sistema ordinistico, ivi inclusi i Consigli di disciplina, per i provvedimenti di competenza nei confronti dell'interessato.

Associazioni di Ordini e Ordini di altre professioni presso i quali l'interessato svolga determinate funzioni.

Enti previdenziali di iscrizione dell'interessato.

Uffici giudiziari competenti per provvedimenti coinvolgenti l'interessato.

Amministrazioni in sede di controllo delle dichiarazioni sostitutive rese ai fini del DPR 445/2000.

Enti pubblici e privati dai quali l'interessato abbia ricevuto incarichi professionali.

Ogni altra Autorità per la verifica della sussistenza di requisiti contrattuali o di legge inerenti gli iscritti all'Albo e all'Elenco speciale.

RILEVANTI FINALITÀ DI INTERESSE PUBBLICO

Art. 67 del d.lgs. n. 196/2003.

Art. 68 del d.lgs. n. 196/2003.

Art. 71 del d.lgs. n. 196/2003.

CONSERVAZIONE DEI DATI

Per tutti i trattamenti, salvi quelli di seguito indicati: 10 anni decorrenti dalla data di cessazione del rapporto da cui deriva il singolo trattamento dei dati.

Per i dati trattati ai fini di pagamenti da effettuarsi periodicamente ad anno o in termini più brevi: 5 anni decorrenti dalla data di cessazione del rapporto da cui deriva il singolo trattamento dei dati.

Al termine del periodo di conservazione i dati verranno cancellati o anonimizzati.

DENOMINAZIONE DEL TRATTAMENTO

ELEZIONE E NOMINA DEGLI ORGANI E DEGLI ORGANISMI.

DESCRIZIONE E SCOPO DEL TRATTAMENTO

I dati sono trattati al fine dell'elezione o della nomina di iscritti all'Albo o all'Elenco speciale in organi ed organismi degli Ordini (ivi incluse commissioni e simili).

In questi trattamenti rientrano quelli effettuati:

- per l'indizione e l'organizzazione delle elezioni dei consigli degli Ordini;
- per la nomina del seggio elettorale ai fini delle elezioni dei consigli degli Ordini;
- per le candidature a consiglieri degli Ordini;
- per le operazioni di voto nelle elezioni dei consigli degli Ordini;
- per la proclamazione degli eletti nei consigli degli Ordini;
- per ogni altra operazione necessaria per le elezioni dei consigli degli Ordini;
- per l'avvio, l'istruttoria e la definizione dei procedimenti di nomina di componenti di organi non elettivi ed organismi degli Ordini (ivi incluse commissioni e simili);
- per ogni altra operazione necessaria per la nomina di componenti di organi non elettivi ed organismi degli Ordini (ivi incluse commissioni e simili);
- per la verifica di ipotesi di conflitti di interessi, incandidabilità, incompatibilità ed ineleggibilità inerenti gli organi o organismi degli Ordini (ivi incluse commissioni e simili), nonché per la verifica dei requisiti necessari.

NATURA DI DATI TRATTATI

Dati personali.

Dati sensibili e giudiziari aventi ad oggetto:

- stato di salute dell'interessato;
- convinzioni politiche e sindacali, religiose, filosofiche e di altro genere equiparabile dell'interessato;
- informazioni sull'interessato contenute nel casellario giudiziale e nel certificato dei carichi pendenti.

MODALITÀ DEL TRATTAMENTO

Raccolta presso gli interessati e presso terzi.

Elaborazione con documenti cartacei e con modalità informatiche.

BASE GIURIDICA DEL TRATTAMENTO

Normativa legislativa e regolamentare istitutiva del Consiglio Nazionale e degli Ordini Regionali dei Geologi.

Normativa legislativa e regolamentare in materia di elezioni del Consiglio Nazionale e degli Ordini Regionali

dei Geologi.

Normativa legislativa e regolamentare in materia di nomina di organi ed organismi del Consiglio Nazionale e degli Ordini Regionali dei Geologi.

Normativa legislativa e regolamentare per la tenuta dell'Albo e dell'Elenco speciale.

Normativa legislativa e regolamentare in materia di documentazione amministrativa, ivi inclusa quella sul relativo accesso.

Normativa legislativa e regolamentare in materia anticorruzione e trasparenza.

Normativa legislativa e regolamentare in materia di amministrazione digitale.

Normativa legislativa e regolamentare in materia di procedimenti, giudiziali e stragiudiziali, di natura amministrativa, civile, contabile, penale e tributaria.

Normativa legislativa e regolamentare in materia di formazione professionale continua.

INTERESSATI AL TRATTAMENTO

Iscritto all'Albo o all'Elenco speciale.

DESTINATARI DEI DATI

Organi ed organismi del sistema ordinistico, ivi inclusi i Consigli di disciplina, per i provvedimenti di competenza nei confronti dell'interessato.

Associazioni di Ordini e Ordini di altre professioni presso i quali l'interessato svolga determinate funzioni.

Enti previdenziali di iscrizione dell'interessato.

Uffici giudiziari competenti per provvedimenti coinvolgenti l'interessato.

Amministrazioni in sede di controllo delle dichiarazioni sostitutive rese ai fini del DPR 445/2000.

Compagnie di assicurazioni ove richiesto o previsto.

Ogni altra Autorità per la verifica della sussistenza di requisiti contrattuali o di legge inerenti gli iscritti all'Albo e all'Elenco speciale.

RILEVANTI FINALITÀ DI INTERESSE PUBBLICO

Art. 61 del d.lgs. n. 196/2003.

Art. 65 del d.lgs. n. 196/2003.

CONSERVAZIONE DEI DATI

Per tutti i trattamenti, salvi quelli di seguito indicati: 10 anni decorrenti dalla data di cessazione del rapporto da cui deriva il singolo trattamento dei dati.

Per i dati trattati ai fini di pagamenti da effettuarsi periodicamente ad anno o in termini più brevi: 5 anni decorrenti dalla data di cessazione del rapporto da cui deriva il singolo trattamento dei dati.

Al termine del periodo di conservazione i dati verranno cancellati o anonimizzati.

DENOMINAZIONE DEL TRATTAMENTO

ATTIVITÀ DI FORMAZIONE DEGLI ISCRITTI ALL'ALBO E ALL'ELENCO SPECIALE.

DESCRIZIONE E SCOPO DEL TRATTAMENTO

I dati sono trattati al fine della gestione delle attività di iscrizione ai ed erogazione dei corsi di formazione obbligatoria e facoltativa per iscritti all'Albo e all'Elenco speciale.

In questi trattamenti rientrano quelli effettuati:

- per l'iscrizione ai corsi;
- per l'organizzazione dei corsi;
- per l'erogazione della formazione;
- per le attività di valutazione all'esito dei corsi;
- per le attività di controllo, monitoraggio e vigilanza sui corsi erogati e sulla effettiva partecipazione da parte degli iscritti;
- per l'autorizzazione a soggetti terzi ad erogare la formazione;
- per l'esenzione dalle attività formative;
- per controlli sulle autocertificazioni e sulla documentazione prodotta a fini formativi.

NATURA DI DATI TRATTATI

Dati personali.

Dati sensibili e giudiziari aventi ad oggetto:

- stato di salute dell'interessato;
- stato di salute dei familiari dell'interessato;
- convinzioni politiche e sindacali, religiose, filosofiche e di altro genere equiparabile dell'interessato;
- informazioni sull'interessato contenute nel casellario giudiziale e nel certificato dei carichi pendenti.

MODALITÀ DEL TRATTAMENTO

Raccolta presso gli interessati e presso terzi.

Elaborazione con documenti cartacei e con modalità informatiche.

BASE GIURIDICA DEL TRATTAMENTO

Normativa legislativa e regolamentare istitutiva del Consiglio Nazionale e degli Ordini Regionali dei Geologi.

Normativa legislativa e regolamentare in materia di formazione continua.

Normativa legislativa e regolamentare per la tenuta dell'Albo e dell'Elenco speciale.

Normativa legislativa e regolamentare in materia di documentazione amministrativa, ivi inclusa quella sul

relativo accesso.

Normativa legislativa e regolamentare in materia anticorruzione e trasparenza.

Normativa legislativa e regolamentare in materia di amministrazione digitale.

Normativa legislativa e regolamentare in materia di procedimenti, giudiziali e stragiudiziali, di natura amministrativa, civile, contabile, penale e tributaria.

INTERESSATI AL TRATTAMENTO

Iscritto all'Albo o all'Elenco speciale.

Persone fisiche eroganti formazione.

DESTINATARI DEI DATI

Organi ed organismi del sistema ordinistico, ivi inclusi i Consigli di disciplina, per i provvedimenti di competenza nei confronti dell'interessato.

Associazioni di Ordini e Ordini di altre professioni presso i quali l'interessato svolga determinate funzioni.

Amministrazioni in sede di controllo delle dichiarazioni sostitutive rese ai fini del DPR 445/2000.

Enti pubblici e privati eroganti la formazione.

Ministero della Giustizia per pareri sugli enti formatori.

Ogni altra Autorità per la verifica della sussistenza di requisiti contrattuali o di legge con riferimento all'erogazione ed alla ricezione di attività formative.

RILEVANTI FINALITÀ DI INTERESSE PUBBLICO

Art. 68 del d.lgs. n. 196/2003.

Art. 86 del d.lgs. n. 196/2003.

Art. 95 del d.lgs. n. 196/2003.

CONSERVAZIONE DEI DATI

Per tutti i trattamenti, salvi quelli di seguito indicati: 10 anni decorrenti dalla data di cessazione del rapporto da cui deriva il singolo trattamento dei dati.

Per i dati trattati ai fini di pagamenti da effettuarsi periodicamente ad anno o in termini più brevi: 5 anni decorrenti dalla data di cessazione del rapporto da cui deriva il singolo trattamento dei dati.

Al termine del periodo di conservazione i dati verranno cancellati o anonimizzati.

DENOMINAZIONE DEL TRATTAMENTO

STIPULA ED ESECUZIONE DI CONTRATTI CON PRESTATORI DI BENI, LAVORI E SERVIZI.

DESCRIZIONE E SCOPO DEL TRATTAMENTO

I dati sono trattati al fine di consentire agli interessati di accedere agli affidamenti di prestazioni di beni, lavori e servizi, nonché di eseguire i medesimi, a favore degli Ordini.

In questi trattamenti rientrano quelli effettuati:

- per l'acquisizione delle domande di partecipazione alla procedura per l'affidamento delle prestazioni;
- per la verifica dei requisiti necessari per eseguire le prestazioni;
- per la stipula del contratto avente ad oggetto l'erogazione delle prestazioni;
- per l'esecuzione del contratto, ivi inclusi gli obblighi di pagamento;
- per la gestione di ogni stato patologico del contratto, ivi inclusa la risoluzione;
- per gestione di procedimenti amministrativi e giurisdizionali inerenti il contratto, ivi inclusi quelli per accordi bonari e transazioni.

NATURA DI DATI TRATTATI

Dati personali.

Dati sensibili e giudiziari aventi ad oggetto:

- stato di salute dell'interessato;
- origine etnica dell'interessato;
- convinzioni politiche e sindacali, religiose, filosofiche e di altro genere equiparabile dell'interessato;
- vita sessuale dell'interessato, con riferimento ad una eventuale rettificazione di attribuzione di sesso;
- informazioni sull'interessato contenute nel casellario giudiziale e nel certificato dei carichi pendenti.

MODALITÀ DEL TRATTAMENTO

Raccolta presso gli interessati e presso terzi.

Elaborazione con documenti cartacei e con modalità informatiche.

BASE GIURIDICA DEL TRATTAMENTO

Normativa legislativa e regolamentare istitutiva del Consiglio Nazionale e degli Ordini Regionali dei Geologi.

Normativa legislativa e regolamentare in materia di contratti pubblici.

Normativa legislativa e regolamentare in materia di documentazione amministrativa.

Normativa legislativa e regolamentare in materia anticorruzione e trasparenza.

Normativa legislativa e regolamentare in materia assistenziale e previdenziale.

Normativa legislativa e regolamentare in materia di sicurezza e salute sui luoghi di lavoro.

Normativa legislativa e regolamentare in materia di amministrazione digitale.

Normativa legislativa e regolamentare in materia di amministrazione e contabilità degli enti pubblici non

economici.

Normativa legislativa e regolamentare in materia di procedimenti, giudiziali e stragiudiziali, di natura amministrativa, civile, contabile, penale e tributaria.

Contratto di prestazione di beni, lavori o servizi.

INTERESSATI AL TRATTAMENTO

Prestatori di beni, lavori e servizi se persone fisiche.

DESTINATARI DEI DATI

Amministrazioni in sede di controllo delle dichiarazioni sostitutive rese ai fini del DPR 445/2000.

Enti assistenziali, previdenziali e assicurativi.

Autorità legali di pubblica sicurezza ai fini assistenziali e previdenziali.

Compagnie di assicurazioni dei prestatori.

Enti competenti in materia di igiene e sicurezza nei luoghi di lavoro.

Autorità giudiziarie.

Ogni altra Autorità per la verifica della sussistenza di requisiti contrattuali o di legge nei confronti dei prestatori di beni, lavori o servizi.

RILEVANTI FINALITÀ DI INTERESSE PUBBLICO

Art. 66 del d.lgs. n. 196/2003.

Art. 67 del d.lgs. n. 196/2003.

Art. 68 del d.lgs. n. 196/2003.

CONSERVAZIONE DEI DATI

Per tutti i trattamenti, salvi quelli di seguito indicati: 10 anni decorrenti dalla data di cessazione del rapporto da cui deriva il singolo trattamento dei dati.

Per i dati trattati ai fini di pagamenti da effettuarsi periodicamente ad anno o in termini più brevi: 5 anni decorrenti dalla data di cessazione del rapporto da cui deriva il singolo trattamento dei dati.

Al termine del periodo di conservazione i dati verranno cancellati o anonimizzati.

DENOMINAZIONE DEL TRATTAMENTO

CONSULENZA AMMINISTRATIVO-CONTABILE E LEGALE. CONTENZIOSO GIUDIZIALE E STRAGIUDIZIALE.

DESCRIZIONE E SCOPO DEL TRATTAMENTO

I dati sono trattati al fine di fornire ai consulenti elementi necessari all'espletamento delle consulenze affidate.

In questi trattamenti rientrano quelli effettuati:

- per fornire ai consulenti informazioni necessarie, anche ai fini istruttori o di accertamento, per lo svolgimento delle funzioni istituzionali e per la tutela degli Ordini;
- per fornire ai difensori legali elementi necessari per la tutela degli interessi di difesa e di azione degli Ordini, in sede giudiziale e stragiudiziale, ovvero per istruire la relativa pratica ovvero per la gestione di contenziosi in corso;
- per fornire alle autorità pubbliche competenti per legge, ivi inclusa quella giudiziaria, dati in possesso degli Ordini, anche in caso di richiesta o ordine delle dette autorità.

NATURA DI DATI TRATTATI

Dati personali.

Dati sensibili e giudiziari aventi ad oggetto:

- stato di salute dell'interessato;
- dati inerenti la salute di familiari dell'interessato;
- origine etnica dell'interessato;
- convinzioni politiche e sindacali, religiose, filosofiche e di altro genere equiparabile dell'interessato;
- vita sessuale dell'interessato;
- informazioni sull'interessato contenute nel casellario giudiziale e nel certificato dei carichi pendenti.

MODALITÀ DEL TRATTAMENTO

Raccolta presso gli interessati e presso terzi.

Elaborazione con documenti cartacei e con modalità informatiche.

BASE GIURIDICA DEL TRATTAMENTO

Normativa legislativa e regolamentare istitutiva del Consiglio Nazionale e degli Ordini Regionali dei Geologi.

Normativa legislativa e regolamentare in materia di contratti pubblici.

Normativa legislativa e regolamentare in materia di incarichi individuali di collaborazione, consulenza, formazione, ricerca e studio.

Normativa legislativa e regolamentare in materia di documentazione amministrativa, ivi inclusa quella sul relativo accesso.

Normativa legislativa e regolamentare in materia anticorruzione e trasparenza.

Normativa legislativa e regolamentare in materia assistenziale, previdenziale e sindacale.

Normativa legislativa e regolamentare in materia di sicurezza e salute sui luoghi di lavoro.

Normativa legislativa e regolamentare in materia di formazione, obbligatoria o facoltativa, dei professionisti iscritti all'Albo o all'Elenco e dei lavoratori.

Normativa legislativa e regolamentare in materia di amministrazione digitale.

Normativa legislativa e regolamentare in materia di esercizio della professione, ivi inclusa quella relativa all'abilitazione all'esercizio, all'esercizio abusivo e all'interdizione dall'esercizio della professione.

Normativa legislativa e regolamentare in materia di gestione e tenuta dell'Albo e dell'Elenco speciale.

Normativa legislativa e regolamentare in materia di riconoscimento dei titoli di studio per l'accesso alla professione.

Normativa legislativa e regolamentare in materia di amministrazione e contabilità degli enti pubblici non economici.

Normativa legislativa e regolamentare in materia di elezioni e nomine in e da parte di organi ed organismi degli Ordini, anche ai fini del loro commissariamento a seguito di scioglimento.

Normativa legislativa e regolamentare in materia di iscrizione all'Albo o all'Elenco e di ogni connessa modifica.

Normativa legislativa e regolamentare in materia di processi e connessi procedimenti amministrativi, civili, contabili, penali e tributari.

Contratti di prestazione di beni, lavori e servizi.

Contratti di lavoro subordinato, anche collettivi, di lavoro parasubordinato e di collaborazione.

Contratti di prestazioni d'opera professionale, ivi inclusi quelli determinanti il conferimento di mandati alle liti.

INTERESSATI AL TRATTAMENTO

Iscritto all'Albo o all'Elenco speciale.

Dipendenti e collaboratori.

Prestatori di beni, lavori e servizi se persone fisiche.

DESTINATARI DEI DATI

Avvocatura distrettuale e generale dello Stato, ai fini della gestione del contenzioso giurisdizionale.

Autorità giurisdizionali di qualsiasi ordine e funzione, arbitri, amministrazioni interessate o controinteressate nei vari contenziosi.

Organi di polizia giudiziaria.

Uffici del lavoro ai fini di tentativi di conciliazione.

Autorità e uffici contabili, tributari e fiscali.

Organi consultivi per finalità normative o similari.

Liberi professionisti, ai fini di patrocinio o di consulenza, compresi quelli di controparte quando dovuto.

Compagnie di assicurazione ove richiesto o previsto.

Altre parti, pubbliche o private, coinvolte nel contenzioso, quando dovuto.

RILEVANTI FINALITÀ DI INTERESSE PUBBLICO

Art. 66 del d.lgs. n. 196/2003.

Art. 67 del d.lgs. n. 196/2003.

Art. 68 del d.lgs. n. 196/2003. Art. 71 del d.lgs. n. 196/2003.
CONSERVAZIONE DEI DATI Per tutti i trattamenti, salvi quelli di seguito indicati: 10 anni decorrenti dalla data di cessazione del rapporto da cui deriva il singolo trattamento dei dati. Per i dati trattati ai fini di pagamenti da effettuarsi periodicamente ad anno o in termini più brevi: 5 anni decorrenti dalla data di cessazione del rapporto da cui deriva il singolo trattamento dei dati. Al termine del periodo di conservazione i dati verranno cancellati o anonimizzati.

7. INDICAZIONI OPERATIVE

Avendo come riferimento la sintesi del processo di adeguamento al GDPR proposta nei paragrafi che precedono, si riportano di seguito le principali attività che gli Ordini devono espletare al fine di conformarsi ai dettati del Regolamento.

Al riguardo si tenga conto che eventuali enti fondati o controllati dagli Ordini debbono porre in essere le attività di adeguamento al GDPR e possono usufruire delle presenti Linee Guida. Tali enti debbono, però, tener conto della loro diversa natura giuridica e della residuale corrispondenza dei trattamenti di dati personali da loro effettuati rispetto a quelli degli Ordini, nonché dell'eventuale delega di funzioni e compiti istituzionali da parte del singolo Ordine, ove possibile.

IL DPO

OBBLIGO PER GLI ORDINI DI DESIGNARE UN DPO

L'articolo 37, comma 1, del GDPR recita testualmente: "*Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta [...] il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico […]*".

In considerazione della natura di enti pubblici non economici degli Ordini, questi sono obbligati a nominare un DPO.

L'obbligo della nomina di un DPO per gli Ordini viene affermato anche all'esito di un'analisi che, pur tralasciando la loro natura giuridica pubblica, si soffermi su elementi oggettivi che caratterizzano i trattamenti effettuati dai medesimi.

Infatti, l'articolo 37 del GDPR, così come interpretato dalle Linee guida del Gruppo di Lavoro art. 29 sulla figura del DPO, riconosce l'obbligo di nominare un DPO quando ricorrono tra le altre, le seguenti condizioni:

- il trattamento dei dati rientra come "attività principale" del titolare;
- vi è lo svolgimento di attività di "monitoraggio regolare e sistematico degli interessati su larga scala".

Gli Ordini trattano i dati dei soggetti interessati curando la tenuta e l'aggiornamento dell'Albo e dell'Elenco speciale ed, essendo ciò sicuramente necessario per l'espletamento di uno dei fondamentali compiti istituzionali a cui gli Ordini stessi sono preposti, il trattamento può cosniderarsi attività principale.

Gli Ordini svolgono attività di monitoraggio regolare e sistematico nei confronti degli iscritti all'Albo e all'Elenco speciale, e quindi su larga scala, quanto meno sotto i profili deontologici e a quelli legati alla formazione continua obbligatoria.

LA SELEZIONE DEL DPO

Purché vengano rispettate le condizioni previste dal Regolamento relativamente alle competenze del DPO, sopra indicate, il titolare ha discrezionalità nella scelta del soggetto a cui affidare tale compito.

In ogni caso, gli Ordini, stante la loro natura, debbono rispettare le disposizioni di selezione, in materia di contratti pubblici e di pubblico impiego, applicabili agli enti pubblici non economici, pur potendo seguire, ove possibile, procedure semplificate per l'attribuzione della funzione ai propri dipendenti o per l'affidamento diretto del ruolo ad un soggetto esterno, nel rispetto dei principi di prevenzione e risoluzione delle incompatibilità e dei conflitti di interessi.

IL DPO INTERNO

Il DPO può essere un dipendente dell'Ordine e deve essere designato in funzione delle qualità professionali ed, in particolare, come già visto:

- della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati "*determinata in base ai trattamenti di dati effettuati e alla protezione richiesta per i dati personali oggetto di trattamento*"; e
- della "*capacità di assolvere i compiti di cui all'articolo 39*" del GDPR.

Importante chiarire che il DPO non deve ricevere istruzioni, soprattutto sull'approccio da seguire nel caso specifico, sul come condurre gli accertamenti su un reclamo, sulla necessità di consultare o meno l'Autorità Garante per la Protezione dei Dati Personali, sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati.

Il dipendente è, dunque, ammesso come DPO, ma allo stesso tempo deve essere assicurata l'assoluta autonomia ed indipendenza dal titolare del trattamento.

Nella pratica:

- il titolare o il responsabile del trattamento non possono impartire alcuna istruzione per quanto riguarda lo svolgimento dei compiti affidati al DPO;
- il DPO non può essere penalizzato o rimosso dall'incarico in rapporto allo svolgimento dei propri compiti;
- non deve sussistere alcuna ipotesi di conflitto di interessi o di incompatibilità, anche con riguardo a eventuali ulteriori compiti e funzioni.

Pur potendo essere un dipendente dell'Ordine è necessario chiarire che, per la richiesta terzietà della posizione di DPO, il suo ruolo non può essere ricoperto da soggetti che, all'interno dell'Ordine, abbiano il potere di definire le finalità o modalità del trattamento di dati personali.

Inoltre, il Gruppo di Lavoro articolo 29 ha esplicitamente chiarito che può sussistere conflitto di interesse del DPO con i ruoli di responsabile del personale e di responsabile del sistema informativo.

Può, altresì, ritenersi che i funzionari che all'interno dell'Ordine svolgono funzioni che hanno un impatto sulla definizione delle finalità e modalità di trattamento dei dati non potranno essere selezionati come DPO.

Ugualmente sussistono concreti rischi di conflitto di interessi tra il ruolo del DPO e quello di membro del Consiglio dell'Ordine, dal momento che il consigliere fa parte dell'organo di indirizzo politico e gestionale del titolare del trattamento.

L'Autorità Garante per la Protezione dei Dati Personali ha ritenuto non consigliabile l'attribuzione delle funzioni di DPO al responsabile per la prevenzione della corruzione e per la trasparenza, considerando che la molteplicità degli adempimenti che incombono su tale figura potrebbe rischiare di creare un cumulo di impegni tali da incidere negativamente sull'effettività dello svolgimento dei compiti che il GDPR attribuisce al DPO.

IL DPO ESTERNO

In considerazione della portata innovativa del ruolo del DPO, nonché dei requisiti e delle competenze che quest'ultimo deve possedere, è verosimile che la scelta ricada su un soggetto esterno all'organizzazione dell'Ordine.

La funzione di DPO può essere esercitata in base all'atto di conferimento dell'incarico ad una persona fisica o giuridica.

In tale ultimo caso, è indispensabile che ciascun soggetto appartenente alla persona giuridica e operante quale DPO soddisfi tutti i requisiti applicabili come fissati dal GDPR.

Al contempo, si potranno associare le competenze e le capacità individuali di più soggetti per l'espletamento del ruolo di DPO, affinché il contributo collettivo fornito da tali soggetti consenta di rendere alla clientela un servizio più efficiente. Per favorire una corretta e trasparente organizzazione interna e prevenire conflitti di interesse a carico dei componenti il *team*, è, però, opportuno procedere ad una chiara ripartizione dei compiti all'interno dello stesso gruppo e di prevedere che sia un solo soggetto a fungere da contatto principale e "incaricato" rispetto al titolare.

UN UNICO DPO PER PIÙ ORDINI

Ai sensi dell'articolo 37, comma 3, del GDPR è ammessa la designazione di un unico DPO per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione.

Si può, dunque, nominare un unico DPO a condizione che quest'ultimo sia facilmente raggiungibile da ciascuno degli Ordini.

Il concetto di raggiungibilità si riferisce ai compiti del DPO, quale punto di contatto per gli interessati, per l'Autorità Garante per la Protezione dei Dati Personali e per i soggetti interni all'Ordine, visto che uno dei compiti del DPO consiste nell'"*informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento*".

Proprio perché il DPO è chiamato a una molteplicità di funzioni, il titolare o il responsabile del trattamento deve assicurarsi che un unico DPO per più enti sia in grado di adempiere in modo efficiente a tali funzioni, anche se designato da una molteplicità di autorità e organismi pubblici.

Pertanto, in caso di scelta di nomina di un unico DPO, l'atto di nomina stesso dovrà includere un riferimento all'esito positivo della valutazione effettuata dal titolare o responsabile sull'adeguatezza di tale scelta.

LA NOMINA DEL DPO

Il GDPR prevede all'articolo 37, comma 1, che il titolare e il responsabile del trattamento designino il DPO.

Da ciò deriva, quindi, che l'atto di designazione è parte costitutiva dell'adempimento.

Nel caso in cui la scelta del DPO ricada su un dipendente, occorre formalizzare un apposito atto di designazione.

In caso, invece, di ricorso a soggetti esterni all'Ordine, la designazione costituirà parte integrante dell'apposito atto di affidamento dell'incarico redatto in base a quanto previsto dall'articolo 37 del GDPR.

Indipendentemente dalla natura e dalla forma dell'atto utilizzato, è necessario che nell'atto sia individuato in maniera inequivocabile il soggetto che opererà come DPO, riportandone espressamente:

- le generalità;
- i compiti;
- le funzioni che questi sarà chiamato a svolgere in ausilio al titolare/responsabile del trattamento;
- l'eventuale assegnazione di compiti aggiuntivi.

Nell'atto di designazione e conferimento dell'incarico devono risultare succintamente indicate anche le motivazioni che hanno indotto l'Ordine a individuare, nel soggetto selezionato, il proprio DPO, al fine di

consentire la verifica del rispetto dei requisiti previsti dall'articolo 37 del GDPR, anche mediante rinvio agli esiti delle procedure di selezione interna o esterna effettuata.

I dati di contatto del DPO sono pubblicati sul sito internet dell'Ordine e comunicati all'Autorità Garante per la Protezione dei Dati Personali

ALLEGATO A: Schema di atto di designazione e di conferimento dell'incarico per il DPO.

I dati di contatto del DPO vanno pubblicati sul sito web istituzionale dell'Ordine e a comunicati all'Autorità Garante per la Protezione dei Dati Personali.

L'Autorità Garante per la Protezione dei Dati Personali ha messo a disposizione una procedura on line per la comunicazione dei dati di contatto del DPO al link: https://servizi.gpdp.it/comunicazione-rpd/compilaModulo.

ALLEGATO B: Istruzioni per la compilazione on line del modello di comunicazione dei dati di contatto del DPO all'Autorità Garante per la Protezione dei Dati Personali.

IL REGISTRO DEI TRATTAMENTI

Dalle Linee guida dell'Autorità Garante per la Protezione dei Dati Personali relative all'applicazione del Regolamento si legge che la tenuta del Registro dei trattamenti non costituisce un adempimento formale, bensì **parte integrante di un sistema di corretta gestione dei dati personali**.

Per tale motivo, risulta necessario che ogni Ordine adotti il proprio Registro dei trattamenti.

Al fine di una corretta e completa redazione del Registro dei trattamenti si rileva che, come già affermato sopra, la mappatura dei trattamenti effettuati dagli Ordini costituisce elemento essenziale da cui partire per la predisposizione del Registro.

Pertanto, al fine di agevolare gli Ordini, si fornisce uno schema di Registro dei trattamenti fondato sulla mappatura dei trattamenti di cui alla precedente sezione, precisando, quindi, che lo stesso è stato predisposto tenendo conto della generalità dei trattamenti effettuati e delle casististe che coinvolgono gli Ordini, con la conseguenza che esso dovrà essere verificato ed eventualmente integrato, nel corso del tempo, dal singolo Ordine alla luce delle proprie peculiarità.

ALLEGATO C: Schema di Registro dei trattamenti.

L'ADEGUAMENTO DELL'INFORMATIVA PRIVACY

Come chiarito sopra, è necessario verificare la documentazione privacy già in uso e valutarne l'adeguatezza alle prescrizioni del Regolamento.

L'informativa sul trattamento sarà adeguata al GDPR se:

- esplicita l'identità ed i dati di contatto del titolare del trattamento;
- indica i dati di contatto del DPO;
- rende note la finalità del trattamento e la base giuridica;
- specifica di chi sia il legittimo interesse perseguito dal trattamento;
- contiene eventuali destinatari o categorie di destinatari dei dati personali;
- esplicita un eventuale trasferimento dei dati personali a Paesi Terzi e, in caso affermativo, con quali strumenti;
- rivela per quanto tempo i dati verranno conservati e i criteri per indicare quel periodo;

- indica i diritti fondamentali dell'interessato;
- esplicita il diritto di revoca al consenso, in qualsiasi momento;
- contiene il diritto di presentare un reclamo all'Autorità Garante per la Protezione dei Dati Personali;
- rende noto che tipo di comunicazione dei dati personali sia un obbligo legale, contrattuale o un requisito necessario per la conclusione di un contratto;
- rivela quali processi automatizzati comporti il trattamento (compresa la profilazione) ed eventualmente le informazioni sulla logica di tali processi e le conseguenze per l'interessato.

Per agevolare l'attività di adeguamento degli Ordini si fornisce uno schema di informativa per ognuna delle principali categorie di interessati: dipendenti (o collaboratori); iscritti; prestatori di beni, lavori e servizi (ivi inclusi consulenti).

Si precisa che i suddetti schemi sono stati predisposti tenendo conto della generalità dei trattamenti effettuati e delle casististe che coinvolgono gli Ordini, con la conseguenza che essi dovranno essere verificati ed eventualmente integrati, nel corso del tempo, dal singolo Ordine alla luce delle proprie peculiarità.

ALLEGATO D: Schema di informativa per i dipendenti.

ALLEGATO E: Schema di informativa per iscritti.

ALLEGATO F: Schema di informativa per prestatori di beni, lavori e servizi.

VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

Un'analisi meramente testuale delle previsioni del Regolamento porterebbero a concludere per la sussistenza in capo agli Ordini dell'obbligo di effettuare una DPIA.

Il comma 3 dell'articolo 35 del GDPR, infatti, esplicitamente prevede che la valutazione d'impatto è richiesta nei casi, tra gli altri, di "*trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10.*"

La valutazione d'impatto potrebbe rendersi, quindi, necessaria dal momento che, come concluso nella sezione sulla "mappatura dei trattamenti" effettuati, gli Ordini trattano dati sensibili e giudiziali su larga scala.

Tuttavia, il Gruppo di Lavoro art. 29, nelle Linee guida già sopra citate sulla DPIA, ha ricompreso tra i casi di esenzione dall'obbligo di svolgere la DPIA quello in cui "*le tipologie di trattamento sono state verificate da un'autorità di controllo prima del maggio 2018 in condizioni specifiche che non hanno subito modifiche*".

I trattamenti di dati sensibili e giudiziali effettuati da alcuni ordini professionali, tra cui gli Ordini in questione, sono stati oggetto di specifico parere positivo dell'Autorità Garante per la Protezione dei Dati Personali, che, con provvedimento reso il 7 dicembre 2006, ha ritenuto l'adozione del regolamento conforme allo schema proposto dal Ministero della Giustizia, condizione sufficiente per legittimare e ammettere, senza ulteriori adempimenti, il trattamento dei dati sensibili e giudiziari da parte degli Ordini stessi.

Il parere positivo dell'Autorità Garante per la Protezione dei Dati Personali e l'effettiva adozione da parte del singolo Ordine del regolamento appaiano, ragionevolmente, come condizione di esenzione dell'obbligo della DPIA, qualora i trattamenti siano effettivamente quelli indicati nel regolamento e vengano effettuati alle medesime condizioni e modalità ivi richiamate.

Pertanto, i singoli titolari, insieme ai propri DPO designati, dovranno solo verificare che i trattamenti effettuati in concreto siano quelli riportati nel regolamento adottato e, in un'ottica di maggiore responsabilizzazione, potranno, qualora ritenuto necessario, procedere alla DPIA per particolari trattamenti considerati di maggior rischio.

ALLEGATO G: Schema di regolamento proposto dal Ministero della Giustizia ed approvato dall'Autorità Garante per la Protezione dei Dati Personali.

ALLEGATO H: Linee Guida Gruppo di Lavoro art. 29 su DPIA.

Per l'eventuale DPIA si riporta anche il link al software ritenuto utile: https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-dataprotection-impact-assesment.

NOMINA DEI RESPONSABILI ESTERNI

La nomina dei responsabili esterni da parte dei singoli Ordini diventa un altro passo cruciale per garantire l'adeguamento alle prescrizioni del Regolamento.

L'articolo 28 del GDPR, infatti, delinea in dettaglio i rapporti tra titolare e responsabile, stabilendo innanzitutto che si debba ricorrere a Responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, in modo tale che il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato.

La nomina ha l'essenziale ruolo di dimostrare non solo la sussistenza di tale rapporto tra titolare e responsabile, ma soprattutto la funzione di fornire indicazioni chiare e conformi al Regolamento da parte del titolare, nonché il soddisfacimento dei requisiti imposti in capo al responsabile.

Su tali basi emerge un chiaro obbligo per gli Ordini di disporre di nomine scritte e accettate da parte dei responsabili dei trattamenti.

I responsabili devono, infatti, essere nominati dall'Ordine che agisce in qualità di titolare del trattamento attraverso un contratto di nomina che dovrà essere redatto in forma scritta e dovrà disciplinare i seguenti elementi:

- oggetto, durata, natura e finalità del trattamento;
- categorie di soggetti interessati e tipo di dati personali oggetto del trattamento;
- obblighi e diritti del titolare del trattamento.

In pratica, è importante che ogni Ordine provveda:

- alla mappatura di tutti i soggetti a cui è demandata la gestione del trattamento dei dati derivante dallo svolgimento di attività che vengono effettuate per conto dell'Ordine;
- alla verifica di contratti eventualmente già in essere, per accertarne la compatibilità con l'obbligo di nomina del responsabile;
- all'inserimento puntuale, negli atti e nei contratti, delle pattuizioni necessarie per soddisfare i requisiti previsti dal GDPR, anche con riguardo alle garanzie di rispetto dei principi del GDPR, che i responsabili devono possedere.

Al fine di adempiere all'obbligo in questione, si fornisce un esempio di nomina di responsabile che, salvo verifiche di esigenze e/o casi particolari, può essere utilizzato dagli Ordini per nominare in futuro i responsabili e/o intervenire sui rapporti già in essere con soggetti che già agiscono in qualità di responsabili nel trattamento dei dati effettuato per conto degli Ordini stessi.

ALLEGATO I: Schema di contratto per il trattamento dei dati personali e la nomina dei responsabili.

MISURE DI SICUREZZA

Come per altri adempimenti imposti dal GDPR, anche per le misure di sicurezza da adottare si richiede una valutazione specifica e dettagliata del titolare che tenga conto, in estrema sintesi, della specificità dei trattamenti effettuati sia in termini di quantità e natura dei dati trattati sia in termini di tecniche e modalità di trattamento.

Su tali basi risulta estremamente complesso, se non addirittura contrario all'impostazione del Regolamento, individuare un elenco tassativo di iniziative da intraprendere in materia di sicurezza al fine di garantire la conformità alle previsioni del GDPR ed in particolare al suo articolo 22.

Con l'intento di agevolare i singoli Ordini nello svolgimento di specifiche e mirate valutazioni, si ritiene utile formulare, quindi, una proposta di strumenti che possano ragionevolmente essere considerati idonei ad offrire un livello di sicurezza adeguato al trattamento dei dati personali e soprattutto dei dati sensibili e giudiziari effettuato dagli Ordini.

Nell'espletamento di tale compito si cita preliminarmente la previsione dell'Autorità Garante per la Protezione dei Dati Personali inserita nelle Linee guida sull'applicazione del Regolamento, che, in caso di soddisfacimento concreto delle condizioni ivi previste, porterebbe alla soluzione immediata e finale della questione: "*per alcune tipologie di trattamenti (quelli di cui all'art. 6, paragrafo 1), lettere c) ed e) del regolamento* [c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento; e) 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] *potranno restare in vigore le misure di sicurezza attualmente previste attraverso le disposizioni di legge volta per volta applicabili; il Garante esplicitamente chiarisce che tale ipotesi si verifica per i trattamenti di dati sensibili svolti dai soggetti pubblici per finalità di rilevante interesse pubblico nel rispetto degli specifici regolamenti attuativi (ex artt. 20 e 22 Codice), ove questi ultimi contengano disposizioni in materia di sicurezza dei trattamenti*".

Al medesimo scopo di cui sopra, si procede ad un'analisi in dettaglio delle misure di sicurezza sino ad ora imposte da precedenti fonti normative e regolamentari ai trattamenti in questione, che debbono ritenersi ancora attuali nei limiti sopra indicati in virtù della sopravvenuta entrata in vigore del GDPR.

- **Misure minime di sicurezza previste dall'art. 33 del Codice della privacy e dettagliate nell'Allegato B al Codice stesso.**

Trattamenti con l'ausilio di strumenti elettronici

Ogni Ordine che effettua trattamenti con strumenti elettronici è tenuto ad adottare, con le modalità previste dell'Allegato B al Codice della privacy, le seguenti misure minime:

- autenticazione informatica;
- utilizzazione di un sistema di autorizzazione;
- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
- protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
- adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
- adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

Ogni incaricato dall'Ordine al trattamento dei dati personali deve essere dotato di credenziali proprie e riservate di autenticazione, tra le quali:

- un codice identificativo associato ad una password che deve:
  - avere almeno 8 caratteri, ovvero il massimo consentito dallo strumento elettronico se inferiore a 8;
  - non contenere riferimenti agevolmente riconducibili all'incaricato; e
  - essere subito modificata dall'incaricato al primo utilizzo e successivamente con cadenza semestrale, se l'incaricato effettuata trattamento di dati personali, o ogni 3 mesi qualora il trattamento riguardi dati sensibili e/o giudiziari.
- un dispositivo di autenticazione detenuto e usato esclusivamente dal singolo incaricato (es. tessera magnetica, tessera NFC, Smart-Card, etc.) associato ad un'eventuale e facoltativa password o codice identificativo;
- tecniche di autenticazione biometrica (es. impronte digitali, iride dell'occhio, etc.) associate ad un'eventuale e facoltativa password o codice identificativo.

Va specificato altresì che:

- il codice identificativo di cui sopra, una volta assegnato ad un incaricato, non potrà più essere riassegnato ad altri soggetti, nemmeno in epoca successiva;
- le credenziali non utilizzate da almeno 6 mesi devono essere disattivate (a meno che non siano state preventivamente autorizzate quali credenziali per soli scopi di gestione tecnica, che prevedono pertanto periodi di inattività anche più lunghi del semestre);
- le credenziali devono essere disattivate anche quando l'incaricato che le utilizzi perda le qualità che gli consentono di utilizzarle per trattare i dati personali (es. promozione ad incarico differente, licenziamento etc.).

Va sottolineato, inoltre, più volte che ogni incaricato dall'Ordine deve essere istruito dal titolare o dal responsabile circa le necessarie cautele per curare tali codici, nonché per non lasciare incustodito o accessibile a terzi lo strumento elettronico utilizzato per il trattamento dei dati.

Relativamente al sistema di autorizzazione, infine, va precisato che tale sistema di autorizzazione deve:

- essere predisposto anteriormente all'inizio del trattamento;
- strutturato in modo tale da limitare l'accesso dei singoli incaricati solo ai dati necessari per effettuare le operazioni di trattamento;
- verificato periodicamente, e come minimo annualmente, così da confermare i diversi profili già autorizzati, rideterminarli, ampliando o restringendo le aree di trattamento, ovvero eliminarli se divenuti obsoleti.

Trattamenti senza strumenti elettronici

In caso di trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici, è necessario che gli Ordini adottino le seguenti misure minime:

- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;
- previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;
- previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.

- **Misure previste dall'articolo 22 del Codice della privacy per il trattamento di dati sensibili e giudiziari.**

L'articolo 22 del Codice della privacy ha da tempo introdotto espressamente misure di sicurezza ulteriori rispetto a quelle previste per la generalità dei trattamenti quando vengono trattati dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati.

In particolare, devono essere adottati sistemi di cifratura o criptatura che rendono non identificabile l'interessato.

Inoltre, il medesimo articolo prescrive che i dati idonei a rivelare lo stato di salute e la vita sessuale devono essere conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo.

Come più dettagliatamente indicato nella sezione relativa alla "mappatura dei trattamenti", i trattamenti effettuati dagli Ordini ricadono evidentemente nell'ipotesi prevista dal citato articolo 22 (dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati) e come tali, in adesione alle previsione del Codice della privacy e quindi ben prima dell'entrata in vigore del GDPR, devono essere effettuati adottando tecniche di cifratura o criptazione.

- **Misure minime per la sicurezza ICT delle pubbliche amministrazioni.**

In attuazione della Direttiva 1° agosto 2015 del Presidente del Consiglio dei Ministri, che emana disposizioni finalizzate a consolidare lo stato della sicurezza informatica nazionale, AgID ha provveduto ad emanare l'elenco ufficiale delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni".

Già a partire dal dicembre 2017, gli Ordini dovevano adottare, quindi, almeno le misure minime previste dall'AgID.

Le misure individuate dall'AgID sono un insieme ordinato e ragionato di controlli, di natura tecnica od organizzativa, che è stato predisposto al fine di fornire agli Ordini un riferimento pratico per valutare e innalzare il proprio livello di sicurezza informatica.

Le misure indicate, si dividono in tre diversi livelli:

- il livello minimo è quello al quale ogni Ordine, indipendentemente dalla sua natura e dimensione, deve necessariamente conforme;
- i livelli successivi sono richiesti sin da subito alle organizzazioni più esposte a rischi e, a tendere, a tutte le amministrazioni in un percorso di continuo miglioramento del livello di sicurezza.

È ragionevole ritenere che, allo stato attuale del quadro normativo, gli Ordini sono tenuti, ove non vi abbiano già provveduto, ad adottare tempestivamente:

1. **le misure minime *ex* articolo 33 e Allegato B del Codice della privacy sopra indicate (si veda: ALLEGATO L);**
2. **le ulteriori misure di criptazione o cifratura previste dall'articolo 22 del Codice della privacy sopra riportate;**
3. **le misure minime per la sicurezza informatica di cui al modulo di implementazione dell'AgID (si veda: ALLEGATO M);**
4. **il regolamento per il trattamento dei dati sensibili e giudiziari come da schema proposto dal Ministero della Giustizia ed approvato dal Garante (si veda: ALLEGATO G).**

Per completezza e in un'ottica di responsabilizzazione dei singoli Ordini, si aggiunge che l'articolo 32 del GDPR propone una lista di possibili ulteriori misure da adottare che sono:

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

DATA BREACH

Con specifico riferimento ai trattamenti dei dati svolti dagli Ordini, fermo quanto già indicato sopra, appare opportuno precisare che l'Autorità Garante per la Protezione dei Dati Personali, con il provvedimento del 2 luglio 2015, avente ad oggetto "*Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche*", già prevedeva l'obbligo per le amministrazioni pubbliche di comunicare, in quel caso era previsto nel minor termine di 48 ore, all'indirizzo databreach.pa@pec.gpdp.it le violazioni dei dati personali (*data breach*) verificatisi nell'ambito delle banche dati di cui sono titolari gli stessi Ordini.

Al fine di poter gestire in maniera efficace un eventuale *data breach*, si raccomanda di individuare in maniera chiara almeno il soggetto e le procedure organizzative per:

1. **la raccolta delle segnalazioni interne;**
2. **il rilievo di elementi che hanno determinato l'eventuale violazione;**
3. **la comunicazione al DPO dell'evento.**

Per agevolare l'eventuale espletamento dell'obbligo si rinvia all'apposito modello di segnalazione di data breach (ALLEGATO N).

8. COORDINAMENTO CON ALTRA NORMATIVA

L'adeguamento da parte degli Ordini alla disciplina privacy introdotta dal Regolamento deve tenere in debita considerazione anche le altre principali disposizioni normative e regolamentari cui le attività degli Ordini stessi sono sottoposte e che hanno un impatto sullo svolgimento delle operazioni di trattamento dei dati personali svolte.

In particolare, deve tenersi conto della disciplina in materia di:

- anticorruzione e trasparenza;
- accesso ai documenti amministrativi;
- semplificazione amministrativa.

Ai sensi della legge 190/2012 e del d.lgs. 33/2013 in materia di anticorruzione e trasparenza, l'Ordine, in persona del responsabile dell'anticorruzione e della trasparenza, provvede alla pubblicazione di dati, informazioni e documenti nel rispetto dei seguenti principi:

a) pubblicazione dei dati personali solo ove sia obbligatoria;
b) anonimizzazione, all'atto della pubblicazione, dei dati personali per cui non risulti indispensabile la pubblicazione;
c) pubblicazione dei dati comuni tenendo conto della necessità, pertinenza e non eccedenza;
d) pubblicazione dei dati sensibili solo ove sia indispensabile per le finalità di trasparenza;
e) pubblicazione dei dati giudiziari e disciplinari entro gli stretti limiti dettati dalla normativa sull'Albo e sull'Elenco speciale;
f) divieto di pubblicazione dei dati sulla vita sessuale e sullo stato di salute;
g) riutilizzo di dati personali, a seguito di pubblicazione in virtù di accesso civico, nei limiti che risultino compatibili con le finalità per cui sono stati raccolti.

Alla luce della normativa sull'accesso ai documenti amministrativi, di cui alla legge 241/1990 e al d.lgs. 33/2013, il trattamento dei dati effettuato dagli Ordini in virtù di accesso documentale, accesso civico e generalizzato, al fine di conformarsi alla normativa sulla protezione dei dati personali, deve garantire il rispetto:

a) dei diritti inviolabili e delle libertà fondamentali dell'interessato;
b) dell'identità personale dell'interessato, ivi incluso il nome;
c) della dignità dell'interessato, ivi incluse la reputazione e l'immagine;
h) della sfera morale, relazionale e sociale dell'interessato.

Inoltre, la valutazione di una qualunque delle ipotesi di accesso verrà condotta anche verificando, sulla base dei principi privacy, se i dati personali da rendere conoscibili attraverso l'accesso stesso non risultino sproporzionati, eccedenti e non pertinenti.

Con riferimento agli atti dei procedimenti disciplinari nei confronti degli iscritti all'Albo e all'Elenco speciale, che non sono soggetti ad obbligo di pubblicazione ai fini della trasparenza, si ricorda che è precluso l'accesso civico e generalizzato, nonché, salvo specifiche eccezioni a tutela del diritto dell'interessato richiedente, quello documentale ai sensi della legge 241/1990, in considerazione della particolare incidenza dell'ostensione di tali atti sulla riservatezza dei rispettivi interessati.

Infine, con riferimento alle prescrizioni del d.P.R. 445/2000 in materia di semplificazione amministrativa, si ricorda che i certificati medici e sanitari non possono essere sostituiti da altro documento, salvo diverse disposizioni della normativa di settore.

9. SCHEDA RIEPILOGATIVA

Gli Ordini devono assicurare, ed essere in grado di comprovare, il rispetto dei principi applicabili al trattamento dei dati personali, eseguendo le seguenti principali attività:

- la designazione del DPO;
- la comunicazione del DPO all'Autorità Garante per la Protezione dei Dati Personali;
- l'istituzione del Registro dei trattamenti;
- l'esame dei rapporti contrattuali con i responsabili esterni del trattamento e la conseguente adozione eventuale di un contratto per il trattamento dei dati e nomina a responsabile;
- l'aggiornamento delle informative;
- la verifica dell'adozione delle misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato ai trattamenti effettuati, tenendo conto di quelle già adottate, ivi incluse quelle di cui allo schema di regolamento proposto dal Ministero della Giustizia;
- l'adozione di procedure interne per la gestione di eventuali *data breach*;
- l'avvio di attività interne di formazione e sensibilizzazione GDPR e i suoi impatti sulle attività dell'Ordine.

ALLEGATI