Consiglio Nazionale
dei Dottori Commercialisti
e degli Esperti Contabili

LINEE GUIDA

LINEE GUIDA PER L'ADEMPIMENTO DEGLI OBBLIGHI PRIVACY NEGLI ORDINI PROFESSIONALI

AREE DI DELEGA CNDCEC
Compliance e modelli organizzativi delle imprese

COMMISSIONE DI STUDIO
Privacy Ordini professionali

CONSIGLIERE DELEGATO
Eliana Quintili

PRESIDENTE
Marco Manganiello

GIUGNO 2024

Consiglio Nazionale
dei Dottori Commercialisti
e degli Esperti Contabili

Area di delega "Compliance e modelli organizzativi delle imprese"

A cura della Commissione di studio "Privacy Ordini professionali"

Consigliere delegato

Eliana Quintili

Presidente

Marco Manganiello

Segretario

Andrea Onori

Componenti

Giuliano Angeli
Floriana Carlino
Claudia Cevenini
Aldo Giacomo Colantuono
Raffaele Cuomo
Raffaele D'Arienzo
Andrea Di Gialluca
Marilù Fragalà
Marco Giannini
Giuseppe Liuzzi
Laura Macci
Marco Marchetti
Francesco Mariani Ripa
Salvatore Passafaro
Cristina Renna
Roberta Santopietro
Luisa Tucci
Albert Überbacher
Armando Urbano
Mauro Verdimonti
Paola Zambon

Staff tecnico

Annalisa De Vivo – *Ufficio Legislativo CNDCEC*

Sommario

Introduzione

A sei anni dall'entrata in vigore del Regolamento europeo in materia di protezione dei dati personali, il bilancio del percorso di *compliance* degli Ordini professionali evidenzia risultati variabili e, nonostante gli sforzi, non sempre rivela una conformità sostanziale.

La *ratio* del disallineamento tra *compliance* formale ed effettiva è in larga parte riconducibile alla percezione talvolta incompleta, da parte degli Ordini professionali, dei rischi e dei potenziali danni conseguenti ad una gestione non corretta dei dati comunemente trattati, da quelli relativi agli Albi professionali ai dati previdenziali e di giustizia interna, fino alla gestione delle caselle di posta elettronica ordinaria e certificata.

Sul tema, fin dal suo insediamento il Consiglio Nazionale ha manifestato la propria volontà di fornire un supporto operativo agli Ordini territoriali: a tal scopo, verso la fine del 2022 è stata predisposta una check list, al fine di ottenere un primo riscontro in merito al grado di conformità degli Ordini territoriali alla normativa privacy. La check list è stata compilata da 101 Ordini territoriali e i dati raccolti sono stati elaborati dalla Commissione di studio "Privacy Ordini professionali", istituita nell'ambito dell'area di delega "Compliance e modelli organizzativi delle imprese" del CNDCEC.

L'analisi delle informazioni ricevute ha consentito di individuare e calibrare le più efficaci attività di supporto da fornire agli Ordini territoriali per consentire il corretto assolvimento degli obblighi privacy, tra cui l'elaborazione, da parte della predetta Commissione di studio, di Linee Guida finalizzate ad agevolare l'implementazione, all'interno degli Ordini, di un vero e proprio modello organizzativo privacy.

In particolare, nella predisposizione del presente documento si è tenuto ben presente l'obiettivo di fornire soluzioni specifiche a problematiche ricorrenti nella gestione degli adempimenti privacy da parte degli Ordini; alla medesima esigenza risponde la modulistica riportata nell'appendice del documento: dal fac-simile del registro dei trattamenti alle informative privacy, fino ai moduli per l'esercizio dei diritti degli interessati e per le nomine dei soggetti autorizzati al trattamento dei dati personali.

Tutto ciò nel presupposto che, al netto dei comprensibili errori sul campo, per essere davvero conforme alla privacy un Ordine professionale dovrebbe innanzi tutto comprendere la rilevanza della disciplina, degli adempimenti di sicurezza da porre in essere, delle regole da osservare e della formazione da erogare, a salvaguardia di tutti i soggetti interessati ai vari trattamenti dei dati.

Eliana Quintili
Consigliera CNDCEC delegata Area "Compliance e modelli organizzativi delle imprese"

PARTE PRIMA

Il trattamento dei dati personali – aspetti operativi

1. Le basi giuridiche e le finalità del trattamento

Per lo svolgimento delle funzioni istituzionali ad essi demandate, gli Ordini professionali possono trattare dati di carattere personale nel rispetto dei limiti stabiliti dalle leggi e dai regolamenti.

Il "trattamento" è 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.

La "base giuridica" è rinvenibile nelle disposizioni normative che rendono lecite determinate attività e/o operazioni di trattamento.

Il trattamento dei dati personali effettuato dall'Ordine professionale, in quanto soggetto pubblico, viene considerato lecito solo se il trattamento è necessario:

a) per adempiere ad un obbligo legale al quale è soggetto il titolare del trattamento (art. 6, par. 1, lett. c), GDPR[1]); quindi occorre sempre verificare che vi sia una disposizione di legge o di regolamento per effettuare un trattamento di dati personali;

b) per l'esecuzione di un compito connesso all'esercizio di pubblici poteri di cui è investito il titolare (art. 6, par. 1, lett. e), GDPR).

Si precisa che gli Ordini sono disciplinati:

- dal d.lgs. 28 giugno 2005, n. 139[2] e dal successivo d.P.R. 7 agosto 2012 n. 137[3];
- dai regolamenti approvati dal CNDCEC.

Le finalità del trattamento devono principalmente essere ricercate nell'ambito delle finalità istituzionali degli Ordini professionali, che riguardano:

- l'organizzazione e la gestione dei procedimenti inerenti all'iscrizione, all'aggiornamento e alla verifica della sussistenza dei requisiti per la permanenza nell'albo o nell'elenco speciale, nonché alla tenuta del registro dei tirocinanti;

[1] È il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di dati e che abroga la direttiva 95/46/CE (Regolamento Generale sulla Protezione Dati). Nel presente documento sono frequenti i riferimenti a tale Regolamento attraverso l'utilizzo dell'acronimo "GDPR" e il rinvio alle disposizioni in esso contenute, volutamente non riportate nel testo per agevolarne uno sviluppo maggiormente incentrato sul focus operativo.
[2] Costituzione dell'Ordine dei dottori commercialisti e degli esperti contabili, a norma dell'articolo 2 della legge 24 febbraio 2005, n. 34.
[3] Regolamento recante riforma degli ordinamenti professionali, a norma dell'articolo 3, comma 5, del decreto-legge 13 agosto 2011, n. 138, convertito, con modificazioni, dalla legge 14 settembre 2011, n. 148.

- l'organizzazione e la gestione degli aspetti finanziari conseguenti all'iscrizione all'Ordine, legati al contributo annuale di iscrizione all'albo o nell'elenco speciale, nonché alle eventuali tasse per il rilascio di certificati, copie dei pareri per la liquidazione degli onorari e altro;
- la regolamentazione e la gestione della formazione professionale continua, nonché la vigilanza sull'assolvimento di tale obbligo;
- l'invio delle comunicazioni, pubblicazioni o informative a carattere istituzionale a favore degli iscritti;

ma possono anche essere riferite ad altri adempimenti, come quelli relativi alla gestione del personale, o all'assolvimento di specifici obblighi di legge (es. normativa anticorruzione, sicurezza sul lavoro, ecc.).

La regola generale è che l'Ordine non è tenuto a richiedere il consenso per il trattamento dei dati personali degli iscritti.

2. Le indicazioni per l'informativa privacy da fornire agli iscritti

L'Ordine deve portare a conoscenza degli iscritti una serie di informazioni che riguardano le modalità del trattamento dei dati personali. Le informazioni che devono essere fornite sono elencate nell'art. 13 del GDPR, a cui si rinvia per un approfondimento.

In Appendice si riporta un fac-simile di informativa da fornire agli iscritti che, pur presentando caratteristiche comuni, deve essere adattata alle modalità di trattamento effettuate da ciascun Ordine.

Nell'informativa occorre prestare particolare attenzione ai soggetti a cui vengono comunicati i dati personali, che possono essere quelli previsti da una disposizione di legge o regolamento, nonché quelli nominati responsabili del trattamento per svolgere particolari attività (ad esempio, la società che realizza eventuali tessere per gli iscritti).

3. La valutazione dei rischi inerenti al trattamento dei dati personali

Ciascun Ordine, in base al proprio contesto operativo, è tenuto a predisporre una valutazione dei rischi al fine di individuare le misure di sicurezza ritenute più idonee per fronteggiare i rischi individuati.

Per effettuare la valutazione dei rischi si segnala quale strumento di ausilio il Tool di Enisa che è rinvenibile nel sito del Garante per la protezione dei dati personali al link: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9254237.

4. Le misure di sicurezza tecniche e organizzative

Particolare attenzione va rivolta alle misure di sicurezza che devono essere implementate per proteggere i dati personali trattati dai rischi riguardanti violazioni:

1. della riservatezza;
2. dell'integrità;
3. della disponibilità.

È fondamentale che ciascun Ordine, in base al proprio contesto operativo, predisponga un'analisi dei rischi, anche con l'intervento del soggetto che si interessa della parte informatica, al fine di definire le misure di sicurezza più adeguate.

La sicurezza riguarda la protezione dei dati a prescindere dagli strumenti utilizzati per il loro trattamento; un ruolo centrale è assunto dalla sicurezza IT, in quanto il trattamento dei dati avviene prevalentemente con modalità informatiche.

L'adozione delle misure di sicurezza deve essere vista come una necessità imprescindibile: si pensi alle conseguenze che un attacco hacker potrebbe avere per l'Ordine e per gli iscritti nel caso in cui i backup non vengano eseguiti e i dati siano conseguentemente irrecuperabili.

L'implementazione delle misure di sicurezza informatiche richiede, innanzitutto, la nomina di un soggetto che gestisca e controlli l'infrastruttura informatica dell'Ordine; tale soggetto assume il ruolo di "amministratore di sistema", con nomina a responsabile del trattamento dei dati personali ai sensi dell'art. 28 GDPR.

La sicurezza delle informazioni è trattata anche dagli standard ISO e in particolare da ISO 27701[4] e 27002[5].

Al riguardo si segnalano:

1. il tool di ENISA (European Union Agency for Cybersecurity) elaborato per "testare" la sicurezza delle piccole e medie organizzazioni, applicabile anche ad un Ordine professionale;
2. il framework Nazionale per la cybersecurity e la Data Protection;
3. i controlli CIS (Center for Internet Security);
4. le regole NIST (National Institute of Standards and Technology).

Di seguito si riporta l'elenco delle misure di sicurezza applicabili ad un Ordine professionale.

Inventario degli asset	- Inventario degli hardware, compresi i dispositivi portatili. L'inventario deve indicare: l'indirizzo IP, il nome del computer, il personale a cui è affidata la risorsa

[4] UNI CEI EN ISO/IEC 27701:2021 – Tecniche di sicurezza - Estensione a ISO/IEC 27001 e ISO/IEC 27002 per la gestione delle informazioni in ambito privacy - Requisiti e linee guida.
[5] UNI CEI EN ISO/IEC 27002:2023 – Sicurezza delle informazioni, cybersecurity e protezione della privacy - Controlli di sicurezza delle informazioni.

	- Inventario dei software utilizzati, assicurandosi che vengano utilizzati solo i software supportati dai fornitori - Elenco delle banche dati cartacee e informatiche, classificandole in base ai rischi privacy - Elenco dei soggetti che possono accedere alle banche dati, soprattutto se contengono dati particolari e giudiziari
Definizione dei ruoli e formalizzazione incarichi	- Il personale che tratta i dati personali (dipendenti e collaboratori) deve ricevere specifica lettera di incarico con indicato l'ambito di trattamento - I soggetti esterni che trattano i dati per conto dell'Ordine (consulente del lavoro per tenuta paghe, società che gestisce il sistema informatico, ecc.), devono aver stipulato un accordo ai sensi dell'art. 28 del GDPR in qualità di "responsabili del trattamento"
Policy di sicurezza	- Elaborazione di un documento di *risk analysis* che consenta di attivare le misure di sicurezza da implementare e/o da migliorare in base al progresso tecnologico (tale documento viene elaborato da un esperto in cybersecurity) - Predisposizione della policy per l'utilizzo delle attrezzature informatiche, compresa la gestione delle credenziali di autenticazione - Predisposizione di un piano di formazione per i soggetti che trattano i dati personali
Policy di gestione degli incidenti	- Individuazione della persona incaricata di gestire eventuali incidenti - Predisposizione di un documento che indichi la risposta agli incidenti, compresi i casi in cui occorre effettuare la notifica al Garante della Privacy
Policy di gestione degli account	- Utilizzo delle credenziali individuali per accedere ai sistemi informatici, possibilmente a due sistemi di autenticazione (strong authentication o autenticazione multi-fattore) - Ulteriori accorgimenti quali utilizzo di psw complesse, rinnovo periodico delle psw, limite ai tentativi di accesso - Utilizzo di credenziali univoche per accedere alle risorse informatiche, evitando di creare account condivisi - Blocco degli account inattivi e, in caso di dipendenti che hanno lasciato l'Ordine, cancellazione degli account dopo un periodo non superiore a 3 mesi - Limitazione dei privilegi di accesso in base alle attività da svolgere e al ruolo ricoperto
Sicurezza di rete	- Ricorso a personale tecnico qualificato per la configurazione e gestione della rete informatica - Aggiornamento costante dell'infrastruttura di rete - Divieto di esecuzione di applicazioni scaricate da fonti non attendibili - Impostazione del blocco automatico della sessione in caso di mancato utilizzo della postazione per un determinato periodo di tempo (tale azione, peraltro, non attiene esclusivamente alla "sicurezza di rete") - Implementazione di meccanismi di **filtraggio di rete**, quali firewall o software per il rilevamento delle intrusioni - Implementazione di sistemi di crittografia della rete (VPN) - Gestione delle reti WI-FI mediante crittografia (WPA3 o WPA2) e separazione della rete aperta agli ospiti dalla rete interna
Gestione delle vulnerabilità	- Divieto di utilizzare sistemi operativi non più assistiti dal fornitore - Applicazione delle patch di sicurezza che vengono rilasciate dai produttori (mediante verifica che siano installate con regolarità) - Divieto di assegnare diritti privilegiati (es.: amministratore di sistema) ad utenti che non hanno competenze di sicurezza informatica - Altro
Protezione della Posta	- Utilizzo di soli client di posta elettronica e di browser pienamente supportati e aggiornati alla versione più recente rilasciata dal fornitore

elettronica e del Browser web	- Utilizzo dei servizi di filtro DNS su tutte le risorse per bloccare l'accesso ai domini riconosciuti come pericolosi (configurazione di rete)
Protezione contro i Malware	- Protezione di tutti i PC con software antivirus - Regolare aggiornamento dei software antivirus - Disabilitazione dell'esecuzione e riproduzione automatica per i supporti rimovibili - Formazione degli utenti ai fini del corretto utilizzo delle attrezzature informatiche
Crittografia	- Adozione di un sistema di crittografia per le banche dati che contengono dati particolari e giudiziari
Gestione dei Backup	- Esecuzione di backup automatizzati di tutte le risorse in funzione - (consigliabile) Per la procedura di backup, utilizzo della strategia di backup 3-2-1: (3) Conservare almeno 3 copie dei dati (2) Conservare 2 copie in due luoghi diversi (1) Conservare almeno 1 copia in un luogo al di fuori della sede dell'Ordine - Archiviazione dei dati su uno spazio di archiviazione regolarmente sottoposto a backup accessibile tramite la rete interna dell'Ordine piuttosto che sulle workstation (policy di archiviazione) - Verifica quotidiana dei file di log dei backup da parte dei soggetti a ciò preposti, per controllare che le copie siano state completate correttamente e che non vi siano stati errori - Utilizzo di un sistema di alert sul regolare funzionamento del backup - Esecuzione periodica dei test di ripristino sui backup effettuati
Protezione dei locali[6]	- Controllo dell'accesso ai locali per evitare accessi a persone non autorizzate, installando allarmi antintrusione o altri sistemi di sicurezza - Installazione di rilevatori di fumo e sistemi antincendio - Definizione di una politica di gestione delle chiavi di ingresso - Protezione fisica delle apparecchiature informatiche (es.: elevazione contro possibili allagamenti) - Formalizzazione delle procedure per l'accesso agli uffici fuori dall'orario di lavoro
Formazione del personale	- Formazione del personale sul contenuto delle disposizioni normative in materia di privacy e sulla gestione operativa dei dati - Sensibilizzazione del personale che accede all'infrastruttura informatica sui rischi della rete (es.: come riconoscere un attacco informatico)

5. La valutazione di impatto – DPIA

La valutazione d'impatto si inserisce nel più ampio contesto giuridico sulla protezione dei dati, rappresentato da un approccio basato sul rischio e sulle misure di accountability.

Non tutti i trattamenti effettuati da un titolare devono essere sottoposti a DPIA, ma solo quelli caratterizzati da *un rischio elevato*, tenuto conto – recita la norma – della natura, dell'oggetto, del contesto e delle finalità del trattamento.

La valutazione di impatto può anche essere richiesta come obbligo da una normativa che istituisce delle attività; ad esempio, in materia di whistleblowing, l'art. 13 del d.lgs. 24/2023 prevede che le

[6] Al riguardo, giova evidenziare che alcune misure di sicurezza fisiche dipendono anche dal luogo e da eventuali incidenti passati.

misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato siano definite sulla base di una valutazione d'impatto sulla protezione dei dati.

Tenuto conto che gli Ordini sono obbligati ad adeguarsi alle disposizioni di cui al d.lgs. 24/2023, in Appendice si riporta una esemplificazione di valutazione d'impatto su tale attività.

La DPIA consiste in un documento che deve contenere alcuni elementi necessari, per comodità suddivisi nelle sezioni di seguito riportate[7].

Sezione 1 - Contesto

In questa sezione è fornita una visione complessiva del trattamento o dei trattamenti oggetto di DPIA ed è presentato l'oggetto della valutazione d'impatto.

Nella sezione 1 il titolare deve descrivere i seguenti punti:

Punti	Descrizione	Esempi
Qual è il trattamento in considerazione	- Breve descrizione del trattamento in esame, della sua natura, delle finalità, del contesto - Identificazione del titolare del trattamento e degli eventuali responsabili del trattamento - Elencazione delle normative, delle regole o standard di riferimento applicabili al trattamento, sia utili sia obbligatori (es. i codici di condotta approvati)	Descrizione dell'organigramma privacy dell'Ordine
Quali sono i dati trattati	Descrizione dettagliata della tipologia di dati personali trattati e dei soggetti interessati a cui si riferiscono	- Dati anagrafici (nome, cognome, codice fiscale) - Dati di contatto (indirizzo e-mail, numero di telefono) - Dati particolari (relativi alla salute, all'appartenenza sindacale) - Dati giudiziari
Qual è il ciclo di vita del dato	Descrizione dell'intero ciclo dei dati, dalla loro raccolta alla loro cancellazione	- Come vengono raccolti i dati? - Come vengono archiviati i dati? - Come vengono trasferiti i dati? - Come vengono cancellati i dati?
Quali sono le risorse utilizzate a supporto dei dati	Descrizione dei processi e delle risorse dedicate alla gestione dei dati personali	- Risorse software - Risorse hardware - Archivi cartacei

Sezione 2 – Principi fondamentali

[7] Le indicazioni per la conduzione della valutazione d'impatto prendono riferimento dalle linee guida CNIL e dal relativo software https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assessment

Questa sezione permette di dimostrare l'implementazione degli strumenti necessari per consentire agli interessati di esercitare i loro diritti.

Nella sezione 2 il titolare deve descrivere i seguenti punti:

Punti	Descrizione	Esempi
Presupposti di liceità	Indicazione della base giuridica o delle basi giuridiche su cui si fonda il trattamento	- Esecuzione di un contratto (art. 6.1., lett. b), GDPR) - Adempimento di un obbligo di legge (art. 6.1., lett. c), GDPR) - Consenso dell'interessato (art. 6.1., lett. a), GDPR)
Finalità del trattamento	Descrizione delle finalità per cui i dati sono trattati	- Esecuzione di un contratto - Adempimento di obblighi di legge
Principio di minimizzazione	Descrizione delle circostanze che dimostrano la limitazione della raccolta di dati personali al minimo necessario per la specifica finalità	Es. per le finalità di natura contrattuale: raccogliere solo i dati personali necessari all'instaurazione e gestione del contratto
Periodo di conservazione dei dati	Indicazione del periodo di tempo in cui i dati personali vengono conservati (deve essere definito un periodo di conservazione per ciascun tipo di dato, motivandolo in rapporto alle esigenze del trattamento e/o all'esistenza di vincoli di legge)	Es. per le finalità di natura contrattuale: 10 anni dalla conclusione del contratto
Informativa agli interessati	Descrizione delle modalità con cui viene fornita l'informativa ai sensi degli artt. 13-14 GDPR	Per i dipendenti all'atto di assunzione, per i candidati in fase di colloquio
Esercizio dei diritti riconosciuti dagli artt. 15-22 GDPR	Descrizione delle modalità messe a disposizione del titolare per consentire agli interessati di formulare richieste in materia di privacy	Un canale dedicato come un indirizzo mail privacy@_____, la presenza di una procedura interna per gestire le istanze degli interessati
Trasferimento di dati personali verso Paesi Terzi	Descrizione dei dati personali soggetti a trasferimento verso Paesi Extra UE/non appartenenti allo Spazio Economico Europeo	Utilizzo di *standard contractual clauses* (fattispecie non ricorrente per gli Ordini professionali)

Sezione 3 – Valutazione e analisi dei rischi e individuazione delle misure di sicurezza

Questa sezione permette di valutare i rischi per la sicurezza e riservatezza dei dati, alla luce delle misure esistenti o pianificate. Per la conduzione della valutazione d'impatto si può far riferimento alle linee guida CNIL e al relativo software https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assessmen. Per le misure di sicurezza si rinvia a quanto precedentemente indicato.

Sezione 4 – Conclusione DPIA

La DPIA si conclude con le seguenti attività:

- **predisposizione di un piano d'azione:** consente di definire un piano condiviso delle misure da adottare, delle responsabilità di esecuzione nonché di verifica e consapevolezza del rischio residuo.
- **Predisposizione di un piano di monitoraggio del trattamento:** la DPIA non è da intendersi come un'attività da effettuarsi *una tantum*, ma è un processo che deve essere aggiornato ogniqualvolta le condizioni lo rendano necessario, in base ai cambiamenti di contesto e tecnologici sia interni che esterni.

Si ricorda che:

- ai sensi dell'art. 35, n. 2, GDPR, è previsto che il titolare del trattamento chieda un parere del Responsabile della protezione dei dati/DPO durante la DPIA. Questo parere potrebbe essere sfavorevole all'attuazione del trattamento, senza che ciò limiti il potere decisionale del titolare del trattamento che in tal caso, però, si assumerebbe la responsabilità di tale scelta.
- Ai sensi dell'art. 35, n. 9, GDPR, il titolare, se del caso, raccoglie il parere degli interessati o loro rappresentanti, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti.

6. Le violazioni della sicurezza ("data breach")

All'interno dell'Ordine, come in tutte le organizzazioni, può porsi il problema della violazione di sicurezza (*data breach*) 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.

Una violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità di dati personali.

Di seguito, alcuni possibili esempi di incidenti di sicurezza che possono determinare un *data breach*, da valutarsi caso per caso:

- attacco hacker con esfiltrazione di dati personali (accesso o acquisizione dei dati da parte di terzi non autorizzati);
- furto di un pc con *database* che contengono dati personali (furto o perdita di dati personali);
- alterazione dei dati personali degli iscritti da parte della segreteria;
- impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc.;
- perdita o distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità;

- invio di documenti tramite e-mail in "Cc" anziché "Ccn" (divulgazione non autorizzata dei dati personali).

In caso di *data breach*, l'art. 33 del GDPR prevede la notifica al Garante, da effettuarsi entro 72 ore dal momento in cui si è venuti a conoscenza della violazione dei dati personali, a meno che sia improbabile che quest'ultima presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, la stessa è corredata dei motivi del ritardo.

A partire dal 1° luglio 2021, la notifica di una violazione di dati personali deve essere inviata al GPDP (il Garante per la Protezione dei Dati Personali) tramite un'apposita procedura telematica, resa disponibile nel portale dei servizi online dell'Autorità e raggiungibile all'indirizzo https://servizi.gpdp.it/databreach/s/[8].

Nella stessa pagina è disponibile un facsimile, da non utilizzare per la notifica al Garante, ma utile per vedere in anteprima i contenuti che andranno comunicati.

Per semplificare gli adempimenti previsti per i titolari del trattamento, il Garante ha ideato e messo a disposizione un apposito **strumento di autovalutazione (self assessment)** che consente di individuare le azioni da intraprendere a seguito di una violazione dei dati personali derivante da un incidente di sicurezza.

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

Dal punto di vista operativo, ciascun Ordine deve predisporre un regolamento/procedura con gli step da intraprendere in caso di *data breach*. Tale Regolamento dovrà indicare:

a) i soggetti a cui comunicare il *data breach* (DPO, Consiglio, ecc.);
b) le azioni da intraprendere per porre rimedio alla violazione;
c) la valutazione del *data breach* e le modalità per l'eventuale notifica al Garante e per la comunicazione agli interessati;
d) le modalità da utilizzare per documentare l'incidente, anche se non ha comportato un *data breach*.

7. Il responsabile per la protezione dati (RPD/DPO)

In quanto enti pubblici non economici a carattere associativo, per gli Ordini professionali la designazione del RPD rappresenta un obbligo ai sensi dell'art. 37, par. 1, lett. a), del GDPR. La designazione del RPD deve essere notificata al Garante per la protezione dei dati personali (https://www.garanteprivacy.it/responsabile-della-protezione-dei-dati-rpd-).

[8] Si veda il Provvedimento GPDP del 27 maggio 2021.

Gli Ordini professionali devono provvedere alla nomina del RPD nel rispetto di quanto statuito nel GDPR, tenendo conto delle indicazioni fornite dal Gruppo di lavoro c.d. "Articolo 29" o "WP29"[9] e dal Garante per la protezione dei dati personali.

Il ruolo di RPD può essere ricoperto da un soggetto interno all'organizzazione del titolare o del responsabile del trattamento, oppure può essere affidato a soggetti esterni. Si precisa che, in considerazione delle dimensioni e dell'organizzazione tipiche degli Ordini territoriali, difficilmente un Consiglio sarà in grado di individuare all'interno dell'Ordine un soggetto in possesso dei requisiti richiesti dalla norma.

In entrambi i casi, infatti, i soggetti nominati devono essere in grado di garantire l'effettivo assolvimento dei compiti che il GDPR assegna a tale figura. Il RPD individuato all'interno andrà nominato mediante specifico atto di designazione (ad es. lettera d'incarico), mentre quello individuato all'esterno sarà nominato mediante un contratto di servizi. Tali atti, da redigere in forma scritta, dovranno contenere la designazione del RPD e indicare espressamente i compiti ad esso attribuiti, le risorse assegnate per il loro svolgimento, nonché ogni altra utile informazione in rapporto al contesto di riferimento.

Qualora sia successivamente conferito incarico a un soggetto diverso, si rammenta che la mancata comunicazione della variazione della nomina del RPD, così come la mancata nomina del RPD o l'omessa comunicazione della nomina del RPD, espongono l'Ordine all'applicazione delle sanzioni previste dal GDPR.

È bene ricordare che il RPD non risponde personalmente in caso di inosservanza del GDPR. Quest'ultimo chiarisce, infatti, che spetta al titolare del trattamento o al responsabile del trattamento garantire ed essere in grado di dimostrare che le operazioni di trattamento siano conformi alle disposizioni del Regolamento stesso (art. 24, par. 1). L'onere di assicurare il rispetto della normativa in materia di protezione dei dati ricade sul titolare del trattamento o sul responsabile del trattamento.

In base all'art. 37, par. 5, GDPR, il RPD "*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 di cui all'articolo 39*".

Requisiti del RPD

❖ **Conoscenze specialistiche**

Il livello di conoscenza specialistica richiesto deve essere proporzionato alla sensibilità, complessità e quantità dei dati sottoposti a trattamento. Ad esempio, se un trattamento riveste particolare complessità oppure comporta un volume consistente di dati sensibili, il livello di conoscenze specialistiche e di supporto richiesto al RPD sarà necessariamente elevato.

[9] Il Gruppo di lavoro "Articolo 29" (WP29), istituito dalla direttiva 95/46/CE, si è occupato delle questioni relative alla tutela della privacy e dei dati personali fino al 25 maggio 2018 (entrata in vigore del GDPR), data a partire dalla quale è stato sostituito dall'EDPB (European Data Protection Board).

Ne consegue la necessità per l'Ordine di tenere conto degli elementi sopra indicati nella scelta del RPD.

❖ **Qualità professionali**

L'art. 37, par. 5, GDPR non specifica le qualità professionali da prendere in considerazione ai fini della nomina di un RPD; tuttavia, è opportuno che la scelta di un RPD ricada su un soggetto che abbia una comprovata conoscenza della normativa e delle prassi nazionali ed europee in materia di protezione dei dati e un'approfondita conoscenza del GDPR.

È utile prendere in considerazione anche la conoscenza, da parte del candidato, dello specifico settore di attività e della struttura organizzativa dell'Ordine.

❖ **Capacità di assolvere i propri compiti**

La capacità di assolvere i compiti da parte del RPD è legata non solo alle qualità professionali e alle conoscenze, ma anche alla sua integrità e ai suoi standard deontologici; questo perché il RPD svolge un ruolo chiave nel promuovere la cultura della protezione dei dati all'interno dell'ente e contribuisce a dare attuazione ad elementi essenziali del Regolamento, quali i principi fondamentali del trattamento, i diritti degli interessati, la protezione dei dati sin dalla fase di progettazione (*privacy by design*) e per impostazione predefinita (*privacy by default*), i registri delle attività di trattamento, la sicurezza dei trattamenti e la notifica e comunicazione delle violazioni di dati personali.

***

Nominare un RPD privo di adeguate competenze, oltre che minare gravemente la sicurezza dei trattamenti effettuati, comporterebbe la violazione degli artt. 5 e 37 del GDPR, con conseguente applicazione delle sanzioni previste dall'art. 83 GDPR.

La conoscenza specialistica e le qualità professionali possono essere verificate dall'Ordine chiedendo al potenziale RPD di documentare la propria esperienza professionale anche attraverso la partecipazione ad attività formative specialistiche (ad esempio master, corsi di studio e professionali) o di indicare esperienze lavorative in organizzazioni simili a quella dell'Ordine professionale.

Nella scelta del RDP, al fine di prevenire la possibilità di ricevere un'assistenza inadeguata, l'Ordine dovrebbe tenere in considerazione i seguenti ulteriori elementi:

a) il numero di incarichi già ricoperti dalla società o dal professionista al quale si intende affidare l'incarico;
b) in caso di società, il possesso dei requisiti da parte del referente persona fisica.

Il RPD sarà in grado di svolgere adeguatamente i propri compiti se:

➢ **è coinvolto dall'Ordine in tutte le questioni riguardanti la protezione dei dati personali.**

Ai sensi dell'art. 38 GDPR, il titolare del trattamento e il responsabile del trattamento assicurano che il RPD sia "*tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali*".

È essenziale che l'Ordine coinvolga il RPD tempestivamente su ogni questione relativa al trattamento e alla protezione dei dati: ad esempio, se deve essere predisposta una valutazione di impatto (DPIA), il Regolamento prevede espressamente che il RPD sia coinvolto fin dalle fasi iniziali; il titolare del trattamento ha l'obbligo di consultarlo nell'effettuazione della DPIA. Inoltre, è importante che il RPD partecipi ai gruppi di lavoro che volta per volta si occupano delle attività di trattamento.

A titolo esemplificativo, occorrerà garantire:

- la presenza del RPD ogniqualvolta debbano essere assunte decisioni che impattano sulla protezione dei dati. Il RPD deve disporre tempestivamente di tutte le informazioni pertinenti in modo da poter rendere una consulenza adeguata;
- che il parere del RPD riceva sempre la dovuta considerazione. In caso di disaccordo è buona prassi per l'Ordine documentare le motivazioni che hanno portato a condotte difformi da quelle raccomandate dal RPD;
- che il RPD sia consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente.

➢ **È dotato delle risorse necessarie**

L'art. 38, par. 2, GDPR obbliga il titolare del trattamento o il responsabile del trattamento a sostenere il RPD "*fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica*". Ciò significa che:

- il RPD deve avere tempo sufficiente per l'espletamento dei compiti che gli sono affidati. Questo soprattutto in caso di designazione di un RPD interno, oppure di RPD esterno, ma che debba occuparsi di altre incombenze oltre che di protezione dati, poiché il rischio è che le attività che il RPD è chiamato a svolgere finiscano per essere trascurate a causa di conflitti con altre priorità.
- Il RPD deve avere un supporto adeguato in termini di risorse finanziarie, infrastrutture (sede, attrezzature, strumentazione) e, ove opportuno, personale.
- Il titolare del trattamento deve dare comunicazione ufficiale della nomina del RPD a tutto il personale, in modo da garantire che la sua presenza e le sue funzioni siano note all'interno dell'Ordine.
- l'Ordine deve garantire l'accesso del RPD a tutte le informazioni inerenti alle attività che prevedono un trattamento di dati personali, così da fornirgli supporto e *input* essenziali.
- In base alle dimensioni e alla struttura dell'Ordine, può essere necessario costituire un gruppo di lavoro RPD (formato dal RPD stesso e dal personale), definendone la struttura interna, oltre ai compiti e alle responsabilità individuali.

➢ **È indipendente nell'adempimento delle proprie funzioni e compiti.**

L'indipendenza del RPD può essere garantita rispettando le seguenti raccomandazioni:

- ***il RPD non deve ricevere istruzioni***

L'Ordine deve consentire al RPD di operare con un grado sufficiente di autonomia all'interno della propria organizzazione; ciò significa che il RPD, nell'esecuzione dei compiti, non deve ricevere istruzioni sull'approccio da seguire nel caso specifico, né sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati.

Se l'Ordine assumesse decisioni incompatibili con il GDPR e/o con le indicazioni fornite dal RPD, quest'ultimo dovrebbe avere la possibilità di manifestare il proprio dissenso al Consiglio dell'Ordine.

- ***Rimozione o penalizzazioni in rapporto all'adempimento dei compiti di RPD***

Il GDPR prevede che il RPD "*non sia rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti*".

Il divieto di penalizzazioni a cui fa riferimento il GDPR si applica solo con riguardo a quelle penalizzazioni eventualmente derivanti dallo svolgimento dei compiti "propri" del RPD. Ad esempio, un RPD può ritenere che un determinato trattamento comporti un rischio elevato e quindi raccomandare al titolare del trattamento di condurre una valutazione di impatto; se il titolare non concorda con la valutazione del RPD, non è ammissibile che quest'ultimo sia rimosso dall'incarico per avere formulato la raccomandazione in oggetto.

Le penalizzazioni possono assumere molte forme e avere natura diretta o indiretta: ad esempio, potrebbero consistere, nel caso di un RPD interno, nella mancata o ritardata promozione, nel blocco delle progressioni di carriera, nella mancata concessione di incentivi rispetto ad altri dipendenti. È sufficiente anche la sola minaccia della penalizzazione. Sarebbe invece legittima l'interruzione del rapporto con il RPD per motivazioni diverse dallo svolgimento dei compiti che gli sono propri: per esempio in caso di gravi violazioni deontologiche.

- ***Conflitto di interessi***

Il GDPR prevede che il RPD possa "*svolgere altri compiti e funzioni*" a condizione che il titolare del trattamento o il responsabile del trattamento si assicuri che "*tali compiti e funzioni non diano adito a un conflitto di interessi*".

L'Ordine può quindi affidare ulteriori compiti e funzioni al RPD, ma solo a condizione che non comportino un conflitto di interessi: ad esempio, il RPD non può rivestire, all'interno dell'Ordine, un ruolo che comporti la definizione delle finalità o modalità del trattamento di dati personali.

Si ha un conflitto di interessi in capo al RPD se questi si trova in una di queste situazioni:

- ha ruoli manageriali di vertice nell'Ente;
- ricopre posizioni gerarchicamente inferiori alle precedenti, ma che comportano comunque la determinazione di finalità o mezzi del trattamento;
- rappresenta (RPD esterno) l'Ordine in un giudizio che includa problematiche in materia di protezione dei dati.

Compiti del RPD

Il GDPR assegna al RPD i seguenti compiti:

- **sorvegliare l'osservanza del GDPR**, valutando i rischi di ogni trattamento alla luce della natura, dell'ambito di applicazione, del contesto e delle finalità.

  Il RPD deve controllare che l'Ordine rispetti il GDPR, sia raccogliendo informazioni per individuare i trattamenti effettuati, analizzandoli e verificandone la conformità, sia svolgendo attività di informazione, consulenza e indirizzo nei confronti dell'Ordine stesso.

- Collaborare con l'Ordine, laddove necessario, nel condurre una **valutazione di impatto sulla protezione dei dati (DPIA).**

  In particolare, l'Ordine può consultare il RPD sulle seguenti tematiche:

  - se occorre condurre o meno una DPIA;
  - quale metodologia adottare nel condurre una DPIA;
  - se condurre la DPIA con le risorse interne ovvero esternalizzando tale attività;
  - quali cautele/accorgimenti applicare nel trattamento dei dati, comprese misure tecniche e organizzative, per attenuare i rischi per i diritti delle persone interessate;
  - se la DPIA sia stata condotta correttamente o meno e se le conclusioni raggiunte (procedere o meno con il trattamento e quali salvaguardie applicare) siano conformi al GDPR.

  Qualora l'Ordine non concordi con le indicazioni fornite dal RPD, è necessario che la documentazione relativa alla DPIA riporti specificamente per iscritto le motivazioni per cui si è ritenuto di non conformarsi.

- **Informare e sensibilizzare** l'Ordine e i dipendenti di quest'ultimo riguardo agli obblighi derivanti dal GDPR e da altre disposizioni in materia di protezione dei dati.
- **Cooperare con il Garante e fungere da punto di contatto** su ogni questione connessa al trattamento, facilitando così l'accesso del Garante ai documenti e alle informazioni necessarie per adempiere ai propri compiti ed esercitare i propri poteri di indagine, correttivi, autorizzativi e consultivi.
- **Supportare** l'Ordine in ogni attività connessa al trattamento di dati personali, anche con riguardo alla tenuta di un **registro delle attività di trattamento.**

  Il GDPR prevede che siano il titolare o il responsabile del trattamento – e non il RPD – a tenere i registri delle attività di trattamento rispettivamente svolte.

  È comunque possibile chiedere al RPD di predisporre l'inventario dei trattamenti e tenere un registro di tali trattamenti sulla base delle informazioni fornite dai vari uffici o unità che trattano dati personali dell'Ordine professionale.

Designazione del RPD e pubblicità della nomina

Dal punto di vista operativo, una volta selezionato il RDP, l'Ordine deve:

- designarlo; a tal proposito il Garante, nel proprio sito, ha messo a disposizione uno schema di atto di designazione;
- pubblicare i dati di contatto del RPD sul proprio sito e comunicarli al Garante per la protezione dei dati personali.

In assenza dei predetti adempimenti, è vanificata la necessaria trasparenza informativa dell'Ordine nei confronti sia degli interessati, che in questo modo non sanno dell'esistenza di una figura cui rivolgere le istanze in materia di trattamento dei propri dati personali, che del Garante, venendo meno quel punto di contatto essenziale per lo svolgimento dei propri compiti istituzionali.

I dati di contatto del RPD (almeno un indirizzo di posta elettronica ordinaria, eventualmente integrata con un indirizzo PEC) dovranno essere pubblicati all'interno di una sezione del sito *web* dell'Ordine facilmente riconoscibile dall'utente e accessibile già dalla homepage, oltre che nell'ambito della sezione dedicata all'organigramma dell'Ordine e ai relativi contatti. È consigliabile che l'Ordine renda disponibile una casella istituzionale *ad hoc* attribuita specificamente al RPD; non è necessario che sul sito dell'Ordine sia indicato anche il nominativo del RPD.

Per la comunicazione al Garante del RPD nominato, così come per la variazione e la revoca del nominativo del medesimo, è prevista un'apposita procedura *online*. Tale procedura rappresenta l'unico canale di contatto utilizzabile ed è reperibile alla pagina https://servizi.gpdp.it/comunicazionerpd/s/, ove sono riportate anche le apposite istruzioni e le relative FAQ.

8. Il registro delle attività di trattamento

Gli Ordini professionali, in quanto titolari del trattamento dei dati personali ai sensi dell'art. 30 del GDPR, sono tenuti, tra l'altro, ad adottare il Registro delle attività di trattamento.

È necessario precisare che, secondo la citata disposizione normativa, l'obbligo su riportato non si applica alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, di dati genetici, biometrici, dati relativi alla salute, alla vita o all'orientamento sessuale o di dati relativi a condanne penali e a reati.

Tuttavia - dato che si tratta di uno strumento da considerarsi parte integrante di un sistema di corretta gestione dei dati personali - è opportuno che tutti i titolari (e, quindi, anche gli Ordini), a prescindere

dalle dimensioni dell'organizzazione, si dotino del registro dei trattamenti e, in ogni caso, compiano un'accurata ricognizione dei trattamenti svolti e delle loro caratteristiche.

A tal proposito, si rammenta quanto affermato dall'Autorità Garante: "Al di fuori dei casi di tenuta obbligatoria del Registro, anche alla luce del considerando 82 del RGPD, il Garante ne raccomanda la redazione a tutti i titolari e responsabili del trattamento, in quanto strumento che, fornendo piena contezza del tipo di trattamenti svolti, contribuisce a meglio attuare, con modalità semplici e accessibili a tutti, il principio di accountability e, al contempo, ad agevolare in maniera dialogante e collaborativa l'attività di controllo del Garante stesso"[10].

Sul tema, si invita altresì a consultare il documento interpretativo del 19 aprile 2018 del Gruppo ex art. 29, reperibile al seguente link: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=624045.

Il registro contiene le seguenti informazioni:

- il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento e del responsabile della protezione dei dati;
- le finalità del trattamento;
- una descrizione delle categorie di interessati e delle categorie di dati personali;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

Tale registro è tenuto in forma scritta, anche in formato elettronico.

Si rammenta che, ove richiesto, il titolare del trattamento mette il registro a disposizione dell'autorità di controllo.

In Appendice viene riportato un fac-simile di registro delle attività di trattamento.

[10] https://www.garanteprivacy.it/registro-delle-attivita-di-trattamento

PARTE SECONDA

I diritti degli iscritti (interessati al trattamento dei dati)

1. I diritti

L'impianto normativo europeo e nazionale è incentrato sulla tutela dei dati personali di un individuo (c.d. interessato), nonché sulla trasparenza in merito alle attività di trattamento poste in essere dai soggetti destinatari, in modo da garantire all'interessato un effettivo controllo sulle proprie informazioni e sui propri dati, anche attraverso l'esercizio di specifici diritti previsti dal GDPR.

Nel presente paragrafo si prendono in considerazione gli iscritti all'albo, all'elenco speciale e al registro dei tirocinanti. in quanto interessati.

Altre categorie di interessati i cui dati possono essere trattati dall'Ordine Professionale possono essere quelle dei dipendenti, degli stagisti, dei collaboratori e dei fornitori (persone fisiche).

Di seguito si propone uno schema riepilogativo dei diritti degli interessati:

Diritto di accesso	L'interessato ha il diritto di chiedere all'Ordine se quest'ultimo effettua un trattamento di dati che lo riguardano e, nel caso in cui ciò avvenga, ha il diritto di ottenere l'accesso ai dati personali per conoscere le informazioni elencate nell'art. 15 del GDPR, a cui si rinvia. L'Ordine dovrà garantire tutte le tutele previste in tale caso, soprattutto per quanto riguarda la segretezza e la riservatezza della richiesta. A titolo meramente indicativo, nel caso di consegna di dato su supporto cartaceo, l'Ordine potrà procedere con identificazione del soggetto che ritira il fascicolo, chiedendo esibizione di delega nel caso in cui si tratti di soggetto delegato. Ove invece il dato sia fornito elettronicamente, l'Ordine dovrà predisporre un sistema di consultazione sicuro prevedendo, ad esempio, un accesso riservato con identificazione mediante nome utente e password.
Diritto di rettifica	L'interessato può richiedere che l'Ordine, senza ingiustificato ritardo, rettifichi i suoi dati personali inesatti o integri i dati incompleti. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa. In questo caso è la stessa norma a dettare una possibile procedura da seguire: l'Ordine acquisisce la dichiarazione da parte dell'iscritto sia in modalità cartacea sia in modalità elettronica, fermo restando che la trasmissione a mezzo PEC è quella che conferisce carattere legale e ufficiale alla comunicazione resa.
Diritto di cancellazione	L'interessato ha il diritto di ottenere dall'Ordine, senza ingiustificato ritardo, la cancellazione dei dati personali che lo riguardano se sussiste uno dei motivi seguenti: a) i dati personali non sono più necessari rispetto alle finalità per i quali sono stati raccolti e trattati; b) l'interessato revoca il consenso; c) l'interessato si oppone al trattamento dei dati; d) i dati sono stati trattati illecitamente; e) sorge un obbligo legale di cancellazione. Resta inteso che l'Ordine procederà a dare seguito alle richieste dell'interessato, fatti salvi gli obblighi di legge in materia ordinistica.

Diritto di limitazione di trattamento	L'interessato ha il diritto di ottenere dall'Ordine la limitazione del trattamento quando ricorre una delle seguenti ipotesi: a) contestazione dell'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati; b) trattamento illecito e opposizione alla cancellazione dei dati personali con richiesta di limitato utilizzo; c) il titolare del trattamento non ne ha più bisogno ai fini del trattamento, ma i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria; d) l'interessato si è opposto al trattamento ai sensi dell'art. 21, par. 1, GDPR, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato. Il diritto alla limitazione prevede che il dato personale sia "contrassegnato" in attesa di determinazioni ulteriori; pertanto, è opportuno che l'Ordine preveda nei propri sistemi informativi (elettronici o meno) misure idonee a tale scopo (ad esempio, l'inserimento nelle anagrafiche degli interessati di appositi flag da spuntare per impedire al titolare del trattamento e agli addetti che vengano trattati i dati sottoposti a "limitazione"). Resta inteso che l'Ordine procederà a dare seguito alle richieste dell'interessato, fatti salvi gli obblighi di legge in materia ordinistica.
Diritto di opposizione	L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano connessi a ragioni di interesse pubblico o all'esercizio di pubblici poteri. In questo caso l'Ordine si astiene dal trattare ulteriormente i dati personali dell'iscritto, salvo che dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per i casi di accertamento, esercizio o difesa di un diritto in sede giudiziaria.

Al fine di consentire l'esercizio dei diritti dell'interessato, l'Ordine deve implementare una procedura interna specifica, che può prevedere:

a) la compilazione di un modulo predefinito (si veda il fac-simile di modulo riportato in Appendice);

b) l'invio del modulo a mezzo mail, PEC, posta ordinaria ecc.

c) le modalità e la tempistica da rispettare per dar seguito alla richiesta[11].

2. I regolamenti

I regolamenti hanno lo scopo di definire e portare a conoscenza del personale dell'Ordine le procedure (o policy) che vengono adottate per un corretto e adeguato trattamento dei dati personali. Inoltre, i regolamenti servono per comprovare il rispetto dei principi generali previsti dall'art. 5 del GDPR e, insieme agli altri documenti (registro dei trattamenti, informative, ecc.), rappresentano la "accountability" dell'Ordine.

Nel dettaglio, si suggerisce a ciascun Ordine di predisporre:

[11] Ai sensi dell'art. 12, co. 3, del GDPR, il titolare del trattamento deve fornire riscontro "senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste. Il titolare del trattamento informa l'interessato di tale proroga, e dei motivi del ritardo, entro un mese dal ricevimento della richiesta".

a) il regolamento per l'utilizzo delle attrezzature informatiche, ivi compreso l'utilizzo della posta elettronica[12];

b) il regolamento per il trattamento dei dati personali, dove vengono disciplinate le modalità del trattamento;

c) il regolamento per l'esercizio dei diritti degli interessati;

d) il regolamento contenente una procedura in caso di *data breach*.

Tali regolamenti, una volta definiti, devono essere diffusi tramite un'attività di formazione rivolta al personale dipendente e in generale a tutti i soggetti che trattano dati personali all'interno dell'Ordine.

In quanto atti organizzativi, i regolamenti richiedono l'approvazione da parte del Consiglio dell'Ordine.

[12] Al riguardo si veda GPDP, *Lavoro: le linee guida del Garante per posta elettronica e internet*, in Gazzetta Ufficiale n. 58 del 10 marzo 2007.

PARTE TERZA

Gli aspetti privacy e i dipendenti degli ordini professionali

1. Gli adempimenti privacy verso i dipendenti degli Ordini

Con riferimento ai dipendenti degli Ordini, ai fini privacy, è necessario:

a) rendere adeguata **informativa** redatta secondo i contenuti previsti dall'art. 13 del GDPR prima di iniziare le operazioni di trattamento dei dati. L'informativa privacy deve essere consegnata al dipendente all'atto dell'assunzione. Il trattamento dei dati personali del dipendente non richiede il consenso del lavoratore, in quanto trova la propria base giuridica nel contratto di lavoro e nei relativi obblighi di legge. Il consenso specifico del dipendente deve invece essere richiesto nel caso in cui debbano essere trattati dati che esulano da quelli necessari alla normale gestione del rapporto di lavoro: può trattarsi, ad esempio, della pubblicazione di dati e immagini[13] sul sito web istituzionale. In questo caso il consenso può anche essere negato, senza alcuna conseguenza sul rapporto di lavoro. In generale, è opportuno segnalare nell'informativa la presenza di eventuali strumenti che possono raccogliere dati personali per i quali sono richieste delle procedure specifiche, come un sistema di rilevazione presenze o un impianto di videosorveglianza.

b) **Autorizzare** il dipendente al trattamento dei dati personali. La nomina di un soggetto autorizzato deve essere effettuata in modo accurato, documentata e deve indicare chiaramente le responsabilità e i permessi di gestione dei dati nell'ambito dei compiti attribuiti al soggetto autorizzato, nonché le limitazioni delle sue azioni. Inoltre, il soggetto autorizzato deve essere adeguatamente formato sulla protezione dei dati personali ed essere in grado di garantire la riservatezza e la sicurezza del trattamento dei dati. Con riguardo alle **attività di trattamento**, a titolo esemplificativo queste potranno avere ad oggetto:

   - la gestione anagrafica degli iscritti all'Ordine;
   - la gestione anagrafica dei componenti del Consiglio dell'Ordine, del Consiglio di Disciplina, dell'Organismo di Composizione della Crisi (OCC), dei dipendenti e dei fornitori dell'Ordine;
   - la gestione dei dati inseriti nelle eventuali piattaforme di formazione;
   - la gestione dei dati inerenti al sito web, ove sia presente un'area riservata, o da altre applicazioni;
   - la gestione della corrispondenza cartacea ed elettronica;
   - la gestione dei servizi di informazione e di formazione professionale continua;
   - la gestione degli iscritti alle newsletter;

[13] In tal caso, si rammenta la necessità di far sottoscrivere apposita liberatoria ai sensi degli artt. 10 e 320 c.c. e degli artt. 96 e 97 della Legge 22 aprile 1941, n. 633.

- la gestione inerente al registro dei visitatori;
- la gestione dell'albo, dei registri e degli elenchi degli iscritti e dei tirocinanti;
- l'organizzazione e gestione degli esami di Stato;
- la gestione dei dati in materia disciplinare (ricorsi/reclami);
- la gestione dei dati in materia elettorale e dei membri degli organi elettivi;
- le attività di formazione sia obbligatoria sia facoltativa degli iscritti e la gestione delle iscrizioni;
- la gestione dei consulenti e dei fornitori;
- la gestione dei dipendenti;
- la gestione del contenzioso giudiziale e stragiudiziale;
- la gestione delle informazioni acquisite in sede di prestazione di attività di assistenza e consulenza agli iscritti.

Naturalmente, l'elenco dovrà essere di volta in volta valutato in considerazione delle specifiche attività di trattamento poste in essere dagli incaricati del trattamento nell'ambito dell'Ordine di appartenenza.

È consigliabile che l'Ordine – ferma restando la possibilità di individuare le modalità ritenute più opportune – predisponga un **atto formale** di nomina dei propri soggetti designati, contenente altresì le **istruzioni necessarie al trattamento dei dati personali** (si veda il fac-simile di nomina fornito nell'Appendice).

c) **Formare** il dipendente al trattamento dei dati personali. Si suggerisce di predisporre formalmente un piano di formazione almeno annuale da comunicare ai dipendenti (e ai neo assunti), in modo che ciascuna persona che agisca sotto l'autorità dell'Ordine nel trattamento di dati personali possa agevolmente comprendere e rispettare le politiche che lo stesso ha adottato. È opportuno documentare ogni decisione presa in relazione al piano di formazione, alla sua efficacia e al suo monitoraggio e miglioramento.

All'interno di ciascun Ordine Professionale è necessario definire un **organigramma privacy** che dovrà indicare, oltre all'Ordine in quanto titolare del trattamento, gli eventuali contitolari, i responsabili del trattamento, il responsabile della protezione dei dati e i soggetti autorizzati al trattamento dei dati personali.

2. L'individuazione dei soggetti autorizzati

Con riferimento ai soggetti autorizzati a trattare i dati all'interno dell'Ordine, sicuramente dovranno essere designati e formati i dipendenti, i collaboratori[14] e le figure apicali.

Attesa la natura degli Ordini professionali, difficilmente è presente personale interno non impegnato nel trattamento di dati personali, con mansioni che escludano, ad esempio, l'uso dei dispositivi e l'accesso agli archivi cartacei ed elettronici.

Saranno quindi designati:

- dipendenti (impiegati in vari uffici: segreteria, amministrazione, altro);
- collaboratori;
- amministratore di sistema (se interno);
- componenti del Consiglio dell'Ordine;
- componenti delle commissioni (sia interne che commissioni di studio);
- referente OCC.

Ovviamente ciascun soggetto avrà autorizzazioni e permessi differenti in base alla propria funzione, vedendosi assegnati solo i trattamenti necessari nel rispetto del principio di minimizzazione. Il trattamento dei dati personali deve avvenire in base al principio del "*need to know*", in quanto gli stessi non devono essere condivisi, comunicati o inviati a persone a cui non sono necessari per lo svolgimento delle mansioni lavorative assegnate (anche nel caso in cui queste persone siano a loro volta designate al trattamento dati).

[14] Per collaboratori si intendono tutti quei soggetti che operano sotto la supervisione del titolare e utilizzano mezzi e strumenti del titolare.

PARTE QUARTA

I rapporti privacy con i soggetti esterni fornitori di beni e/o servizi

In merito al trattamento dei dati relativi ai fornitori di beni e/o servizi, è necessaria la puntuale identificazione del titolare e del responsabile del trattamento: il primo determina finalità e mezzi del trattamento, il secondo esegue le operazioni di trattamento per conto e sulla base delle istruzioni del titolare.

Con riferimento ai fornitori di servizi è necessario porre attenzione a quelli che offrono servizi che presuppongono anche un trattamento dei dati personali per conto dell'Ordine. Taluni vengono qualificati come "responsabili del trattamento", altri come "titolari autonomi": ad esempio, il medico competente che tratta i dati personali dei dipendenti dell'Ordine assume il ruolo di "titolare autonomo", mentre il consulente del lavoro per la tenuta delle paghe quello di "responsabile del trattamento".

È fondamentale, quindi, identificare i presupposti in base ai quali ci si trova ad interagire con un autonomo titolare del trattamento o con un responsabile del trattamento dei dati.

1. L'identificazione del responsabile del trattamento

Come evidenziato dalle Linee guida EDPB 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR, le due condizioni fondamentali per la qualifica di un soggetto quale responsabile del trattamento ex art. 28 GDPR sono:

a) essere un soggetto distinto rispetto al titolare del trattamento;
b) trattare i dati personali per conto del titolare del trattamento.

Una volta identificato il responsabile del trattamento, occorre definire all'interno di uno specifico contratto, ovvero altro atto giuridico che vincoli il responsabile del trattamento al titolare del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento (si veda l'art. 28, par. 3, GDPR).

Il GDPR indica dettagliatamente una serie di doveri in capo al responsabile che l'atto di designazione deve necessariamente prevedere. Adozione delle misure tecniche e organizzative di sicurezza, supporto nella compliance del titolare, comunicazione al titolare di eventuali *data breach*: sono alcune delle forme con cui il Regolamento mira a rendere consapevole il responsabile del trattamento.

Stipulato l'accordo di nomina a responsabile del trattamento, il titolare e il responsabile dovranno collaborare al fine di trattare i dati personali conformemente alla normativa e nel rispetto dei diritti degli interessati. Tra gli obblighi del responsabile del trattamento vi è, infatti, quello di mettere a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto

degli obblighi di cui al citato art. 28 GDPR, nonché di consentire le attività di revisione, comprese le ispezioni, realizzate dal titolare del trattamento o da altro soggetto da questi incaricato.

Il titolare è dunque legittimato ad effettuare controlli nei confronti del responsabile del trattamento, al fine di verificare l'operato dello stesso, consentendogli di dimostrare di aver controllato e di controllare i soggetti che trattano dati personali per suo conto. Sarà comunque opportuno disciplinare all'interno dell'accordo le modalità di effettuazione di eventuali controlli e richieste da parte del titolare al responsabile, in modo da evitare possibili contestazioni.

L'atto di designazione del responsabile del trattamento deve avere forma scritta (in virtù del principio di non discriminazione, anche elettronica).

Il responsabile del trattamento ha facoltà di designare, previa autorizzazione scritta del titolare, un altro responsabile (comunemente denominato "sub-responsabile"). In tal caso, il contratto o l'atto giuridico vincolante il sub-responsabile non avrà contenuto autonomo, ma dovrà riprodurre gli obblighi in materia di protezione dei dati indicati nell'atto con cui il titolare ha nominato il responsabile iniziale. In caso di inadempimento del sub-responsabile ai prescritti obblighi, sarà il responsabile che l'ha designato a risponderne nei confronti del titolare.

2. Alcuni responsabili del trattamento dell'Ordine

Come chiarito, per individuare quali tra i fornitori dell'Ordine possono qualificarsi come responsabili, occorre tenere in considerazione tutti i trattamenti effettuati, anche quelli limitati e occasionali; devono essere comunque selezionati solo fornitori di servizi che garantiscano il rispetto del regolamento e la tutela dei diritti privacy degli interessati.

Per meglio comprendere quanto specificato nel dettato normativo di riferimento, si riportano alcuni casi messi in luce dal Garante per la Protezione dei dati personali: ad esempio, deve essere considerato autonomo titolare del trattamento il medico competente, il quale tratta dati personali in applicazione della disciplina in materia di igiene e sicurezza sul lavoro, così come l'avvocato che fornisce una consulenza, in quanto non si limita ad offrire il proprio servizio sulla base delle istruzioni ricevute, ma svolge il proprio incarico in maniera autonoma.

Più in generale, ferma restando la necessità di valutare caso per caso il contenuto del contratto tra le parti, è possibile identificare i seguenti responsabili del trattamento:

- il consulente del lavoro (per l'elaborazione delle buste paga), che assume la veste di responsabile del trattamento quando tratta i dati dei dipendenti dei clienti in base all'incarico da questi ricevuto;
- le società di servizi incaricate della gestione del sito web o dei servizi cloud, che assumono la responsabilità esterna nel trattamento dei dati personali;

- le società di servizi di videosorveglianza, purché abbiano accesso diretto e immediato alle videoregistrazioni. Ad esempio, l'istituto di vigilanza privata che gestisce un impianto di videosorveglianza per un cliente dovrà essere designato da quest'ultimo quale responsabile del trattamento e ricevere al contempo le istruzioni previste, con particolare riguardo all'indicazione dei termini di conservazione delle immagini.

PARTE QUINTA

Focus operativi

1. La privacy e la formazione professionale continua

Per una corretta applicazione della metodologia di seguito descritta è necessario identificare i soggetti coinvolti nel processo di trattamento e assegnare specifiche responsabilità e diritti in relazione alle attività delle diverse fasi.

Per l'ambito "Formazione Continua" è consigliabile nominare, previo parere del RPD, un owner (assessor) del processo, vale a dire un responsabile dell'applicazione della metodologia di assessment, che ha il compito di:

- assegnare i ruoli previsti dal processo di implementazione ed esecuzione della metodologia;
- programmare e supervisionare lo svolgimento del processo;
- coordinare le attività di definizione dei contenuti per le fasi dei controlli operativi e di monitoraggio;
- acquisire e conservare tutte le evidenze documentali dell'esecuzione e manutenzione della metodologia.

Nelle due schede che seguono sono sintetizzati gli adempimenti privacy nell'organizzazione degli eventi di formazione.

TRATTAMENTO: formazione professionale continua - organizzazione evento in presenza		
Descrizione del processo. Il Consiglio dell'Ordine valuta le proposte formative, formulate anche dalle Commissioni di studio o da altri soggetti, e delibera in merito a quelle per le quali richiedere l'accreditamento al Consiglio Nazionale. La segreteria comunica gli eventi validati al CNDCEC attraverso il portale dedicato, chiedendo il riconoscimento dei crediti formativi. La segreteria invia, tramite e-mail, la locandina dell'evento formativo agli iscritti. La partecipazione degli iscritti viene rilevata da un addetto dell'Ordine il giorno dell'evento tramite il passaggio del badge dell'iscritto su apposito rilevatore o mediante la firma apposta dallo stesso su un elenco cartaceo; se non è presente l'incaricato dell'Ordine, l'elenco degli iscritti all'evento è gestito dall'Ente organizzatore che, dopo aver rilevato le presenze, lo invierà alla segreteria dell'Ordine.		
ADEMPIMENTO	**DOCUMENTO DA PRODURRE E CONSERVARE**	**SOGGETTI COINVOLTI**
Richiesta accreditamento da parte della Commissione di studio o di un Ente terzo	In aggiunta alla corrispondenza relativa alla formalizzazione della richiesta di accreditamento: • Accettazione/comunicazione formale resa dai relatori e dagli intervenuti all'evento circa la loro partecipazione	- Commissione di studio dell'Ordine - Ente terzo - Addetti autorizzati
Inserimento evento sul portale del CNDCEC	Non rilevante ai fini privacy	Non rilevante ai fini privacy

Comunicazione dell'evento agli iscritti all'Ordine tramite e-mail	- Non rilevante ai fini dei processi della Commissione di studio - Rilevante sulla sicurezza dei sistemi	- Amministratore di sistema - Addetti autorizzati che devono operare nel perimetro delle istruzioni ricevute
Eventuale richiesta di iscrizione all'evento da parte degli iscritti sul portale dell'Ordine	- Non rilevante ai fini dei processi della commissione di studio - Rilevante sulla sicurezza dei sistemi	Amministratore di sistema
Richiesta di iscrizione all'evento da parte degli iscritti con e-mail	- Non rilevante ai fini dei processi della Commissione di studio - Rilevante sulla sicurezza dei sistemi	- Amministratore di sistema - Addetti autorizzati che devono operare nel perimetro delle istruzioni ricevute
Richiesta di iscrizione all'evento da parte degli iscritti in presenza il giorno dell'evento	- Non rilevante ai fini dei processi della Commissione di studio - Rilevante sulla sicurezza dei sistemi	Addetti autorizzati che devono operare nel perimetro delle istruzioni ricevute
Acquisizione delle presenze con badge	- Non rilevante ai fini dei processi della Commissione di studio - Rilevante sulla sicurezza dei sistemi	- Amministratore di sistema - Addetti autorizzati che devono operare nel perimetro delle istruzioni ricevute
Acquisizione delle presenze con modello cartaceo	Foglio presenze	Addetti autorizzati che devono operare nel perimetro delle istruzioni ricevute
Attestazione della formazione	- Non rilevante ai fini dei processi della Commissione di studio - Rilevante sulla sicurezza dei sistemi	- Amministratore di sistema - Addetti autorizzati che devono operare nel perimetro delle istruzioni ricevute
Video registrazione e foto dell'evento	Liberatoria ai fini privacy e per lo sfruttamento economico delle immagini/video/audio	Gli intervenuti all'evento (per l'autorizzazione all'utilizzo e alla diffusione di immagini/video/audio)
Inoltro e-mail agli iscritti con materiale dell'evento	- Non rilevante ai fini dei processi della Commissione di studio - Rilevante sulla sicurezza dei sistemi	- Amministratore di sistema - Addetti autorizzati che devono operare nel perimetro delle istruzioni ricevute
Comunicazione con Enti terzi (per esempio: consegna elenco partecipanti all'evento)	Non rilevante ai fini dei processi della Commissione di studio	Addetti autorizzati che devono operare nel perimetro delle istruzioni ricevute
Rapporti con formatori e società esterne	Evidenze contrattuali	- Ordine - Commissioni di studio dell'Ordine - Addetti autorizzati

TRATTAMENTO: formazione professionale continua - organizzazione evento a distanza

Descrizione del processo. L'evento svolto a distanza si svolge attraverso l'utilizzo di piattaforme informatiche. Il Consiglio dell'Ordine valuta le proposte formative, formulate anche dalle Commissioni di studio o da altri soggetti, e delibera in merito a quelle per le quali richiedere l'accreditamento al Consiglio Nazionale. La segreteria comunica gli eventi validati al CNDCEC attraverso il portale dedicato, chiedendo il riconoscimento dei crediti formativi. La segreteria invia, tramite e-mail, la locandina dell'evento agli iscritti, i quali chiedono di partecipare con diverse modalità (iscrizione diretta sulla piattaforma, invio di richiesta d'iscrizione tramite e-mail). Successivamente la segreteria dell'Ordine o l'Ente terzo inviano agli iscritti all'evento il link da utilizzare per accedere al webinar con le eventuali credenziali di accesso.

ADEMPIMENTO	DOCUMENTO DA PRODURRE E CONSERVARE	SOGGETTI COINVOLTI E COSA FARE
Richiesta accreditamento da parte della Commissione di studio o Ente terzo	In aggiunta alla corrispondenza relativa alla formalizzazione della richiesta di accreditamento: Accettazione/comunicazione formale resa dai relatori e degli intervenuti all'evento circa la loro partecipazione	- Commissioni di studio dell'Ordine - Enti terzi - Addetti autorizzati che devono operare nel perimetro delle istruzioni ricevute
Inserimento evento sul portale del CNDCEC	- Non rilevante ai fini dei processi della Commissione di studio - Rilevante sulla sicurezza dei sistemi	- Amministratore di sistema - Addetti autorizzati che devono operare nel perimetro delle istruzioni ricevute
Comunicazione dell'evento all'iscritto	- Non rilevante ai fini dei processi della Commissione di studio - Rilevante sulla sicurezza dei sistemi	- Amministratore di sistema - Addetti autorizzati che devono operare nel perimetro delle istruzioni ricevute
Richiesta di iscrizione all'evento da parte degli iscritti sul portale dell'Ordine	- Non rilevante ai fini dei processi della Commissione di studio - Rilevante sulla sicurezza dei sistemi	- Amministratore di sistema - Addetti autorizzati che devono operare nel perimetro delle istruzioni ricevute
Richiesta di iscrizione all'evento da parte degli iscritti con e-mail	- Non rilevante ai fini dei processi della Commissione di studio - Rilevante sulla sicurezza dei sistemi	- Amministratore di sistema - Addetti autorizzati che devono operare nel perimetro delle istruzioni ricevute
Acquisizione delle presenze con estratto log della piattaforma di formazione	- Non rilevante ai fini dei processi della Commissione di studio - Rilevante sulla sicurezza dei sistemi	- Amministratore di sistema - Addetti autorizzati che devono operare nel perimetro delle istruzioni ricevute
Attestazione della formazione	- Non rilevante ai fini dei processi della Commissione di studio - Rilevante sulla sicurezza dei sistemi	- Amministratore di sistema - Addetti autorizzati che devono operare nel perimetro delle istruzioni ricevute
Inoltro e-mail agli iscritti con materiale dell'evento	- Non rilevante ai fini dei processi della Commissione di studio - Rilevante sulla sicurezza dei sistemi	Addetti autorizzati che devono operare nel perimetro delle istruzioni ricevute
Comunicazione con Enti terzi (per esempio: consegna elenco partecipanti all'evento)	Non rilevante ai fini dei processi della Commissione di studio	Addetti autorizzati che devono operare nel perimetro delle istruzioni ricevute

Rapporti con formatori e società esterne	Evidenze contrattuali	- Ordine - Commissioni di studio dell'Ordine Addetti autorizzati

2. La privacy e il whistleblowing

In quanto enti pubblici non economici, gli Ordini professionali sono soggetti alla disciplina di cui al d.lgs. 10 marzo 2023, n. 24 (c.d. Decreto Whistleblowing), che disciplina la protezione delle persone che segnalano violazioni di disposizioni normative nazionali o dell'Unione europea che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato, di cui siano venute a conoscenza in un contesto lavorativo pubblico o privato.

Invero, gli Ordini professionali devono valutare solo gli adeguamenti alla nuova disciplina, atteso che la normativa previgente (art. 54-*bis* d.lgs. 165/2001, abrogato dal nuovo Decreto) già prescriveva l'adozione di sistemi di whistleblowing quali misure per il trattamento del rischio corruttivo[15].

In particolare, ove non l'abbia già adottato, l'Ordine deve predisporre un Regolamento per la gestione delle segnalazioni, nel quale fornisce informazioni sul canale dedicato, sulle procedure e sui presupposti per effettuare le segnalazioni interne ed esterne. È opportuno pubblicare detto Regolamento nel sito dell'Ordine affinché ne sia garantita la conoscibilità e visibilità alle persone che, pur non frequentando abitualmente l'Ordine, intrattengano un rapporto giuridico con lo stesso.

Non essendo questa la sede opportuna per soffermarsi sui profili sostanziali della disciplina di cui al Decreto Whistleblowing, di seguito si approfondiscono esclusivamente gli aspetti legati al trattamento dei dati personali in quanto l'Ordine deve istituire un canale di segnalazione interna che garantisca la riservatezza dell'identità della persona segnalante, della persona coinvolta e della persona comunque menzionata nella segnalazione, nonché del contenuto della segnalazione e della relativa documentazione.

La gestione del canale di segnalazione interna deve essere affidata al Responsabile per la Prevenzione della Corruzione e per la Trasparenza (RPCT).

Le modalità di segnalazione

La segnalazione interna può avvenire con le seguenti modalità:

Per la segnalazione in forma scritta

- **piattaforma informatica** liberamente accessibile dal sito dell'Ente.

  Il canale utilizzabile per le segnalazioni deve essere criptato e avere delle impostazioni definite in modo tale che i dati della segnalazione siano scorporati dai dati identificativi del segnalante e automaticamente inoltrati, per l'avvio tempestivo dell'istruttoria, al RPCT. Quest'ultimo deve

[15] Sull'argomento si veda CNDCEC, *Anticorruzione e trasparenza: Decreto legislativo 10 marzo 2023, n. 24 (Whistleblowing) – eventuale adeguamento delle procedure*, Informativa 12 luglio 2023, n. 94. In particolare, nell'allegato all'Informativa sono fornite utili indicazioni operative.

ricevere una comunicazione di avvenuta presentazione, unitamente al codice identificativo della stessa (senza ulteriori elementi di dettaglio).

I dati identificativi del segnalante devono essere custoditi in forma crittografata e accessibili soltanto al RPCT e, se ritenuto necessario da quest'ultimo, al dipendente allo stesso eventualmente assegnato.

Soltanto il RPCT deve avere accesso alla propria area riservata e alle informazioni di dettaglio delle varie segnalazioni ricevute.

- ***Segnalazione brevi manu.*** In tal caso, per poter usufruire della garanzia della riservatezza è necessario che la segnalazione venga inserita in una doppia busta chiusa inviata alla sede dell'Ordine che rechi all'esterno la dicitura "All'attenzione del Responsabile della Prevenzione della corruzione riservata/personale".

Per la segnalazione in forma orale

- ***linea telefonica registrata o altro sistema di messaggistica vocale registrato.*** Nel caso in cui per la segnalazione sia utilizzata una linea telefonica registrata o un altro sistema di messaggistica vocale registrato, la segnalazione, previo consenso della persona segnalante, è documentata a cura del RPCT mediante registrazione su un dispositivo idoneo alla conservazione e all'ascolto oppure mediante trascrizione integrale. In caso di trascrizione, la persona segnalante può verificare, rettificare o confermare il contenuto della trascrizione mediante la propria sottoscrizione.
- ***Linea telefonica non registrata o un altro sistema di messaggistica vocale non registrato.*** Se per la segnalazione si utilizza una linea telefonica non registrata o un altro sistema di messaggistica vocale non registrato, la segnalazione è documentata per iscritto mediante resoconto dettagliato della conversazione a cura del RPCT. La persona segnalante può verificare, rettificare e confermare il contenuto della trascrizione mediante la propria sottoscrizione.
- ***Incontro diretto***. Se la persona segnalante richiede direttamente al RCPT un incontro diretto, che dovrà essere fissato nel più breve tempo possibile, la segnalazione, previo consenso della persona segnalante, è documentata a cura dal RPCT mediante registrazione su un dispositivo idoneo alla conservazione e all'ascolto, oppure mediante verbale. In caso di verbale, la persona segnalante può verificare, rettificare e confermare il verbale dell'incontro mediante la propria sottoscrizione. L'identità del segnalante dovrà essere conosciuta solo dal RPCT, che è tenuto a garantirne la riservatezza.

Le segnalazioni pervenute, i relativi atti istruttori e tutta la documentazione di riferimento sono conservati e catalogati in apposito archivio debitamente custodito dal RPCT.

Il RPCT deve inoltre curare la tenuta del registro dove vengono annotate in ordine cronologico le segnalazioni ricevute e l'esito delle stesse.

L'annotazione deve avvenire nel rispetto della riservatezza dell'identità della persona segnalante e delle persone coinvolte, attribuendo un numero progressivo di identificazione delle segnalazioni.

Gli obblighi di riservatezza

La presenza di una segnalazione che abbia i requisiti di ammissibilità comporta l'applicazione di misure di tutela di riservatezza nei termini di seguito illustrati:

- l'identità del segnalante non può essere rivelata a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni;
- la protezione riguarda non solo il nominativo del segnalante, ma anche tutti gli elementi della segnalazione dai quali si possa ricavare, anche indirettamente, l'identificazione del segnalante;
- la protezione della riservatezza è estesa all'identità delle persone coinvolte e delle persone menzionate nella segnalazione fino alla conclusione dei procedimenti avviati in ragione della segnalazione, nel rispetto delle medesime garanzie previste in favore della persona segnalante.

A tal fine l'unico soggetto che può essere autorizzato dall'Ordine al trattamento dei dati del segnalante è il RPCT (e l'eventuale dipendente assegnato al ruolo), il quale ha l'obbligo di mantenere la riservatezza sull'identità del segnalante e delle persone coinvolte nella segnalazione, nonché delle altre persone menzionate nella segnalazione.

Laddove nello svolgimento delle proprie istruttorie abbia necessità di rivelare a terzi l'identità del segnalante, il RPCT dovrà previamente ottenere il **consenso** dell'interessato e delle persone coinvolte nella rivelazione; a loro volta i terzi informati dovranno essere autorizzati al trattamento dei dati e garantire l'obbligo di riservatezza sulle informazioni acquisite.

Nel procedimento disciplinare attivato contro il presunto autore della condotta segnalata, l'identità del segnalante non può essere rivelata nel caso in cui la contestazione dell'addebito disciplinare sia fondata su accertamenti distinti e ulteriori rispetto alla segnalazione, anche se conseguenti alla stessa. Nel caso in cui l'identità del segnalante risulti indispensabile alla difesa del soggetto cui è stato contestato l'addebito disciplinare, questa può essere rivelata solo dietro **consenso espresso** del segnalante.

Il RPCT deve dare avviso alla persona segnalante, mediante comunicazione scritta, delle ragioni della rivelazione dei dati riservati nelle ipotesi di procedimento disciplinare e in tutti quei casi in cui la rivelazione è indispensabile anche ai fini della difesa della persona coinvolta.

La violazione dell'obbligo di riservatezza è fonte di responsabilità disciplinare, fatte salve le ulteriori fonti di responsabilità previste dall'ordinamento.

Il trattamento dei dati personali

Il trattamento di dati personali relativi al ricevimento e alla gestione delle segnalazioni è effettuato dal RPCT quale soggetto autorizzato al trattamento. Ogni trattamento dei dati personali deve essere effettuato nel rispetto dei princìpi europei e nazionali in materia di protezione di dati personali.

Conseguentemente, i dati personali devono essere trattati in modo lecito, corretto e trasparente nei confronti dei soggetti interessati. Possono essere raccolti esclusivamente i dati necessari per gestire e dare seguito alle segnalazioni o denunce. I dati inesatti relativi alla specifica segnalazione gestita devono essere cancellati o rettificati tempestivamente; nel caso in cui i dati non utili siano raccolti accidentalmente, gli stessi devono essere cancellati senza ritardo.

L'Ordine deve fornire *ex ante* ai possibili interessati (segnalanti, segnalati, persone interessate dalla segnalazione, facilitatori, ecc.) un'informativa sul trattamento dei dati personali ai sensi degli artt. 13 e 14 GDPR e adottare misure appropriate a tutela dei diritti e delle libertà degli interessati.

Inoltre, i diritti degli interessati di cui agli artt. 15-22 GDPR possono essere esercitati nei limiti di quanto previsto dall'art. 2-*undecies* del d.lgs. 196/2003 (Codice della Privacy)[16]; i suddetti diritti non possono essere esercitati da parte di alcuni interessati coinvolti nella segnalazione (segnalati e/o altre persone) se da ciò può derivare un pregiudizio effettivo e concreto alla tutela della riservatezza dell'identità della persona segnalante.

L'esercizio dei medesimi diritti può, in ogni caso, essere ritardato, limitato o escluso con comunicazione motivata e resa senza ritardo all'interessato, a meno che la comunicazione possa compromettere la finalità della limitazione, per il tempo e nei limiti in cui ciò costituisca una misura necessaria e proporzionata, tenuto conto dei diritti fondamentali e dei legittimi interessi dell'interessato, al fine di salvaguardare la riservatezza dell'identità del segnalante.

La segnalazione è, inoltre, sottratta all'accesso previsto dagli artt. 22 e ss. l. 241/1990 (accesso agli atti amministrativi), nonché dagli artt. 5 e ss. d.lgs. 33/2013 (accesso civico).

Le segnalazioni interne e la relativa documentazione devono essere conservate per il tempo necessario al trattamento della segnalazione e, comunque, non oltre 5 anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione, nel rispetto degli obblighi di riservatezza di cui alla normativa europea e nazionale in materia di protezione di dati personali.

Le misure per la tutela dei diritti e delle libertà degli interessati

La documentazione cartacea relativa alle segnalazioni deve essere conservata in armadi/cassetti muniti di serratura la cui chiave sia nella disponibilità esclusiva del RPCT e/o dell'eventuale dipendente allo stesso assegnato.

Il fornitore della piattaforma deve assicurare l'adozione di misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato agli specifici rischi derivanti dai trattamenti effettuati nell'ambito del whistleblowing.

La piattaforma utilizzata deve prevedere, tra l'altro:

[16] D.lgs. 30 giugno 2003, n. 196 – Codice in materia di protezione dei dati personali (recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE).

- strumenti di crittografia;
- controllo degli accessi logici;
- tracciabilità delle attività effettuate dagli utenti e dal sistema (in compatibilità con la massima confidenzialità richiesta dal processo di whistleblowing).

Il fornitore deve garantire un'adeguata sicurezza dei canali informatici e dell'hardware utilizzato e, inoltre, deve prevedere:

i) audit periodici di sicurezza per gestire adeguatamente le vulnerabilità tecniche,

ii) una manutenzione periodica correttiva ed evolutiva in materia di sicurezza,

iii) un sistema adeguato di backup e sistemi di protezione adeguata contro i malware.

Sintesi degli adempimenti privacy degli Ordini

Di seguito si fornisce una check list riepilogativa delle attività da svolgere affinché il sistema whistleblowing sia conforme alla normativa sulla privacy:

- il fornitore della piattaforma per la gestione del whistleblowing deve essere nominato **responsabile del trattamento** ai sensi dell'art. 28 GDPR o dell'art. 18 del d.lgs. 51/2018[17].
- Il RPCT (e l'eventuale persona assegnata allo stesso) deve essere nominato quale **autorizzato al trattamento**.
- Deve essere predisposta un'informativa per gli interessati (segnalanti, segnalati, persone interessate dalla segnalazione, facilitatori, ecc.) i cui dati personali sono trattati nella gestione del whistleblowing. Nella parte dell'informativa dedicata ai diritti degli interessati è opportuno specificare che i diritti di cui agli artt. 15-22 GDPR possono essere esercitati nei limiti di quanto previsto dall'art. 2-*undecies* del Codice della Privacy, ovvero che i suddetti diritti non possono essere esercitati da parte di alcuni interessati coinvolti nella segnalazione (segnalati e/o altre persone coinvolte nella segnalazione) se dall'esercizio di tali diritti può derivare un pregiudizio effettivo e concreto alla tutela della riservatezza dell'identità della persona segnalante.

  L'esercizio dei medesimi diritti può, in ogni caso, essere ritardato, limitato o escluso con comunicazione motivata e resa senza ritardo all'interessato, a meno che la comunicazione possa compromettere la finalità della limitazione, per il tempo e nei limiti in cui ciò costituisca una misura necessaria e proporzionata, tenuto conto dei diritti fondamentali e dei legittimi interessi dell'interessato, al fine di salvaguardare la riservatezza dell'identità del segnalante.

  In tali casi, i diritti dell'interessato possono essere esercitati anche tramite il Garante con le modalità di cui all'art. 160 del Codice Privacy. In tale ipotesi, il Garante informa l'interessato di

[17] D.lgs. 18 maggio 2018, n. 51 - Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.

aver eseguito tutte le verifiche necessarie o di aver svolto un riesame, nonché del diritto dell'interessato di proporre ricorso giurisdizionale.

- Deve essere aggiornato il Registro delle attività di trattamento.
- Deve essere effettuata la valutazione d'impatto sulla protezione dei dati (DPIA).

3. La gestione del sito web

Ogni Ordine territoriale, in quanto titolare del trattamento, è tenuto a conformare il proprio sito web istituzionale alla normativa e alle prassi vigenti in materia di protezione dei dati personali.

Ciò riguarda sia i trattamenti che avvengono in modo automatizzato, sia quelli derivanti dal conferimento volontario dei dati da parte degli utenti (es. mediante moduli da compilare).

Si formulano di seguito alcune osservazioni sugli aspetti maggiormente rilevanti.

Informative privacy sito

Le informative privacy sono intese a rispettare il principio di trasparenza del GDPR e devono essere concise, trasparenti, intelligibili e facilmente accessibili, formulate con un linguaggio semplice e chiaro, fornite per iscritto o con altri mezzi, anche in combinazione con icone standardizzate, leggibili da dispositivo automatico.

Il Garante ha messo a disposizione icone liberamente utilizzabili, accessibili a questo link: https://www.garanteprivacy.it/temi/informativechiare.

Secondo la Prassi del Comitato Europeo per la Protezione dei dati (EDPB):

- al momento della raccolta dei dati personali in ambiente online dovrebbe essere fornito un link all'informativa privacy, o tali informazioni dovrebbero messe a disposizione sulla stessa pagina in cui sono raccolti i dati personali;
- tutte le organizzazioni che hanno un sito Internet dovrebbero pubblicarvi una informativa sulla privacy;
- su ogni pagina del sito dovrebbe essere chiaramente visibile un link diretto all'informativa privacy che riporti una dicitura di uso comune (come "Privacy", "Informativa sulla privacy" o "Informativa sulla protezione dei dati");
- non sono considerati facilmente accessibili un posizionamento o codici cromatici tali da rendere il testo o il link meno visibile o difficile da individuare in una pagina Internet;
- è raccomandato l'uso di dichiarazioni/informative sulla privacy stratificate, che consentano agli utenti di consultare le sezioni dell'informativa di loro interesse;

- tutte le informazioni rivolte agli interessati dovrebbero comunque essere disponibili in un unico luogo o in un documento completo, facilmente accessibile per poter consultare il testo nella sua interezza;
- oltre alle informative privacy stratificate è possibile utilizzare pop-up contestuali "just-in-time", notifiche touch 3D o "hover-over" e apposite dashboard, video e notifiche vocali su smartphone; vignette, infografica o diagrammi.

L'approccio stratificato consente di collegare le varie categorie di informazioni e inserire tutte le informazioni in un'unica informativa sulla schermata.

Le informative non dovrebbero essere "mere pagine annidate" in altre che richiedono diversi clic per arrivare all'informazione voluta: il design e il layout del primo strato dell'informativa dovrebbero fornire agli interessati una visione generale chiara delle informazioni e del luogo e modo in cui queste possono essere trovate tra i diversi strati. È essenziale garantire la coerenza delle informazioni presenti negli strati.

Il Comitato Europeo raccomanda che il primo strato/la prima modalità informativa comprenda: i dettagli delle finalità del trattamento, l'identità del titolare e una descrizione dei diritti dell'interessato. Tali informazioni dovrebbero essere portate direttamente all'attenzione dell'interessato nel momento della raccolta dei dati, ossia visualizzate quando l'interessato compila il modulo online.

Le informative di legge e le funzionalità devono risultare pienamente accessibili e conformi alla normativa e prassi vigenti indipendentemente dal dispositivo (es. personal computer, tablet, smartphone) e dal sistema operativo (es. Microsoft, Apple o Linux) utilizzati.

Ove l'Ordine metta a disposizione anche una applicazione mobile ("app"), secondo la prassi europea:

- le informazioni necessarie dovrebbero essere messe a disposizione presso uno "store" online prima del download;
- una volta installata l'app, le informazioni devono continuare a essere facilmente accessibili al suo interno, ad esempio garantendo che le informazioni non siano mai a più di due "tocchi" di distanza (ad es. includendo un'opzione "Privacy" / "Protezione dei dati" nella funzione di menù dell'app);
- l'informativa sulla privacy dovrebbe essere specifica alla app e non la mera informativa generica dell'ente proprietario dell'app o che la mette a disposizione pubblicamente.

Consenso

Nei casi in cui il trattamento è basato sul consenso, questo dovrebbe essere prestato mediante un'azione positiva inequivocabile, deliberata ad esempio con la selezione di un'apposita casella, la scelta di impostazioni tecniche o qualsiasi altra dichiarazione o comportamento che indichi chiaramente che l'interessato accetta il trattamento previsto.

La richiesta di consenso formulata digitalmente deve essere chiara, non ambigua, concisa e non interferire immotivatamente con il servizio per il quale il consenso è espresso.

Il silenzio o l'inattività da parte dell'interessato, o la semplice prosecuzione dell'uso normale di un sito web non costituiscono comportamenti da cui evincere una chiara manifestazione attiva di scelta.

L'accettazione globale di condizioni generali di servizio non equivale a un'azione positiva inequivocabile ai fini del consenso.

L'utilizzo di caselle di consenso preselezionate non è ritenuto valido ai sensi del GDPR. Il GDPR non consente ai titolari l'impiego di caselle preselezionate o procedure di rinuncia (opt-out) che richiedono un intervento dell'interessato per rifiutare il consenso (c.d. "caselle di rinuncia").

Gli Ordini devono essere in grado di gestire in modo corretto e documentare adeguatamente i consensi manifestati mediante il sito web e le relative revoche. È importante verificare con l'eventuale sviluppatore e/o gestore esterno del sito web come siano gestite le banche di dati dei consensi, la loro coerenza con la manifestazione di volontà degli interessati e l'adeguatezza ai fini probatori in caso di controllo.

L'interessato deve poter revocare il proprio consenso in qualsiasi momento, senza pregiudizio, senza costi e con la stessa facilità con cui lo ha espresso, ad esempio mediante la stessa interfaccia web.

Per tutta la durata dei trattamenti basati sul consenso effettuati mediante il sito web, incombe sull'Ordine l'onere di documentare che l'interessato è stato informato e che la propria procedura ha soddisfatto tutti i criteri pertinenti per la validità del consenso.

Trattandosi di un contesto online, tale obbligo potrebbe essere soddisfatto conservando informazioni sulla sessione in cui è stato espresso il consenso, oltre alla documentazione della procedura di consenso al momento della sessione, nonché a una copia delle informazioni fornite all'interessato in quel momento.

Non è ritenuto sufficiente fare solo riferimento a una corretta configurazione del sito web.

Il GDPR non stabilisce alcun termine per la durata del consenso laddove, ovviamente, non sia revocato dall'interessato (con tutte le azioni conseguenti alla revoca). Nondimeno, è evidente che laddove i trattamenti dovessero cambiare o evolversi in misura considerevole, il consenso originale non è più valido e occorrerà ottenere un nuovo consenso. Come migliore prassi è raccomandato di aggiornare il consenso a intervalli appropriati.

I cookie

I cookie sono piccoli file di testo inviati dai siti web ai dispositivi degli utenti, dove sono memorizzati e poi trasmessi nuovamente agli stessi siti alla visita successiva. Essi rendono gli accessi ai siti più semplici e veloci, in quanto le informazioni memorizzate non devono più essere reperite ed elaborate dai dispositivi dopo il primo accesso; possono inoltre semplificare la fruizione di servizi web (es. compilazione di un modulo online).

I cookie possono raccogliere e trattare diversi dati personali (es. indirizzo IP, nome utente, identificativo univoco, e-mail) e altre impostazioni (es. lingua, tipo di dispositivo utilizzato, ecc.).

Queste informazioni potrebbero essere utilizzate anche per scopi di marketing e profilazione ed eventualmente condivise con soggetti terzi.

Gli utenti devono essere preventivamente messi al corrente dell'uso di cookie da parte del sito web mediante apposita informativa, redatta in linguaggio semplice e chiaro, facilmente accessibile, dislocata su più livelli o anche resa mediante più canali e modalità (es. pop up informativi, assistenti virtuali, chatbot, ecc.)

Se sono utilizzati solo cookie tecnici, l'informazione può essere resa disponibile in home page o nell'informativa generale del sito web.

Se si utilizzano anche altri cookie e identificatori non tecnici, occorre mostrare un banner a comparsa immediata e di adeguate dimensioni, che contenga:

- un comando per chiudere il banner senza prestare il consenso (es. una 'x' in alto a destra);
- l'indicazione che il sito utilizza cookie tecnici e se del caso, previo consenso dell'utente, cookie di profilazione o altri strumenti di tracciamento, indicando le relative finalità (informativa breve);
- il link alla privacy policy contenente l'informativa completa, inclusi gli eventuali altri soggetti destinatari dei dati personali, i tempi di conservazione dei dati e le modalità per esercitare i diritti di cui al Regolamento;
- un comando per accettare tutti i cookie o anche altre tecniche di tracciamento;
- il link a un'altra area nella quale poter scegliere in modo analitico le funzionalità, le terze parti e i cookie che si vogliono installare e, tramite due ulteriori comandi, poter modificare le scelte già fatte, prestando il consenso all'impiego di tutti i cookie se non dato in precedenza o revocandolo, anche in unica soluzione, se già espresso.

A tale riguardo preme precisare che è buona prassi l'impiego di un segno grafico, una icona o altro accorgimento tecnico che indichi, anche in modo essenziale – ad esempio nel footer di ogni pagina del dominio – lo stato dei consensi resi dall'utente, consentendone l'eventuale modifica o aggiornamento.

L'area dedicata alle scelte di dettaglio dovrà essere raggiungibile anche tramite un ulteriore link posizionato nel footer di qualsiasi pagina del dominio.

Il c.d. "scrolling" (i.e. scorrere la pagina web) non è considerato uno strumento adatto per raccogliere un consenso idoneo, a meno che tale atto non sia inserito in un processo più articolato, ove l'utente possa generare un evento, registrabile e documentabile, presso il server del sito web, che possa essere considerato un'azione positiva idonea a manifestare la volontà inequivocabile di acconsentire al trattamento.

Anche nel caso dei cookie, l'Ordine in quanto titolare deve essere in grado di dimostrare l'avvenuta corretta acquisizione del consenso.

Le eventuali caselle da utilizzare per manifestare il consenso non devono essere preselezionate dal sistema.

Eventuali meccanismi vincolanti in cui gli utenti sono obbligati, senza alternativa, ad acconsentire alla ricezione di cookie o di altri strumenti di tracciamento (c.d. "cookie wall") sono ritenuti illeciti.

Diverso il caso in cui il sito offra agli utenti anche la possibilità di accedere – senza dare il proprio consenso all'installazione e uso di cookie – a contenuti o servizi equivalenti.

Altri aspetti rilevanti

Collegamento ad altri siti web

Gli utenti dovrebbero essere informati nel caso in cui dovessero passare dal sito web dell'Ordine ad altro sito web gestito da terzi (ad es. per la formazione professionale continua).

L'Ordine dovrebbe vigilare affinché i trattamenti effettuati per il tramite dei siti web di terzi operanti per conto del medesimo siano coerenti con la normativa e la prassi vigenti, inclusa la disciplina sui cookie, nonché il contenuto delle informative privacy e le pattuizioni contrattuali.

Ad esempio, se il terzo – fornitore dell'Ordine – dovesse essere inquadrato come responsabile del trattamento, lo stesso non dovrà proporre agli interessati una autonoma informativa privacy (adempimento del titolare), creando potenziale confusione.

I social widget/plugin social

Quando gli utenti navigano su un sito web che include il widget "mi piace" di Facebook – o di altri social network – alcuni loro dati personali (es. informazioni relative a indirizzo IP e alla stringa del browser) sono trasmessi a Facebook Ireland, indipendentemente dal fatto che abbiano cliccato sul pulsante "mi piace" o che siano iscritti al social network.

Gli Ordini che inseriscono sul proprio sito web il pulsante "mi piace" di Facebook devono fornire ai visitatori del sito tutte le informazioni previste dalla normativa e prassi vigente, inclusa la loro eventuale identità di contitolari per le operazioni di raccolta e trasmissione dei dati a Facebook Ireland. Inoltre, dovrebbero ottenere il consenso preventivo per le operazioni di trattamento di cui sono corresponsabili, a meno che non sussista una diversa base giuridica che consenta loro di agire diversamente.

Trasferimento dati verso paesi terzi

I dati raccolti e trattati mediante il sito web possono essere trasferiti fuori dall'Unione Europea solo in presenza di una delle condizioni di legittimazione previste dal GDPR (es. consenso, decisione di adeguatezza della Commissione Europea, garanzie adeguate, ecc.).

È essenziale che quanto specificato nell'informativa, in eventuali accordi per il trattamento dei dati con fornitori e servizi esterni e nel Registro dei trattamenti siano coerenti.

Ad esempio, per rendere un'adeguata informativa, un Ordine non deve dichiarare che i dati sono trattati in Italia o all'interno dell'Unione Europea e poi avvalersi di servizi che prevedono la conservazione dei dati su server extra UE (es. per il servizio di newsletter).

Foto e video

La pubblicazione di immagini e video che ritraggano persone fisiche sul sito web dell'Ordine può avvenire solo nel rispetto della normativa e delle prassi vigenti.

Gli interessati devono essere previamente informati e – ove non vogliano essere ripresi – deve essere data loro la possibilità di farlo, ad esempio con appositi accorgimenti in occasione di seminari e altri eventi dell'Ordine.

Ove non necessario in relazione alle finalità perseguite, occorre astenersi dal trattare dati identificativi, ad esempio riprendendo un'immagine dell'aula senza che i partecipanti siano riconoscibili.

APPENDICE

A. Esempio di DPIA in materia di whistleblowing

Sezione 1 - Contesto

Punti	Descrizione
Qual è il trattamento in considerazione	Il trattamento ha ad oggetto i dati personali dei soggetti che effettuano segnalazioni ai sensi della Direttiva UE 1937/2019 e del d.lgs. 24/2023. Il titolare del trattamento è l'Ordine_____ in persona del legale rappresentante *pro-tempore.* Il responsabile del trattamento è la Società _____ (fornitore della piattaforma _____)
Quali sono i dati trattati	Dati personali comuni e di contatto, dati personali particolari (es. dati relativi alla salute, dati relativi all'appartenenza sindacale), dati giudiziari (es. condanne penali) Interessati: dipendenti e collaboratori che effettuano una segnalazione o che ne sono oggetto, fornitori che effettuano una segnalazione o vengono segnalati
Qual è il ciclo di vita del dato	1) Attivazione e configurazione della piattaforma 2) Utilizzo della piattaforma – invio delle segnalazioni da parte dei segnalanti e accesso alle stesse da parte dei soggetti autorizzati 3) Dismissione della piattaforma (termini contrattuali o di legge) con conseguente cancellazione sicura dei dati da parte del fornitore/provider del servizio.
Quali sono le risorse utilizzate a supporto dei dati	Piattaforma per la gestione delle segnalazioni denominata _____

Sezione 2 – Principi fondamentali

Punti	Descrizione
Presupposti di liceità	Il trattamento si fonda sulla base giuridica dell'adempimento di un obbligo di legge a cui è tenuto il titolare (art. 6.1, lett. c), GDPR).
Finalità del trattamento	Il trattamento è finalizzato esclusivamente alla gestione della segnalazione e all'adempimento degli obblighi legali previsti dalla normativa vigente in materia di whistleblowing.
Principio di minimizzazione	I dati personali raccolti sono solo quelli espressamente necessari alla gestione della segnalazione, come normativamente previsto dall'art. 12 del d.lgs. 24/2023. Il perseguimento delle finalità avviene nel rispetto del principio di minimizzazione (art. 5.1, lett. c), GDPR).
Periodo di conservazione dei dati	Le segnalazioni, interne ed esterne, e la relativa documentazione sono conservate per il tempo necessario al trattamento della segnalazione e comunque non oltre cinque anni, che decorrono dalla data di comunicazione dell'esito finale della procedura di segnalazione, come espressamente previsto dall'art. 14 del d.lgs. 14/2023.
Come vengono informati gli interessati	Es. all'apertura della piattaforma per la ricezione delle segnalazioni

Come fanno gli interessati ad esercitare i diritti riconosciuti dagli artt. 15-22 GDPR	Scrivendo all'indirizzo e-mail privacy@_____
Trasferimento di dati personali verso Paesi Terzi	Attuato/non attuato

Sezione 3 – Valutazione del rischio

Punti	Descrizione
Misure esistenti o pianificate	Descrizione controllo degli accessi logici; l'accesso alla piattaforma avviene esclusivamente attraverso credenziali di accesso, username e password. Le password hanno le seguenti caratteristiche: - Crittografia (descrizione) - Backup (descrizione) - Sicurezza dell'hardware (descrizione)
Valutazione dei rischi	- Accesso illegittimo - Modifiche indesiderate - Perdita dei dati

Sezione 4 – Considerazioni conclusive

Punti	Descrizione
Conclusioni DPIA	- Rischio accettabile /Rischio non accettabile - Piano d'azione - Eventuale parere DPO/parti interessate

B. Fac-simile modulo "esercizio dei diritti dell'interessato in materia di protezione dei dati personali"

(artt. 15-22 del Regolamento (UE) 2016/679)

Il/La sottoscritto/a _____ nato/a a _____ il _____ esercita con la presente richiesta i seguenti diritti di cui agli artt. 15-22 del Regolamento (UE) 2016/679:

1. Accesso ai dati personali
(art. 15 del Regolamento (UE) 2016/679)

Il sottoscritto *(barrare solo le caselle che interessano)*:

☐ chiede conferma che sia o meno in corso un trattamento di dati personali che lo riguardano;
☐ in caso di conferma, chiede di ottenere l'accesso a tali dati, una copia degli stessi e tutte le informazioni previste alle lettere da a) a h) dell'art. 15, paragrafo 1, del Regolamento (UE) 2016/679, e in particolare;

- 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 o organizzazioni internazionali;
- il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- l'origine dei dati (ovvero il soggetto o la specifica fonte dalla quale essi sono stati acquisiti);
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione, e le informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

2. Richiesta di intervento sui dati
(artt. 16-18 del Regolamento (UE) 2016/679)

Il sottoscritto chiede di effettuare le seguenti operazioni *(barrare solo le caselle che interessano)*:

☐ rettificazione e/o aggiornamento dei dati (art. 16 del Regolamento (UE) 2016/679);
☐ cancellazione dei dati (art. 17, paragrafo 1, del Regolamento (UE) 2016/679), per i seguenti motivi *(specificare quali)*:

a) _____;

b) _____;

c) _____;

☐ (nei casi previsti all'art. 17, paragrafo 2, del Regolamento (UE) 2016/679) l'attestazione che il titolare ha informato altri titolari di trattamento della richiesta dell'interessato di cancellare link, copie o riproduzioni dei suoi dati personali;

☐ limitazione del trattamento (art. 18) per i seguenti motivi *(barrare le caselle che interessano)*:

- ☐ si contesta l'esattezza dei dati personali;
- ☐ il trattamento dei dati è illecito[18];
- ☐ i dati sono necessari per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
- ☐ opposizione al trattamento dei dati ai sensi dell'art. 21, paragrafo 1, del Regolamento (UE) 2016/679[19].

La presente richiesta riguarda (indicare i dati personali, le categorie di dati o il trattamento cui si fa riferimento):

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

3. Opposizione al trattamento

(art. 21, paragrafo 1 del Regolamento (UE) 2016/679)

☐ Il sottoscritto si oppone al trattamento dei suoi dati personali ai sensi dell'art. 6, paragrafo 1, lettera e) o lettera f), per i seguenti motivi legati alla sua situazione particolare (specificare):

_____
_____
_____
_____
_____
_____
_____

[18] Art. 18, par. 1, lett. b), GDPR: il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo.

[19] Art. 18, par. 1, lett. d), GDPR: l'interessato si è opposto al trattamento ai sensi dell'art. 21, paragrafo 1, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

4. Opposizione al trattamento per fini di marketing diretto
(art. 21, paragrafo 2 del Regolamento (UE) 2016/679)

☐ Il sottoscritto si oppone al trattamento dei dati effettuato a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

Il sottoscritto:

☐ chiede di essere informato, ai sensi dell'art. 12, paragrafo 4 del Regolamento (UE) 2016/679, al più tardi entro un mese dal ricevimento della presente richiesta, degli eventuali motivi che impediscono al titolare di fornire le informazioni o svolgere le operazioni richieste.

☐ Chiede, in particolare, di essere informato della sussistenza di eventuali condizioni che impediscono al titolare di identificarlo come interessato, ai sensi dell'art. 11, paragrafo 2, del Regolamento (UE) 2016/679.

Recapito per la risposta[20]:

Via/Piazza _____
Comune _____ Provincia _____ Codice postale _____

oppure

e-mail/PEC:

Eventuali precisazioni

Il sottoscritto precisa (fornire eventuali spiegazioni utili o indicare eventuali documenti allegati):

_____
_____
_____
_____
_____
_____

(Luogo e data)

(Firma)

[20] Allegare copia di un documento di riconoscimento in corso di validità.

C. Fac-simile nomina soggetto autorizzato al trattamento dei dati personali con specifici compiti e funzioni

(art. 2-quaterdecies d.lgs. 196/2003 e art. 29 Reg. UE 2016/679)
(Personale interno - Modello specifico per compiti e funzioni)

L'Ordine dei Dottori Commercialisti e degli Esperti Contabili di _____ (c.f. _____e p.i. _____) con sede legale in _____ via_____ tel. _____ fax _____ mail _____, con sede in _____, titolare del trattamento dei dati raccolti ai sensi dell'art. 4, par. 1, n. 7, GDPR, in persona del Presidente e legale rappresentante _____

NOMINA

Il/La signor/a _____ nato/a a _____ il _____ (c.f. _____ doc. id. n. _____) nella sua qualità di [inserire il particolare ruolo nell'Ordine: dipendente/collaboratore/altro] _____ impiegato addetto al _____, **soggetto autorizzato al trattamento dei dati personali.**

AUTORIZZA

l'incaricato a svolgere, all'interno dell'Ente, le seguenti attività di trattamento dei dati, necessarie allo svolgimento propria prestazione lavorativa, e relative alle finalità sotto individuate.

Tab. 1 Scheda trattamenti

Area:	☐ Segreteria ☐ Amministrazione ☐ Servizi IT	☐ Formazione ☐ Consiglio dell'Ordine ☐ Consiglio di disciplina ☐ Commissione_____ ☐ Altro:_____
Attività di trattamento dati personali affidata:	Da descrivere a cura dell'Ente	
Tipologia di trattamento e finalità:	Da descrivere a cura dell'Ente	
Tipologia di dati trattati:	Da descrivere a cura dell'Ente	
Permessi di gestione dei dati:	☐ Lettura ☐ Modifica ☐ Inserimento	☐ Cancellazione ☐ Stampa ☐ Manutenzione

Durata autorizzazione:	☐ Per la durata del rapporto di lavoro ☐ Fino al _____

In ottemperanza a quanto previsto dal Codice Privacy e dal GDPR, il soggetto autorizzato dovrà attenersi alle istruzioni relative alla tutela dei dati e delle informazioni, sia in termini di sicurezza, sia in materia di riservatezza.

Di seguito, vengono forniti i principi generali e le specifiche istruzioni per l'assolvimento del compito assegnato:

1. il trattamento dei dati deve essere effettuato in modo lecito e corretto;
2. i dati personali devono essere raccolti e registrati unicamente per finalità inerenti all'attività svolta, previste e dichiarate e, pertanto, in conformità alle informazioni comunicate agli interessati;
3. i dati personali devono essere trattati, in formato sia elettronico che cartaceo, esclusivamente al fine di adempiere alle obbligazioni nascenti dall'incarico conferito e, in ogni caso, per scopi determinati, espliciti e, comunque, in termini compatibili con gli scopi di riservatezza per i quali i dati sono stati raccolti;
4. è necessaria la verifica costante della correttezza dei dati trattati e, ove necessario, il loro aggiornamento;
5. è necessaria la verifica costante che i dati risultino pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono stati raccolti o successivamente trattati, secondo le indicazioni ricevute dal titolare del trattamento;
6. ogni autorizzato al trattamento dei dati personali è tenuto ad osservare tutte le misure di protezione e sicurezza atte a evitare rischi di distruzione o perdita anche accidentale dei dati, accessi non autorizzati, trattamenti non consentiti o non conformi alle finalità della raccolta;
7. in ogni operazione del trattamento deve essere garantita la massima **riservatezza** e in particolare:
   - è vietato comunicare e/o diffondere i dati senza la preventiva autorizzazione del titolare;
   - l'accesso ai dati deve essere limitato all'espletamento delle proprie mansioni ed esclusivamente negli orari di lavoro;
   - in caso di allontanamento, anche temporaneo, dalla postazione di lavoro, occorre verificare che non vi sia possibilità da parte di terzi (anche se colleghi o comunque appartenenti alla struttura) di accedere ai dati personali per i quali era in corso una qualunque operazione di trattamento, mediante supporto cartaceo o informatico;
   - le credenziali di autenticazione assegnate devono essere riservate e conservate con la massima segretezza, così come i dispositivi di autenticazione in possesso e uso esclusivo;
   - è necessario raccogliere, registrare e conservare i dati presenti negli atti e documenti contenuti nei fascicoli e nei supporti informatici, avendo cura che l'accesso ad essi sia possibile solo ai soggetti autorizzati;
   - la parola chiave, quando è prevista dal sistema di autenticazione, deve essere composta da lettere (maiuscole o minuscole) e/o numeri, anche in combinazione fra loro, consta di almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'incaricato. Per costruire la password occorre utilizzare almeno tre dei seguenti tipi di carattere: maiuscolo (A, B, C, ecc.); minuscolo (a, b, c, ecc.); numero (0, 1, 2, ecc.); carattere speciale (es: !, $, #, %);

- nella scelta della parola chiave non devono essere utilizzate date di nascita, nomi o cognomi propri o di parenti;
- la parola chiave non deve essere uguale alla matricola o alla user-id;
- l'autorizzato al trattamento dei dati personali deve modificare la componente riservata delle credenziali di autenticazione (parola chiave) al primo utilizzo;
- è vietato trasferire, comunicare e/o diffondere i dati al di fuori dell'Ordine e creare nuove autonome banche dati, salvo preventiva autorizzazione del titolare del trattamento;
- è consentito svolgere operazioni di trattamento unicamente su dati/banche dati ai quali il soggetto autorizzato ha legittimo accesso, nel corretto svolgimento del rapporto di lavoro, e utilizzare a tal fine gli strumenti indicati o messi a disposizione dall'Ordine;

8. nell'esercizio delle proprie mansioni, al momento della raccolta dei dati, l'autorizzato consegna agli interessati il modulo contenente l'informativa di cui all'art. 13 del GDPR, quando previsto, ed eventualmente raccoglie il consenso, ove necessario per le finalità perseguite[21];
9. i dati personali devono essere conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali gli stessi sono stati raccolti o successivamente trattati;
10. i dati devono essere trattati, custoditi e controllati mediante l'adozione delle misure di sicurezza disposte dal titolare del trattamento, al fine di evitare la distruzione, la perdita o l'accesso non autorizzato da parte di terzi, in relazione alle diverse classifiche operative;
11. è vietato comunicare a terzi (anche se colleghi o comunque appartenenti alla struttura) in qualsiasi forma, la/le propria/e credenziale/i di autenticazione, necessaria/e per il trattamento dei dati personali con strumenti elettronici;
12. devono essere segnalate al titolare del trattamento, in relazione alla funzione assegnata, eventuali situazioni di rischio per la sicurezza dei dati di cui il soggetto autorizzato è venuto a conoscenza (es. la violazione della password, il tentativo di accesso non autorizzato ai sistemi), anche quando riguardino i soggetti esterni autorizzati all'accesso;
13. è necessario avvisare tempestivamente il proprio responsabile gerarchico qualora si abbia evidenza, o anche solo il sospetto, che sia in corso una violazione dei dati personali che coinvolga dati particolari e non.

Per i trattamenti di dati personali effettuati anche senza l'ausilio di strumenti elettronici dai soggetti autorizzati al trattamento dei dati personali, devono essere osservate tutte le disposizioni previste nei Regolamenti e nelle procedure/privacy policy adottate dall'Ordine.

Gli obblighi relativi alla riservatezza, alla comunicazione e alla diffusione dovranno essere scrupolosamente osservati anche in seguito all'eventuale cessazione dall'incarico che con la presente le viene assegnato, ovvero dal rapporto di lavoro attualmente in essere con l'Ordine.

Inoltre, La informiamo che:

1. le credenziali di autenticazione attribuite al soggetto autorizzato per il trattamento di dati personali con strumenti elettronici saranno disattivate in caso di non uso per una durata di 3-6 mesi e nel caso in cui il soggetto autorizzato dovesse perdere la qualità che gli consente l'accesso ai dati personali stessi;

[21] Da inserire ove al soggetto autorizzato sia affidata questa attività.

2. con riferimento all'accesso ai dati e agli strumenti elettronici consentito esclusivamente al soggetto autorizzato mediante uso della componente riservata della credenziale, al fine di assicurare la disponibilità per il titolare dei detti dati e/o degli strumenti elettronici, in caso di prolungata assenza o di impedimento del soggetto autorizzato, l'accesso agli stessi sarà effettuato mediante l'utilizzo dei privilegi forniti agli addetti alla gestione dei sistemi ICT, nominati amministratori di sistema, i quali informeranno tempestivamente l'autorizzato circa l'intervento effettuato;
3. l'aggiornamento dell'individuazione dell'ambito del trattamento consentito in qualità di soggetto autorizzato (come di quello consentito a ciascun altro singolo incaricato) avrà luogo con cadenza annuale.

Tali funzioni dovranno essere svolte seguendo le indicazioni che Le sono state impartite dal titolare del trattamento, nonché nel rispetto delle norme privacy e delle tecniche acquisite durante la formazione erogata.
Le istruzioni per l'assolvimento dei compiti assegnati, relativamente al trattamento dei dati personali ad essi connessi, sono contenute nel mansionario di cui sopra.

_____, lì _____

Il titolare del trattamento

[timbro e firma]

_____-_____

Per ricezione e presa visione,

L'autorizzato

[firma chiara, per esteso e leggibile]

_____

D. Fac-simile informativa trattamento dati personali iscritti all'Ordine

A norma dell'art. 13 del Regolamento UE 2016/679 (GDPR) e del d.lgs. 196/2003 "Codice in materia di protezione dei dati personali", è nostra cura fornirle alcune informazioni relative al trattamento dei Suoi dati personali nel contesto delle attività svolte dall'Ordine.

Titolare del trattamento dei dati personali.
Il titolare del trattamento dei dati personali è l'Ordine dei Dottori Commercialisti e degli Esperti Contabili di_____

Responsabile della protezione dei dati personali.
Il titolare del trattamento ha provveduto alla nomina di un responsabile della protezione dei dati i cui dati di contatto sono: _____

Finalità del trattamento
I dati personali oggetto del trattamento saranno trattati dall'Ordine esclusivamente per le finalità di tipo istituzionale indicate nel d.lgs. 139/2005, "Costituzione dell'Ordine dei Dottori Commercialisti e degli Esperti Contabili, a norma dell'art. 2 della l. 24 febbraio 2005, n. 34" e delle altre norme che regolano la professione del Dottore Commercialista e dell'Esperto Contabile.
In particolare, i trattamenti verranno effettuati:

- per consentire l'iscrizione nell'albo, nell'elenco speciale o nel registro dei tirocinanti, ivi compresi gli adempimenti di tutti gli obblighi di natura contabile, fiscale e istituzionale discendenti dall'iscrizione (pagamento contributi annuali, iscrizione ai corsi di formazione, pareri di liquidazione e di congruità degli onorari, inserimento e variazioni dati, procedimenti disciplinari, altre attività istituzionali previste dall'ordinamento della professione del Dottore Commercialista e dell'Esperto Contabile);
- per la verifica della sussistenza dei requisiti di legge inerenti all'iscrizione all'albo;
- per la gestione degli obblighi formativi come disciplinati dal Regolamento attuativo della FPC approvato dal Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili (conteggio ore, rilevazione presenze, ecc.);
- per la formulazione di pareri in materia di liquidazione di onorari a richiesta del professionista o della pubblica amministrazione;
- per l'invio di circolari istituzionali, anche tramite e-mail;
- per la pubblicazione dei dati identificativi e di contatto all'interno dell'albo (liberamente consultabile all'interno del sito web istituzionale)

Base giuridica del trattamento dei dati personali
La base giuridica del trattamento risiede nel d.lgs. 139/2005 e nelle altre norme che regolano la professione del Dottore Commercialista e dell'Esperto Contabile (art. 6, par. 1, lett. c), GDPR). Inoltre, il trattamento è necessario per l'esecuzione di un compito connesso all'esercizio di pubblici poteri di cui è investito l'Ordine art. 6, par. 1, lett. e), GDPR).
Il conferimento dei dati personali è obbligatorio; il suo rifiuto a fornire i dati comporterà l'impossibilità di procedere con l'iscrizione e con l'adempimento delle finalità sopra elencate.

Tipologia di dati trattati

L'Ordine potrebbe trattare, oltre ai Suoi dati comuni (anagrafici, di contatto e finanziari), dati qualificabili come "categorie particolari di dati personali" e cioè quei dati che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona. A mero titolo di esempio si richiama la comunicazione di dati relativi alla salute per la richiesta di esenzione dagli obblighi formativi.

L'Ordine potrebbe trattare anche dati personali relativi a condanne penali e reati, al fine di dare attuazione alle norme del d.lgs. 139/2005, del d.P.R. 137/2012 e dei relativi regolamenti di attuazione.

Soggetti a cui è possibile comunicare i dati

Nei casi previsti dalla legge, da regolamenti o per espletare attività connesse con gli scopi istituzionali dell'Ordine, i Suoi dati potranno essere comunicati a soggetti terzi quali:

- il Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili, le Casse di Previdenza nonché altri Ordini territoriali;
- la Procura della Repubblica, il Tribunale e gli altri Uffici Giudiziari per le comunicazioni obbligatorie connesse con l'iscrizione/cancellazione dall'albo, dall'elenco speciale e dal registro dei tirocinanti;
- l'Anagrafe tributaria per le pratiche connesse con l'iscrizione/cancellazione dall'albo, dall'elenco speciale e dal registro dei tirocinanti;
- le società incaricate dall'Ordine della realizzazione di tessere professionali ovvero della gestione del sito web, dell'invio delle newsletter dell'Ordine;
- i soggetti nominati responsabili del trattamento.

Diffusione dei dati personali

I Suoi dati personali quali nome, cognome, codice fiscale, Comune, CAP, tipo di iscrizione, sezione, anno iscrizione, indirizzi PEC, saranno diffusi attraverso il sito web dell'Ordine dei Dottori Commercialisti e degli Esperti Contabili nella sezione "ricerca iscritto".

Trasferimento dei dati ad un paese terzo o organizzazioni internazionali

Non è previsto alcun trasferimento dei dati verso Paesi extra UE né verso organizzazioni internazionali.

Modalità del trattamento e periodo di conservazione dei dati

Il trattamento sarà svolto in forma automatizzata e/o manuale ad opera di soggetti appositamente autorizzati.

Diritti degli interessati

Gli interessati hanno il diritto di ottenere dall'Ordine, nei casi previsti dalla normativa, l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che li riguarda o di opporsi al trattamento. Può esercitare i Suoi diritti con richiesta scritta inviata all'Ordine _____ o all'indirizzo PEC _____

Diritto di reclamo

Gli interessati che ritengono che il trattamento dei dati personali a loro riferiti avvenga in violazione di quanto previsto dal Regolamento hanno il diritto di proporre reclamo al Garante per la protezione dei

dati personali (www.garanteprivacy.it), come previsto dall'art. 77 del Regolamento stesso, o di adire le opportune sedi giudiziarie (art. 79 del Regolamento).

Luogo e data _____

FIRMA
(per presa visione dell'informativa)

_____

E. Fac-simile informativa trattamento dati personali dipendenti

In conformità con quanto previsto dal Regolamento UE 2016/679/UE – GDPR, l'Ordine dei Dottori Commercialisti e degli Esperti Contabili di _____, in qualità di titolare del trattamento, desidera informarla che i Suoi dati personali e quelli relativi ai Suoi familiari da Lei forniti saranno raccolti esclusivamente ai fini dell'instaurazione e della gestione del rapporto di lavoro e saranno trattati nel rispetto degli obblighi e dei principi di legge in materia di privacy.

TITOLARE DEL TRATTAMENTO
Il titolare del trattamento dei Suoi dati e di quelli dei Suoi familiari da Lei forniti è l'Ordine dei Dottori Commercialisti e degli Esperti Contabili di _____ avente sede a _____; e-mail_____; pec _____.
(eventuale) l'Ordine dei Dottori Commercialisti e degli Esperti Contabili di _____ ha nominato il dott. _____ quale responsabile della protezione dei dati contattabile al seguente recapito _____.

TIPOLOGIA DI DATI, FINALITÀ E BASE GIURIDICA DEL TRATTAMENTO
Il trattamento avrà come oggetto dati personali quali, ad esempio:

- dati identificativi e recapiti
- dati del nucleo familiare
- dati relativi alla posizione lavorativa
- dati reddituali
- coordinate bancarie per effettuare i pagamenti
- altri dati strettamente necessari al perseguimento della finalità oggetto della presente informativa

Il titolare potrà inoltre venire a conoscenza di "categorie particolari di dati", ai sensi dell'art. 9 GDPR, idonee a rivelare lo stato di salute, l'adesione ad un sindacato o ad un partito politico, la titolarità di cariche pubbliche, convinzioni religiose. La conservazione dei documenti contenenti tali dati sarà sottoposta a particolari misure di sicurezza.
I Suoi dati potranno essere trattati sia con strumenti informatici che cartacei e verranno raccolti dal titolare direttamente presso di Lei o mediante consultazione di pubblici registri, elenchi e altre fonti pubbliche.
I Suoi dati saranno trattati per le seguenti finalità:

- gestione di tutti gli aspetti legati al rapporto di lavoro, per la quale la base giuridica è rappresentata dalla necessità di adempiere al contratto di lavoro;
- gestione degli adempimenti previdenziali, fiscali e contabili, per la quale la base giuridica è rappresentata dalla necessità di adempiere agli obblighi imposti dalla legge in materia civile, previdenziale e fiscale;
- gestione degli adempimenti in materia di sicurezza sul lavoro, per la quale la base giuridica è rappresentata dalla necessità di adempiere ad un obbligo di legge;
- gestione degli adempimenti in materia di medicina del lavoro, per la quale la base giuridica è rappresentata dalla necessità per finalità di medicina preventiva o di medicina del lavoro e valutazione della capacità lavorativa del dipendente.

Il conferimento dei Suoi dati personali è necessario per l'instaurazione e gestione del rapporto di lavoro e per consentire al titolare di adempiere agli obblighi di legge. Il mancato conferimento comporterebbe l'impossibilità di instaurazione o la gestione del rapporto stesso.

DESTINATARI O EVENTUALI CATEGORIE DI DESTINATARI DEI DATI PERSONALI

I Suoi dati personali verranno trattati dal personale interno del titolare, autorizzato al trattamento secondo istruzioni impartite nel rispetto della normativa in materia di privacy e sicurezza dei dati.
Per le finalità sopra indicate, i dati potranno essere comunicati alle seguenti categorie di soggetti:

- Professionisti, società, associazioni o studi professionali che prestino al titolare assistenza e/o consulenza per finalità amministrative, contabili, fiscali, di tutela legale;
- Enti previdenziali e assistenziali
- Autorità fiscali e tributarie
- Pubbliche Amministrazioni
- Fondi o Casse private di previdenza e assistenza
- Fornitori di servizi IT
- Istituti bancari
- Medici o studi medici ai fini degli obblighi in materia di igiene e sicurezza del lavoro

Tali soggetti esterni opereranno come titolari autonomi o come responsabili esterni del trattamento. Sarà possibile conoscere l'identità di tali soggetti contattando direttamente l'Ordine.

TRASFERIMENTI DEI DATI AD UN PAESE TERZO O A ORGANIZZAZIONI INTERNAZIONALI

I Suoi dati non saranno oggetto di trasferimento verso paesi Extra UE né verso organizzazioni internazionali.

PERIODO DI CONSERVAZIONE DEI DATI PERSONALI OVVERO CRITERI UTLIZZATI PER DETERMINARE TALE PERIODO

I Suoi dati personali saranno conservati per l'intera durata del rapporto di lavoro e al termine dello stesso saranno conservati per ulteriori 10 anni per esigenze di natura contabile, fiscale, civilistica e processuale.

DIRITTI DELL'INTERESSATO

In relazione ai trattamenti dei dati personali sopra evidenziati, Lei potrà esercitare i diritti di cui agli artt. 15-21 del GDPR (diritto di accesso, di rettifica, di cancellazione, di limitazione del trattamento, diritto alla portabilità dei dati, diritto di opposizione, di revoca e di reclamo).
Lei ha inoltre il diritto di revocare in qualsiasi momento il consenso rilasciato al titolare, senza pregiudicare la liceità del trattamento dei dati effettuato prima della revoca.
Lei potrà in qualsiasi momento esercitare i Suoi diritti scrivendo al seguente indirizzo mail/pec _____oppure inviando raccomandata con A.R. al seguente indirizzo _____
Qualora ritenesse che il trattamento dei Suoi dati sia contrario alla legge, potrà proporre reclamo all'Autorità Garante per la protezione dei i dati personali (www.garanteprivacy.it) ai sensi dell'art. 77 del GDPR.
In nessun caso i dati raccolti per le finalità sopraindicate saranno sottoposti a trattamenti automatizzati, compresa la profilazione ai sensi dell'art. 22 del GDPR.

Luogo e data _____

FIRMA
(per presa visione dell'informativa)

_____

F. Fac-simile informativa sul trattamento dei dati personali fornitori

In conformità con quanto previsto dal Regolamento UE 2016/679/UE – GDPR, l'Ordine dei Dottori Commercialisti e degli Esperti Contabili di _____, in qualità di titolare del trattamento, desidera informarla che i Suoi dati personali da Lei forniti saranno trattati come segue:

1. Dati oggetto del trattamento

Ai fini dell'esplicazione dell'attività di cui al contratto tra le parti, dobbiamo utilizzare alcuni Suoi dati personali. Si tratta di dati anagrafici identificativi, dati contabili, di pagamento e recapiti (indirizzo, utenza telefonica fissa, cellulare, fax, e-mail).

2. Finalità del trattamento, base giuridica e natura obbligatoria o facoltativa del trattamento

Le finalità del trattamento cui sono destinati i Suoi dati sono collegate all'assolvimento dei rapporti contrattuali e precontrattuali in essere tra le parti e per l'adempimento di norme e obblighi di legge cui il titolare del trattamento è soggetto.

Si precisa che il conferimento di detti dati ha natura obbligatoria nel senso che, diversamente, non saremmo in grado di adempiere, totalmente o parzialmente, al mandato sopra citato, e che i Suoi dati potranno essere raccolti anche presso altri soggetti.

L'eventuale rifiuto a fornire tali dati potrà determinare l'impossibilità di perfezionare il contratto con il fornitore.

L'eventuale trattamento dei Suoi dati per finalità ulteriori e diverse rispetto a quelle indicate sarà oggetto di specifica e autonoma informativa e apposito consenso, non vincolante per lo svolgimento del contratto in oggetto.

Il mancato consenso al lecito trattamento di tali dati non impedisce l'esecuzione di un contratto di fornitura (con il fornitore) di cui l'interessato è parte, né l'esecuzione di misure precontrattuali adottate su richiesta dello stesso.

3. Titolare del trattamento

Il titolare del trattamento dei dati è: **L'Ordine dei Dottori Commercialisti e degli Esperti Contabili di** _____ con sede in _____ (__), Via _____ n. __, Partita Iva: _____ mail _____

Il titolare nomina responsabili del trattamento all'atto del conferimento da parte dello stesso di incarichi esterni per lo svolgimento dei quali è necessario condividere i Suoi dati, tra coloro che presentano 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.

4. **Responsabile per la Protezione dati**

Il titolare del trattamento ha provveduto alla nomina di un responsabile della protezione dei dati contattabile ai seguenti recapiti: _____

5. Modalità del trattamento e di conservazione dei dati

Il trattamento e la conservazione dei dati verranno effettuati con l'ausilio di mezzi e strumenti informatici automatizzati e/o cartacei, tali da permetterle l'accesso ai Suoi dati personali in ns. possesso, secondo le modalità più idonee a garantirne l'integrità, l'aggiornamento, la sicurezza e la

riservatezza, proteggendoli altresì da trattamenti non autorizzati e/o illeciti nonché dalla perdita, distruzione o dal danneggiamento accidentale.
Fatte salve le comunicazioni che vengano effettuate in ottemperanza ad obblighi di legge, i dati potranno essere comunicati a soggetti esterni che svolgono specifici incarichi per conto dello scrivente, previo loro espresso impegno alla tutela dei Suoi dati personali in conformità alle disposizioni della presente Informativa e alle norme sul responsabile del trattamento di cui agli artt. 28 e seguenti del Regolamento UE 2016/679, nonché alle norme di legge applicabili.

6. Destinatari dei dati personali

I Suoi dati saranno resi conoscibili al nostro personale amministrativo interno, appositamente autorizzato, e ai nostri collaboratori esterni, a tal fine nominati responsabili del trattamento, il cui elenco è disponibile presso la nostra sede.

7. Trasferimenti dei dati

Non è previsto il trasferimento dei Suoi dati personali a destinatari che potrebbero trovarsi al di fuori dello Spazio Economico Europeo.

8. Durata del trattamento e termini di cancellazione

Il trattamento dei dati avrà luogo per tutta la durata dei rapporti instaurati tra le parti e, successivamente alla conclusione del rapporto in essere, per ottemperare agli adempimenti di legge di natura civilistica e fiscale applicabili, nonché ad ogni altro adempimento/obbligo di legge cui è tenuto il titolare.
I Suoi dati personali saranno conservati per 10 anni per esigenze di natura contabile, fiscale, civilistica e processuale.

9. Diritti dell'interessato

In ogni momento Lei potrà esercitare, con richiesta scritta nei confronti del titolare del trattamento sopra individuato, tutti i diritti riconosciuti dalla normativa europea e interna applicabili e, in particolare, dagli artt. 12-22 del Regolamento Europeo e dalle disposizioni attuative, nonché dalla normativa nazionale in vigore, e in particolare:

a) il diritto di ottenere la conferma dell'esistenza o meno di dati che La riguardano, anche se non ancora registrati, e la loro comunicazione in forma intellegibile;
b) il diritto di ottenere gratuitamente l'accesso e/o la copia dei Suoi dati personali oggetto di trattamento con l'indicazione di tutti gli aspetti rilevanti al trattamento previsti dal Regolamento Ue;
c) il diritto di ottenere gratuitamente l'aggiornamento, la rettificazione di dati inesatti, la limitazione del trattamento oppure, quando ne ha interesse, l'integrazione dei dati;
d) il diritto di opporsi, in tutto o in parte al trattamento dei dati personali che La riguardano ancorché pertinenti alle finalità della raccolta per motivi legittimi o di revocare, in tutto o in parte, il proprio consenso, ove esso sia necessario;
e) il diritto di proporre reclamo ad una autorità di controllo - Garante per la protezione dei dati personali (www.garanteprivacy.it) o autorità giudiziaria.

Luogo e data _____

FIRMA
(per presa visione dell'informativa)

_____

G. Fac-simile informativa e consenso per pubblicazione foto iscritti sulla pagina web[22]

Con la presente, Ti informiamo circa il trattamento dei dati effettuato in occasione della pubblicazione della fotografia di ogni iscritto al nostro Ordine in apposita sezione della pagina web _____
Titolare del trattamento dei dati personali oggetto della presente informativa è l'**Ordine dei Dottori Commercialisti e degli Esperti Contabili di _____**
Il Responsabile della protezione dati può essere contattato in caso di necessità al seguente indirizzo e-mail:

_____

I dati personali oggetto della presente informativa saranno trattati nel rispetto della normativa vigente in materia di protezione dei dati da soggetti autorizzati dal titolare e da responsabili ai sensi dell'art. 28 del GDPR. Tali dati potranno altresì essere trattati da soggetti designati quali amministratori di sistema ai sensi del Provvedimento del Garante per la Protezione dei Dati Personali del 27 novembre 2008 s.m.i.

FINALITÀ E MODALITÀ DI TRATTAMENTO
I dati personali verranno trattati per mezzo di strumenti informatico/telematici per finalità legate all'implementazione della pagina web del nostro Ordine, prevedendo l'inserimento, su base volontaria, della fotografia di ogni iscritto che vorrà aderire all'iniziativa. Il trattamento avverrà per mezzo di strumenti e con modalità volti ad assicurare la protezione dei dati e nel rispetto di quanto definito dagli articoli 32 e ss. del GDPR e della normativa nazionale vigente in materia.

BASE GIURIDICA E LICEITÀ DEL TRATTAMENTO
La base giuridica del trattamento è rappresentata dal consenso espresso dell'interessato ai sensi degli artt. 6 e 7 del GDPR.

NATURA DEL CONFERIMENTO E CONSEGUENZE DEL RIFIUTO
Il conferimento dei dati oggetto della presente informativa è facoltativo e l'eventuale rifiuto a fornire tali dati non avrà alcuna conseguenza se non l'impossibilità per il titolare del trattamento di pubblicare la fotografia dell'iscritto.

DIRITTI DELL'INTERESSATO
Ai sensi e per gli effetti di cui al GDPR, Ti sono riconosciuti i diritti di cui agli artt. 12 e seguenti del GDPR.
Presa visione dell'informativa sul trattamento dei dati personali:
Io sottoscritto _____
ACCONSENTO AL TRATTAMENTO DEI DATI ☐
oppure
NON ACCONSENTO AL TRATTAMENTO DEI DATI ☐

Data _____ Firma _____

[22] È necessario affiancare tale documento all'apposita liberatoria ai sensi degli artt. 10 e 320 c.c. e degli artt. 96 e 97 della Legge 22 aprile 1941, n. 633.

H. Fac-simile registro delle attività di trattamento

REGISTRO DELLE ATTIVITA' DI TRATTAMENTO AI SENSI DELL'ART. 30 , p. 1 del REGOLAMENTO UE 2016/679

DENOMINAZIONE DEL TITOLARE

DATI DI CONTATTO DEL TITOLARE
(sede, n. tel. Indirizzo email)

PROCESSO	TRATTAMENTO	BREVE DESCRIZIONE DEL TRATTAMENTO	FINALITA' TRATTAMENTO	NORMA DI RIFERIMENTO PER INDIVIDUARE LE FINALITA' ISTITUZIONALI	CATEGORIA INTERESSATI	CATEGORIA DATI TRATTATI	BASE GIURIDICA DEL TRATTAMENTO	TERMINI DI CANCELLAZIONE	MISURE DI SICUREZZA	CATEGORIA DESTINATARI COMUNICAZIONE	AFFIDATO A TERZI S/N
GESTIONE ALBO PROFESSIONALE	Trattamento dati personali degli iscritti	Trattamento dei dati necessari alla gestione delle pratiche di iscrizione all'ordine, alla valutazione di idoneità e alla prestazione dei servizi correlati all'iscrizione compreso incasso quote	Gestione pratiche amministrative e servizi destinati agli iscritti	D.lgs 139/2005	Iscritti albo	Dati comuni	(Art. 6 par. 1 lett. C GDPR) Trattamento necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento	indeterminato			
AUTOCERTIFICAZIONE INCOMPATIBILITA'	Trattamento dati personali degli iscritti	Invio del modello al fine di assolvere all'obbligo di verifica periodica della sussistenza dei requisiti di legge per l'iscrizione all'Albo e alla verifica di eventuali cause di incompatibilità	Obbligo di verifica periodica della sussistenza dei requisiti di legge per l'iscrizione all'Albo e alla verifica di eventuali cause di incompatibilità.	D.lgs 139/2005 art. 4	Iscritti albo	Dati comuni e dati giudiziari di cui all'art. 10 del GDPR	(Art. 6 par. 1 lett. c) GDPR) Trattamento necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento	indeterminato			
ATTIVITà DELLE COMMISSIONI	Trattamento dati personali degli iscritti	Tattamento dei dati necessari alla gestione delle attività previste da i gruppi di lavoro (inserimento nelle commissioni, ecc.)	Gestione delle attività delle commissioni	D.lgs 139/2005 e regolamento dell'Ordine	Iscritti albo	Dati comuni	(Art. 6 par. 1 lett. e) GDPR) Trattamento necessario per l'esecuzione di un compito connesso all'esercizio di pubblici poteri di cui è investito il titolare	indeterminato			
GESTIONE OBBLIGHI FORMATIVI	Trattamento dati personali degli iscritti	Trattamento per la gestione degli obblighi formativi come disciplinati dal Regolamento Attuativo della FPC (conteggio ore, rilevazione presenze, ecc.) compresi quelli necessari per organizzazione eventi.	gestione degli obblighi formativi	Dpr 137/2012 art. 7	Iscritti albo	Dati comuni e dati particolari cui all'art. 9 del GDPR	(Art. 6 par. 1 lett. c) GDPR) Trattamento necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento	indeterminato			
GESTIONE RELATIVA AI PROCEDIMENTI DISCIPLINARI	Trattamento dati personali degli iscritti	trattamento per la gestione dei procedimenti disciplinari nei confronti degli iscritti	Attività e tenuta dei fascicoli relativi a procedimenti disciplinari	D.lgs 139/2005	Iscritti albo	Dati comuni e dati giudiziari di cui all'art. 10 del GDPR	(Art. 6 par. 1 lett. c) GDPR) Trattamento necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento	indeterminato			
INVIO DI CIRCOLARI ISTITUZIONALI	Trattamento dati personali degli iscritti	invio periodico tramite email di circolari e informazioni istituzionali	Comunicazioni istituzionali	D.lgs 139/2005	Iscritti albo	Dati comuni	(Art. 6 par. 1 lett. e) GDPR) Trattamento necessario per l'esecuzione di un compito connesso all'esercizio di pubblici poteri di cui è investito il titolare	durata iscrizione			

LIQUIDAZIONE PARCELLE E PARERI DI CONGRUITA'	Trattamento dati personali degli iscritti	Attività efettuata previa richiesta	liquidazione parcelle e pareri di congruità	D.lgs 139/2005	Iscritti albo	Dati comuni	(Art. 6 par. 1 lett. c) GDPR) Trattamento necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento	indeterminato			
GESTIONE REGISTRO PRATICANTI	Trattamento dati personale dei praticati	trattamento dei dati necessari alla tenuta del registro dei praticanti	Gestione pratiche amministrative e servizi destinati agli iscritti	Dpr 137/2012 art. 6	praticanti	dati comuni	(Art. 6 par. 1 lett. c) GDPR) Trattamento necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento	indeterminato			
GESTIONE DEI CANALI SOCIAL	Dati di contatto	trattamento dei dati necessari alla gestione dei canali social	Consentire la gestione dei canali social network	GDPR	utenti del sito	dati comuni	Art. 6 par. 1 lett. a) GDPR) Consenso dell'interessato	Da determinare in ragione delle specificità sui canali social			
GESTIONE DEL SITO INTERNET	Dati di contatto	trattamento dei dati necessari a consentire la navigazione del sito e dei dati di contatto qualora venissero richieste informazioni e/o servizi	Consentire la navigazione del sito internet, gestione richieste pervenute tramite il sito		utenti del sito	dati comuni	Art. 6 par. 1 lett. e) GDPR) Trattamento necessario per l'esecuzione di un compito connesso all'esercizio di pubblici poteri di cui è investito il titolare				
GESTIONE AMMINISTRATIVA CONTABILE	Trattamento dati bandi di selezione	Gestione dei dati dei candidati che partecipano alle procedure di selezione	Consentire lo svolgimento delle prove di selezione, gestione graduatorie e assegnazioni	T.U. Pubblico impiego (D.lgs. 165/2001)	candidati	dati comuni (CV e prove)	Art. 6 par. 1 lett. c) GDPR) Trattamento necessario per adempiere ad un obbligo legale	10 ANNI			
	Trattamento dati dei dipendenti o contrattti assimilati	Gestione amministrativa del personale (monitoraggio presenze del personale, cedolini paga, gestione pratiche per i nuovi inserimenti, etc.)	Finalità giuridica ed economica del personale	CCNL di riferimento	dipendenti	Dati comuni, dati particolari art. 9 GDPR	Art. 6 par. 1 lett. b) GDPR) Trattamento necessario per l'esecuzione di un obbligo contrattuale. (Art. 9 par. 1 lett. b GDPR) Trattamento necessario per assolvere ad obblighi....	10 ANNI			-
	Trattamento dati dei fornitori	gestione contratti e fatture dei fornitori	GESTIONE DEI FORNITORI	Codice civile	fornitori	Dati comuni	Art. 6 par. 1 lett. b) GDPR) Trattamento necessario per l'esecuzione di un obbligo contrattuale.	10 ANNI			-
GESTIONE SALUTE E SICUREZZA SUL LAVORO AI SENSI DEL D.Lgs. 81/08	trattamento dati dei dipendenti	adempimenti di legge relativi alla sicurezza sul lavoro	adempiere agli obblighi sulla sicurezza sul lavoro	D.lgs. N. 81/08	dipendenti	Dati comuni e dati particolari cui all'art. 9 del GDPR	Art. 6 par. 1 lett. c) GDPR) Trattamento necessario per adempiere ad un obbligo legale Art. 9 par. 1 lett. b GDPR) Trattamento necessario per assolvere ad obblighi....	durata del rapporto lavorativo			

ANTICORRUZIONE E TRASPARENZA	trattamento dei dati ai fini anticorruzione e trasparenza	il trattamento dei dati è effettuato tenendo conto delle indicazioni ANAC e del Garante Privacy	adempimenti obbligo su anticorruzione e trasparenza	Legge 6 novembre 2012, n. 190 e Decreto legislativo 14 marzo 2013, n. 33, art. 2-bis, co. 2, lett. a) e art. 3, co. 1-ter	Dipendenti, fornitori, professionisti	Dati comuni	Art. 6 par. 1 lett. c) GDPR) Trattamento necessario per adempiere ad un obbligo legale				
WHISTLEBLOWING	trattamento dei dati personali dei soggetti whistleblowing	Il trattamento dei dati è effettuato in base al regolamento interno whistleblowing per gestire la segnalazione	Per consentire la gestione della segnalzione	D.Lgs. 24/2023	segnalanti e segnalati	Dati comuni, dati particolari art. 9 GDPR, dati giudiziari art. 10 gdpr	Art. 6 par. 1 lett. c) GDPR) Trattamento necessario per adempiere ad un obbligo legale	5ANNI			-
ARCHIVIO E PROTOCOLLO INFORMATICO	Trattamento dei dati personali per protocollo	Gestione del protocollo in entrata e in uscita	Gestione del protocollo informatico nelle fasi di entrata/uscita al fine di fornire evidenza degli invvi.	Decreto del Presidente della Repubblica n. 445/2000	Dipendenti, fornitori, professionisti	Dati comuni	Art. 6 par. 1 lett. c) GDPR) Trattamento necessario per adempiere ad un obbligo legale	illimitato			-
VIDEOSORVEGLIANZA	videosorveglianza	attività di videosorveglianza del sede	protezione del patrimonio		soggetti che accedono alla sede	Dati comuni	Art. 6 par. 1 lett. f) GDPR) Trattamento necessario per il perseguimento del legittimo interesse del titolare	24/48 ore			
IMMAGINI E VIDEO	trattamento delle immagini	Attività di trattamento delle immagini dei partecipanti ad aventi organizzati dall'Ordine o per conto dell'Ordine	pubblicazione e diffusione a scopo divulgativo dell'attività dell'Ordine		soggetti ripresi	Dati comuni	(Art. 6 par. 1 lett. a) GDPR) - Consenso				
ATTIVITA' DI MANUTENZIONE E ASSISTENZA IT	Gestione e controllo dell'infrastruttura IT aziendale	attività di manutenzione e gestione dell'infrastruttura informatica	gestione e assistenza informatica		dipendenti, fornitori, iscritti all'Albo, praticanti	Dati comuni	Art. 6 par. 1 lett. f) GDPR) Trattamento necessario per il perseguimento del legittimo interesse del titolare				

NOTA: LE MISURE DI SICUREZZA INFORMATICA SONO INDICATE IN APPOSITO ALLEGATO

DATA CRERAZIONE
DATA AGGIORRNAMENTO

I. Fac-simile registro dei *data breach*[23]

REGISTRO DELLE VIOLAZIONI DI DATI PERSONALI (DATA BREACH)
(art. 33 del Regolamento (UE) 2016/679 - RGPD)

CODICE			SEGNALAZIONE			
Ruolo svolto	Protocollo evento	Data ultimo aggiornamento	Periodo evento	Ulteriori informazioni sul periodo dell'evento	Momento in cui il titolare/responsabile è venuto a conoscenza dell'evento	Modalità con la quale il titolare/responsabile è venuto a conoscenza dell'evento

VIOLAZIONE						
Descrizione della violazione	Natura della violazione	Causa della violazione	Descrizione dell'incidente di sicurezza	Descrizione delle categorie di dati personali	Descrizione dei sistemi e delle infrastrutture IT coinvolti nell'incidente, con indicazione della loro ubicazione	Misure di sicurezza tecniche e organizzative adottate per garantire la sicurezza dei dati, dei sistemi e delle infrastutture IT coinvolti

INTERESSATI e DATI				CONSEGUENZE			
Categoria di dati personali oggetto di violazione	Volume dei dati personali oggetto di violazione	Categorie di interessati coinvolti nella violazione	Numero di interessati coinvolti nella violazione	Possibili conseguenze della violazione sugli interessati	Ulteriori considerazioni sulle possibili conseguenze	Potenziali effetti negativi per gli interessati	Ulteriori considerazioni sugli effetti negativi per gli interessati

GRAVITA'	RIMEDI		ATTENUAZIONE			
Stima della gravità della violazione	Misure adottate per porre rimedio alla violazione	Misure di cui si propone l'adozione per porre rimedio alla violazione	Misure adottate per prevenire simili violazioni future	Misure di cui si propone l'adozione per prevenire simili violazioni future	Tipo di notifica	Sogetto che ha
	E' applicata una procedura per la gestione degli accessi; Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee; Sono definiti i ruoli e le responsabilità; Sono definiti i termini di conservazione e le condizioni di impiego dei dati.; Sono stabiliti programmi di formazione e sensibilizzazione; Viene eseguita una regolare formazione del personale; I soggetti preposti al trattamento - "soggetti autorizzati", sono appositamente individuati e sono loro fornite le istruzioni necessarie; Sono garantite la riservatezza, integrità e disponibilità dei dati;					

[23] Fare "doppio clic" sull'immagine per visualizzare il foglio di lavoro editabile.