# Determinazione sulla designazione e compiti del Data Protection Officer

SOMMARIO

# I. INTRODUZIONE

## A. SCOPO

La presente policy ha lo scopo di documentare la decisione assunta dallo Studio STUDIO DENTISTICO ASS.TO DOTT.BOSCARINI-DOTT.SSA CORDIOLI (“**Studio**”) con riferimento alla necessità o meno della designazione del Data Protection Officer (DPO), la verifica di un conflitto di interessi, i compiti e le funzioni del medesimo.

Salvo diversamente previsto all’interno di questo documento, tutti i termini riportati con lettera iniziale maiuscola si riferiscono alle definizioni riportate nel GDPR e riportate per comodità nella sezione “Glossario e Acronimi”.

## B. NORMATIVA DI RIFERIMENTO

Articolo 37

**Designazione del responsabile della protezione dei dati**

1. Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta:

a) il trattamento è effettuato da un’autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;

b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure

c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all’articolo 9 o di dati relativi a condanne penali e a reati di cui all’articolo 10.

2. Un gruppo imprenditoriale può nominare un unico responsabile della protezione dei dati, a condizione che un responsabile della protezione dei dati sia facilmente raggiungibile da ciascuno stabilimento.

3. Qualora il titolare del trattamento o il responsabile del trattamento sia un’autorità pubblica o un organismo pubblico, un unico responsabile della protezione dei dati può essere designato per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione.

4. Nei casi diversi da quelli di cui al paragrafo 1, il titolare e del trattamento, il responsabile del trattamento o le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o di responsabili del trattamento possono o, se previsto dal diritto dell’Unione o degli Stati membri, devono designare un responsabile della protezione dei dati. Il responsabile della protezione dei dati può agire per dette associazioni e altri organismi rappresentanti i titolari del trattamento o i responsabili del trattamento.

5. Il responsabile della protezione dei dati 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.

6. Il responsabile della protezione dei dati può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi.

7. Il titolare del trattamento o il responsabile del trattamento pubblica i dati di contatto del responsabile della protezione dei dati e li comunica all’autorità di controllo.

Articolo 38

**Posizione del responsabile della protezione dei dati**

1. Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.
2. Il titolare e del trattamento e il responsabile del trattamento sostengono il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 39 fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica.
3. Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti. Il responsabile della protezione dei dati non è rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti. Il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento.
4 Gli interessati possono contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento.
5. Il responsabile della protezione dei dati è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti, in conformità del diritto dell'Unione o degli Stati membri.
6. Il responsabile della protezione dei dati può svolgere altri compiti e funzioni. Il titolare del trattamento o il responsabile del trattamento si assicura che tali compiti e funzioni non diano adito a un conflitto di interessi.

Articolo 39

**Compiti del responsabile della protezione dei dati**

1. Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti:
a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
b) sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;
d) cooperare con l'autorità di controllo; e
e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.
2. Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

## C. DOCUMENTI DI RIFERIMENTO

1. Regolamento Generale sulla Protezione dei dati personali (UE) 2016/679
2. Procedura per la gestione dei Data Breach

3. Procedura sull'esercizio dei diritti dell'Interessato
4. Registro dei Trattamenti ex art. 30 GDPR
5. Linee guida sulla data protection by design e by default

## D. GLOSSARIO E ACRONIMI

**Autorità di Controllo:** l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 GDPR;
**Dati Biometrici:** i Dati Personali ottenuti da un Trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
**Dati Comuni:** sono tutti i Dati Personali che non appartengono alle categorie dei Dati Particolari e Dati Giudiziari;
**Dati Genetici:** i Dati Personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
**Dati Giudiziari:** Dati Personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza;
**Dati Particolari:** Dati Personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;
**Dati relativi alla Salute:** i Dati Personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
**Dato Personale**: qualsiasi informazione riguardante una persona fisica identificata o identificabile (**"Interessato"**); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
**DPO** o **Data Protection Officer**: è una persona fisica, nominata obbligatoriamente nei casi di cui all'art. 37.1 GDPR dal Titolare o dal Responsabile del Trattamento e deve possedere una conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati per assisterli nel rispetto a livello interno del GDPR;
**GDPR** o **Regolamento:** Regolamento Generale sulla Protezione dei dati personali (UE) 2016/679;
**Gruppo Imprenditoriale**: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;
**Incaricato/i o Persona/e Autorizzata/e:** si tratta dei Collaboratori autorizzati al Trattamento dei Dati Personali sotto la diretta autorità del Titolare e/o del Responsabile ex artt. 4(10) e 29 del GDPR. Stante la definizione fornita dal Gruppo di Lavoro Articolo 29 dell'Opinione 2/2017 questa definizione ricomprende: dipendenti ed ex dipendenti, dirigenti, sindaci, collaboratori e lavoratori a partita IVA, lavoratori a chiamata, part-time, *job-sharing*, contratti a termine, stage, senza distinzione di ruolo, funzione e/o livello, nonché consulenti e fornitori dello Studio e, più in generale, tutti coloro che utilizzino od abbiano utilizzato Strumenti Aziendali o Strumenti Personali operino sulla Rete Aziendale ovvero siano a conoscenza di informazioni aziendali rilevanti quali, a titolo esemplificativo e non esaustivo: (a) i Dati Personali di clienti, dipendenti e fornitori, compresi gli indirizzi di posta elettronica; (b) tutte le informazioni aventi ad oggetto informazioni confidenziali di natura commerciale, finanziaria o di strategia di business; nonché (c) i dati e le informazioni relative ai processi aziendali, inclusa la realizzazione di marchi, brevetti e diritti di proprietà industriale, la cui tutela prescinde dagli effetti pregiudizievoli che potrebbe comportare la diffusione delle medesime;

**Pseudonimizzazione:** il Trattamento dei Dati Personali in modo tale che i Dati Personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali Dati Personali non siano attribuiti a una persona fisica identificata o identificabile;

**Responsabile del Trattamento** o **Responsabile**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta Dati Personali per conto del Titolare del Trattamento; deve presentare garanzie sufficienti di attuare misure tecniche e organizzative adeguate in modo tale che il Trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato;

**Titolare del Trattamento** o **Titolare:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del Trattamento di dati personali; quando le finalità e i mezzi di tale Trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il Titolare o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

**Trattamento** o **Trattato/Trattati:** qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a Dati Personali o insiemi di Dati Personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

**Violazione Dei Dati Personali** ovvero **Data Breach:** è la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai Dati Personali trasmessi, conservati o comunque Trattati.

## II. LA FIGURA DEL DPO

Il DPO è un soggetto designato obbligatoriamente dal titolare o dal responsabile del trattamento nei casi di cui all'art. 37.1 GDPR:

a) amministrazioni ed enti pubblici, fatta eccezione per le autorità giudiziarie;
b) l'attività principale consiste in Trattamenti che, per la loro natura, il loro oggetto o le loro finalità, richiedono il monitoraggio regolare e sistematico degli Interessati su larga scala;
c) l'attività principale consiste nel Trattamento, su larga scala, di Dati Particolari e/o Dati Giudiziari.

Quando la nomina è obbligatoria, il DPO deve:

- possedere un'adeguata conoscenza della normativa e delle prassi di gestione dei Dati Personali, anche in termini di misure tecniche e organizzative o di misure atte a garantire la sicurezza dei dati;
- adempiere alle sue funzioni in piena indipendenza e in assenza di conflitti di interesse;
- svolgere i suoi compiti garantendo il segreto e la riservatezza;
- operare alle dipendenze del Titolare o del Responsabile oppure sulla base di un contratto di servizio (DPO esterno).

Ai sensi dell'art. 37.6 GDPR, lo Studio può designare come DPO un soggetto interno, a mezzo di un atto di designazione, facente parte del personale dipendente; oppure con apposito contratto di servizi, un soggetto esterno all'organizzazione aziendale, che può essere una persona fisica o giuridica: in tale ultimo caso, i compiti stabiliti per il DPO sono assolti da un team operante sotto l'autorità di un contatto principale designato nel contratto di servizi come "responsabile".

Un Gruppo Imprenditoriale può nominare un unico DPO, a condizione che questa sia facilmente raggiungibile da ciascuno stabilimento.

### A. CONFLITTO DI INTERESSI

Il DPO non può rivestire ruoli o svolgere funzioni, che, all'interno dell'organizzazione aziendale, comportano la definizione delle finalità o modalità del Trattamento di Dati Personali (es. in caso in caso in cui il DPO sia designato tra soggetti interni all'organizzazione aziendale, sussiste conflitto di interessi, con riguardo alle seguenti qualifiche e funzioni: Amministratore delegato; responsabile operativo; responsabile finanziario; responsabile direzione marketing; responsabile risorse umane; responsabile IT ecc.).
Il DPO, all'atto di nomina, deve auto-dichiarare di non essere in conflitto di interesse con riguardo alle proprie funzioni di Responsabile della Protezione dei Dati Personali.

### B. PUBBLICAZIONE E COMUNICAZIONE DEI DATI DI CONTATTO

Una volta nominato, i dati di contatto del DPO (nome, cognome, indirizzo di posta elettronica, indirizzo PEC, indirizzo di posta cartacea, numero di telefono dedicato e numero di fax dedicato) devono essere tempestivamente:

a) comunicati via e-mail o nella intranet aziendale o nelle informative alle Persone Autorizzate;
b) pubblicati sul sito web dello Studio[1];
c) comunicati alla/e Autorità di Controllo.

Inoltre, il contatto telefonico del DPO deve essere inserito nell'elenco telefonico interno, e il ruolo ed il nominativo del DPO nell'organigramma aziendale.

### C. COMPITI DEL DPO

Il DPO ha il compito di:

a) sorvegliare l'osservanza del GDPR, valutando i rischi di ogni Trattamento alla luce della natura, dell'ambito di applicazione, del contesto e delle finalità;
b) collaborare con il Titolare/Responsabile, laddove necessario, nel condurre una valutazione di impatto sulla protezione dei dati (DPIA);
c) informare e sensibilizzare il Titolare o il Responsabile, nonché i dipendenti di questi ultimi, riguardo agli obblighi derivanti dal Regolamento e da altre disposizioni in materia di protezione dei dati;
d) cooperare con l'Autorità di Controllo e fungere da punto di contatto per la medesima su ogni questione connessa al Trattamento;
e) fungere da punto di contatto con l'Interessato per l'esercizio dei diritti di cui agli artt. 15-22 del GDPR;
f) supportare il Titolare o il Responsabile in ogni attività connessa al Trattamento di Dati Personali, anche con riguardo all'eventuale tenuta di un registro delle attività di trattamento (art. 30 GDPR).

[1] In base all'articolo 37, settimo paragrafo, del GDPR non è necessario pubblicare anche il nominativo del DPO. Seppure ciò rappresenti con ogni probabilità una buona prassi, spetta al titolare del trattamento o al responsabile del trattamento e allo stesso RPD stabilire se si tratti di un'informazione necessaria o utile nelle specifiche circostanze (cfr. Linee Guida sui responsabili della protezione dei dati del Gruppo di Lavoro Art. 29, adottate il 13 dicembre 2016 ed emendate e adottate in data 5 aprile 2017).

## D. AUTONOMIA E INDIPENDENZA

Nell'esecuzione dei compiti il DPO non deve ricevere istruzioni, in particolare sull'approccio da seguire nel caso specifico; sui risultati attesi; su come condurre gli accertamenti su un reclamo; se consultare o meno l'Autorità di Controllo; sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei Dati Personali; inoltre, il DPO risponde direttamente ai vertici della struttura del Titolare, anche in caso di dissenso rispetto alle decisioni incompatibili con il GDPR, adottate dal Responsabile e/o dal Titolare del Trattamento.
Il DPO deve adottare un metodo pragmatico selettivo e sistematico e stabilire un ordine di priorità nell'attività svolta assegnando una attenzione prioritaria alle questioni che presentino maggiori rischi in termini di protezione dei Dati Personali.
Il DPO deve elaborare e sottoporre ai vertici della struttura del Titolare la redazione di una relazione annuale delle attività svolte.
Nel caso in cui il DPO sia un soggetto interno (dipendente), non può essere né rimosso né penalizzato direttamente o indirettamente (per esempio mancata o ritardata promozione; blocco delle progressioni di carriera; mancata concessione di incentivi rispetto ad altri dipendenti ecc.) per l'adempimento dei propri compiti; mentre, se è esterno all'organizzazione, quindi esercita le sue funzioni in base ad un contratto di servizi, non è ammessa la risoluzione ingiustificata del contratto in relazione alle attività eseguite nell'ambito dello svolgimento dei propri compiti ex art. 39 GDPR, e tantomeno può essere rimosso il singolo soggetto appartenente alla persona giuridica che svolge le funzioni di DPO.
Al fine di svolgere questi compiti, il Titolare o il Responsabile del trattamento dovranno mettere a disposizione del DPO le risorse umane e finanziarie necessarie all'adempimento dei suoi compiti.

## E. CASI DI CONSULTAZIONE PREVENTIVA OBBLIGATORIA DEL DPO

È obbligatorio richiedere la consultazione preventiva al DPO:

a) in tutti i casi in cui debbano essere assunte decisioni che impattano sulla protezione dei Dati Personali; in tali casi il DPO è chiamato a rendere una consulenza idonea – tale parere deve essere tenuto in debita considerazione; è necessario documentare, in caso di disaccordo, le motivazioni che hanno portato a condotte difformi da quelle raccomandate dal DPO;
b) in caso di Violazione dei Dati Personali o altro incidente (cfr. Procedura per la gestione dei Data Breach);
c) in caso di DPIA, secondo quanto previsto dalla Procedura di Data Protection Impact Assessment;
d) In caso di sviluppo interno o esterno di prodotti e sistemi basati sulle nuove tecnologie, affinché il DPO possa pre-valutare le misure di protezione dei Dati Personali e di sicurezza adottate dallo sviluppatore fin dalla progettazione/sviluppo (cfr. Linee guida sulla data protection by design e by default).

## III. DETERMINAZIONE DELLO STUDIO MONOPROFESSIONALE SULLA NOMINA DEL DPO (BARRARE UNA DELLE CASELLE CHE SEGUONO)

Tenuto conto degli artt. 37, 38 e 39 del Regolamento, lo Studio **NON ritiene di dover procedere** alla nomina di un DPO in quanto:

- ☐ l'attività principale non consiste in trattamenti che, per la loro natura, il loro oggetto o le loro finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
- ☐ l'attività principale non consiste nel trattamento, su larga scala, di dati sensibili, relativi alla salute o alla vita sessuale, genetici, giudiziari e biometrici;
- ☐ è già stato nominato un DPO di Gruppo anche in nome e per conto dello Studio.

## IV. DETERMINAZIONE IN CASO DI SOCIETÀ TRA PROFESSIONISTI, DI STUDIO ASSOCIATO

Tenuto conto degli artt. 37, 38 e 39 del Regolamento, lo Studio **NON ritiene di dover procedere** alla nomina di un DPO in quanto:

- ☐ l'attività principale non consiste in trattamenti che, per la loro natura, il loro oggetto o le loro finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
- ☐ l'attività principale non consiste nel trattamento, su larga scala, di dati sensibili, relativi alla salute o alla vita sessuale, genetici, giudiziari e biometrici;
- ☐ è già stato nominato un DPO di Gruppo anche in nome e per conto dello Studio.

## V. DETERMINAZIONE IN CASO DI SOCIETÀ TRA PROFESSIONISTI, DI STUDIO ASSOCIATO (E DI STUDIO MONOPROFESSIONALE IN CASO DI NOMINA SU BASE VOLONTARIA)

Tenuto conto degli artt. 37, 38 e 39 del Regolamento, lo Studio **ritiene di dover procedere** alla nomina di un DPO in quanto:

- ☐ l'attività principale non consiste in trattamenti che, per la loro natura, il loro oggetto o le loro finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
- ☐ l'attività principale non consiste nel trattamento, su larga scala, di dati sensibili, relativi alla salute o alla vita sessuale, genetici, giudiziari e biometrici.

Il DPO è stato designato con delibera del _____ .