



ISTRUZIONI OPERATIVE PER LA CORRETTA PREDISPOSIZIONE DELLA DOCUMENTAZIONE PRIVACY ai sensi del Regolamento UE 2016/679 ("GDPR")

INDICE

A. PREMESSA	2
1. Titolare del Trattamento	3
2. Responsabile del Trattamento	4
3. Incaricato o Persona Autorizzata al Trattamento	4
4. Ulteriori definizioni rilevanti	4
B. DOCUMENTAZIONE	7
1. Policy sugli strumenti IT	7
2. Contratto per il Trattamento dei Dati Personali	9
• <i>Come compilare il contratto per il Trattamento dei Dati Personali: aspetti rilevanti</i>	11
3. Autorizzazione al Trattamento di Dati Personali	12
4. Autorizzazione al Trattamento di Dati Personali in qualità di Amministratore di Sistema	13
5. Informativa per i dipendenti/collaboratori/tirocinanti.....	17
6. Informativa per i pazienti.....	18
7. Privacy Policy.....	20
8. Registro dei trattamenti.....	22
9. Determinazione sul <i>Data Protection Officer</i> (DPO)	24
• <i>Indicazioni per completare i modelli di delibera per la designazione del DPO</i>	25
10. <i>Data Protection Impact Assessment</i> (DPIA).....	26
• <i>Come compilare il DPIA</i>	28
11. <i>Linee guida sul data protection by design e by default</i>	28



12.	Procedura per la gestione del <i>Data Breach</i>	29
13.	Procedura di cooperazione con l'autorità di controllo	29
14.	Procedura per l'esercizio dei diritti dell'interessato.....	29
15.	Policy sulla conservazione dei Dati Personali	30
16.	Policy sulla base legale del trattamento.....	30

A. PREMESSA

La normativa in materia di protezione dei dati personali, così come modificata a seguito dell'adozione del Regolamento UE 2016/679 (in seguito, "Regolamento" o "GDPR"), rimane - così come già avvenuto per la previgente disciplina di cui al D.lgs. n. 196/2003 ("Codice Privacy") - una disciplina "fattuale" e/o sostanzialistica, che pertanto si articola sulla base delle effettive operazioni di trattamento di dati personali che vengono poste in essere all'interno di un determinato contesto sociale, professionale, ecc. e non sulla base di risultanze meramente formali.

La documentazione fornita costituisce pertanto un insieme di modelli utili al professionista per fronteggiare le diverse e principali ipotesi che possano risultare integrate nella propria struttura, che tuttavia richiede necessariamente uno sforzo interpretativo del professionista e/o dello Studio dentistico - oltre che naturalmente un effettivo utilizzo della documentazione stessa - al fine di osservare le vigenti disposizioni applicabili in materia di protezione dei dati personali.

Le istruzioni operative fornite in questo documento illustrano come devono essere compilati i documenti previsti dalla nuova normativa. Utilizzando la piattaforma messa a disposizione da ANDI molte delle informazioni da inserire nei documenti vengono precompilate, in particolare i dati e le informazioni dello Studio. Ogni documento scaricato dalla piattaforma deve comunque essere letto e verificato da parte del professionista e/o dello Studio dentistico, ed eventualmente completato e integrato come indicato in queste istruzioni operative.

Per poter scaricare i documenti, nella piattaforma occorre inserire le informazioni relative a:

- **Anagrafica studio** (si intende per ogni partita IVA; se per una partita IVA sono presente altre sedi operative oltre alla sede legale vanno indicate in "Indirizzi altri studi");
- **Lavoratori** (dipendenti, collaboratori, tirocinanti, ..., ove presenti);
- **Responsabili** (ovvero i nominativi dei Responsabili del trattamento di dati, ove presenti);
- **Destinatari** (ovvero le terze parti a cui vengono trasferiti i dati personali, ove presenti);
- **Attività di trattamento** (ovvero l'elenco delle attività di trattamento di dello Studio in qualità di titolare).

Nelle istruzioni che seguono vengono elencati tutti i dati che devono essere modificati e completati da parte del professionista e/o dello Studio dentistico, anche quelli eventualmente precompilati dalla piattaforma.

Al fine di compilare correttamente la documentazione, è inoltre di fondamentale importanza che ogni professionista e/o Studio che si accinga a intraprendere le attività di allineamento privacy nell'ambito della propria struttura individui correttamente i ruoli privacy sulla base di quello che effettivamente avviene

nella propria struttura professionale. Per agevolarne la comprensione, si riporta di seguito una sintetica descrizione delle principali figure in materia di protezione dei dati personali, così come prevista anche nella sezione "Glossario e Acronimi" delle singole policy e procedure.

1. Titolare del Trattamento

È la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del Trattamento di dati personali. Nel caso dello Studio dentistico, sarà quindi necessario verificare chi determini effettivamente le finalità del trattamento.

	Titolarità autonoma
Titolare di Studio mono-professionale	<p>Caso in cui il libero professionista è titolare di uno Studio mono-professionale:</p> <p>non è rilevante che l'attività venga svolta in uno o in più Studi dentistici (cioè collocati in differenti sedi fisiche). Ciò che conta è la capacità di determinare autonomamente le finalità e i mezzi del trattamento dei dati (es. il professionista decide autonomamente se svolgere marketing nei confronti dei propri pazienti, quali strumenti utilizzare, ecc.).</p> <p><u>La documentazione andrà compilata inserendo il nominativo del singolo professionista quale Titolare del trattamento.</u></p>
Due o più liberi professionisti che svolgono la propria attività in uno Studio privo di personalità giuridica	<p>Caso in cui due o più liberi professionisti svolgano - ognuno autonomamente - la propria attività in una medesima struttura non dotata di personalità giuridica (dunque né Studio associato, né Società tra professionisti quali S.r.l., S.a.s., ecc.):</p> <p>si tratta dunque di una mera condivisione di uno spazio fisico, nel quale ognuno decide autonomamente mezzi e finalità del trattamento dei dati (es. ogni professionista decide autonomamente se svolgere marketing nei confronti dei propri pazienti, quali strumenti utilizzare, ecc.).</p> <p><u>Ogni singolo professionista dovrà compilare autonomamente - in qualità di Titolare del trattamento dei dati - la documentazione fornita.</u></p>
Società tra professionisti (S.r.l., S.a.s., ecc.)	<p>Caso in cui il professionista sia socio di una società tra professionisti (S.r.l., S.a.s., ecc.):</p> <p><u>la documentazione dovrà essere completata indicando quale titolare del trattamento dei dati il nominativo della persona giuridica, cioè la ragione sociale della Società tra professionisti.</u></p>
Studio associato	<p>Caso in cui il professionista sia socio di uno Studio associato:</p> <p>anche in tal caso, posto che anche lo Studio associato è dotato di personalità giuridica, <u>la documentazione dovrà essere completata indicando quale titolare del trattamento dei dati il nominativo della persona giuridica, cioè dello Studio associato, purché le finalità e i mezzi del trattamento siano definiti congiuntamente da tutti gli associati dello Studio.</u></p>



2. Responsabile del Trattamento

Il Responsabile del trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta Dati Personali per conto del Titolare del Trattamento.

È necessario che il Responsabile del trattamento presenti 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.

I soggetti che agiscono tipicamente in qualità di responsabili del trattamento possono essere, a titolo esemplificativo: il commercialista, il consulente del lavoro, società che gestiscono la manutenzione del sito Internet, società che offrono servizi di data center, consulenti in ambito fiscale, legale, ecc.

3. Incaricato o Persona Autorizzata al Trattamento

Si tratta dei soggetti autorizzati al Trattamento dei Dati Personali che operano sotto la diretta autorità del Titolare e/o del Responsabile ex art. 29 del GDPR. Stante la definizione fornita dal Gruppo di Lavoro Articolo 29 dell'[Opinione n. 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, 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 pazienti, dipendenti, collaboratori e fornitori, compresi gli indirizzi di posta elettronica; (b) tutte le informazioni aventi ad oggetto informazioni confidenziali di natura sanitaria, commerciale, finanziaria; 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.

4. Ulteriori definizioni rilevanti

Archivio: qualsiasi insieme strutturato di Dati Personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

Aree Sensibili: sono quei luoghi fisici o della Rete Aziendale in cui vengono Trattati Dati Particolari e/o Dati Giudiziari relativi a persone fisiche; e/o luoghi in cui vengono gestiti e consultati documenti riservati a cui è assolutamente vietato accedere se non per motivi di servizio;

Autorità di Controllo: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 GDPR;

Consenso dell'Interessato o Consenso: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'Interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i Dati Personali che lo riguardano siano oggetto di Trattamento;

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;

Destinatario/i: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di Dati Personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di Dati Personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate Destinatari; il Trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del Trattamento;

Device Fissi: si intendono gli strumenti informatici non facilmente removibili dal perimetro dello Studio quali personal computer, server locali, stampanti affidati alle Persone Autorizzate per uso professionale;

Device Mobili: in generale si intendono quegli strumenti informatici che per loro natura sono facilmente asportabili dal perimetro aziendale quali chiavette USB, SD cards, hard disk esterni, tablet e smartphone utilizzati dalla Persone Autorizzate per uso professionale;

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;

Limitazione Di Trattamento: il contrassegno dei Dati Personali conservati con l'obiettivo di limitarne il Trattamento in futuro;

Processo Decisionale Automatizzato: decisione basata unicamente sul Trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona;



Profilazione: qualsiasi forma di Trattamento automatizzato di Dati Personali consistente nell'utilizzo di tali Dati Personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

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

Rappresentante: la persona fisica o giuridica stabilita nell'Unione che, designata dal Titolare del trattamento o dal Responsabile del trattamento per iscritto ai sensi dell'articolo 27 GDPR, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del GDPR;

Rete Aziendale: rappresenta il perimetro digitale dello Studio, possibilmente contenente Dati Personali e/o informazioni riservate, comprensivo dei dispositivi hardware/software sia per la gestione dei servizi interni (es. switch, LAN, Wi-Fi) che dei collegamenti da o verso l'esterno (es. boundary router, SSH, VPN).

Strumenti Aziendali: l'insieme di Device Fissi e Device Mobili concessi in comodato d'uso dallo Studio alle Persone Autorizzate al fine di svolgere le proprie mansioni, comprensivi altresì di eventuali strumenti di diagnostica necessari per l'erogazione della prestazione medica (es. radiografo);

Strumenti Personali: i Device Mobili di proprietà delle Persone Autorizzate autorizzati ad essere impiegati per uso professionale;

Terzo: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il Titolare del Trattamento, il Responsabile del Trattamento e le Persone Autorizzate al Trattamento dei Dati Personali sotto l'autorità diretta del Titolare o del Responsabile;

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;

Trattamento Transfrontaliero: a) Trattamento di Dati Personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un Titolare del Trattamento o Responsabile del Trattamento nell'Unione ove il Titolare o il Responsabile siano stabiliti in più di uno Stato membro; oppure, b) Trattamento di Dati Personali che ha luogo nell'ambito delle attività di un unico stabilimento di un Titolare o Responsabile nell'Unione, ma che incide o probabilmente incide in modo sostanziale su Interessati in più di uno Stato membro;

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.

B. DOCUMENTAZIONE

Di seguito vengono fornite le istruzioni operative per procedere alla compilazione, integrazione e - se necessario - alla modifica della documentazione prodotta con riferimento alle Policy e Procedure che potranno essere adottate all'interno dello Studio per osservare quanto previsto dalla vigente normativa in materia di protezione dei dati personali, così come risultante dal combinato delle norme previste dalla GDPR e dai Provvedimenti applicabili del Garante per la protezione dei dati personali.

1. Policy sugli strumenti IT

È il documento che contiene le indicazioni e istruzioni dello Studio in merito all'utilizzo, da parte delle Persone Autorizzate, degli Strumenti Aziendali e degli Strumenti Personali che comportino il trattamento dei Dati Personali, tra cui i Dati Particolari quali i dati relativi alla salute dei pazienti.

- Nella sezione "**Scopo**" dell'Introduzione, inserire il nome e cognome del/i professionista/i titolare/i dello Studio oppure la ragione sociale della società in caso di società tra professionisti o altra persona giuridica. Se è stato nominato un Responsabile della protezione dei dati personali ai sensi dell'art. 37 del Regolamento UE 2016/679 ("Data Protection Officer" o "DPO"), occorre indicare (nella riga vuota a disposizione in fondo al paragrafo "Scopo") tale circostanza ed inserire il dato di contatto del DPO (es.: "*Lo Studio ha nominato un Responsabile della protezione dei dati al quale potrà rivolgersi scrivendo una email a: dpo@_____*").

- Nella sezione "**Regole comuni per Device Fissi e Device Mobili**" sono previsti i divieti di massima in merito all'uso degli Strumenti Aziendali da verificare e, se necessario, modificare come opportuno. In particolare, si precisa che è stato descritto di default un sistema di sicurezza impostato in modo tale da:

- a) impedire l'accesso a siti non pertinenti con l'attività lavorativa o che offrano contenuti palesemente violativi del diritto d'autore¹;
- b) consentire l'accesso ai dati e ai sistemi cui ha accesso la persona autorizzata da parte di personale tecnico a ciò incaricato (che svolga dunque mansioni di amministratore di sistema²);
- c) richiamare l'uso di sistemi di share aziendali a titolo presuntivo e meramente eventuale;
- d) descrivere una serie di misure di sicurezza (*Antivirus, Firewall, Cifratura supporti, ecc.*) che potranno essere verificate (ed eventualmente modificate, ove necessario) con l'ausilio di competenti funzioni tecniche.

- Nella sezione "**Regole particolari per Device Mobili**" è previsto, oltre ad una serie di prescrizioni che occorre verificare (e modificare, ove necessario), anche un riferimento alla Virtual Private Network (VPN).

¹ Sul punto precisiamo che il monitoraggio completo contrasta con l'Opinione n. 2/2017 del Gruppo di lavoro Articolo 29, perché collide con il principio di *subsidiarity* ("*less intrusive means*") e con la possibilità di uso promiscuo dei *device*. Filtering e proxy appaiono come misure meno incisive e più in linea con il principio di data protection by design.

² Per una precisa definizione di tale figura, si veda il Provvedimento del Garante per la protezione dei dati personali "[Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008](#)".



- Nella sezione "**Autorizzazione degli Strumenti Personali**" sono indicate alcune configurazioni di default (*MAM, VPN, strong authentication*) che potranno essere valutate ed eventualmente adottate, ove necessario con il supporto delle competenti funzioni tecniche.

- Nella sezione "**Ricognizione, riconsegna e ripristino di strumenti aziendali, strumenti personali, supporti cartacei e oggetti personali**" è previsto un articolato iter per procedere alla restituzione dello Strumento Aziendale ed alla successiva cancellazione dei dati ivi contenuti, che occorre verificare (e modificare, ove necessario).

- Nella sezione "**Utilizzo della Rete Aziendale**" è previsto di default l'applicazione - sulla Rete Aziendale - di sistemi di registrazione degli accessi, proxy e sistemi di content filtering in grado di impedire, l'accesso a siti non pertinenti con l'attività lavorativa o che offrono contenuti palesemente violativi del diritto d'autore, che lo Studio è chiamato a verificare (e modificare, ove necessario).

- Nella sezione "**Wi-Fi guest e VPN**" abbiamo ipotizzato la predisposizione all'interno dello Studio di una rete Wi-fi guest, cioè una rete utilizzabile dai pazienti o dagli altri soggetti ospiti dello Studio (nonché eventualmente dai dipendenti o collaboratori per ragioni di carattere personale), che vi invitiamo a verificare (e modificare, ove necessario);

- Nella sezione "**Utilizzo della posta elettronica**" abbiamo previsto una serie di prescrizioni da osservare nella gestione degli account di posta elettronica, che vi invitiamo a verificare con attenzione (e modificare, ove necessario);

- Nella sezione "**Procedure per l'auto-reply, assenze e accesso alla posta elettronica da parte dello Studio**" è prevista una procedura da osservare in caso di assenze programmate, che consenta di rendere edotto il mittente dell'assenza del destinatario. Inoltre, in caso di assenze non programmate della Persona Autorizzata, è prevista una procedura che consenta - ove opportuno per improrogabili necessità legate all'attività lavorativa - di conoscere il contenuto della casella di posta elettronica della persona assente, garantendo adeguata tutela alla riservatezza di quest'ultima (presenza di un Fiduciario o di un amministratore di sistema).

- Nella sezione "**Utilizzo dei social media**" sono previste alcune prescrizioni di massima che si consiglia di mantenere in caso vengano utilizzati social media riferibili allo Studio.

- Nella sezione "**Gestione delle credenziali**" sono indicate una serie di prescrizioni da osservare nella gestione di username e password - tra cui la modifica della password ogni 3 mesi e le modalità di disattivazione in caso di mancato utilizzo - che vi invitiamo a verificare (e modificare, ove necessario).



- Nella sezione "**Controllo ordinario (ove applicabile)**" è richiamata la possibilità per lo Studio - ove la struttura dimensionale del medesimo sia tale da giustificarne una concreta applicabilità - di verificare l'utilizzo della Rete Aziendale, anche mediante file di log (il tempo di conservazione di tali log è stata previsto, di default, non superiore ai 6 mesi).

- Nella sezione "**Controllo straordinario (ove applicabile)**" è richiamata la possibilità per lo Studio - ove la struttura dimensionale del medesimo sia tale da giustificarne una concreta applicabilità - di accedere anche alla memoria di massa degli Strumenti Aziendali o Personali, esclusivamente in caso di sospetto del verificarsi (anche potenziale) di fatti illeciti e/o condotte/eventi aventi rilevanza penale e/o inadempimenti contrattuali e/o fatti/eventi e/o condotte aventi rilevanza disciplinare, ferme restando le opportune segnalazioni all'autorità di pubblica sicurezza.

- Nella sezione "**Diritti degli interessati**" è necessario indicare l'indirizzo (fisico e/o email) presso cui lo Studio vorrà ricevere le eventuali richieste di esercizio dei diritti degli interessati, cioè - nel caso di specie - le Persone Autorizzate (dipendenti, collaboratori, ecc.).

- L'Allegato A "**To do List**" riepiloga le prescrizioni rilevanti contenute nella Policy sugli strumenti IT: ove si sia proceduto ad apportare modifiche e/o integrazioni al testo proposto, sarà necessario verificare che il contenuto di tale allegato sia coerente con il resto della Policy.

- L'Allegato B "**Footer**" rappresenta una proposta di testo da inserire in calce alle email delle Persone Autorizzate, che potrà essere completata con l'indicazione del nominativo dello Studio.

- L'Allegato C "**Istruzioni per la cifratura degli strumenti aziendali e degli allegati contenenti dati particolari**" contiene dei suggerimenti di carattere generale per proteggere adeguatamente i dati memorizzati sugli Strumenti Aziendali (sistemi di cifratura). Lo Studio è tenuto a verificare - anche con il supporto delle competenti funzioni tecniche - l'applicabilità di tecniche di cifratura all'interno dello Studio e - ove possibile - sviluppare ulteriormente tale allegato al fine di prevedere adeguate misure di sicurezza nel trattamento dei Dati Particolari, quali i dati relativi alla salute dei pazienti.

2. Contratto per il Trattamento dei Dati Personali

Ogni qualvolta una società (o un libero professionista) svolge servizi per conto del Titolare che abbia ad oggetto il Trattamento di Dati Personali di titolarità del medesimo (es. laboratorio odontotecnico, commercialista, fornitore di piattaforme di marketing, provider di posta elettronica, ecc.), occorre che il rapporto tra le parti ai fini del trattamento dei dati personali del Titolare sia disciplinato da un contratto ex art. 28 GDPR.

Si riporta di seguito il testo dell'art. 28 del Regolamento, che disciplina il ruolo del Responsabile del Trattamento:

Responsabile del trattamento



1. Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.

2. Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.

3. I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata 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. Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento:

a) tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;

b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;

c) adotti tutte le misure richieste ai sensi dell'articolo 32;

d) rispetti le condizioni di cui ai paragrafi 2 e 4 per ricorrere a un altro responsabile del trattamento;

e) tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III;

f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;

g) su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati; e

h) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato.

Con riguardo alla lettera h) del primo comma, il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il presente regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.



4. *Quando un responsabile del trattamento ricorre a un altro responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, su tale altro responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento di cui al paragrafo 3, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento. Qualora l'altro responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile.*

5. *L'adesione da parte del responsabile del trattamento a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare le garanzie sufficienti di cui ai paragrafi 1 e 4 del presente articolo.*

6. *Fatto salvo un contratto individuale tra il titolare del trattamento e il responsabile del trattamento, il contratto o altro atto giuridico di cui ai paragrafi 3 e 4 del presente articolo può basarsi, in tutto o in parte, su clausole contrattuali tipo di cui ai paragrafi 7 e 8 del presente articolo, anche laddove siano parte di una certificazione concessa al titolare del trattamento o al responsabile del trattamento ai sensi degli articoli 42 e 43.*

7. *La Commissione può stabilire clausole contrattuali tipo per le materie di cui ai paragrafi 3 e 4 del presente articolo e secondo la procedura d'esame di cui all'articolo 93, paragrafo 2.*

8. *Un'autorità di controllo può adottare clausole contrattuali tipo per le materie di cui ai paragrafi 3 e 4 del presente articolo in conformità del meccanismo di coerenza di cui all'articolo 63.*

9. *Il contratto o altro atto giuridico di cui ai paragrafi 3 e 4 è stipulato in forma scritta, anche in formato elettronico.*

10. *Fatti salvi gli articoli 82, 83 e 84, se un responsabile del trattamento viola il presente regolamento, determinando le finalità e i mezzi del trattamento, è considerato un titolare del trattamento in questione.*

I Trattamenti da parte del Responsabile devono essere disciplinati da un contratto o altro atto giuridico, anche in forma elettronica o dal Titolare o da altro Responsabile (previa autorizzazione scritta del Titolare, specifica o generale).

A tal fine il Titolare dovrà utilizzare il Contratto per il Trattamento dei Dati Personali reso disponibile, da compilare secondo le istruzioni che seguono:

- **Come compilare il contratto per il Trattamento dei Dati Personali: aspetti rilevanti**

- Nel "Preambolo", sezione C, occorre inserire il nominativo del Titolare e il nominato della società (o del libero professionista) che agisce quale Responsabile del Trattamento.

La successiva sezione D richiede di inserire una breve descrizione del servizio fornito dal Responsabile (es. gestione delle buste paga, fornitura del servizio di posta elettronica, erogazione di servizi di hosting, ecc.) e i riferimenti dell'eventuale contratto di servizio/ordine d'acquisto in essere con il fornitore/Responsabile del Trattamento.



- Art. 1, "**Definizioni**": alla voce "Responsabile" indicare il nominativo del Responsabile; alla voce "Titolare" indicare il nominativo dello Studio dentistico (o del Dottore in caso di Studio mono-professionale).

- Art. 2, "**Ruoli Privacy**": alla lett. b) occorre inserire il nominativo della società (o del libero professionista) che agisce quale Responsabile.

- Art. 5, "**Sub-responsabili**": per sub-responsabili si intendono i sub-fornitori del Responsabile. Nel Contratto trattamento dati fornitovi è previsto il generale diniego del Titolare nei confronti del Responsabile a servirsi di sub-responsabili. Laddove intendiate autorizzare l'utilizzo di sub-responsabili da parte del Responsabile, lo Studio potrà richiedere una consulenza specialistica per modificare opportunamente il Contratto per il Trattamento dei Dati Personali.

- Art. 6, "**Trasferimento dei Dati Personali**": è previsto il generale diniego per il Responsabile di trasferire i Dati Personali del Titolare al di fuori dello Spazio Economico Europeo e dell'UE. Laddove il Responsabile trasferisca i Dati Personali al di fuori dello Spazio Economico Europeo e dell'UE si potrà richiedere una consulenza specialista per modificare opportunamente il Contratto per il Trattamento dei Dati Personali e identificare le basi giuridiche che possono essere utilizzate per trasferire Dati Personali a soggetti terzi (ad esempio, per verificare se l'adeguatezza del Paese terzo è stata riconosciuta tramite una decisione della Commissione Europea; per utilizzare le clausole contrattuali tipo, per verificare se sia necessario raccogliere il Consenso dell'Interessato, ecc.).

- Art. 9, "**Restituzione dei Dati Personali e cancellazione**": da completare con l'indicazione del termine entro il quale il Responsabile deve restituire i dati personali del Titolare nel caso in cui venga formulata tale richiesta.

L'**Allegato 1** deve essere completato come opportuno ai punti 3, 4, 5 e 6 inserendo le informazioni in merito al Trattamento dei Dati Personali che rilevano nell'ambito del rapporto tra il Titolare e il Responsabile.

L'**Allegato 2** deve essere completato con le misure di sicurezza tecniche ed organizzative che il Titolare richiede al Responsabile e che il Responsabile si impegna a garantire nell'ambito dell'erogazione del servizio. In alternativa, il Titolare potrà richiedere al Responsabile di completare tale allegato con l'indicazione delle misure da questi garantite nell'ambito dell'erogazione del servizio. Sul punto sono state fornite indicazioni tecniche, che il Titolare dovrà verificare e confermare o, se del caso, modificare.

Nel caso in cui il Titolare voglia disciplinare i rapporti privacy tra le parti anche nel contratto di servizi in essere tra le stesse, potrà richiedere una consulenza specialistica al fine di ottenere una specifica clausola "privacy" da inserire nel contratto di servizi tra le stesse.

3. Autorizzazione al Trattamento di Dati Personali



Si tratta del documento che sostituisce - dal punto di vista privacy - la precedente "nomina a incaricato del trattamento" ex art. 30 del Codice Privacy (l'obbligo permane immutato ex art. 29 del Regolamento) e che potrà essere consegnata a tutti i dipendenti e/o collaboratori e/o tirocinanti, attuali o futuri, dello Studio che trattino dati personali di titolarità dello Studio medesimo su supporti cartacei e/o informatici.

L'Autorizzazione al Trattamento di Dati Personali contiene istruzioni specifiche con riferimento ai Trattamenti svolti per conto dello Studio e attraverso la quale la Persona Autorizzata assume un obbligo di riservatezza che perdurerà ben oltre la cessazione del rapporto lavorativo o di collaborazione.

Assieme all'Autorizzazione al Trattamenti di Dati Personali, la Persona autorizzata riceve - ove adottata - la Policy sugli strumenti IT che ricomprende istruzioni riferibili alla gestione delle credenziali affidate, all'uso della posta elettronica, alla Rete Aziendale ed agli Strumenti Aziendali e/o Strumenti Personali, nonché l'informativa privacy dedicata ai dipendenti/collaboratori/tirocinanti dello Studio.

L'intestazione dell'Autorizzazione deve essere completata con il nominativo del dipendente/collaboratore/tirocinante e l'indicazione della relativa qualifica professionale (es. assistente alla poltrona, responsabile delle attività di segreteria), con il profilo autorizzativo assegnato e poi con il nominativo dello Studio (o del Dottore in caso di Studio mono-professionale) ed i relativi riferimenti della sede. Le informazioni richieste per la compilazione di documento vanno inserite nella piattaforma nella sezione "Lavoratori". I dati del dipendente/collaboratore/tirocinante saranno precompilati nel pdf generato.

In calce, il documento - oltre che sottoscritto - potrà essere compilato con l'indicazione (eventuale) di uno/due Fiduciari indicati dalla Persona Autorizzata, che fungeranno da garanti della medesima in caso sia necessario per il Titolare- per improrogabili esigenze legate all'attività lavorativa - accedere al suo account di posta elettronica o alla memoria di massa dei suoi Strumenti Aziendali o Personali nelle ipotesi previste dalla Policy sugli strumenti IT.

L'Autorizzazione e l'informativa privacy sottoscritte dal dipendente/collaboratore/tirocinante dovranno essere adeguatamente archiviate da parte del Titolare.

4. Autorizzazione al Trattamento di Dati Personali in qualità di Amministratore di Sistema

In attesa di conoscere eventuali aggiornamenti sulla figura dell'Amministratore di Sistema da parte dell'Autorità di Controllo in linea con le nuove previsioni del GDPR, ove lo Studio preveda di servirsi di persone a cui sono assegnate funzioni con mansioni di Amministratore di Sistema per il trattamento di dati personali di titolarità dello Studio, sarà necessario osservare i seguenti adempimenti.

La figura dell'Amministratore di Sistema costituisce una peculiarità del legislatore italiano, prevista dal Provvedimento del Garante per la protezione dei dati personali *Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di*



amministratore di sistema del 27 novembre 2008 (G.U. n. 300 del 24 dicembre 2008), così come modificato in base al Provvedimento del 25 giugno 2009 (di seguito, "Provvedimento").

Con la definizione di "Amministratore di Sistema" si individuano generalmente, in ambito informatico, figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Ai fini del presente provvedimento vengono però considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi;

Si veda la FAQ 1) del Provvedimento: Cosa deve intendersi per "amministratore di sistema"? In assenza di definizioni normative e tecniche condivise, nell'ambito del Provvedimento dell'Autorità di Controllo, l'Amministratore di Sistema è assunto quale figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati Trattamenti di Dati Personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi quali i sistemi ERP (Enterprise resource planning) utilizzati in grandi aziende e organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui Dati Personali.

L'Autorità di Controllo non ha inteso equiparare gli "operatori di sistema" di cui agli articoli del Codice penale relativi ai delitti informatici, con gli "amministratori di sistema": questi ultimi sono dei particolari operatori di sistema, dotati di specifici privilegi.

Anche il riferimento al d.P.R. 318/1999 nella premessa del Provvedimento è puramente descrittivo poiché la figura definita in quell'atto normativo (ormai abrogato) è di minore portata rispetto a quella cui si fa riferimento nel Provvedimento.

Non rientrano invece nella definizione quei soggetti che solo occasionalmente intervengono (p.es., per scopi di manutenzione a seguito di guasti o malfunzioni) sui sistemi di elaborazione e sui sistemi software.

In seguito ad un'intensa attività interpretativa volta ad analizzare il perimetro di applicazione del Provvedimento e ad interpretare la definizione di Amministratore di Sistema di cui al Provvedimento stesso, si è convenuto che sono da considerarsi Amministratori di Sistema le figure che rispondono ai seguenti criteri:

- ✓ possono modificare i privilegi di accesso ai dati delle Persone Autorizzate come previsto dal Provvedimento (dove si legge nelle considerazioni preliminari: [...] compiti [...] *spettano tipicamente all'amministratore di sistema: dalla realizzazione di copie di sicurezza (operazioni di backup e recovery dei dati) alla custodia delle credenziali alla gestione dei sistemi di autenticazione e di autorizzazione*);
- ✓ possono modificare i livelli di accesso del sistema;

- 
- ✓ possono modificare la configurazione del sistema, ad esempio modificando gli accessi da reti esterne o annullando un sistema di autenticazione (Provvedimento - considerazioni preliminari: *Gli amministratori di sistema [...] nelle loro consuete attività sono, in molti casi, concretamente "responsabili" di specifiche fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati*);
 - ✓ gestiscono le policy di backup e i supporti di backup (trasporto/scambio/custodia).

Non sono invece considerati Amministratori di sistema figure che solo occasionalmente intervengono (p.es., per scopi di manutenzione a seguito di guasti o malfunzioni) sui sistemi di elaborazione e sui sistemi software: deve trattarsi di figure professionali dedicate alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati Trattamenti di Dati Personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi quali i sistemi ERP (Enterprise resource planning) utilizzati in grandi aziende e organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui Dati Personali.

Il punto 4.4 del Provvedimento ("Verifica delle attività") richiede che l'operato degli Amministratori di Sistema debba essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei Titolari o dei Responsabili del Trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai Trattamenti dei Dati Personali previste dalle norme vigenti.

È da sottoporre a verifica l'attività svolta dall'Amministratore di Sistema nell'esercizio delle sue funzioni. Va verificato che le attività svolte dall'Amministratore di Sistema siano conformi alle mansioni attribuite, ivi compreso il profilo relativo alla sicurezza.

Valutazione delle caratteristiche soggettive

L'attribuzione delle funzioni di Amministratore di Sistema deve avvenire previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di Trattamento, ivi compreso il profilo relativo alla sicurezza.

Anche quando le funzioni di Amministratore di Sistema o assimilate sono attribuite solo nel quadro di una designazione quale Persona Autorizzata, il Titolare e il Responsabile devono attenersi comunque a criteri di valutazione equipollenti a quelli richiesti per la designazione dei Responsabili ai sensi dell'GDPR.

Si veda sul punto FAQ 20) del Provvedimento: Nella designazione degli amministratori di sistema occorre valutare i requisiti morali? [Rif. comma 2, lettera a] No. Il riferimento alle caratteristiche da prendere in considerazione, al comma 2, lettera a), del dispositivo, è all'esperienza, alla capacità e all'affidabilità del soggetto designato. Si tratta quindi di qualità tecniche, professionali e di condotta, non di requisiti morali".

Designazioni individuali



La designazione quale Amministratore di Sistema deve essere individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

Al riguardo si veda FAQ 7) del Provvedimento: Cosa si intende per descrizione analitica degli ambiti di operatività consentiti all'ADS? [Rif. comma 2, lettera d]. Il Provvedimento prevede che all'atto della designazione di un Amministratore di Sistema, venga fatta "elencazione analitica" degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato, ovvero la descrizione puntuale degli stessi, evitando l'attribuzione di ambiti insufficientemente definiti.

Al riguardo si veda anche FAQ 8) del Provvedimento: Oltre alla job description si deve andare più in dettaglio? Si devono indicare i singoli sistemi e le singole operazioni affidate? No, è sufficiente specificare l'ambito di operatività in termini più generali, per settori o per aree applicative, senza obbligo di specificarlo rispetto a singoli sistemi, a meno che non sia ritenuto necessario in casi specifici”

Elenco degli amministratori di sistema

Gli estremi identificativi delle persone fisiche che agiscono in qualità di Amministratori di Sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti da parte dell'Autorità di Controllo.

Qualora l'attività degli Amministratori di Sistema riguardi anche indirettamente servizi o sistemi che Trattano o che permettono il Trattamento di informazioni di carattere personale dei lavoratori, i Titolari pubblici e privati sono tenuti a rendere nota o conoscibile l'identità degli Amministratori di Sistema nell'ambito delle proprie organizzazioni, secondo le caratteristiche dell'azienda o del servizio, in relazione ai diversi servizi informatici cui questi sono preposti. Ciò, avvalendosi dell'informativa resa agli Interessati nell'ambito del rapporto di lavoro/collaborazione che li lega al Titolare, oppure tramite il disciplinare tecnico di cui al provvedimento dell'Autorità di Controllo n. 13 del 1° marzo 2007 (in G.U. 10 marzo 2007, n. 58) o, in alternativa, mediante altri strumenti di comunicazione interna (ad es., intranet aziendale, ordini di servizio a circolazione interna o bollettini) o tramite procedure formalizzate a istanza del lavoratore. Ciò, salvi i casi in cui tali forme di pubblicità o di conoscibilità siano incompatibili con diverse previsioni dell'ordinamento che disciplinino uno specifico settore.

Servizi in outsourcing

Nel caso di servizi di Amministrazione di Sistema affidati in outsourcing il Titolare o il Responsabile esterno devono conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali Amministratori di Sistema.

Controlli tecnici

Controllo circa:

- ✓ verifica operato e logging 2.e e 2.f FAQs 5, 11, 12, 13, 14, 15 e 16 del Provvedimento

- 
- ✓ per la verifica dell'operato, si verifica la corrispondenza tra mansioni e privilegi attribuiti con cadenza almeno annuale;
 - ✓ si verifica a campione, con cadenza annuale, che i log traccino le attività svolte dagli Amministratori di Sistema;
 - ✓ di verifica, con cadenza annuale, che i log siano conservati correttamente e la correttezza della firma digitale apposta.

Ove lo Studio intenda designare un Amministratore di Sistema all'interno della propria struttura, oltre a seguire le indicazioni di cui alla sezione che precede 3. Autorizzazione al Trattamento di Dati Personali, dovrà consegnare a tale soggetto anche l'Autorizzazione al Trattamento di Dati Personali in qualità di Amministratore di Sistema.

L'Autorizzazione deve essere completata con le informazioni richieste in epigrafe nel documento, nonché nella "Informativa rilasciata ai sensi dell'art. 13 del Regolamento 2016/679" con l'indicazione dell'indirizzo (fisico o email) presso cui il Titolare vuole ricevere le richieste di esercizio dei diritti da parte degli Amministratori di Sistema, e nel relativo allegato.

Tale Autorizzazione dovrà essere archiviata unitamente all'ulteriore documentazione privacy di cui alla sezione 3. che precede.

5. Informativa per i dipendenti/collaboratori/tirocinanti

Questa informativa privacy ex art. 13 del Regolamento dovrà essere consegnata ai dipendenti/collaboratori/tirocinanti dello Studio. I dati dei dipendenti/collaboratori/tirocinanti vanno inseriti nella piattaforma nella sezione "Lavoratori", e saranno precompilati nel documento pdf generato dalla piattaforma, così come i dati del Titolare.

- Nella sezione "Titolare del trattamento", occorre inserire il nominativo del titolare. Se è stato nominato un Responsabile della protezione dei dati personali ai sensi dell'art. 37 del Regolamento UE 2016/679 ("Data Protection Officer" o "DPO"), occorre indicare (nella riga vuota a disposizione in fondo al paragrafo "Titolare del trattamento") tale circostanza ed inserire i dati di contatto del DPO nell'informativa (inserendo ad esempio: "Lo Studio ha nominato un Responsabile della protezione dei dati al quale potrà rivolgersi scrivendo una email a: *dpo@_____*").

- Nella sezione "Finalità, base giuridica e facoltatività del trattamento" sono state indicate le principali finalità che abbiamo identificato nell'attività degli studi dentistici per quanto riguarda la gestione dei rapporti di lavoro o collaborazione. Naturalmente, sarà necessario verificare caso per caso la rispondenza di quanto ivi indicato rispetto ai trattamenti effettivamente posti in essere e modificare come opportuno tale sezione.

- Per ogni finalità inoltre (punto a, b, ecc.) è indicata la relativa base giuridica e la natura - facoltativa o obbligatoria - del conferimento dei dati. Laddove venisse modificato l'elenco delle finalità sarà dunque



necessario modificare coerentemente anche i richiami alle relative basi giuridiche ed alla natura facoltativa/obbligatoria del trattamento.

- Qualora fosse previsto un sistema di videosorveglianza, osserviamo che sarà necessario verificare l'adempimento di diverse incombenze (accordo sindacale o rilascio dell'autorizzazione dell'Ispettorato Territoriale del Lavoro, adeguare i tempi di conservazione delle immagini a quanto prescritto dalla normativa applicabile, ecc.). In tale ipotesi, vi invitiamo a richiedere una consulenza specialistica al fine di redigere come opportuno una informativa ad hoc e procedere con gli ulteriori adempimenti di legge.

- È stata prevista anche la raccolta del consenso del dipendente/collaboratore per l'eventuale utilizzo e diffusione delle relative immagini e/o riprese video tramite i canali a disposizione del Titolare (sito, newsletter, social network, ecc.) raccolte in occasione di eventi e/o manifestazioni. Ove non sia previsto tale trattamento, tale finalità potrà essere eliminata e l'informativa adeguatamente uniformata.

- Nella sezione "**Destinatari e trasferimento dei dati personali**", sono state indicate le categorie più frequenti di destinatari a cui, nell'ambito delle attività professionali, si renda necessario comunicare i dati personali raccolti nella gestione dei rapporti di lavoro/collaborazione. Anche in tal caso bisognerà verificare caso per caso la rispondenza di quanto indicato alla realtà effettiva dello Studio e modificare/integrare come opportuno tale sezione.

- In merito al trasferimento dei dati al di fuori dello Spazio Economico Europeo (SEE), è stata esclusa di default tale ipotesi. Laddove invece vi sia un trasferimento di dati personali extra SEE sarà necessario verificare l'adempimento di diverse incombenze (meccanismo di certificazione, sottoscrizione delle Standard Contractual Clauses, ecc.). Anche per tale ipotesi, sarà possibile richiedere una consulenza specialistica al fine di regolare come opportuno tale trasferimento.

- Nella sezione "**Conservazione dei Dati Personali**" sono stati ipotizzati i criteri applicabili ai fini della relativa conservazione. Naturalmente - previa opportuna valutazione (motivata) da parte del Titolare - tali criteri/tempi di conservazione potranno essere modificati dal Titolare.

- Nella sezione "**I suoi diritti**" è necessario inserire l'indirizzo (fisico o email, o entrambi) presso cui il Titolare del trattamento intende ricevere le eventuali richieste di esercizio dei diritti (accesso, rettifica, cancellazione, ecc.) da parte dei soggetti Interessati.

6. Informativa per i pazienti

Questa informativa privacy ex art. 13 del Regolamento dovrà essere consegnata ai pazienti dello Studio.

- Nella sezione "**Titolare del trattamento**", occorre inserire il nominativo del Titolare del trattamento. Se è stato nominato un Responsabile della protezione dei dati personali ai sensi dell'art. 37 del Regolamento UE 2016/679 ("Data Protection Officer" o "DPO"), occorre indicare tale circostanza ed inserire (nella riga vuota



a disposizione in fondo al paragrafo “Titolare del trattamento”) il dato di contatto del DPO (es.: “*Lo Studio ha nominato un Responsabile della protezione dei dati al quale potrà rivolgersi scrivendo una email a: dpo@_____*”).

- Nella sezione “**Finalità, base giuridica e natura facoltativo o obbligatoria del trattamento**” sono state indicate le principali finalità identificate nell'attività degli studi dentistici. Naturalmente, sarà necessario verificare caso per caso la rispondenza di quanto ivi indicato rispetto ai trattamenti effettivamente posti in essere e modificare come opportuno tale sezione. In particolare, con specifico riferimento alla finalità di marketing, il Titolare dovrà verificare/confermare/modificare i mezzi di comunicazione a tal fine utilizzati secondo le proprie specifiche esigenze.

- Per ogni finalità inoltre (lettere a, b, c, ecc.) è indicata la relativa base giuridica e la natura - facoltativa o obbligatoria - del conferimento dei dati. Laddove venisse modificato l'elenco delle finalità sarà dunque necessario modificare coerentemente anche i richiami alle relative basi giuridiche ed alla natura facoltativa/obbligatoria del trattamento.

- Qualora fosse previsto un sistema di videosorveglianza, osserviamo che sarà necessario verificare l'adempimento di diverse incombenze (sopra meglio richiamate). In tale ipotesi, lo Studio potrà richiedere una consulenza specialistica al fine di redigere come opportuno una informativa ad hoc.

- Nella sezione “**Destinatari e trasferimento dei Dati Personali**”, sono riportate le categorie di destinatari individuate nell'attività degli studi dentistici, cioè i soggetti a cui, per qualunque ragione nell'ambito delle attività professionali, si renda necessario comunicare i dati personali raccolti. Anche in tal caso bisognerà verificare caso per caso la rispondenza di quanto indicato alla realtà effettiva dello Studio e modificare/integrare come opportuno tale sezione.

In particolare, è stata prevista di default anche la finalità di possibile comunicazione dei dati del paziente al medico curante, il cui relativo consenso dovrà essere raccolto per procedere con tale comunicazione. In caso di minori, tale consenso dovrà essere rilasciato dal genitore/tutore legale rappresentante del minore, utilizzando la sezione “**IN CASO DI PAZIENTI MINORENNI**” in calce al tale informativa privacy.

- In merito al trasferimento dei dati al di fuori dello Spazio Economico Europeo (SEE), è stata esclusa di default tale ipotesi. Laddove invece vi sia un trasferimento di dati personali extra SEE sarà necessario verificare l'adempimento di diverse incombenze (meccanismo di certificazione, sottoscrizione delle Standard Contractual Clauses, ecc.). Per tale ipotesi, lo Studio potrà richiedere una consulenza specialistica al fine di regolare come opportuno tale trasferimento.

- Nella sezione “**Conservazione dei Dati Personali**” sono stati ipotizzati i criteri applicabili ai fini della relativa conservazione. Naturalmente - previa opportuna valutazione (motivata) da parte del Titolare - tali criteri/tempi di conservazione potranno essere modificati dal Titolare.



- Nella sezione "I suoi diritti" è necessario inserire l'indirizzo (fisico o email, o entrambi) presso cui il Titolare del trattamento intende ricevere le eventuali richieste di esercizio dei diritti (accesso, rettifica, cancellazione, ecc.) da parte dei soggetti interessati.

7. Privacy Policy

Si tratta di un modello di Privacy Policy dedicato allo Studio titolare di un sito Internet.

- Nelle premesse sarà necessario inserire il nominativo del Titolare del trattamento.

- Nella sezione "Titolare del trattamento", se è stato nominato un Responsabile della protezione dei dati personali ai sensi dell'art. 37 del Regolamento UE 2016/679 ("Data Protection Officer" o "DPO"), indicare tale circostanza ed inserire (nella riga vuota a disposizione in fondo al paragrafo "Titolare del trattamento") il dato di contatto del DPO (es.: "Lo Studio ha nominato un Responsabile della protezione dei dati al quale potrà rivolgersi scrivendo una email a: dpo@_____").

- Nella sezione "Dati di navigazione", inserire il tempo di conservazione di tali dati. Si consiglia di aderire alla prassi del Garante per la protezione dei dati personali che prevede un termine di conservazione di tali dati non superiore a 7 (sette) giorni.

- Nella sezione "Speciali categorie di dati personali", è regolata l'ipotesi che il sito consenta di procedere all'invio di candidatura online degli utenti per eventuali posizioni aperte presso il Titolare (indicata a titolo esemplificativo come sezione "Lavora con noi"). Ove non sia prevista tale ipotesi, tale sezione dovrà essere eliminata. Stesso dicasi per il caso dell'eventuale analisi dei profili social dei candidati a carattere professionale (es. LinkedIn): ove tale circostanza non si verifichi, vi invitiamo a eliminare tale previsione. Al fine di procedere al trattamento di speciali categorie di dati personali da parte del candidato, è stato predisposto un form per la raccolta del relativo consenso. Naturalmente, laddove eliminate tale sezione, non sarà necessario raccogliere il consenso in questione.

- Il Titolare dovrà poi verificare l'applicabilità di quanto previsto nella sezione "Dati forniti volontariamente dall'interessato". In caso non venga in rilievo tale circostanza, tale sezione potrà essere eliminata.

- Nella sezione "Tipologie di cookie utilizzate dal Sito e possibilità di (de-)selezione", sarà necessario verificare - con il supporto delle competenti funzioni tecniche e IT, interne o esterne - i cookie effettivamente serviti sul sito del Titolare e modificare/integrare come opportuno tale sezione. Di default è stato previsto l'utilizzo dei cookie tecnici di prima parte - da inserire nella tabella cookie - e dei cookie di terze parti (ad es.: Google, Facebook, ecc.) per i quali occorre inserire i link alle informative sulla privacy e ai moduli di consensi delle stesse.

In caso di uso di cookie, il Titolare potrà richiedere una consulenza specialistica in materia per poter assolvere correttamente a tutti gli obblighi richiesti. Si ricorda che occorre dare agli utenti la possibilità di selezionare e de-selezionare i singoli cookie di prima parte serviti dal sito e che le scelte degli utenti in



merito ai cookie serviti potranno essere memorizzate mediante l'uso di un cookie tecnico (da poter riportare nella tabella "*Cookie presenti nel Sito*"). La tabella "**Cookie presenti nel Sito**" dovrà essere completata con l'inserimento dei nominativi dei cookie di prima effettivamente serviti tramite il sito, nonché una breve descrizione dei medesimi e il relativo tempo di persistenza. Sarà poi necessario consentire agli utenti di selezionare/de-seleziona i singoli cookie di prima parte servizi tramite il sito.

- Nella sezione "**Finalità del trattamento**" sono state indicate le principali finalità che sono state identificate nell'attività degli studi dentistici per quanto riguarda l'utilizzo del sito web, tra cui, a titolo esemplificativo: trattamenti volti a rispondere a richieste di contatto, di appuntamento, di pareri, per svolgere attività di marketing, adempiere ad obblighi di legge e di regolamento. Naturalmente, sarà necessario verificare caso per caso la rispondenza di quanto ivi indicato rispetto ai trattamenti effettivamente posti in essere e modificare come opportuno tale sezione. In particolare, con specifico riferimento alla finalità di marketing, il Titolare dovrà verificare/confermare/modificare i mezzi di comunicazione a tal fine utilizzati secondo le proprie specifiche esigenze.

- Nella sezione "**Base legale e natura obbligatoria o facoltativa del trattamento**" è indicata - per ogni finalità (lettere a, b, ecc.) - la relativa base giuridica e la natura (facoltativa o obbligatoria) del conferimento dei dati. Laddove venisse modificato l'elenco delle finalità del trattamento sarà dunque necessario modificare coerentemente anche i richiami alle relative basi giuridiche ed alla natura facoltativa/obbligatoria del trattamento.

- Nella sezione "**Destinatari dei dati personali**" sono state indicate le categorie più frequenti di destinatari individuate nell'attività degli studi dentistici, cioè i soggetti a cui, per qualunque ragione nell'ambito delle attività professionali, si renda necessario comunicare i dati personali raccolti tramite il sito web. Anche in tal caso bisognerà verificare caso per caso la rispondenza di quanto indicato alla realtà effettiva dello studio dentistico e modificare/integrare come opportuno tale sezione.

- In merito al trasferimento dei dati al di fuori dello Spazio Economico Europeo (SEE) è stato escluso tale tipologia di trattamento. Laddove invece vi sia un trasferimento di dati personali extra SEE (ad esempio perché i dati sono archiviati in data center ubicati al di fuori dello Spazio Economico Europeo) sarà necessario verificare l'adempimento di diverse incombenze (ad esempio, la necessità o meno di sottoscrizione delle *Standard Contractual Clauses*, ecc.). Per tale ipotesi, il Titolare potrà richiedere una consulenza specialistica al fine di regolare come opportuno tale trasferimento.

- Nella sezione "**Conservazione dei dati**" sono stati ipotizzati i criteri applicabili ai fini della conservazione dei dati personali. Naturalmente - previa opportuna valutazione (motivata) da parte del Titolare - tali criteri/tempi di conservazione potranno essere modificati dal Titolare. Ad esempio, per quanto riguarda l'eventuale analisi dei CV, è stato previsto un termine di conservazione di 1 anno; si tratta di proposte che devono essere confermate.



- Nella sezione "Diritti degli interessati" è necessario inserire l'indirizzo (fisico o email, o entrambi) presso cui il Titolare del trattamento intende ricevere le eventuali richieste di esercizio dei diritti (accesso, rettifica, cancellazione, ecc.) da parte dei soggetti interessati.

- In calce alla Privacy Policy è stato riportato il testo del form per la raccolta del consenso unico marketing, da poter utilizzare in caso di conferma di tale tipologia di trattamento, nonché del consenso al trattamento delle speciali categorie di dati eventualmente trasmessi tramite i CV. Si precisa che tali caselle non dovranno essere pre-flaggate e che in mancanza di rilascio del consenso marketing l'utente potrà comunque accedere ai servizi offerti tramite il sito.

Sono poi state riportate le informative breve cookie (c.d. BANNER COOKIE) per le seguenti ipotesi:

Opzione 1. Uso di cookie di profilazione di prima parte e di terze parti;

Opzione 2. Uso di cookie di profilazione di terze parti;

Opzione 3. Uso di cookie di profilazione di prima parte.

Sempre in merito ai cookie si precisa che nel caso in cui il sito utilizzi unicamente cookie tecnici di prima parte, non sarà necessario pubblicare un'informativa breve (c.d. BANNER COOKIE).

8. Registro dei trattamenti

Si tratta del modello predisposto per redigere il registro dei trattamenti ex art. 30 del Regolamento, che si riporta di seguito:

Registri delle attività di trattamento

1. Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:

a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;

b) le finalità del trattamento;

c) una descrizione delle categorie di interessati e delle categorie di dati personali;

d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;

ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;

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 di cui all'articolo 32, paragrafo 1.

Ogni responsabile del trattamento e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie attività relative al trattamento svolte per conto di un titolare del trattamento, contenente:

a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare



del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;

b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;

c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;

ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

3. I registri di cui ai paragrafi 1 e 2 sono tenuti in forma scritta, anche in formato elettronico.

4. Su richiesta, il titolare del trattamento o il responsabile del trattamento e, ove applicabile, il rappresentante titolare del trattamento o del responsabile del trattamento mettono il registro a disposizione dell'autorità di controllo.

Il Registro è strutturato in 4 documenti precompilati, ove necessario, da scaricare e stampare.

In particolare:

- il **documento 1) Istruzioni** fornisce chiarimenti in merito alla natura del documento ed alla composizione dello stesso. È già precompilato con i dati dello studio;

- il **documento 2) Registro delle attività di trattamento** contiene l'elenco delle **attività di trattamento di dati dello studio in qualità di titolare**. Devi inserire in piattaforma nella sezione **“Attività di trattamento”** le diverse strutture/aree/uffici all'interno dello Studio - ove la struttura dimensionale del medesimo consenta tali distinzioni - che svolgano trattamenti di dati personali (es. Amministrazione, Ufficio Comunicazione, ecc.).

È possibile far generare alla piattaforma le attività di trattamento dati che dovrebbero andar bene per quasi tutti gli Studi. Leggi attentamente e verifica la correttezza delle attività generate dalla piattaforma. Potrai poi modificare o eliminare i dati inseriti, ed eventualmente aggiungere altre attività di trattamento svolte all'interno dello studio.

La maggior parte dei dati (*Finalità, Soggetti Interessati, Tipi di Dati Personali, Categorie di Dati Personali, Base legale, Base legale per le Speciali Categorie di Dati Personali, Responsabili esterni, Destinatari, Tipo di titolare, Trasferimento dei Dati extra UE, Criteri di conservazione*) prevede una scelta multipla, e se indicato sarà possibile anche specificare **“Altro”**.

I dati **“Responsabili esterni”** e **“Destinatari”** si collegano, rispettivamente, al documento 3) **Responsabili** ed al documento 4) **Destinatari**: pertanto, per inserire correttamente le attività di trattamento occorre prima inserire e verificare la correttezza di **Responsabili**, ovvero i nominativi dei responsabili del trattamento del Titolare, e **Destinatari**, ovvero titolari autonomi cui vengono comunicati i dati personali (ad es. INPS, INAIL, Sistema Tessera Sanitaria, ecc.) nelle rispettive sezioni nella piattaforma.

Va inoltre indicato il tempo di conservazione dei Dati Personali trattati dalla struttura interessata ed il relativo criterio individuato: ad es. laddove vi siano degli obblighi di legge (come indicato a titolo meramente esemplificativo per quanto riguarda la normativa tributaria), oppure se si tratti di una scelta discrezionale del Titolare, in termini di necessità (ad es. la scelta di conservare i dati per finalità di tutela



in giudizio) o di opportunità (ad es. nel caso di conservazione dei dati per finalità di marketing fino alla revoca del consenso dell'interessato);

- il **documento 3) Responsabili** va compilato nella sezione “Responsabili” all’interno della piattaforma indicando, come anticipato, i nominativi dei responsabili del trattamento del Titolare, ovvero di coloro che trattino Dati Personali di titolarità dello Studio (es. commercialista, consulente del lavoro, fornitore di servizi di hosting, ecc.), nonché i relativi dati di contatto, la finalità (selezionabile dal menu a tendina tra quelle che state previste di default), una breve descrizione dell’attività svolta e l’indicazione dell’eventuale trasferimento dei dati al di fuori dell’UE da parte del Responsabile (con conseguente indicazione della relativa base legale);

- il **documento 4) Destinatari** va compilato nella sezione “Destinatari” all’interno della piattaforma indicando, come anticipato, i nominativi dei destinatari del Titolare (siano essi contitolari o titolari autonomi) che trattino Dati Personali di titolarità dello Studio per finalità autonome (es. INPS, INAIL, Sistema Tessera Sanitaria, ecc.). Anche in tal caso andranno indicati i relativi dati di contatto, la finalità (selezionabile dal menu a tendina tra quelle che abbiamo previsto di default), una breve descrizione dell’attività svolta e l’indicazione dell’eventuale trasferimento dei dati al di fuori dell’UE da parte del Destinatario (con conseguente indicazione della relativa base legale);

9. Determinazione sul Data Protection Officer (DPO)

Tale documento ha lo scopo di documentare la decisione assunta dal Titolare 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.

Al fine di verificare se sia necessario o meno procedere alla nomina di un DPO nell’ambito della propria struttura, si riporta di seguito il testo dell’articolo 37 del Regolamento:

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.

Nota bene: come indicato nel documento [Determinazione sulla designazione e compiti del Data Protection Officer](#), gli studi mono - professionali non sono tenuti alla nomina di un DPO in considerazione del fatto che non dovrebbe considerarsi *su larga scala* il trattamento di dati personali di pazienti o clienti da parte di un singolo medico (si veda il Considerando 91 del Regolamento e le [Linee guida sui responsabili della protezione dei dati](#) adottate dal Gruppo di lavoro Art. 29).

Si veda a tal riguardo la **sezione III e IV** del documento, che andrà completata come opportuno (ove necessario).

Naturalmente, il Titolare potrà - in totale autonomia - procedere con la nomina di un Responsabile della protezione dei dati, non essendoci alcun divieto per procedere in tal senso, anche nel caso in cui la nomina di un DPO non risulti essere obbligatoria ai sensi dell'art. 37 del Regolamento. Si precisa che in caso di nomina volontaria di un DPO troveranno applicazione tutti i requisiti di cui agli artt. 37-39 del Regolamento per quanto concerne la nomina stessa, lo status e i compiti del DPO esattamente come nel caso di una nomina obbligatoria.

Diversamente, in caso di società tra professionisti o di studi associati, è rimessa alla valutazione del Titolare del trattamento la verifica in merito all'applicabilità al caso di specie delle lettere b) e c) dell'art. 37 del Regolamento.

Si veda a tal riguardo la **sezione V** del documento, che andrà completata come opportuno (ove necessario).

In caso di nomina di un DPO si potranno utilizzare i modelli di delibera forniti rispettivamente per la nomina di un DPO persona fisica (ad esempio un dipendente del Titolare) e di un DPO persona giuridica, in quanto opera sulla base di un contratto di servizi in essere tra il Titolare e il Responsabile della protezione dei dati personali (DPO esterno). I dati del DPO dovranno essere comunicati al Garante per la protezione dati personali mediante il *Modello comunicazione al Garante dei dati del DPO ai sensi dell'art. 37, part. 1 par. 7 del GDPR* riportato nel file "[Modelli di delibera per la designazione del Data Protection Officer](#)".

- [Indicazioni per completare i modelli di delibera per la designazione del DPO](#)



Completare le parti evidenziate in giallo con:

1. data della delibera;

2. dati dello Studio;

3a. dati della persona fisica (si veda Allegato A) che ricoprirà il ruolo di DPO;

3b. dati della persona giuridica (si veda Allegato B) che ricoprirà il ruolo di DPO e relativi dati societari, nonché i dati del contratto di servizi concluso con la persona giuridica nominata DPO;

4. quantum della capacità di spesa eventualmente autorizzata al DPO;

5. luogo in cui saranno resi disponibili i dati di contatto del DPO (es. Intranet, bacheca, reception, ecc.)

10. Data Protection Impact Assessment (DPIA)

Si tratta del modello elaborato per svolgere la Valutazione d'Impatto sulla Protezione dei Dati, prevista dalla normativa europea di prossima attuazione in capo al Titolare del trattamento (*Data Protection Impact Assessment*, "DPIA"). La valutazione è sostanzialmente un'analisi specifica ed analitica dei rischi - e delle eventuali misure mitigatrici da apportare - sui trattamenti di dati personali eventualmente posti in essere dallo Studio. Tali circostanze sono individuate dall'art. 35 del Regolamento a livello generale (comma 1) oppure per determinate ipotesi espressamente tipizzate (comma 3). Per comodità e completezza, si riporta di seguito il testo del citato articolo 35 del Regolamento:

Valutazione d'impatto sulla protezione dei dati

1. *Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.*

2. *Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno.*

3. *La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti:*

a) *una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;*

b) *il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o*

c) *la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.*

La valutazione d'impatto sulla protezione dei dati ai sensi del paragrafo 1. L'autorità di controllo comunica tali elenchi al comitato di cui all'articolo 68.

4. *L'autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi del paragrafo 1. L'autorità di controllo comunica tali elenchi al comitato di cui all'articolo 68.*



5. L'autorità di controllo può inoltre redigere e rendere pubblico un elenco delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati. L'autorità di controllo comunica tali elenchi al comitato.

6. Prima di adottare gli elenchi di cui ai paragrafi 4 e 5, l'autorità di controllo competente applica il meccanismo di coerenza di cui all'articolo 63 se tali elenchi comprendono attività di trattamento finalizzate all'offerta di beni o servizi a interessati o al monitoraggio del loro comportamento in più Stati membri, o attività di trattamento che possono incidere significativamente sulla libera circolazione dei dati personali all'interno dell'Unione.

7. La valutazione contiene almeno:

a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;

c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e

d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

8. rispetto da parte di questi ultimi dei codici di condotta approvati di cui all'articolo 40, in particolare ai fini di una valutazione d'impatto sulla protezione dei dati.

Nel valutare l'impatto del trattamento effettuato dai relativi titolari o responsabili è tenuto in debito conto il

9. Se del caso, il titolare del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti.

10. Qualora il trattamento effettuato ai sensi dell'articolo 6, paragrafo 1, lettere c) o e), trovi nel diritto dell'Unione o nel diritto dello Stato membro cui il titolare del trattamento è soggetto una base giuridica, tale diritto disciplini il trattamento specifico o l'insieme di trattamenti in questione, e sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nell'ambito di una valutazione d'impatto generale nel contesto dell'adozione di tale base giuridica, i paragrafi da 1 a 7 non si applicano, salvo che gli Stati membri ritengano necessario effettuare tale valutazione prima di procedere alle attività di trattamento.

11. Se necessario, il titolare del trattamento procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento.

Come evincibile dalla lettura del comma 3 dell'art. 35 del Regolamento, la valutazione d'impatto è richiesta - tra le varie ipotesi - nei casi in cui venga posto in essere “[...] il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1 [...]”.



Le citate categorie particolari di dati personali ex art. 9, comma 1, del Regolamento ricomprendono anche i “[...] *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*”.

- **Come compilare il DPIA**

Il documento va completato - ove necessario, con il supporto delle competenti funzioni/responsabili IT, interne o esterne - procedendo come indicato nelle istruzioni, e dunque inserendo le informazioni rilevanti in merito al trattamento per cui si vuole svolgere il DPIA (sezioni dalla n. 1 alla n. 9 della colonna A) e - dopo aver risposto alle domande di cui alla sezione n. 10 della colonna A (“SI” / “NO”, inserendo una “X” nel relativo campo) - il file darà in automatico una valutazione in merito alla necessità o meno di svolgere il DPIA. In caso sia richiesto lo svolgimento del DPIA (ovvero se la cella numero 101 si colora in verde ed appare il messaggio: *“È necessario procedere con il DPIA! Compila le informazioni sottostanti”*), sarà necessario proseguire con la compilazione del documento e quindi la sezione “DATA PROTECTION IMPACT ASSESSMENT” (cella 103 e successive).

Completato il “DATA PROTECTION IMPACT ASSESSMENT”, l’analisi dei rischi che segue prende in considerazione il rischio elevato che il progetto/applicativo potrebbe presentare per i diritti e le libertà degli interessati. Per ogni rischio devono essere indicati l’impatto e la probabilità di accadimento assegnando un valore alla voce “*Gravità*” ed uno alla voce “*Probabilità*”. Si tratta di una lista aperta, aggiornabile in ogni momento.

Il sistema moltiplicherà in automatico i valori di “*Gravità*” e “*Probabilità*” inseriti, mostrando il relativo “*Risultato*”. Sarà necessario porre attenzione ai “*Rischi*” evidenziati in giallo e in rosso, che dovranno essere ri-selezionati dal menu a tendina previsto nella colonna “*Rischio*” della tabella successiva, per identificare le misure mitigatrici ritenute idonee a ridurre i medesimi, eventualmente con il supporto delle competenti funzioni tecniche, interne o esterne al Titolare. Il nuovo risultato derivante dall’applicazione delle misure definite per ridurre il rischio indicherà se sarà o meno necessario effettuare una consultazione preventiva ovvero se il rischio è stato adeguatamente ridotto e gestito.

11. Linee guida sul data protection by design e by default

Tali Linee Guida hanno lo scopo di illustrare i presidi interni (es. policy, procedure, misure di sicurezza), che il Titolare del trattamento può implementare per far sì che i trattamenti di dati personali siano allineati a tali nuovi principi. Si riporta di seguito il testo dell’art. 25 del Regolamento:

Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

1. Tenendo conto dello stato dell’arte e dei costi di attuazione, nonché della natura, dell’ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all’atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le



necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.

2. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

3. Un meccanismo di certificazione approvato ai sensi dell'articolo 42 può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2 del presente articolo.

12. Procedura per la gestione del Data Breach

Tale Procedura sulla gestione del Data Breach ha lo scopo di fornire le indicazioni pratiche allo Studio in caso di Violazione dei Dati Personali. In caso di nomina di un DPO sarà necessario coinvolgere il Responsabile della protezione dei dati nelle attività meglio descritte nella citata Procedura.

Il documento deve essere completato ove necessario con l'indicazione, tra le altre, (i) della denominazione dello Studio, (ii) dell'indirizzo (fisico o email) presso cui si vorranno ricevere le segnalazioni di conoscenza di una violazione, (iii) del/degli indirizzo/i a cui il Responsabile deve comunicare la conoscenza dell'avvenuta violazione.

Da valutare inoltre i soggetti (completare ove necessario) eventualmente coinvolti nell'analisi di secondo livello di cui alla sezione C.

13. Procedura di cooperazione con l'autorità di controllo

Tale documento fornisce le indicazioni da seguire per affrontare le visite, richieste di informazioni e/o ispezioni da parte del Garante per la protezione dei dati personali.

Nella sezione III.A occorre completare la tabella ivi contenuta con l'indicazione dei componenti della "Funzione Competente" chiamati a gestire le incombenze relative ad eventuali ispezioni e verifiche, che comprendere il DPO in caso di relativa nomina.

La tabella allegata alla Procedura (si veda sezione IV)., che riflette quella di cui alla sezione III.A, potrà essere ritagliata e consegnata al personale/collaboratori che accolgono personalmente l'Autorità di Controllo.

14. Procedura per l'esercizio dei diritti dell'interessato

Tale Procedura ha lo scopo di fornire indicazioni pratiche con riferimento alle richieste finalizzate all'esercizio dei diritti da parte degli Interessati ex artt. 15-22 GDPR. Dopo aver inserito i riferimenti dello Studio nel campo di applicazione, sarà necessario completare il documento inserendo i mezzi ai quali possono pervenire le richieste da parte degli interessati (si veda sezione II). In particolare, sarà necessario definire la composizione della "Funzione Competente" come opportuno. In caso di nomina di un DPO sarà



necessario coinvolgere anche il Responsabile della protezione dei dati nella gestione delle attività meglio descritte nella citata Procedura.

15. Policy sulla conservazione dei Dati Personali

La “Policy sulla conservazione dei Dati Personali” riporta i criteri da poter utilizzare ai fini della conservazione dei Dati Personali, che dovrà essere verificata e- in caso di conferma - completata con l'indicazione dello Studio titolare del trattamento. I tempi di conservazione dovranno naturalmente essere riflessi anche nel Registro dei trattamenti ex art. 30 GDPR.

16. Policy sulla base legale del trattamento

Tale documento ha lo scopo di riportare i principi legali sottostanti al Trattamento dei Dati Personali nonché quello di elencare le basi giuridiche che possono essere utilizzate dallo Studio. Tale Policy dovrà essere completata con l'indicazione dello Studio titolare del trattamento. Le basi legali utilizzate dal Titolare dovranno essere riflesse nelle informative e nel Registro dei trattamenti ex art. 30 GDPR.