

La Privacy per i professionisti

Martedì 26 Marzo 2019

Sala Montelupo – Domagnano – Repubblica di San Marino

Relatori: Dott. Andrea Cecchetti, Avv. Fabio Righi

Gli step fondamentali per un corretto adeguamento

Audit periodico

- › Verifiche su documenti e procedure
- › Eventuali aggiornamenti

Sicurezza informatica

- › Applicazione delle misure di sicurezza adeguate alla struttura di studio.

Mappatura dei dati e dei processi interni

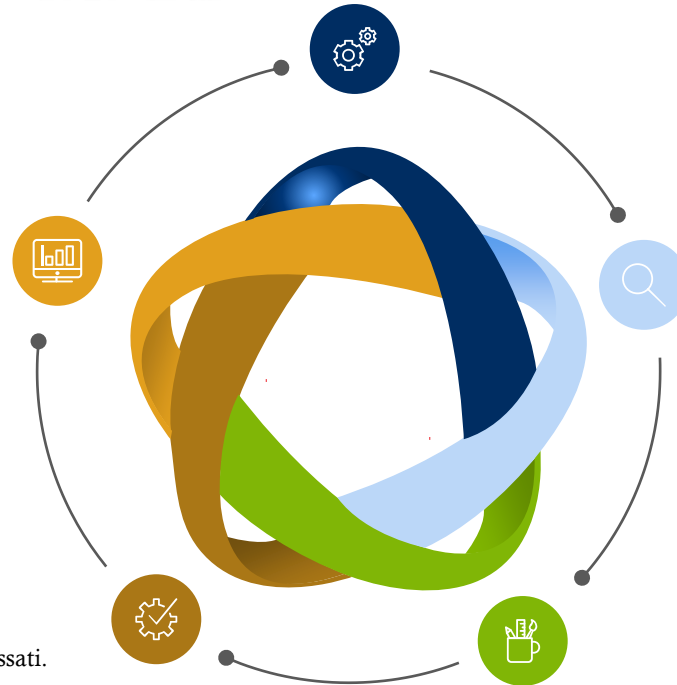
- › Registri delle attività di trattamento.
- › Organigrammi aziendali
- › Flow charts.

Procedure interne

- › Data Breach policy.
- › Politica per i diritti degli interessati.
- › Data retention policy.
- › Formazione dei propri dipendenti e collaboratori

Produzione documentale

- › Accordo di contitolarità tra i soci di studio.
- › Data protection Agreement ed informative per i clienti
- › Atti di nomina dei responsabili esterni.
- › Welcome kit per i dipendenti
- › Politica generale sulla protezione dei dati personali di Studio.



Alcune Definizioni

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 *on line* o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale»
 - ◆ Considerando 30 – GDPR: *Le persone fisiche possono essere associate a identificativi online prodotti dai dispositivi, dalle applicazioni, dagli strumenti e dai protocolli utilizzati, quali gli indirizzi IP, a marcatori temporanei (cookies) o a identificativi di altro tipo, come i tag di identificazione a radiofrequenza. Tali identificativi possono lasciare tracce che, in particolare se combinate con identificativi univoci e altre informazioni ricevute dai server, possono essere utilizzate per creare profili delle persone fisiche e identificarle.*

Alcune Definizioni

Dato personale «particolare»

- Art. 9 GDPR – Art. 8 Legge RSM: «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».

Alcune Definizioni

Trattamento di dati personali

- ◆ «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».
- ◆ **Alcuni esempi:** gestione interna (amministrativa) dei dati personali riferiti al personale dipendente, elaborazione delle dichiarazioni dei redditi della clientela, attività di raccolta di informazioni tramite il sito web ecc.

Alcune Definizioni

Titolare del trattamento – Controller

- ◆ «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».
- ◆ Per finalità si intendono gli obiettivi e gli scopi per cui si pone in essere un trattamento (es: adempimento di un obbligo contrattuale o giuridico).
- ◆ Per i mezzi del trattamento si intendono le modalità mediante le quali si effettua un trattamento di dati personali – cartacee ed elettroniche (es: utilizzo di un software nell'elaborazione del servizio paghe, redazione di un adeguata verifica della clientela in modalità cartacea)
- ◆ **NB:** La Titolarità si sostanzia nel **potere decisionale** che un soggetto ha nel compimento di un trattamento dei dati personali in termini di finalità e modalità del trattamento.

Alcune Definizioni

Responsabile del trattamento - Processor

- ◆ «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento»
- ◆ Un responsabile del trattamento è un soggetto esterno all'organizzazione aziendale, che interviene in una parte del trattamento dei dati personali.
- ◆ Alcuni esempi:
 - ◆ **commercialista che elabora i cedolini paga di un cliente;**
 - ◆ la società di servizi o l'associazione di categoria che effettua formazione nei confronti dei dipendenti di un'azienda;
 - ◆ la software house che produce ed effettua manutenzione periodica su un software gestionale.
- ◆ Non tutti i fornitori sono qualificabili come responsabili del trattamento.

Adeguamento per un professionista o uno studio associato

Raccolta di informazioni

1° Mappatura delle singole operazioni di trattamento

- Suddividere l'attività di uno studio nelle seguenti macrocategorie: Risorse Umane e Amministrazione, Servizi alla clientela, Sicurezza fisica ed informatica.
- A seconda dei singoli trattamenti, il professionista o lo studio associato può qualificarsi come titolare o responsabile del trattamento.

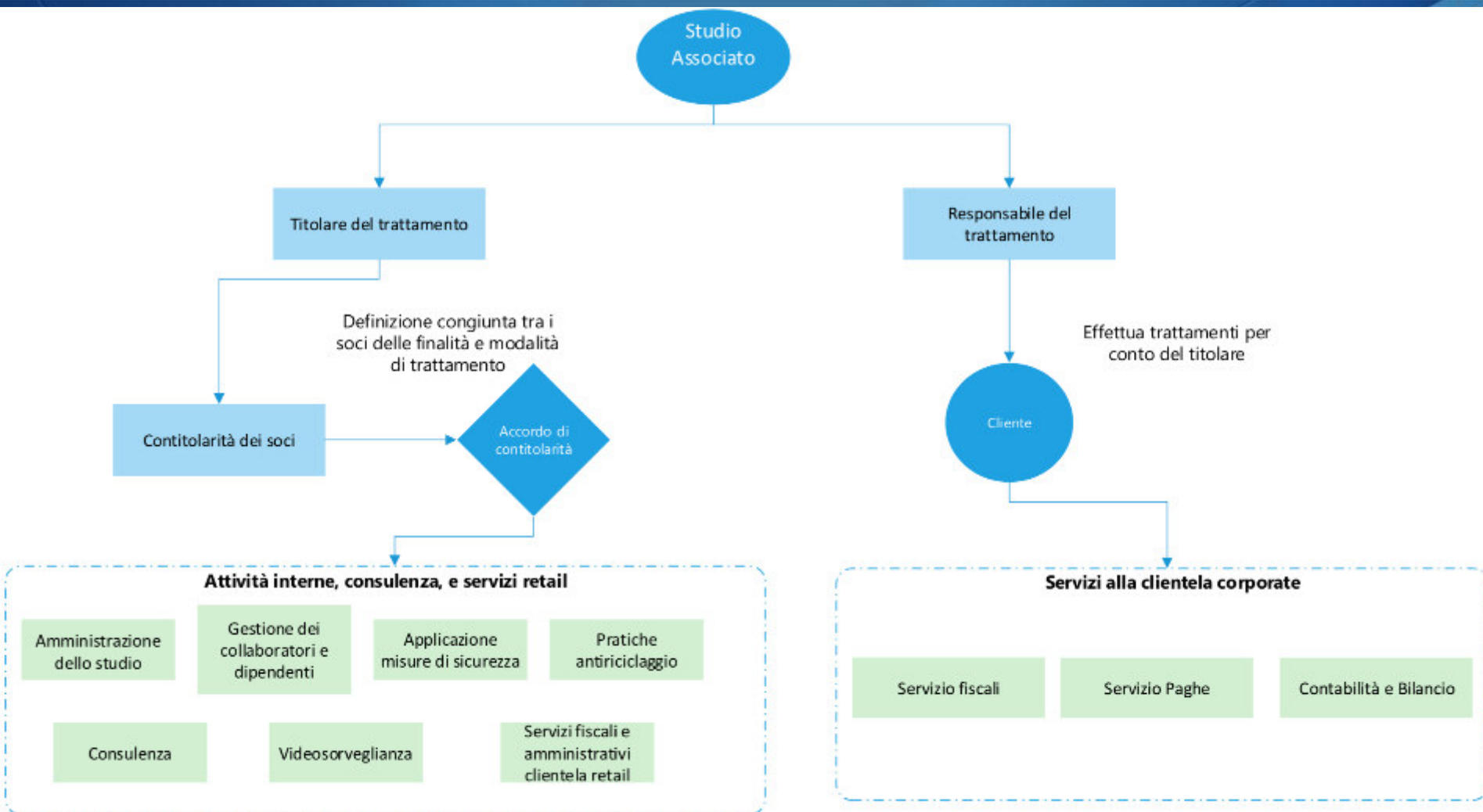
Un esempio pratico:

- **Trattamenti che rientrano nella categoria Risorse Umane:**
 - Raccolta e conservazione delle timbrature;
 - Videosorveglianza;
 - Assolvimento delle pratiche di Sicurezza sul luogo di lavoro e relativa formazione;
 - Gestione interna e suddivisione dei carichi di lavoro, nonché monitoraggio dei lavori;
 - Elaborazione dei cedolini paga e contestuale pagamento dello stipendio;
 - Gestione amministrativa/fiscale (es: elaborazione delle dichiarazioni fiscali)

Adeguamento per un professionista o uno studio associato

Raccolta di informazioni

Il ruolo dello Studio Associato di Commercialisti



Adeguamento per un professionista o uno studio associato

Raccolta di informazioni

Il ruolo dello Studio Associato di Commercialisti Pronuncia dell'Autorità Garante italiana

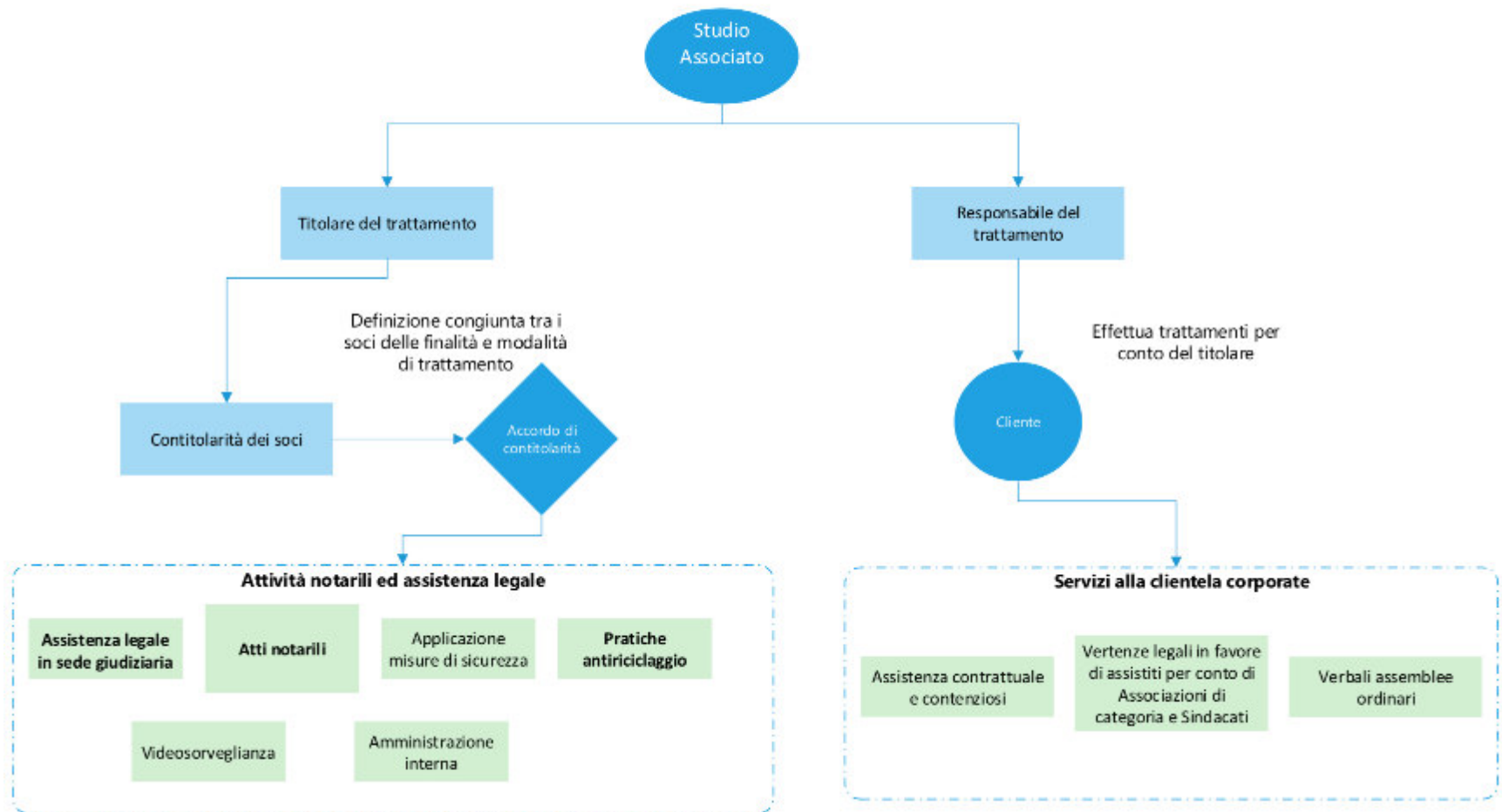
Newsletter n.449 del 7 Febbraio 2019: “i consulenti del lavoro sono “titolari” quando trattano, in piena autonomia e indipendenza, i dati dei propri dipendenti oppure dei propri clienti quando siano persone fisiche, come ad esempio i liberi professionisti determinando puntualmente le finalità e i mezzi del trattamento. Sono, viceversa, “responsabili” quando trattano i dati dei dipendenti dei loro clienti sulla base dell’incarico ricevuto, che contiene anche le istruzioni sui trattamenti da effettuare. E’ il caso, ad esempio, dei consulenti che curano per conto di datori di lavoro la predisposizione delle buste paga, le pratiche relative all’assunzione e al fine rapporto, o quelle previdenziali e assistenziali, trattando una pluralità di dati personali, anche sensibili, dei lavoratori.”

Adeguamento per un professionista o uno studio associato

Raccolta di informazioni

Il ruolo dello Studio Associato di Avvocati

I ruoli dello Studio Associato



Adeguamento per un professionista o uno studio associato

Raccolta di informazioni

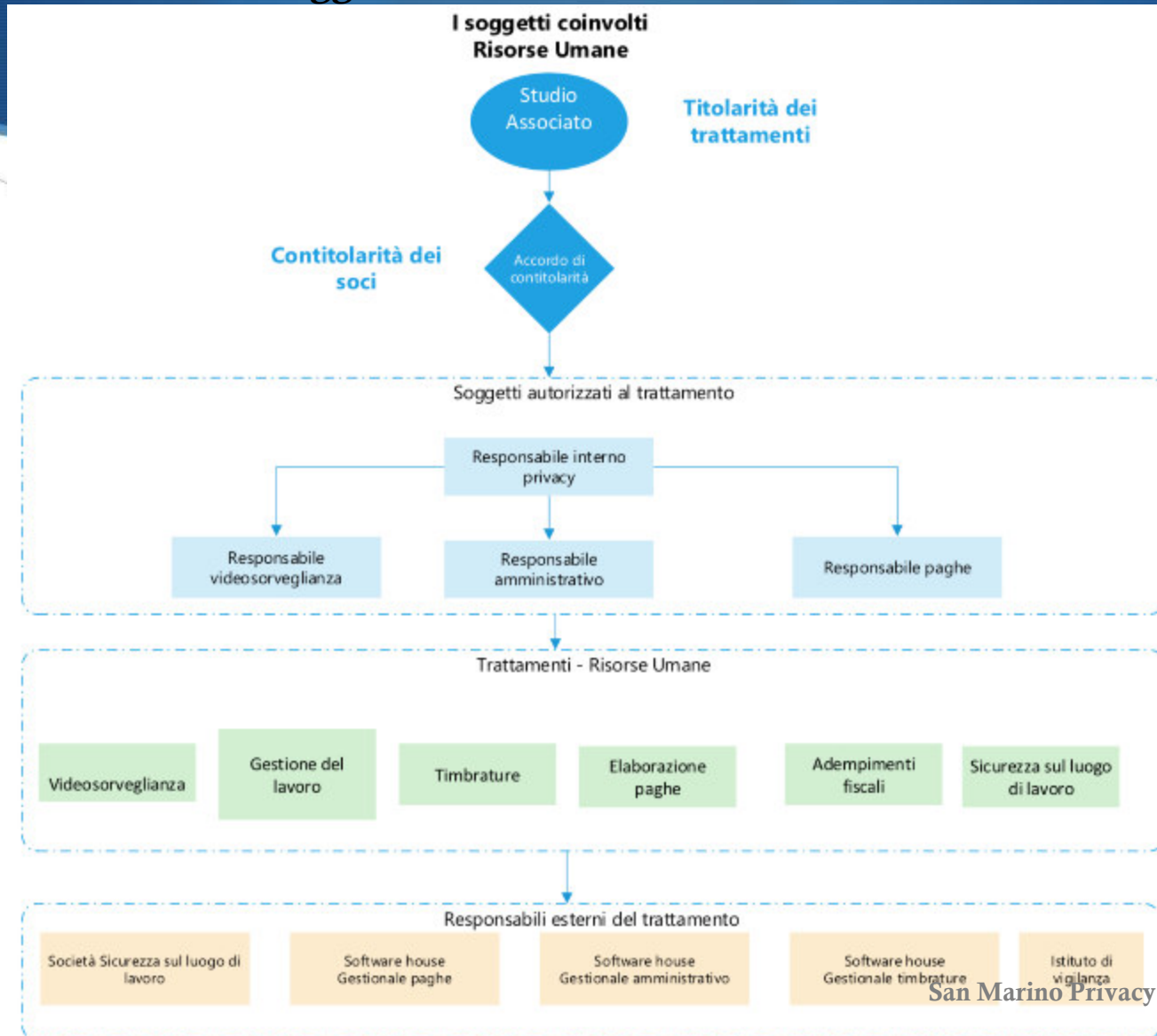
2° Mappatura dei dati personali trattati – Risorse Umane

Trattamento	Dati personali
Raccolta e conservazione timbrature	- Dati personali identificativi (es: nominativi) - Orari di lavoro
Videosorveglianza	- Immagini e videoregistrazioni
Assolvimento pratiche Sicurezza sul luogo di lavoro	- Dati personali identificativi (es: nominativi); - Informazioni sulla posizione lavorativa (es: orario di lavoro, mansioni svolte); - Dati personali particolari (es: cartella sanitaria)
Gestione interna e suddivisione dei carichi di lavoro, nonché monitoraggio dei lavori	- Orario di lavoro; - Dati personali identificativi (es: nominativi)
Elaborazione dei cedolini paga e contestuale pagamento dello stipendio	- Dati personali identificativi (es: nominativi, indirizzo e-mail, residenza e cittadinanza) - Dati personali particolari (es: dati relativi allo stato di salute) - Informazioni sulla posizione lavorativa (es: orario di lavoro, mansioni svolte, stipendio); - Coordinate bancarie.
Gestione amministrativa/fiscale (es: elaborazione delle dichiarazioni fiscali)	- Dati personali identificativi (es: nominativi, residenza e cittadinanza); - Dati personali particolari (es: dati relativi allo stato di salute - deduzioni)

Adeguamento per un professionista o uno studio associato

Raccolta di informazioni

3° I soggetti coinvolti – Risorse Umane



Adeguamento per un professionista o uno studio associato

Raccolta di informazioni

4° Finalità e basi giuridiche – Risorse Umane

Trattamento	Tipologia di dati personali	Basi giuridiche
Raccolta e conservazione timbrature	Dati personali	Adempimento di un obbligo contrattuale
Videosorveglianza	Dati personali	Legittimo interesse (tutela del patrimonio aziendale)
Assolvimento pratiche Sicurezza sul luogo di lavoro	• Dati personali • Dati particolari	• Adempimento di un obbligo Legale • Assolvimento di un obbligo del titolare in materia di diritto del lavoro, sicurezza sociale e protezione sociale
Gestione interna e suddivisione dei carichi di lavoro, nonché monitoraggio dei lavori	Dati personali	Adempimento di un obbligo contrattuale
Elaborazione dei cedolini paga e contestuale pagamento dello stipendio	• Dati personali • Dati particolari	• Adempimento di un obbligo contrattuale • Assolvimento di un obbligo del titolare in materia di diritto del lavoro, sicurezza sociale e protezione social
Gestione amministrativa/fiscale (es: elaborazione delle dichiarazioni fiscali)	• Dati personali • Dati particolari	• Adempimento di un obbligo legale • Consenso

Adeguamento per un professionista o uno studio associato

Raccolta di informazioni

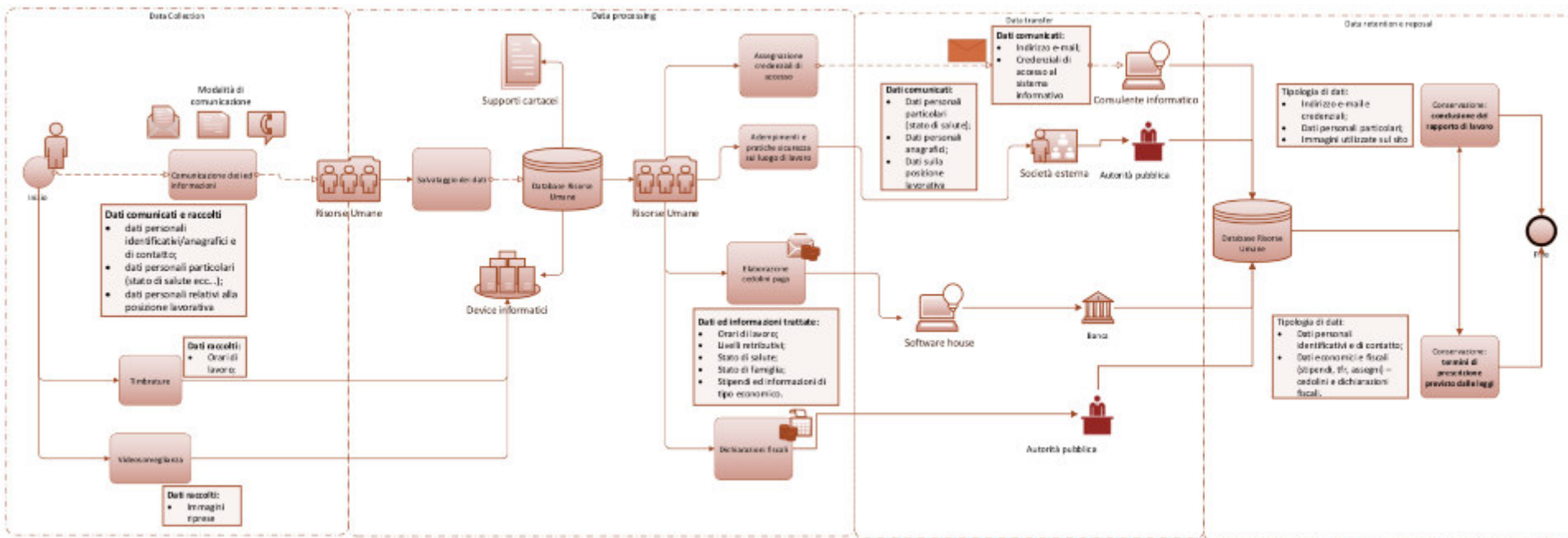
5° Modalità del trattamento e asset – Risorse Umane

Trattamento	Modalità e asset fisici ed informatici
Raccolta e conservazione timbrature	• Informatica (Software applicativo – badge o impianto biometrico e conservazione su Server) • Cartacea (Archivio documentale Risorse Umane)
Videosorveglianza	• Informatica (DVR/ hard disk esterno e software su cellulare aziendale)
Assolvimento pratiche Sicurezza sul luogo di lavoro	• Informatica (scambio di informazioni – posta elettronica e salvataggio sul server) • Cartacea (Archivio documentale – Risorse Umane)
Gestione interna e suddivisione dei carichi di lavoro, nonché monitoraggio dei lavori	• Informatica (Software rapportini orari - posta elettronica) • Cartacea (Mansionari – Risorse Umane)
Elaborazione dei cedolini paga e contestuale pagamento dello stipendio	• Informatica (Software di elaborazione - posta elettronica – Database paghe informatico su server) • Cartacea (Archivio documentale – Risorse Umane)
Gestione amministrativa/fiscale (es: elaborazione delle dichiarazioni fiscali)	• Informatica (Applicativo PA/ database DR informatico su server) • Cartaceo (Archivio DR – Risorse Umane)

Adeguamento per un professionista o uno studio associato

Raccolta di informazioni

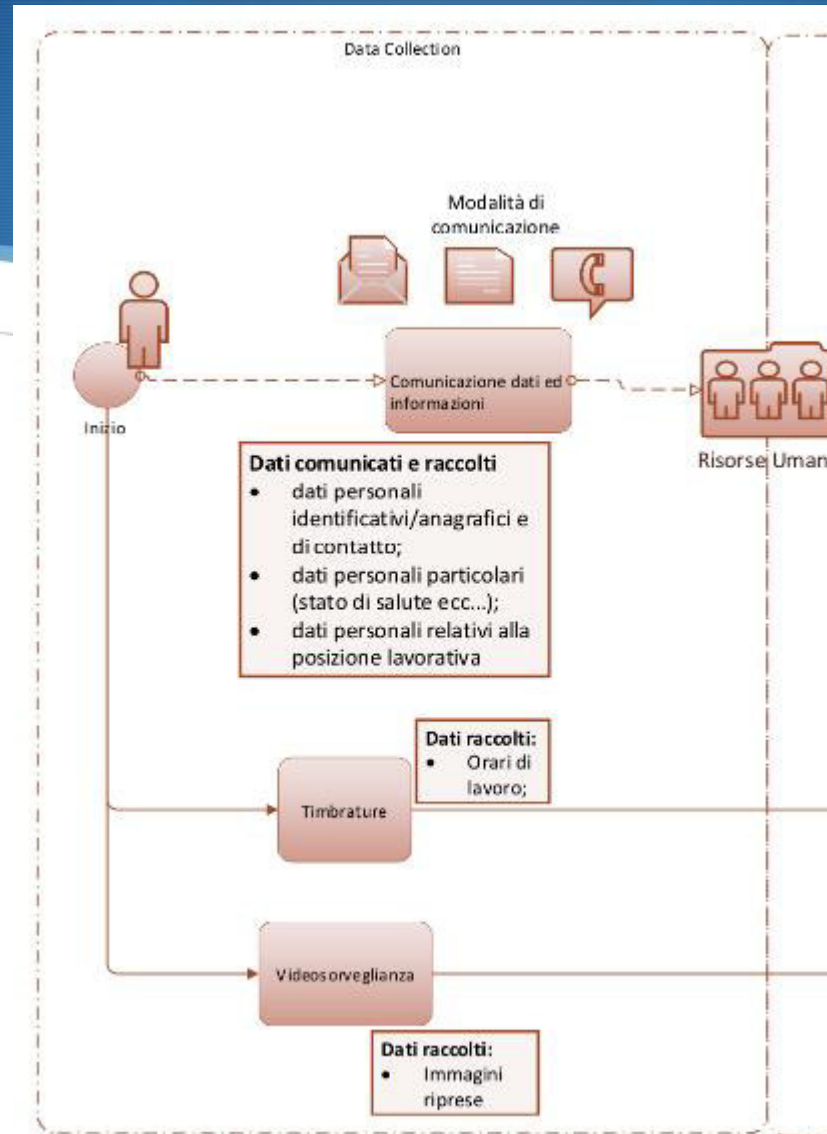
Data flow diagram – Risorse Umane



Adeguamento per un professionista o uno studio associato

Raccolta di informazioni

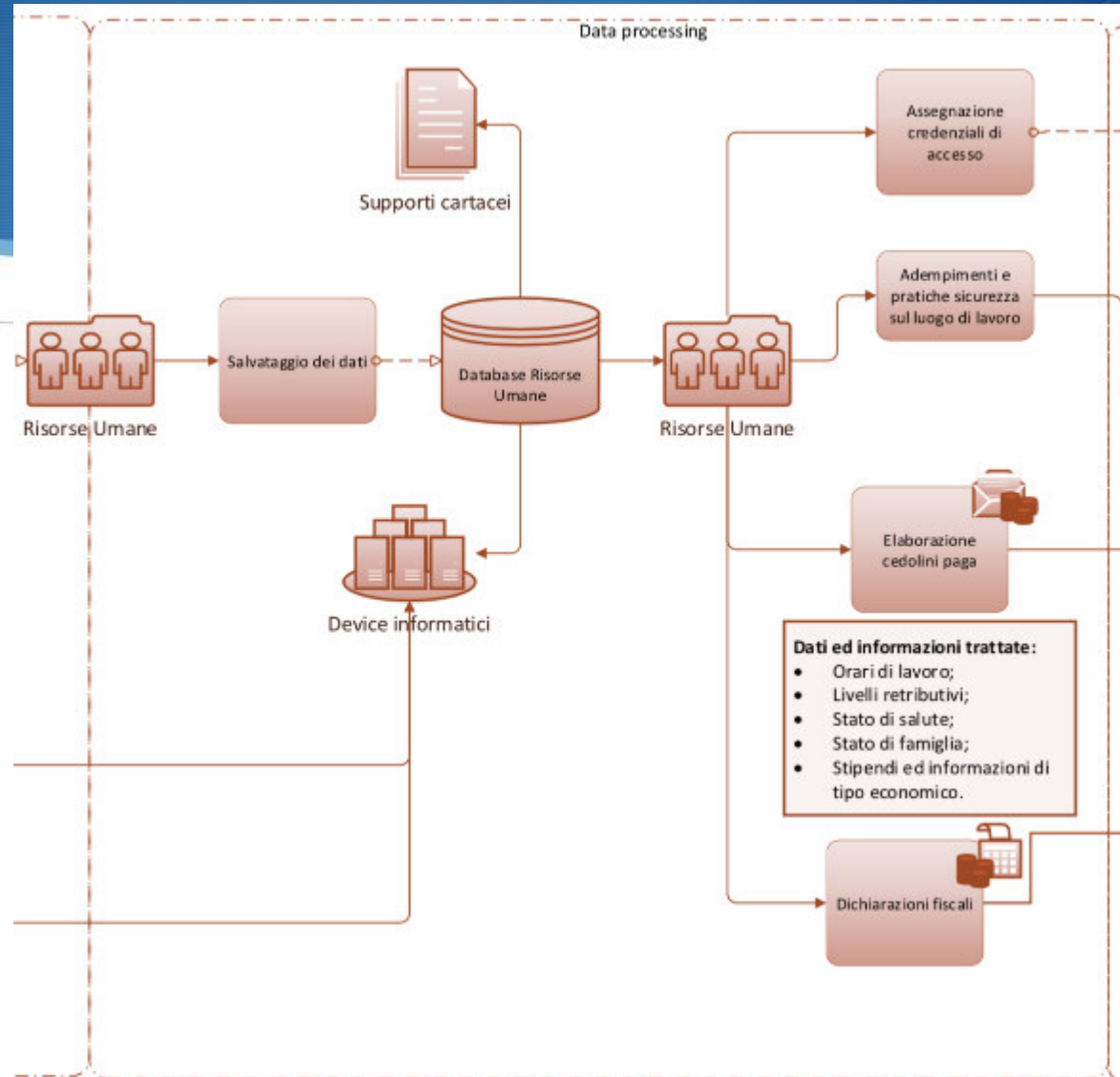
Data flow diagram – Risorse Umane Data Collection



Adeguamento per un professionista o uno studio associato

Raccolta di informazioni

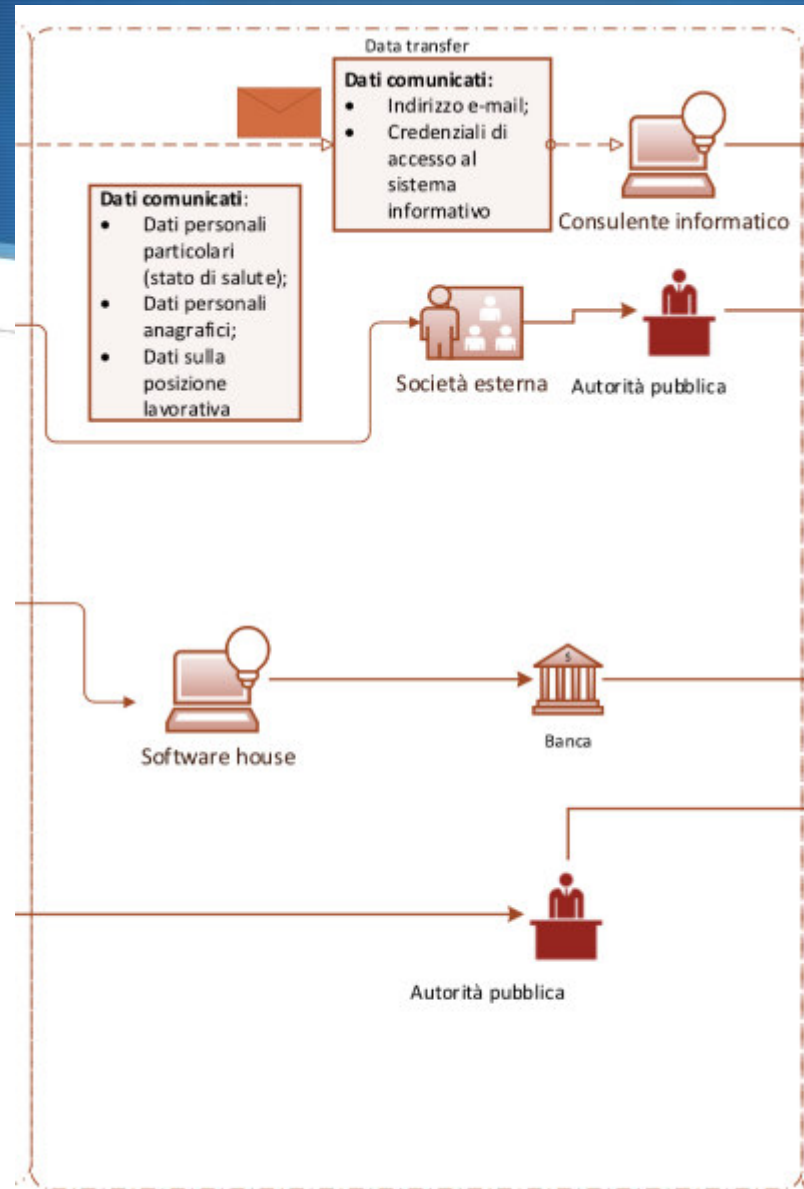
**Data flow diagram
– Risorse Umane
Data Processing**



Adeguamento per un professionista o uno studio associato

Raccolta di informazioni

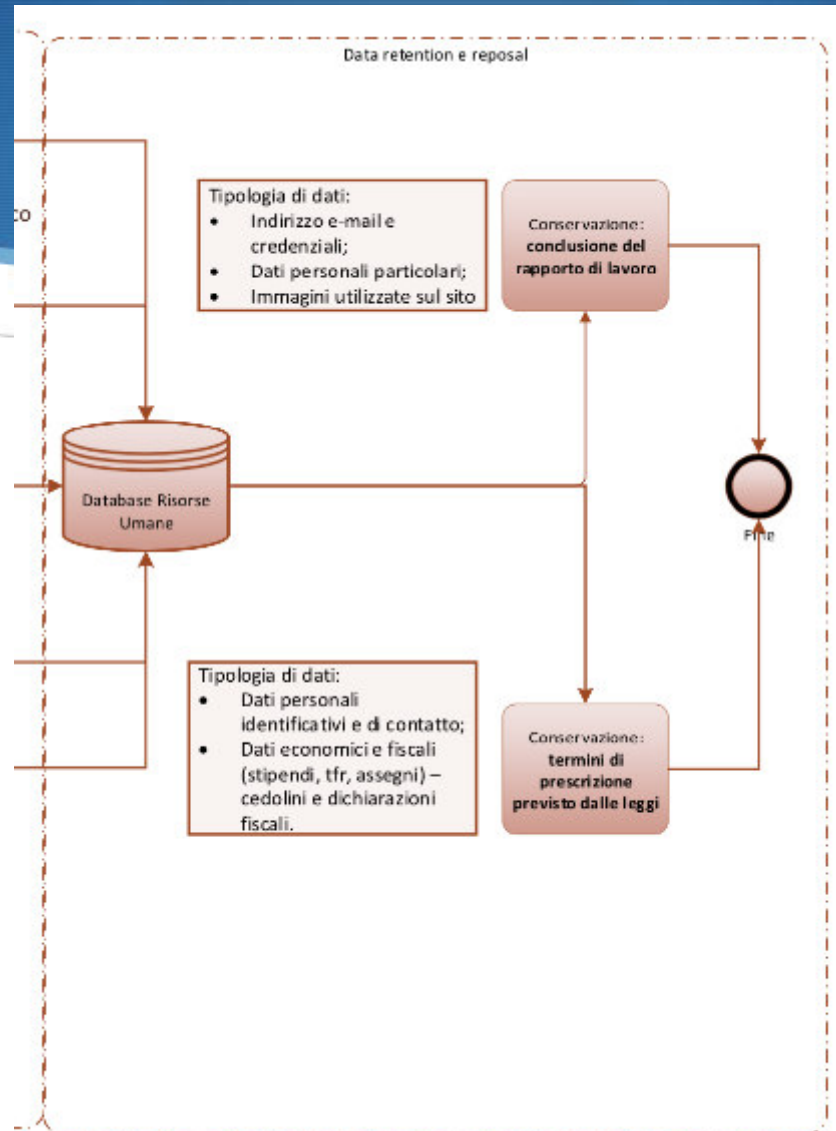
Data flow diagram – Risorse Umane Data Transfer



Adeguamento per un professionista o uno studio associato

Raccolta di informazioni

Data flow diagram – Risorse Umane Data Retention



Adeguamento per un professionista o uno studio associato

Raccolta di informazioni

Riassumendo

Come iniziare un adeguamento privacy?

- 1 – Suddividere lo studio in macro-categorie
- 2 – Individuare per ogni macro-categoria singoli trattamenti di dati personali (caso Risorse Umane)
- 3 – In quali attività lo Studio è titolare ed in quali è responsabile?
- 4 – Individuare i dati personali trattati per ogni singola operazione di trattamento
- 5- Individuare i soggetti coinvolti nelle operazioni di trattamento (soggetti interni ed esterni)
- 6 – Individuare le finalità e le basi giuridiche per ogni singolo trattamento
- 7 – Individuare le modalità e gli asset informatici e fisici
- 8 – Mappatura dell'intero processo (flow chart Risorse Umane)

Adeguamento per un professionista o uno studio associato

Produzione documentale

- Adeguamento per un professionista o uno studio associato
 - **Produzione documentale**
 - Il Registro delle attività di trattamento
 - Organigramma funzionale privacy
 - Accordo di contitolarità
 - L'informativa sul trattamento dei dati personali e i consensi
 - Nomine dei responsabili del trattamento esterni
 - Documenti per i propri collaboratori e dipendenti (“Welcome kit”).

Adeguamento per un professionista o uno studio associato

Produzione documentale

Registro delle Attività di trattamento

Art.30 del GDPR e Art.31 Legge RSM

Contenuto minimo

Dati identificativi e contatto del Titolare, dei contitolari, del rappresentante e del DPO.

Finalità per ogni specifico trattamento

Categorie di dati personali ed interessati coinvolti per ogni specifico trattamento

Categorie di destinatari dei dati personali (soggetti a cui vengono comunicati).

Trasferimenti di dati verso un Paese terzo

Il periodo di conservazione dei dati personali

Descrizione generale delle misure di sicurezza

Adeguamento per un professionista o uno studio associato

Produzione documentale

Registro delle Attività di trattamento

I modelli “semplificati” dell’Autorità Garante Italiana



**GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI**

SCHEDA REGISTRO DEI TRATTAMENTI (per i contenuti vedi FAQ sul registro delle attività di trattamento: <https://www.garanteprivacy.it/regolamento/registro>)

TITOLARE/CONTITOLARE/RAPPRESENTANTE DEL TITOLARE (inserire la denominazione e i dati di contatto)

RESPONSABILE DELLA PROTEZIONE DEI DATI (inserire la denominazione e i dati di contatto)

TIPOLOGIA DI TRATTAMENTO	FINALITÀ E BASI LEGALI DEL TRATTAMENTO	CATEGORIE DI INTERESSATI	CATEGORIE DI DATI PERSONALI	CATEGORIE DI DESTINATARI (indicare eventuali responsabili del trattamento o altri titolari cui i dati siano comunicati)	TRASFERIMENTO DATI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI (indicare il Paese terzo o l'organizzazione internazionale cui i dati sono trasferiti e le "garanzie" adottate ai sensi del capo V del RGPD)	TERMINI ULTIMI DI CANCELLAZIONE PREVISTI	MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE

Adeguamento per un professionista o uno studio associato

Produzione documentale

Registro delle Attività di trattamento

I modelli “semplificati” dell’Autorità Garante Italiana



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

SCHEDA REGISTRO DEI TRATTAMENTI DEL RESPONSABILE/SUB-RESPONSABILE		
<i>[per i contenuti vedi Faq sul registro delle attività di trattamento: https://www.garanteprivacy.it/regolamentoue/registro]</i>		
RESPONSABILE <i>(inserire la denominazione e i dati di contatto)</i>		
TITOLARE/CONTITOLARE/RAPPRESENTANTE DEL TITOLARE <i>(inserire la denominazione e i dati di contatto)</i>		
RESPONSABILE DELLA PROTEZIONE DEI DATI <i>(inserire la denominazione e i dati di contatto)</i>		
CATEGORIA DI TRATTAMENTO	TRASFERIMENTO DATI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI <i>(indicare il Paese verso il quale viene trasferita l'informazione o i dati e la "garanzia" adottata ai sensi del capo IV del RGPD)</i>	MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE

Adeguamento per un professionista o uno studio associato

Produzione documentale

Registro delle Attività di trattamento

Ulteriori Informazioni?

L'obbligo di tenere il registro delle attività di trattamento potrebbe essere l'occasione per raccogliere ulteriori utili informazioni rispetto a quelle indicate nella Normativa, quali ad esempio:

- attività effettuate.
- base giuridica del trattamento.
- elenco terzi coinvolti.
- analisi del rischio per singolo applicativo e/o servizio.
- esistenza di valutazione d'impatto e consultazione preventiva.
- documentazione a supporto del trattamento (es. informativa e consenso)
- procedure per l'esercizio dei diritti dell'interessato.
- provvedimenti specifici dell'autorità di controllo.

Adeguamento per un professionista o uno studio associato

Produzione documentale

Registro delle Attività di trattamento

Le funzioni del Registro

È uno strumento operativo che consente di:

- censire le banche dati e i trattamenti in essere;
- rappresentare l'organizzazione sotto il profilo delle attività di trattamento a fini di informazione, consapevolezza e condivisione interna;
- costituire lo strumento di pianificazione e controllo delle attività di trattamento dei dati personali in modo da garantire la loro integrità, riservatezza e disponibilità;
- ridurre gli sprechi in termini di tempo, risorse, duplicazione delle informazioni;
- ridurre i rischi di eventuali trattamenti illeciti;
- conservare in maniera ordinata e verificabile da terzi le informazioni relative all'adozione delle misure tecniche ed organizzative adeguate ed efficaci finalizzate ad attuare il principio di responsabilizzazione.

Adeguamento per un professionista o uno studio associato

Produzione documentale

Registro delle Attività di trattamento

L'importanza del Registro

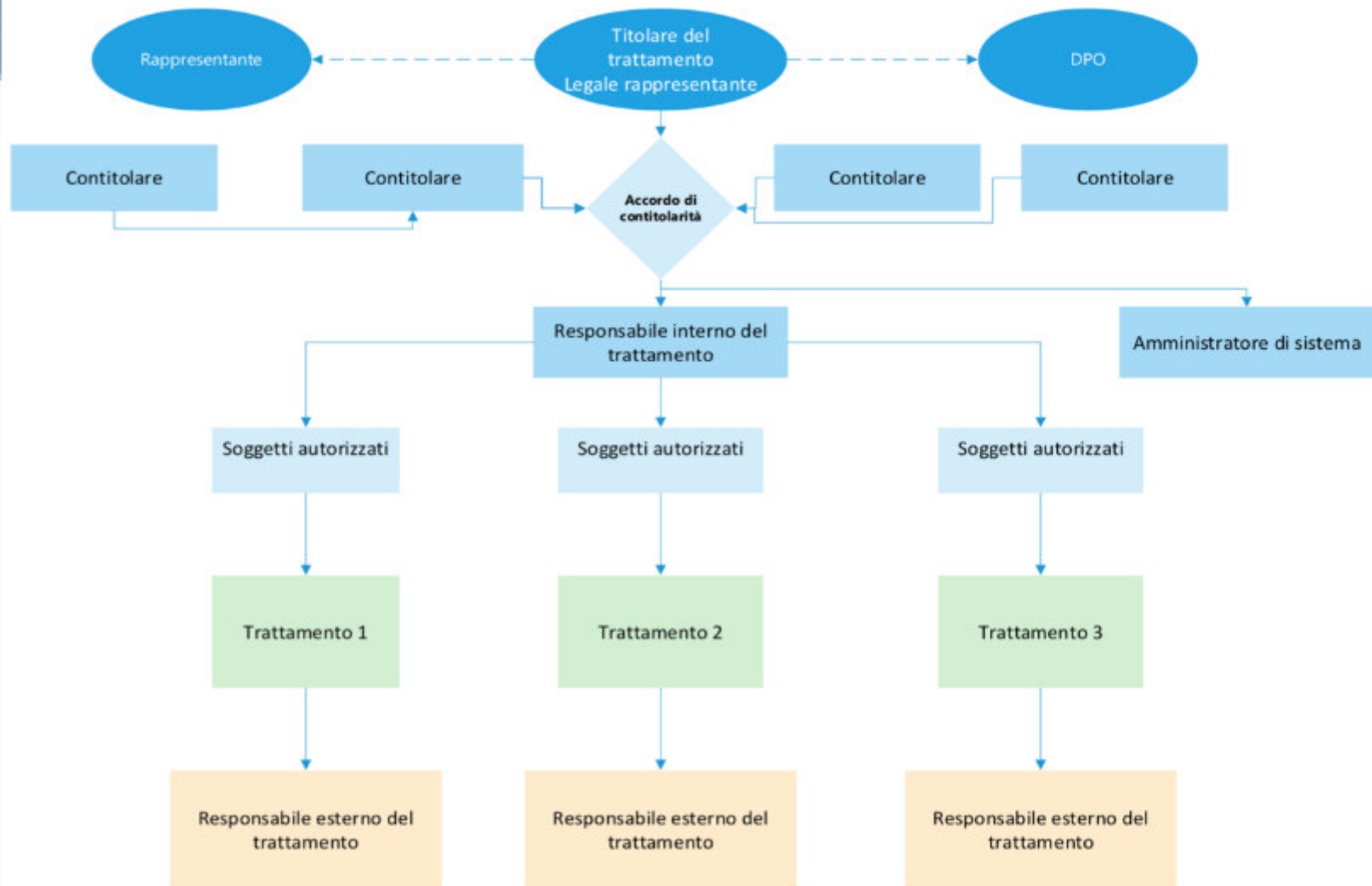
Considerando 82:

“Per dimostrare che si conforma al presente regolamento, il titolare o il responsabile del trattamento dovrebbe tenere un registro delle attività di trattamento effettuate sotto la sua responsabilità. Sarebbe necessario obbligare tutti i titolari e i responsabili del trattamento a cooperare con l'autorità di controllo e a mettere, su richiesta, detti registri a sua disposizione affinché possano servire per monitorare detti trattamenti”.

Adeguamento per un professionista o uno studio associato

Produzione documentale

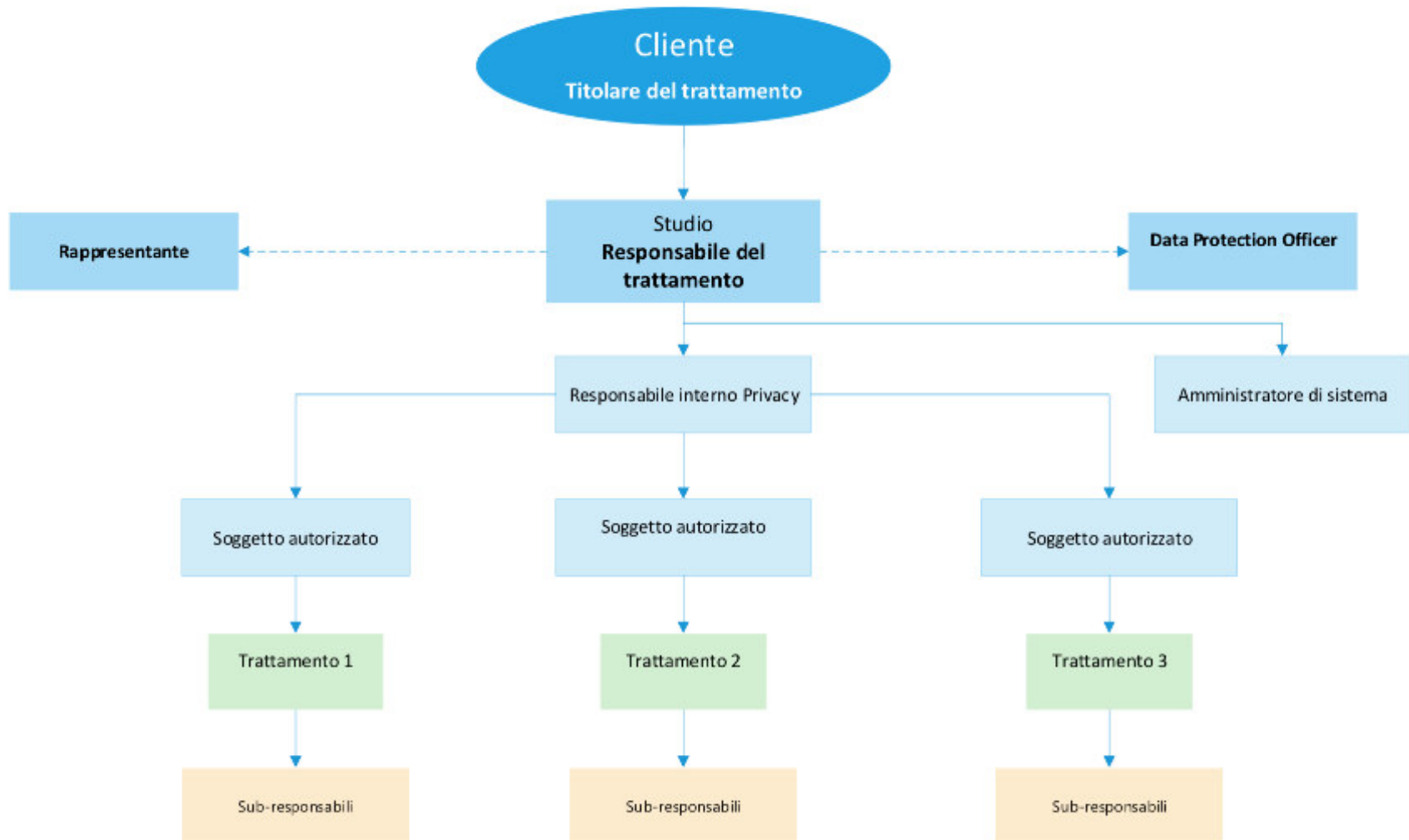
ORGANIGRAMMA AZIENDALE PRIVACY



Adeguamento per un professionista o uno studio associato

Produzione documentale

ORGANIGRAMMA AZIENDALE "PRIVACY"



Adeguamento per un professionista o uno studio associato

Produzione documentale

Accordo di contitolarità

Art.26 GDPR – Art. 28 Legge RSM

Quando due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi si qualificano quali contitolari del trattamento.

- Obbligo di stipulare un accordo di contitolarità che disciplini:
 - quali sono i trattamenti che rientrano nell'accordo.
 - le rispettive responsabilità in merito all'osservanza degli obblighi previsti dalla normativa privacy (normalmente in uno Studio Associato i soci si obbligano in solido a rispettare gli adempimenti previsti).
 - le responsabilità in merito all'esercizio dei diritti dell'interessato e le rispettive funzioni di comunicazione delle informazioni, designando un punto di contatto per gli interessati.

Adeguamento per un professionista o uno studio associato

Produzione documentale

Informative sul trattamento dei dati personali

Contenuto

In caso di raccolta presso l'interessato di dati che lo riguardano, **il titolare dovrà comunicare** (art. 13 GDPR e Legge RSM):

Contenuto minimo
Dati identificativi e contatto del Titolare, dei contitolari, del rappresentante e del DPO.
Finalità e base giuridiche dei trattamenti
l'eventuale legittimo interesse del titolare o di terzi
Categorie di destinatari e dati dei responsabili del trattamento
Trasferimenti di dati verso un Paese terzo
Il periodo di conservazione dei dati personali o i criteri per determinarlo
Esistenza dei diritti dell'interessato
Obbligatorietà nel fornire i dati e le possibili conseguenze
Esistenza di un processo decisionale automatizzato (profilazione)

Adeguamento per un professionista o uno studio associato

Produzione documentale

Informative sul trattamento dei dati personali

Forma

I soggetti interessati hanno il diritto di ricevere adeguate informazioni circa il trattamento e circa l'esercizio dei propri diritti:

- in forma concisa, trasparente, intelligibile e facilmente accessibile.
- in un linguaggio semplice e chiaro.
- per iscritto o con altri mezzi (anche elettronici).
- oralmente (se richiesto dall'interessato). NB: La Legge Sammarinese non prevede tale modalità

Adeguamento per un professionista o uno studio associato

Produzione documentale

Informative sul trattamento dei dati personali

In quali casi redigerla?

L'informativa deve fornirla
sempre il Titolare

Studio Associato

Titolarità del
trattamento

Titolarità del trattamento = potere
decisionale nelle finalità e modalità
di trattamento

In quali trattamenti lo
Studio è Titolare del
trattamento?

Sistema informatico

Consulenza e servizi fiscali
retail

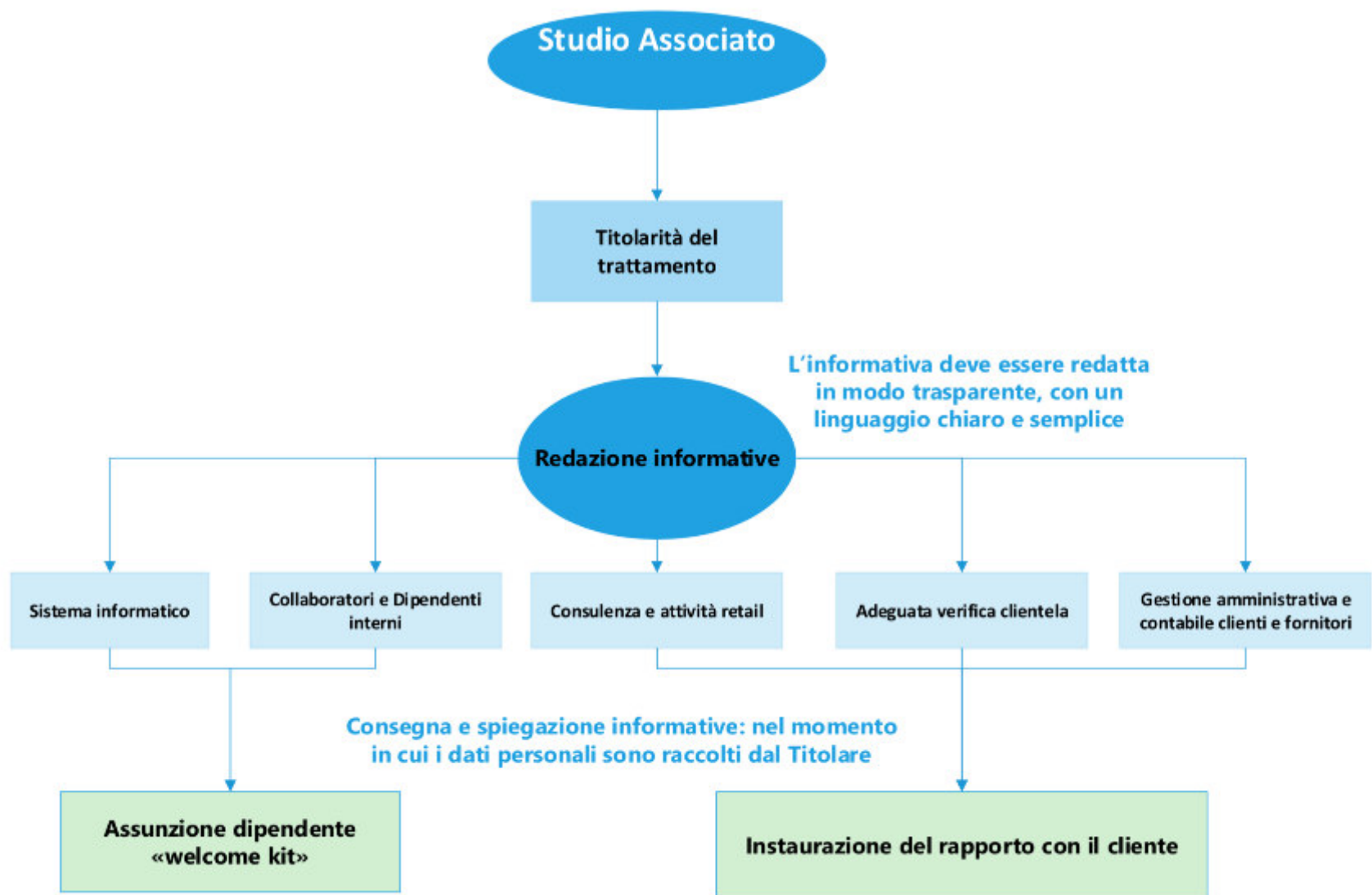
Collaboratori e Dipendenti
interni

Adeguate verifica clientela

Gestione amministrativa e
contabile clienti e fornitori

Adeguamento per un professionista o uno studio associato

Produzione documentale



Adeguamento per un professionista o uno studio associato

Produzione documentale

Informative sul trattamento dei dati personali **Quando non è necessaria per i Dottori Commercialisti ?**

L'informativa sul trattamento dei dati personali non è necessaria in tutti i casi in cui lo Studio si qualifica come responsabile del trattamento, ovvero:

- Servizi di tenuta della contabilità ordinaria e redazione del bilancio civilistico.
- Servizi fiscali, compilazioni dichiarazioni dei redditi (Modelli IGR-P, IGR-O, DAN e Allegati).
- Servizi di elaborazione dei cedolini paga dei clienti.



In tutti i casi indicati, l'informativa deve essere fornita agli interessati coinvolti (dipendenti, clienti e fornitori del cliente di Studio) da parte del cliente di Studio.

Adeguamento per un professionista o uno studio associato

Produzione documentale

Informative sul trattamento dei dati personali **Quando non è necessaria per gli Avvocati?**

L'informativa sul trattamento dei dati personali non è necessaria in tutti i casi in cui lo Studio si qualifica come responsabile del trattamento, ovvero:

- **Attività di assistenza legale affidata da una persona giuridica (società, associazione di categoria, sindacato) per conto di una persona fisica (es: vertenze legali effettuate dal legale nei confronti di un iscritto ad un'associazione sindacale, ove il mandato sia affidato dal soggetto giuridico**
- **Assistenza nella contrattualistica d'impresa e relativi contenziosi.**
- **Verbali d'assemblea, che non comportano l'atto pubblico.**



In tutti i casi indicati, l'informativa deve essere fornita agli interessati coinvolti da parte del cliente di Studio o del soggetto giuridico che propone l'incarico professionale.

Adeguamento per un professionista o uno studio associato

Produzione documentale

Consensi e autorizzazioni al trattamento

Definizione di 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*



Un consenso conforme alla normativa deve integrare un atto positivo inequivocabile:

- dichiarazione scritta, anche attraverso mezzi elettronici.
- linguaggio semplice, chiaro, comprensibile.
- un consenso per ogni finalità di trattamento.

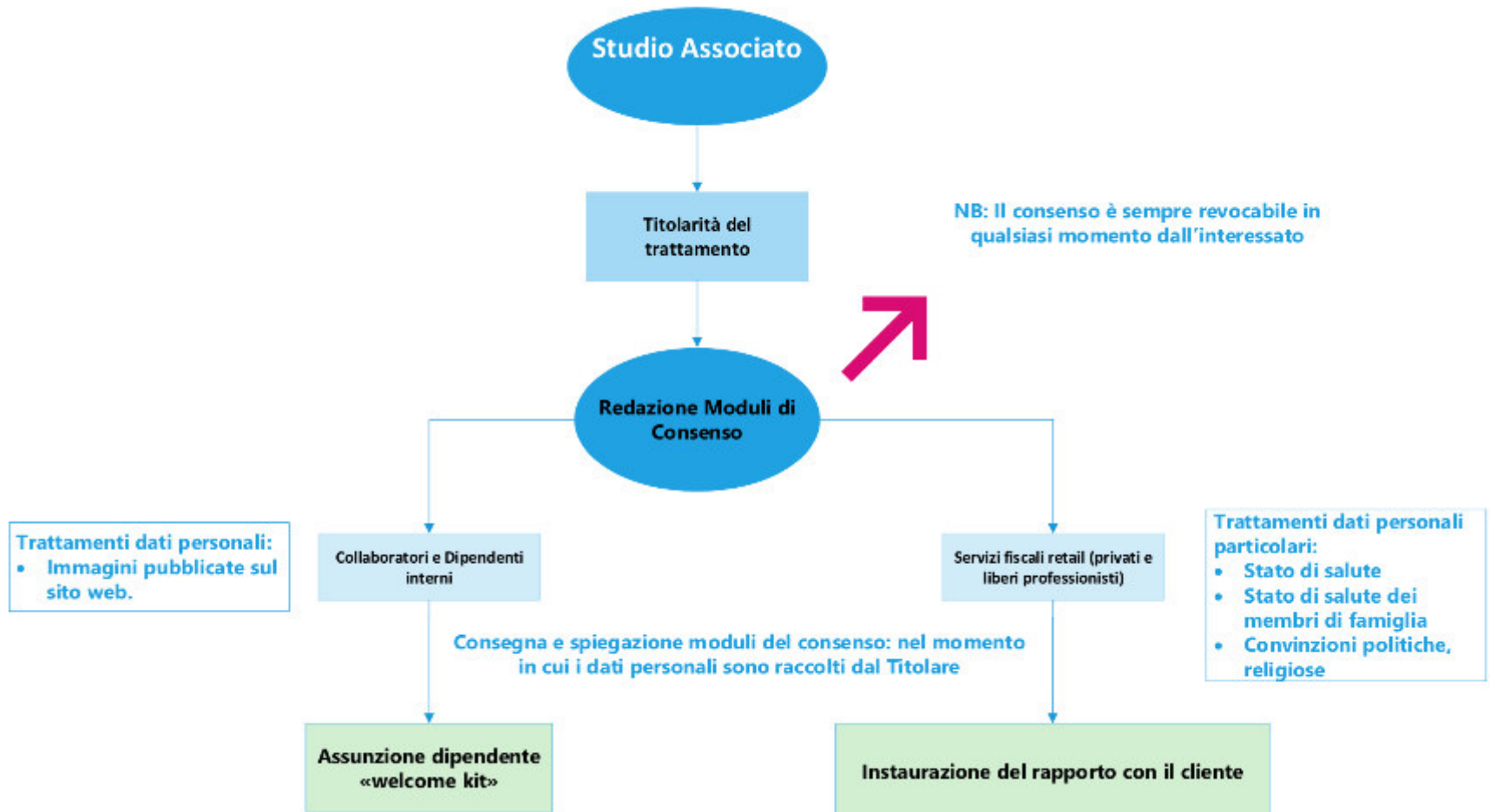
NB: il silenzio, l'inattività o la preselezione di caselle non equivale a consenso.

Adeguamento per un professionista o uno studio associato

Produzione documentale

Consensi e autorizzazioni al trattamento

Quando costituiscono basi giuridiche per lo Studio?



Adeguamento per un professionista o uno studio associato

Produzione documentale

Consensi e autorizzazioni al trattamento

Quando non sono necessari?

I trattamenti dei dati personali effettuati dallo Studio associato nell'ambito dell'attività di **adeguata verifica della clientela** si fondano sulle seguenti basi giuridiche:

- Dati personali identificativi del cliente: **obbligo di legge** - Legge n.92 del 17 Giugno 2008.
- Dati personali particolari (condizione di PEP): **motivo di interesse pubblico** (Art.8 Legge Rsm – Art.9 GDPR - lett.g).



Nota bene: Non è necessario chiedere il consenso al cliente per effettuare i trattamenti indicati.

Adeguamento per un professionista o uno studio associato

Produzione documentale

Consensi e autorizzazioni al trattamento

Quando non sono necessari?

I trattamenti dei dati personali effettuati dallo Studio associato di Avvocati nell'ambito di assistenza legale effettuata nei confronti di un cliente privato dietro sottoscrizione di apposito mandato professionale (es: **difesa in sede giudiziaria**) si fondano sulle seguenti basi giuridiche:

- Dati personali identificativi del cliente: **Obbligo contrattuale.**
- Dati personali particolari: **Trattamento necessario per accertare, esercitare o difendere un diritto in sede giudiziaria** (Art.8 Legge Rsm – Art.9 GDPR - lett.f).
- Dati giudiziari: **trattamento lecito solo sotto il controllo dell'autorità pubblica (Artt. 10 Legge Rsm – GDPR)**



Nota bene: Importante rispettare il principio di minimizzazione, ovvero trattare i dati personali strettamente necessari al raggiungimento delle finalità di trattamento.

Adeguamento per un professionista o uno studio associato

Produzione documentale

Consensi e autorizzazioni al trattamento

Quando non sono necessari?

I trattamenti dei dati personali effettuati dallo Studio associato nell'ambito dell'attività di **elaborazione dei cedolini paga dei propri dipendenti** si fondano sulle seguenti basi giuridiche:

- Dati personali identificativi del dipendente: **Obbligo contrattuale.**
- Dati economici del dipendente (stipendio, assegni, TFR): **Obbligo contrattuale.**
- Dati personali particolari (es: stato di salute): **Obblighi del datore di lavoro in materia di diritto del lavoro** (Art.8 Legge Rsm – Art.9 GDPR - lett.b).



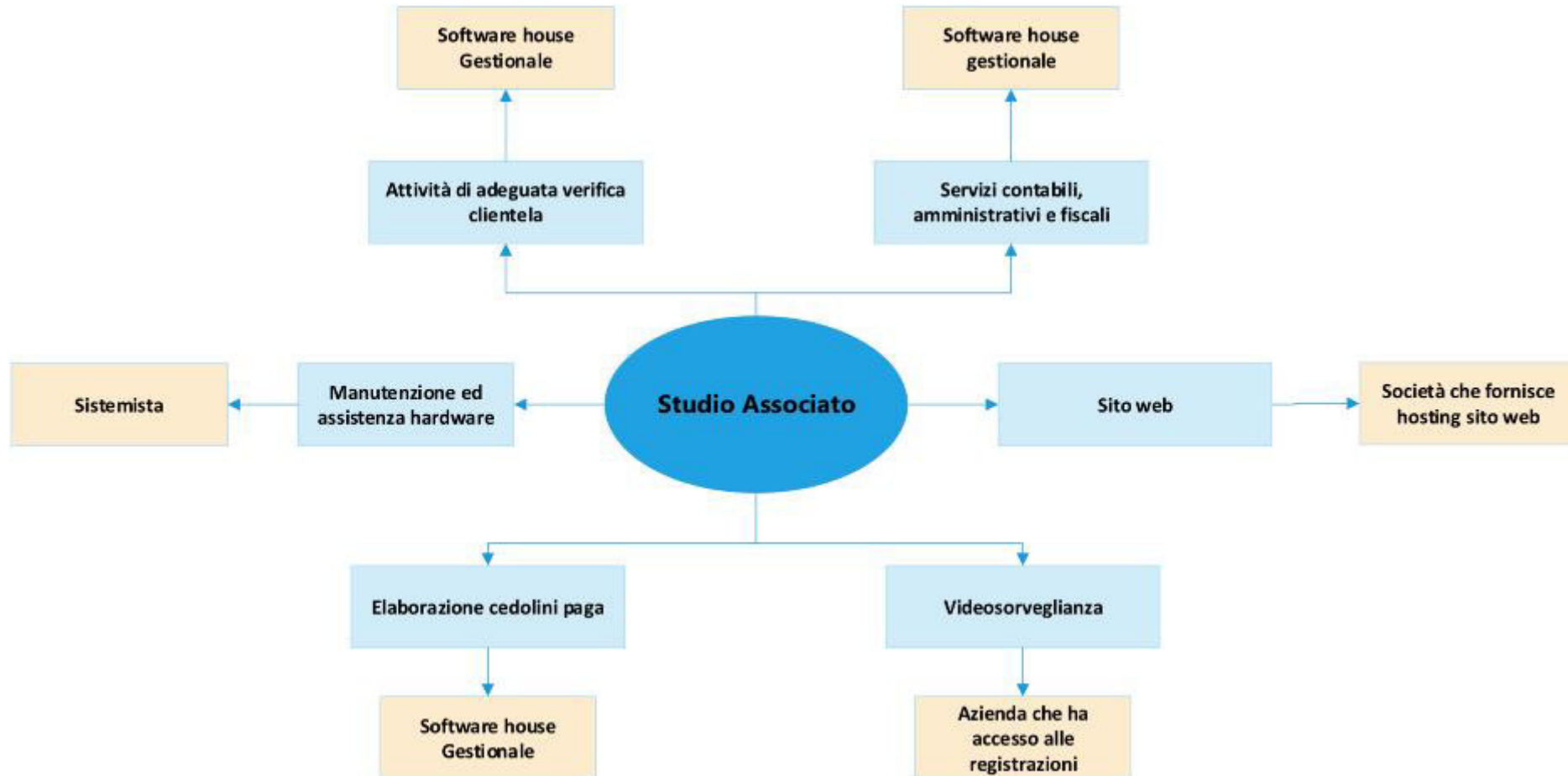
Nota bene: Non è necessario chiedere il consenso al dipendente per effettuare i trattamenti indicati.

Adeguamento per un professionista o uno studio associato

Produzione documentale

Atti di nomina dei responsabili del trattamento

Quali i soggetti da nominare?



Adeguamento per un professionista o uno studio associato

Produzione documentale

Atti di nomina dei responsabili del trattamento

Quando nominarli?

- «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». (art.28 GDPR – art.29 Legge RSM).
- Devono essere nominati solo i fornitori che sono in grado di garantire degli adeguati standard di sicurezza (Attenzione a software house e sistemisti)
- Devono essere nominati prima dell'affidamento dell'incarico.

Adeguamento per un professionista o uno studio associato

Produzione documentale

Atti di nomina dei responsabili del trattamento

Perché nominarli?

- GDPR (art.28) – Legge RSM (art.29) **Obbligo di un rapporto giuridico:** I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico che vincoli il responsabile del trattamento al titolare del trattamento.
- **E' utile associare l'atto di nomina (in forma scritta o in formato elettronico) al contratto commerciale in essere con il fornitore.**
- GDPR (art.29) – Legge RSM (art.30): Il responsabile del trattamento non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento.
- L'atto di nomina deve contenere specifiche istruzioni che il responsabile del trattamento deve rispettare nell'ambito dei trattamenti effettuati per conto del titolare.

Adeguamento per un professionista o uno studio associato

Produzione documentale

Atti di nomina dei responsabili del trattamento

Cosa fare quando lo Studio si qualifica responsabile?

Nei seguenti casi lo studio associato si qualifica responsabile del trattamento, poiché effettua trattamenti di dati per conto dei propri clienti corporate:

- **Servizi di tenuta della contabilità ordinaria e redazione del bilancio civilistico.**
- **Servizi fiscali, compilazioni dichiarazioni dei redditi (Modelli IGR-P, IGR-O, DAN e Allegati).**
- **Servizi di elaborazione dei cedolini paga dei clienti.**
- **Assistenza legale clienti corporate, contenziosi e verbali di assemblea**

Cosa fare in questi casi?

- ❑ **Nel momento della sottoscrizione del mandato professionale, allegare un **Data protection Agreement** (ovvero una proposta di nomina dello Studio quale responsabile del trattamento).**
- ❑ **Per i rapporti esistenti, inoltrare la proposta di nomina via e-mail.**

Adeguamento per un professionista o uno studio associato

Produzione documentale

Documenti per i propri dipendenti e collaboratori

Welcome kit

Nella fase di assunzione o in un secondo momento, i titolari di Studio devono consegnare la seguente documentazione ai propri dipendenti e/o collaboratori:

- **Informativa sul trattamento dei dati personali che li riguardano.**
- **Atti di autorizzazione al trattamento (cd: permissions) – art.29 GDPR, art.30 Legge RSM.**
- **Elenco degli asset informatici dati in dotazione per il corretto svolgimento delle mansioni lavorative (es: pc fisso, portatile, cellulare), nonché le credenziali di accesso al sistema informativo.**
- **Regolamento informatico interno sul corretto utilizzo degli strumenti informatici.**

Adeguamento per un professionista o uno studio associato

Produzione documentale

Documenti per i propri dipendenti e collaboratori

Welcome kit

Regolamento informatico o Piano di sicurezza informatico

chiunque agisca sotto l'autorità del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento (art.29 GDPR – art. 30 Legge RSM)

- Il regolamento informatico deve prevedere regole ed istruzioni per l'utilizzo corretto degli strumenti informatici utilizzati nell'ambito della normale attività lavorativa del dipendente. In particolare disciplina i seguenti ambiti:
 - Utilizzo del Personal Computer.
 - Gestione ed assegnazione delle credenziali di autenticazione.
 - Utilizzo della rete aziendale.
 - Utilizzo e conservazione dei supporti removibili (hard disk, chiavette USB).
 - Utilizzo di PC portatili.
 - Utilizzo della Posta Elettronica.
 - Corretta Navigazione su internet.
 - Utilizzo dei telefoni, fax e fotocopiatrici aziendali.

Adeguamento per un professionista o uno studio associato

Produzione documentale

Riassumendo

Quali sono i documenti da produrre?

- 1 – Registri delle attività di trattamento (Titolare e Responsabile)
- 2 – Organigramma privacy (Titolare e Responsabile)
- 3 – Accordo di contitolarità (solo per i casi in cui si è titolari del trattamento)
- 4 – Informative (solo nei casi in cui si è titolari del trattamento)
- 5 - Atti di nomina dei responsabili esterni del trattamento
- 6 – Data Protection Agreement (nel caso in cui si è responsabili)
- 7 – Welcome kit dipendente (informative, atti di autorizzazione, elenco asset informatici e regolamento informatico)

Adeguamento per un professionista o uno studio associato

Processi e procedure

- Adeguamento per un professionista o uno studio associato
 - **Processi e procedure**
 - Politica generale sulla protezione dei dati personali
 - Data Breach policy
 - Politica per i diritti degli interessati
 - Data Retention policy (politica sui tempi di conservazione)
 - Formazione dei soggetti autorizzati.
 - Applicazione delle misure tecniche di sicurezza

Adeguamento per un professionista o uno studio associato

Processi e procedure

Politica Generale sulla protezione dei dati personali

La politica generale sulla protezione dei dati personali descrive:

- I principi generali di sicurezza adottati dallo Studio.
- Le procedure o i processi che lo Studio ha adottato al fine di garantire riservatezza ai dati personali e alle informazioni trattate.
- Le azioni poste in essere dallo Studio al fine di adempiere agli obblighi di legge previsti dalla Normativa privacy (es: aggiornamento documentazione privacy – informative, consensi, DPA ecc...).
- Gli eventuali obiettivi in tema di protezione dei dati personali che lo Studio si pone di raggiungere per implementare il sistema di gestione dei dati personali.

Adeguamento per un professionista o uno studio associato

Processi e procedure

Data Breach Policy

Violazione dei dati personali

La violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati [Art. 4.12 e Considerando 85 GDPR]



Si possono classificare tre tipologie di violazioni di sicurezza (ISO/IEC 27000: parametri RID):

- **Confidenzialità o riservatezza:** accesso non autorizzato o diffusione del dato.
- **Integrità:** modifica ed alterazione del dato.
- **Disponibilità:** distruzione o perdita del dato.

Adeguamento per un professionista o uno studio associato

Processi e procedure

Data Breach Policy

Notifica alla Data Protection Authority

1. Il **Titolare del trattamento** deve **notificare** al Garante privacy i data breach solo qualora sia **probabile** che la violazione dei dati personali presenti un **rischio** per i diritti e le libertà degli individui (solo persone fisiche). E' onere del Titolare dimostrare al Garante privacy che il rischio per l'interessato non è probabile.
2. La notificazione del data breach al Garante privacy deve avvenire **senza ingiustificato ritardo e, ove possibile, entro 72 ore** dal momento in cui il Titolare ne è **venuto a conoscenza**. Le deroghe dovrebbero essere contenute e motivate.
 - **[Linee Guida WP Art. 29:** dopo esser stato informato di un possibile data breach o qualora esso stesso abbia identificato un incidente di sicurezza, il Titolare potrebbe aver bisogno di un breve periodo di tempo per verificare se l'incidente costituisce effettivamente un data breach. Durante tale periodo il Titolare non può essere considerato come “venuto a conoscenza” del data breach.
3. Il Responsabile deve informare il Titolare, **senza ingiustificato ritardo**, dopo essere venuto a conoscenza di un data breach.
 - **[Linee Guida WP Art. 29:** il Responsabile informa subito il Titolare; se autorizzato può notificare il data breach al Garante privacy ma la responsabilità rimane sempre in capo al Titolare].

Adeguamento per un professionista o uno studio associato

Processi e procedure

Data Breach Policy

Contenuto della Notifica

La notificazione al Garante Privacy deve **almeno descrivere**:

- la **natura** del Data Breach compreso, se possibile, le categorie e il numero approssimativo di interessati e di dati coinvolti;
- il **nome ed i riferimenti di contatto del DPO** o di altri punti di contatto;
- le probabili **conseguenze** del data breach;
- le **misure** adottate o proposte dal Titolare per gestire il data breach.

NB: Se non è possibile fornire tutte le informazioni nello stesso momento, possono essere fornite **in fasi successive**, senza ulteriore ingiustificato ritardo.

- [Linee Guida WP Art. 29: necessario avvisare il Garante privacy che ci saranno ulteriori notifiche; in situazioni eccezionali, nel caso si verifichino particolari e gravi violazioni, al fine di limitare i danni, si può informare prima gli interessati coinvolti e successivamente il Garante privacy].

Adeguamento per un professionista o uno studio associato

Processi e procedure

Data Breach Policy

Valutazione del rischio di un data breach

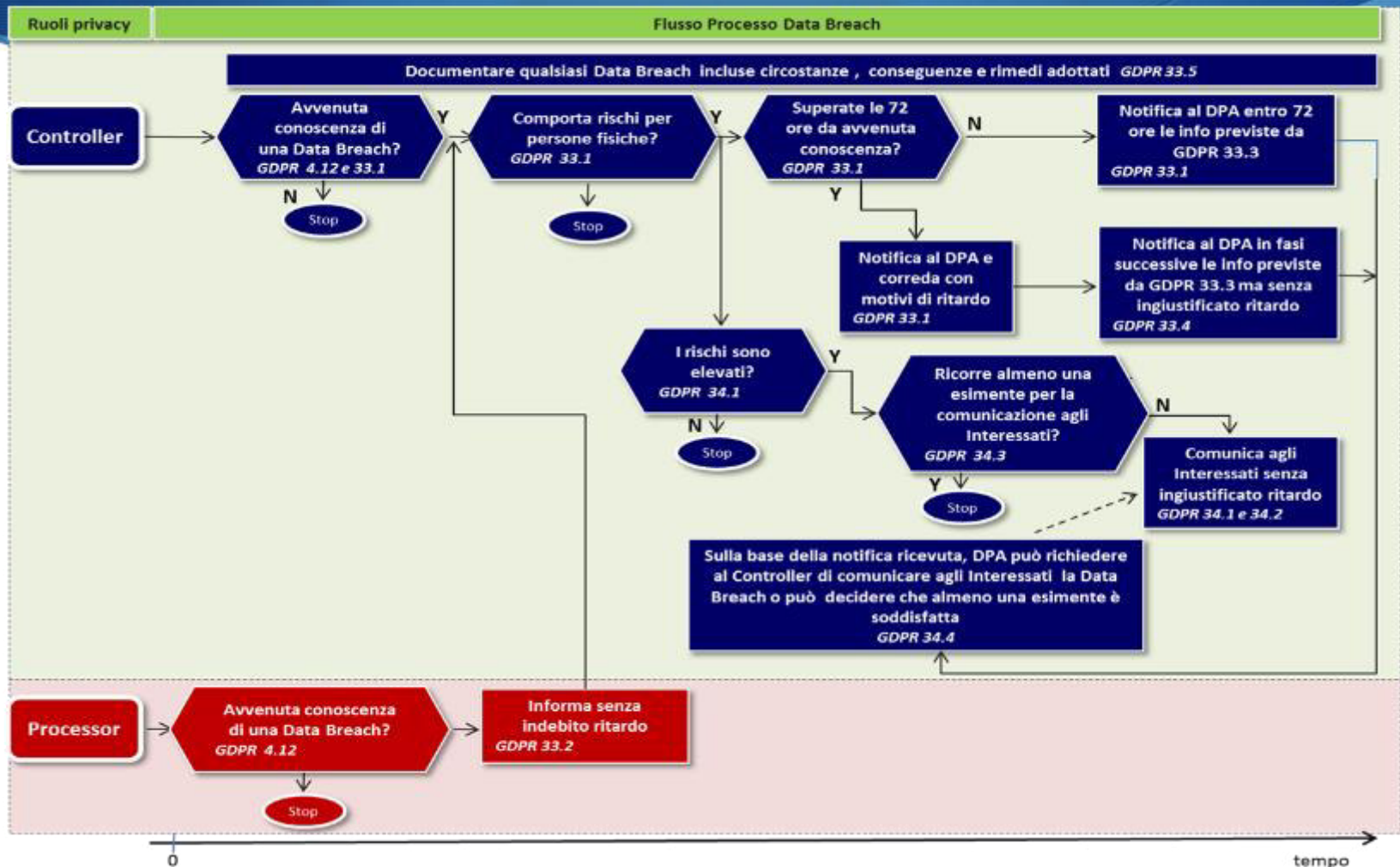
Il GDPR indica che **le violazioni che presentano rischi per gli individui** sono quelle che possono provocare danni fisici, materiali o immateriali, fornendone la seguente elencazione esemplificativa :

- perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti;
- discriminazione, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione;
- decifratura non autorizzata della pseudonimizzazione;
- **perdita di riservatezza dei dati personali protetti da segreto professionale.**
- qualsiasi altro danno economico o sociale significativo alla persona fisica interessata;
- in ogni caso il data breach che riguarda **particolari categorie di dati** (es. dati sensibili, dati genetici, dati giudiziari, dati di minori) o **particolari tipologie di trattamento** (valutazioni di aspetti personali/profilazione, archivi di notevoli dimensioni).

Adeguamento per un professionista o uno studio associato

Processi e procedure

Data Breach Policy



Adeguamento per un professionista o uno studio associato

Processi e procedure

Data Breach Policy

Perché è importante redigere una policy?

➤ **Obbligo di notifica:**

- Lo studio effettua quotidianamente trattamenti di dati personali che sono protetti da segreto professionale ed a fronte di una violazione di sicurezza è obbligato ad effettuare una notificazione all'Autorità garante.
- Inoltre, lo studio per i servizi alla clientela corporate si qualifica quale responsabile del trattamento, con obblighi di informare tempestivamente il cliente in caso di violazioni.

➤ **Obbligo di documentazione:**

- Il titolare deve **documentare qualsiasi violazione** (comprese le circostanze, effetti e azioni correttive adottate) indipendentemente dal fatto che la stessa sia oggetto di notifica al Garante privacy. Tale documentazione deve mettere in grado il Garante privacy di verificare la compliance.

Adeguamento per un professionista o uno studio associato

Processi e procedure

Data Breach Policy

Cosa deve disciplinare la policy?

Lo Studio deve definire ed implementare un processo di **gestione della violazione -Violazione Dati Personali**, che consenta:

- La rilevazione di situazioni di Violazione Dati Personali, anche avvenute nell'ambito dei trattamenti di dati personali affidati a Responsabili –Processor, esterni in modo tempestivo e puntuale.
- Di valutare se un evento di Violazione Dati Personali comporti rischi per i diritti e le libertà fondamentali degli Interessati al fine di attivare il relativo processo di gestione della violazione (notifica ecc..).
- Di esaminare se la gravità dell'evento o la tipologia dei dati violati connoti le caratteristiche di “**rischio elevato**” procedendo, in caso affermativo, a dare corso anche alla Comunicazione agli Interessati (per esempio il caso di una violazione che riguarda i dati sanitari dei dipendenti del cliente a cui si elaborano i cedolini paga).
- Di gestire l'evento di Violazione Dati Personali fino alla sua risoluzione, documentandolo (Registro delle violazioni di dati personali).
- Di apprendere da quanto emerso con l'evento di Violazione Dati Personali per migliorare i processi e le procedure individuando ed applicando le opportune soluzioni volte a mitigare i rischi di nuova occorrenza di simili casi.

DIRITTI DELL'INTERESSATO

Poteri di tipo cognitivo



Poteri di controllo



Poteri di tipo interdittivo



DIRITTI DELL'INTERESSATO

Poteri di tipo cognitivo



Diritto ad essere informato
(art. 12 -13)



Diritto di accesso (art. 15)

DIRITTI DELL'INTERESSATO

Poteri di controllo

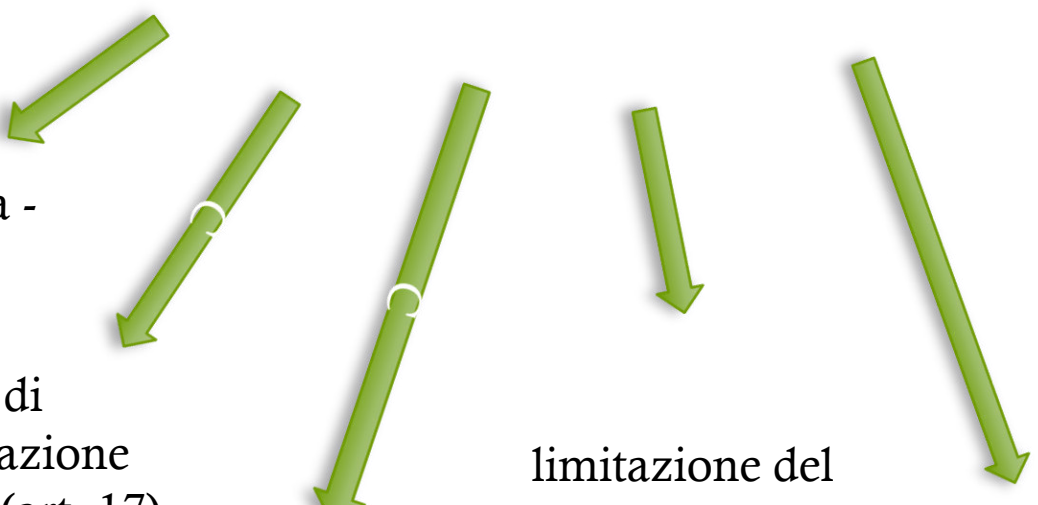


Diagram illustrating the flow of control powers (Poteri di controllo) from the main title 'DIRITTI DELL'INTERESSATO' to specific rights. The flow is indicated by green arrows pointing downwards and outwards from the central title area.

Diritto di rettifica -
integrazione
(art. 16)

Diritto di
cancellazione
(oblio) (art. 17)

Consenso e
revoca del
consenso
(art. 6)

limitazione del
trattamento
(art. 18)

Diritto alla
portabilità dei
dati (art. 20)

DIRITTI DELL'INTERESSATO

Poteri di tipo interdittivo



Diritto di opposizione (artt. 21)

Diritto ad essere informato (art. 12)

Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni in forma **concisa, trasparente, intelligibile e facilmente accessibile**, con un **linguaggio semplice e chiaro**

QUALI INFORMAZIONI



Informazioni ex artt. 13, 14, 15-22, 34

Diritto ad essere informato (art. 12)

- Le informazioni sono fornite per iscritto, o con altri mezzi, anche, se del caso, con mezzi elettronici
- Informazioni ex artt. 13 e 14, fornite in combinazione con icone standardizzate.
- Se presentate elettronicamente devono essere leggibili da un dispositivo automatico

Informazioni da esibire all'interessato in caso di raccolta presso il medesimo (art. 13)

- identità e dati di contatto del titolare e, ove applicabile, del Rappresentante
- dati di contatto del **responsabile** della protezione dei dati, ove applicabile
- **finalità** del trattamento cui sono destinati i dati
- **base giuridica** del trattamento
- **legittimi interessi** del titolare, ove siano la base di legittimità del trattamento
- intenzione di **trasferire** i dati in un paese terzo, esistenza di una decisione di adeguatezza, etc.
- **destinatari** o categorie di destinatari dei dati
- periodo di **conservazione** dei dati o criteri utilizzabili per determinarlo
- esistenza ed indicazione dei **diritti** dell'interessato
- esistenza del diritto di **revoca** del consenso ove previsto
- esistenza del diritto di proporre **reclamo** all'Autorità di controllo
- **obbligo** legale o contrattuale e **conseguenze** del diniego della comunicazione
- esistenza di un **processo decisionale automatizzato**, logica applicata, conseguenze per l'interessato

Termini di esibizione e deroghe all'obbligo informativo di cui all'art. 13

QUANDO



Le informazioni sono fornite nel momento in cui i dati personali sono ottenuti dall'interessato (art. 13, c. 1)

QUINDI



Termini di esibizione e deroghe all'obbligo informativo di cui all'art. 13

AL MOMENTO DELL'AVVIO DEL TRATTAMENTO



Termini di esibizione e deroghe all'obbligo informativo di cui all'art. 13

L'OBBLIGO DI INFORMAZIONI SI APPLICA SEMPRE



Termini di esibizione e deroghe all'obbligo informativo di cui all'art. 13



L'obbligo informativo non si applica se e
nella misura in cui l'interessato dispone già
delle informazioni (art. 13, c. 4)

Dati raccolti presso terzi

Art. 14

Cosa cambia nel caso
della raccolta presso terzi ?



Dati raccolti presso terzi

Art. 14

cambia il momento di esibizione della
informativa

cambia il contenuto dell'obbligo informativo in
favore dell'interessato

vi sono deroghe all'obbligo

Dati raccolti presso terzi

Art. 14

QUANDO FORNISCO LE INFORMAZIONI ?

- a) entro un termine ragionevole dall'ottenimento dei dati personali, ma al più tardi entro un mese, in considerazione delle specifiche circostanze in cui i dati personali sono trattati;
- b) nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, al più tardi al momento della prima comunicazione all'interessato;
- c) nel caso sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati personali.

Dati raccolti presso terzi

Art. 14

Informazioni aggiuntive da esibire all'interessato in caso di raccolta presso terzi

- categorie dei dati trattati
 - fonte da cui hanno origine i dati personali
- (indicare se provengono da fonti accessibili al pubblico)

Dati raccolti presso terzi

Art. 14

Deroghe all'obbligo informativo (art. 14, c. 5)

- a) l'interessato disponga già delle informazioni;
- b) comunicare tali informazioni risulti impossibile o implicherebbe uno sforzo sproporzionato;
- a) qualora i dati personali debbano rimanere riservati conformemente a un obbligo di segreto professionale, compreso un obbligo di segretezza previsto per legge.

(Diritto di accesso dell'interessato)

Art. 15

STRUTTURA DEL DIRITTO

CONFERMA

ACCESSO AI
DATI

ACCESSO ALLE
INFORMAZIONI

COPIA

(Diritto di accesso dell'interessato)

Art. 15

L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, di ottenere l'accesso ai dati personali.



(Diritto di accesso dell'interessato)

Art. 15

e alle seguenti informazioni:

- a) le finalità del trattamento;
- b) le categorie di dati personali in questione;
- c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di Paesi esteri o organizzazioni internazionali;
- d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;

(Diritto di accesso dell'interessato)

art. 15

- f) il diritto di proporre segnalazione o reclamo al Garante per la protezione dei dati personali;
- g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
- h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, commi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

(Diritto di accesso dell'interessato)

Art. 15



DA NON CONFONDERE CON
Accesso agli atti ex L. 160/2011
s.m.i (D.L. 89/2016)
Regolamento 16/2015 accesso
civico)

(Diritto di accesso dell'interessato)

Art. 15

Art.91

(Accesso a documenti amministrativi)

I presupposti, le modalità, i limiti per l'esercizio del diritto di accesso a documenti amministrativi contenenti dati personali, e la relativa tutela giurisdizionale, restano disciplinati dalla Legge 5 ottobre 2011 n.160 e successive modificazioni, anche per ciò che concerne le categorie particolari di dati personali e dei dati personali relativi a condanne penali e reati, nonché le operazioni di trattamento eseguibili in esecuzione di una richiesta di accesso.

(Diritto di accesso dell'interessato)

Art. 15

Rispetto all'accesso agli atti amministrativo:

- È un'istanza semplice!
- la richiesta non prevede formalità particolari. (l'informativa può specificare un modo più agevole per l'esercizio del diritto ma non imporre forme)
- Non ci sono particolari ragioni che l'interessato deve esplicitare

(Diritto di accesso dell'interessato)

Art. 15

CONFERMA

- Su questo aspetto occorre richiamare l'art. 12, c. 1, il quale fissa l'obbligo per il Titolare di adottare **delle misure appropriate [procedure]** per fornire all'interessato le comunicazioni di cui, fra le altre, all'art. 15
- Se il Titolare del trattamento può dimostrare che non è in grado di identificare l'interessato può rifiutare di soddisfare la richiesta dell'interessato **[occorre pertanto anche qui una procedura formalizzata che consenta di fornire la dimostrazione ...]**
- il Titolare può richiedere ulteriori informazioni all'istante se nutre **ragionevoli dubbi** circa la sua identità

(Diritto di accesso dell'interessato)

Art. 15

- Riscontro entro un mese dal ricevimento della richiesta (art. 12 c. 3)
- Termine prorogabile fino a due mesi tenuto conto della complessità e del numero delle richieste (art. 12 c. 3)
- Gratuità (art. 12 c. 5)

(Diritto di accesso dell'interessato)

Art. 15

**SE NEI DATI OGGETTO DELL'ESERCIZIO DEL DIRITTO DI
ACCESSO SONO CONTESTUALI A DATI DI SOGGETTI
TERZI???????**



(Diritto di accesso dell'interessato)

Art. 15

VANNO ESCLUSI !!



(Diritto di accesso dell'interessato)

Art. 15

Il diritto di ottenere una copia deve ledere i diritti e le libertà altrui.



Balance test

(Diritto di accesso dell'interessato)

Art. 15

Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento.



GRATIS

(Diritto di accesso dell'interessato)

Art. 15

In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi.



(Diritto di accesso dell'interessato)

Art. 15

ACCESSO AI DATI

Provvedimento del Garante 23 dicembre 2004, 1121729

Quando chiede di accedere ai dati personali che lo riguardano, l'interessato non è tenuto ad indicare specificamente in quali atti o documenti essi sono contenuti: chi gestisce la banca dati deve comunicare tutte le informazioni in suo possesso.

(Diritto di accesso dell'interessato)

Art. 15

Qualora i dati personali siano trasferiti a un Paese estero o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate relative al trasferimento.

Art. 47 L 171/2018



(Diritto di accesso dell'interessato)

Art. 15

Se l'interessato presenta la richiesta mediante mezzi elettronici, e **salvo indicazione diversa dell'interessato**, le informazioni sono fornite in un formato elettronico di uso comune.



(Diritto di accesso dell'interessato)

Art. 15

Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici *se l'interessato presenta la richiesta mediante mezzi elettronici, le informazioni sono fornite, ove possibile, con mezzi elettronici, salvo diversa indicazione dell'interessato (art. 12, c. 3)*

Articolo 12 L 171/2018

≠

Articolo 12 GDPR

le informazioni non possono essere fornite oralmente

Consenso

Art. 6

DIRITTO AL CONSENSO

O MEGLIO....

DIRITTO DI REVOCA DEL CONSENSO



Consenso

Art. 6

L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento.

La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò.

Il consenso è revocato con la stessa facilità con cui è accordato.

Consenso

Art. 6

La revoca del consenso **potrebbe trovare un limite** nell'esistenza di un **legittimo interesse** da parte del titolare. (Considerando 47)

In tal caso sarà necessario operare un bilanciamento tra gli interessi in gioco



Diritto di Cancellazione (oblio)

Art. 17

OBLIO



Diritto di essere dimenticato o comunque non essere ricordato per fatti passati. Purchè l'informazione abbia perso la caratteristica dell'attualità e di fatto abbia perso l'accezione di fatto di cronaca

Diritto di Cancellazione (oblio)

Art. 17

Di fatto può essere richiesto:

- Per notizie vere ma no più rilevanti
- Per notizie vere ma non aggiornata
- Per notizie false ma non cancellate

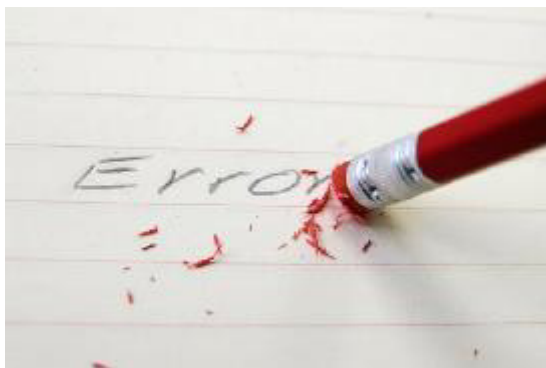
Esiste uno «scontro» tra il diritto all'oblio e il diritto di cronaca

Verità oggettiva, interesse della collettività a conoscere la notizia, utilità sociale dell'informazione

Diritto di Cancellazione (oblio)

Art. 17

l'interessato ha diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali se sussiste uno dei motivi previsti



Diritto di Cancellazione (oblio)

Art. 17

MOTIVI DELLA CANCELLAZIONE

- I dati personali non sono più necessari rispetto alle finalità per cui sono stati raccolti o altrimenti trattati;
- Revoca del consenso o opposizione al trattamento da parte dell'interessato;
- I dati personali sono trattati illecitamente;
- I dati personali devono essere cancellati per adempiere ad un obbligo legale posto a carico del titolare;
- I dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione a minori

Diritto di Cancellazione (oblio)

Art. 17

OBBLIGHI DEL TITOLARE



Il titolare che abbia **reso pubblici dati personali** è tenuto a cancellarli adottando misure ragionevoli, anche tecniche, per **informare i titolari del trattamento che stanno trattando dati personali della richiesta dell'interessato di cancellare** qualsiasi *link*, copia o riproduzione dei suoi dati personali

Diritto di Cancellazione (oblio)

Art. 17

COME FARE A TENERE
SOTTO CONTROLLO IL FLUSSO DI DATI



Diritto di Cancellazione (oblio)

Art. 17

ORGANIZZAZIONE DEI PROCESSI



Diritto di Cancellazione (oblio)

Art. 17

!!ATTENZIONE!!
IL DIRITTO ALL'OBLIO HA DELLE LIMITAZIONI



Diritto di Cancellazione (oblio)

Art. 17

Se il trattamento è necessario:

- per l'esercizio del diritto alla libertà di espressione e di informazione;
- per l'adempimento di un obbligo legale o di un compito di pubblico interesse del titolare;
- per motivi di interesse pubblico nel settore della sanità pubblica;
- ai fini di archiviazione nel pubblico interesse, ricerca scientifica o storica o a fini statistici;
- per l'accertamento, l'esercizio o la difesa di un diritto in sede Giudiziaria;

(Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento)

Art. 19

Il titolare del trattamento **comunica a ciascuno dei destinatari** cui sono stati trasmessi i dati personali **le eventuali rettifiche o cancellazioni o limitazioni del trattamento effettuate,**
salvo

che ciò si riveli **impossibile** o implichi uno **sforzo sproporzionato**.

Il titolare del trattamento comunica all'interessato chi siano tali destinatari qualora l'interessato lo richieda.



(Diritto di limitazione di trattamento)

Art.18

L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento quando ricorre una delle seguenti ipotesi:



(Diritto di limitazione di trattamento)

Art.18

- a)** l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali;
- b)** il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;
- c)** benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
- d)** l'interessato si è opposto al trattamento ai sensi dell'articolo 21, comma 1, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

(Diritto di limitazione di trattamento)

Art.18

COSA DEVO FARE?

CHIAMARE IL TECNICO DEL PC



(Diritto di limitazione di trattamento)

Art.18

La limitazione consiste in un «**contrassegno**»
ovvero un vincolo tecnico

**NON SI APPLICA AI DOCUMENTI
CARTACEI**

(Diritto di limitazione di trattamento)

Art.18

Se il diritto viene esercitato il titolare può solo:

- Conservare i dati;
- Trattarli per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria, oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante.

(Diritto di limitazione di trattamento)

Art.18



L'interessato che ha ottenuto la limitazione del trattamento **è informato dal titolare del trattamento prima che detta limitazione sia revocata.**

Diritto alla Portabilità dei dati

Art. 20

L'interessato ha il diritto di ricevere in un **formato strutturato**, di **uso comune e leggibile** da dispositivo automatico, i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto **di trasmettere tali dati a un altro titolare** del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti, qualora:

- a) il trattamento si basi sul consenso o su un contratto; **e**
- b) il trattamento sia effettuato con mezzi automatizzati.

Diritto alla Portabilità dei dati

Art. 20

l'interessato ha il diritto di ottenere **la trasmissione diretta** dei dati personali da un titolare del trattamento all'altro, **se tecnicamente fattibile**.

Diritto alla Portabilità dei dati

Art. 20

CONSIDERANDO 68

I formati utilizzati per la portabilità o la trasmissione devono garantire un'interoperabilità

Indicazione dei Garanti Europei alle categorie quali i formati e gli standard comuni da utilizzare

Diritto alla Portabilità dei dati

Art. 20

L'esercizio del diritto **lascia impregiudicato l'articolo 17 (oblio)**. Ivi
compreso la limitazione di tale diritto.

Richiesta al titolare di non cancellare i dati

Tale diritto non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

inoltre

Il diritto di cui al comma 1 non deve ledere i diritti e le libertà altrui.

Diritto alla Portabilità dei dati

Art. 20

Il titolare deve assicurarsi che la trasmissione dei dati sia sicura!



(Diritto di opposizione)

Art.21

L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano.

È una manifestazione di volontà recettizia che si esercita solo verso il titolare



(Diritto di opposizione)

Art.21

Se il diritto viene esercitato

**Il titolare del trattamento si astiene dal trattare
ulteriormente i dati personali**

Salvo

che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

(Diritto di opposizione)

Art.21

Si esercita solo nei casi di cui all'articolo 5 comma 1 lett. e) f)

ovvero

e) il trattamento è necessario per l'esecuzione di un compito di **interesse pubblico** o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

f) il trattamento è necessario per il perseguimento del **legittimo interesse** del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore. Tale disposizione non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti.

(Diritto di opposizione)

Art.21

!!ATTENZIONE!!

REVOCA CONSENSO

≠

OPPOSIZIONE

(Diritto di opposizione)

Art.21

REVOCA CONSENSO (dipicamente privato)

Si esercita solo verso i privati e quando la base è il consenso

OPPOSIZIONE

Si esercita sia verso il pubblico sia verso il privato

(Diritti riguardanti le persone decedute) Art.25



(Diritti riguardanti le persone decedute) Art.25

I diritti di cui agli articoli da 15 a 22 riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un **interesse proprio**, o **agisce a tutela dell'interessato**, in qualità di suo erede o mandatario, o per ragioni familiari meritevoli di protezione.

(Diritti riguardanti le persone decedute) Art.25

L'esercizio dei diritti **non è ammesso**

- nei casi previsti dalla legge;
- l'interessato lo ha **espressamente vietato** con dichiarazione scritta presentata al titolare del trattamento.

(Diritti riguardanti le persone decedute) Art.25

La volontà dell'interessato di vietare l'esercizio dei diritti deve essere **specificata**, **libera** e **informata**;

L'interessato ha in ogni momento il diritto di revocare o modificare il divieto.



(Diritti riguardanti le persone decedute) Art.25

TRANNE CHE NEL MOMENTO

Come direbbe Foscolo
«della fatal quiete»



(Diritti riguardanti le persone decedute) Art.25

In ogni caso, il divieto non può produrre effetti pregiudizievoli per l'esercizio da parte dei terzi dei diritti patrimoniali che derivano dalla morte dell'interessato, nonché del diritto di difendere in giudizio i propri interessi.

Adeguamento per un professionista o uno studio associato

Processi e procedure

Politica per i diritti dell'interessato

Perché è importante redigere una policy?

➤ **Obbligo di rispondere alle richieste:**

- Gli interessati coinvolti nei trattamenti effettuati dallo Studio in qualità di Titolare del trattamento (es: i propri dipendenti, i fornitori o clienti) possono in qualsiasi momento esercitare uno dei diritti previsti dalla legge.
- Lo Studio deve valutare se la richiesta è manifestamente infondata o ripetuta nel tempo. L'onere della prova è sempre in capo allo Studio.
- In caso affermativo, può rifiutarsi di rispondere alle richieste, motivando sempre la decisione.
- In caso negativo, deve rispondere alle richieste entro 1 mese dal ricevimento (termine prorogabile a 3 mesi). Il titolare può decidere di addebitare un contributo spese che tiene conto dei costi amministrativi sostenuti se le richieste hanno carattere ripetitivo.

➤ **Obbligo di documentazione:**

- Il titolare deve **documentare qualsiasi richiesta avanzata dal Titolare**. Nel rispetto del principio di responsabilizzazione (accountability) il Titolare deve essere in grado di dimostrare il rispetto delle disposizioni contenuti nella Normativa privacy.

Adeguamento per un professionista o uno studio associato

Processi e procedure

Politica per i diritti dell'interessato

Cosa deve disciplinare la policy?

Lo Studio deve definire ed implementare un processo di **gestione della richieste di esercizio dei diritti da parte degli interessati**, che consenta di :

- Raccogliere le richieste degli interessati: definizione di un punto di contatto.
- Analizzare le richieste degli interessati in relazione al diritto in questione, valutandone la manifesta infondatezza o il carattere ripetitivo.
- Evadere le richieste nei termini temporali corretti.
- Documentare il processo in apposito Registro.

Data Retention Policy

Perché è importante redigere una politica sui tempi di conservazione?

- **Obbligo di legge:** tra le novità introdotte dal GDPR vi è quella della definizione dei **tempi di conservazione** dei dati personali o dei **criteri utilizzati per determinarli** (Artt. 13-14 GDPR e Legge RSM). La determinazione dei tempi di conservazione viene effettuata tenendo conto di:
 - normative nazionali ed internazionali;
 - pronunce da parte dell'Autorità di controllo;
 - contributi della dottrina.

Adeguamento per un professionista o uno studio associato

Processi e procedure

Data Retention Policy

Tipologia di dato personale	Finalità del trattamento	Tempo di conservazione	Riferimento normativo
Dati personali identificativi, nonché dati di tipo economico (stipendi, tfr, ecc..)	Gestione dei dipendenti interni	10 anni	Art. 11 Legge n. 102/2015 – Prescrizione dei diritti di credito.
Dati personali particolari (stato di salute)	Gestione dei dipendenti interni	Alla conclusione del rapporto di lavoro	Esaurimento delle finalità (principio di minimizzazione) – Art. 5 GDPR
Credenziali di accesso al sistema informativo (nome utente e password)	Gestione dei dipendenti interni	Alla conclusione del rapporto di lavoro (disattivazione dell'utente)	Esaurimento delle finalità (principio di minimizzazione) – Art. 5 GDPR.
Dati contabili, fiscali con riferimento ai propri clienti	Servizi Clientela	5 anni (escluso il periodo d'imposta cui si riferiscono)	Art.100 Legge n.166/2013 – Obbligo di conservazione dei documenti fiscali
Dati giudiziari e dati raccolti in assolvimento degli obblighi di adeguata verifica della clientela	Adeguate verifica clientela	5 anni dalla conclusione del rapporto	Legge n.92/2008

Adeguamento per un professionista o uno studio associato

Processi e procedure

Riassumendo

Quali sono i processi e le procedure da adottare?	
1 – Politica generale sulla protezione dei dati personali	Riepilogo dell'intero adeguamento privacy
2 – Data Breach Policy (divulgazione e spiegazione al personale dipendente)	Politica in caso di violazione di dati personali: • Illustrazione ai dipendenti (formazione)
3 – Politica per i diritti degli interessati	Illustrazione ai dipendenti (formazione)
4 – Data retention Policy (tempi di conservazione e cancellazione dei dati)	Illustrazioni ai dipendenti (formazione)

Adeguamento per un professionista o uno studio associato

Processi e procedure

Applicazione misure di sicurezza fisiche

In caso di database o archivi cartacei quali presidi adottare?

- Limitare l'accesso all'ufficio.
- Utilizzare armadiature con serrature e gestire le chiavi di accesso.
- Non archiviare fascicoli o documenti contenenti dati personale in locali dello studio accessibili a tutti.
- Installare gli allarmi nei locali dello studio.

Adeguamento per un professionista o uno studio associato

Processi e procedure

Applicazione misure di sicurezza informatiche

SICUREZZA ONLINE

Le 5 minacce più frequenti

1 Malware

è un software (un programma) creato appositamente per entrare in o danneggiare un computer senza che il proprietario lo sappia.

Le famiglie di malware più frequenti per tipo:



92% delle infezioni da malware rilevate arriva tramite email compromesse

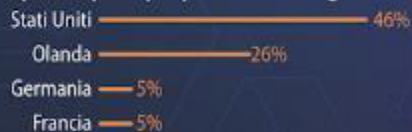


Obiettivo più ricorrente i dispositivi IoT (Internet delle Cose da Internet of Things)

2 Attacchi sul web

Tutte le tecniche disponibili riguardano il reindirizzamento dei browser a siti web nocivi

I primi 4 paesi per provenienza degli attacchi:



Sono in aumento gli incidenti legati ai Content Management Systems (CMS)

3 Attacchi da applicazioni/iniezioni web

Passare ai server o alle app per cellulari vulnerabili degli input nocivi con l'obiettivo di iniettare codice maligno



51% - Le iniezioni ai database SQL sono gli attacchi più frequenti



Spesso sono collegati a ingenti violazioni mondiali di dati

4 Phishing

Tentativo di rubare/intercettare username, password e credenziali bancarie usando email false e siti web contraffatti

Responsabile di più del:



90% infezioni da malware
72% violazioni dei dati nelle organizzazioni



Gli attacchi di phishing sui dispositivi mobili sono cresciuti con una media annuale dell'**85%** dal 2011

5 DDoS

Negazione di servizio distribuita: ha come obiettivo le aziende e le organizzazioni e rende i sistemi o i network inaccessibili agli utilizzatori



59% degli attacchi avviene in Cina



55% degli attacchi dura meno di 90 minuti

Adeguamento per un professionista o uno studio associato

Processi e procedure

Applicazione misure di sicurezza informatiche

Sicurezza del trattamento

Tenendo conto dello **stato dell'arte** e dei **costi** di attuazione, nonché della **natura**, dell'**oggetto**, del **contesto** e delle **finalità** del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento **mettono in atto misure tecniche e organizzative adeguate** per garantire un **livello di sicurezza adeguato al rischio**, che comprendono, tra le altre, se del caso:

- a) la **pseudonimizzazione** e la **cifratura** dei dati personali;
- b) la capacità di assicurare su base permanente la **riservatezza**, l'**integrità**, la **disponibilità** e la **resilienza** dei sistemi e dei servizi di trattamento;
- c) la capacità di **ripristinare tempestivamente** la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- d) una procedura per testare, **verificare e valutare regolarmente l'efficacia delle misure** tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei **rischi presentati dal trattamento che derivano** in particolare dalla **distruzione**, dalla **perdita**, dalla **modifica**, dalla **divulgazione non autorizzata** o dall'**accesso**, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

Applicazione misure di sicurezza informatiche

Stratificazione delle misure di sicurezza

Prevenzione

- ha l'obiettivo di impedire che una minaccia si concretizzi, controllando i punti di vulnerabilità del sistema e proteggendolo dagli attacchi.

Rilevazione

- è finalizzata a rilevare, in seguito ad un incidente, le conseguenze dannose e ad accertare eventuali responsabilità.

Ripristino

- consente di minimizzare i danni con la riattivazione tempestiva del sistema e delle sue funzionalità, senza perdita di dati.

Adeguamento per un professionista o uno studio associato

Processi e procedure

Applicazione misure di sicurezza informatiche

Misure di prevenzione

Misura di sicurezza

Procedura di autenticazione

- Qualcosa che l'utente sa: PIN segreti, password, ecc.
 - Qualcosa che l'utente possiede: smart card.
 - Qualcosa che l'utente è: biometria.
- Spesso si usa la combinazione di credenziali di più tipo per avere un'**autenticazione forte**.

Profili di autorizzazione

- stabiliscono cosa un utente autenticato dal sistema può fare sul sistema stesso.
- Per ogni utente (o gruppo di utenti) definiscono le regole di accesso ai dati (lettura, creazione, modifica, cancellazione) e le regole di accesso ai servizi.

Pseudonimizzazione

La pseudonimizzazione consiste nel sostituire un attributo (solitamente un attributo univoco) di un dato con un altro. Il risultato della pseudonimizzazione può essere un valore del tutto indipendente dal valore originale

Cifratura

opera una trasformazione sui dati, applicando algoritmi con chiavi segrete che garantiscono:

- Riservatezza del dato
- Integrità del dato
- Autenticazione del dato.

Adeguamento per un professionista o uno studio associato

Processi e procedure

Applicazione misure di sicurezza informatiche

Misure di prevenzione

Misura di sicurezza

Firewall, Antivirus e aggiornamenti periodici.

- filtra il passaggio dei dati tra i computer della rete locale e la rete esterna
- blocca le intrusioni, alcuni virus, spyware.

VPN (Virtual Private Network)

- Con la VPN si creano tunnel cifrati per lo scambio sicuro di informazioni sfruttando la rete Interne.

Cancellazione sicura dei dati

- La cancellazione sicura di informazioni si ottiene con:
- programmi informatici (*wiping*) che riscrivono ripetutamente sequenze casuali di 0 e 1 sopra allo spazio liberato (es. Eraser, WipeDisk, Permanet Eraser, DBAN ecc.).
 - formattazione (inizializzazione) a basso livello del supporto di memorizzazione
 - demagnetizzazione (degaussing) dei dispositivi magnetici
 - distruzione dei supporti (punzonatura, deformazione meccanica, ecc.).

Adeguamento per un professionista o uno studio associato

Processi e procedure

Applicazione misure di sicurezza informatiche

Misure di prevenzione

Misura di sicurezza	Applicabilità allo Studio Associato
Procedura di autenticazione	lato client e applicativi (creare una politica sulle credenziali di accesso al sistema)
Profili di autorizzazione	Applicazione nel rispetto delle mansioni e competenze dei dipendenti di Studio.
Pseudonimizzazione	Applicazione limitata – riduce operatività quotidiana
Cifratura	Applicazione solo per i dispositivi elettronici che escono dal perimetro di Studio (pc portatili, smartphone, chiavette USB e hard disk)
Firewall, Antivirus e aggiornamenti periodici.	Applicazione a tutto il sistema informativo
VPN (Virtual Private Network)	Applicazione in particolare nel caso in cui ci si debba connettere al sistema informativo da reti esterne.
Cancellazione sicura dei dati	Applicazione nel rispetto della Data Retention Policy

Adeguamento per un professionista o uno studio associato

Processi e procedure

Applicazione misure di sicurezza informatiche

Misure di rilevazione

Misure di sicurezza

Software che registra i log

file in cui si registrano tutte le operazioni che sono state eseguite sul sistema informatico.

Intrusion Detection System

E' un particolare strumento per monitorare gli accessi abusivi al sistema

➤ Sono registrati gli accessi in autenticazione (compresi i tentativi falliti o rifiutati), gli accessi a determinate aree di sistema o dati considerate critiche, l'esecuzione di determinati programmi o processi, l'installazione o la rimozione di *software*, le modifiche ai *file* di configurazione

Adeguamento per un professionista o uno studio associato

Processi e procedure

Applicazione misure di sicurezza informatiche

Misure di rilevazione

Misure di sicurezza	Applicabilità allo Studio Associato
Software che registra i log	Applicazione a tutte le banche dati di Studio. E' molto importante per controllare accessi non autorizzati in caso di data breach.
Intrusion Detection System	Applicazione al sistema informativo di Studio. Normalmente è un servizio che i Firewall di ultima generazione prevedono.

Adeguamento per un professionista o uno studio associato

Processi e procedure

Applicazione misure di sicurezza informatiche

Misure di ripristino

Misure di sicurezza

Politiche di back-up

- Per limitare la perdita di informazioni è indispensabile il salvataggio dei dati.
- Il *backup* si differenzia per la modalità (completo, differenziale o incrementale) e per la *retention* (ovvero il tempo per cui la copia dei dati viene conservata prima di essere sovrascritta).
- Dove conservare i backup: cassaforte ignifuga, dispositivi remoti

Continuità operativa e Disaster recovery

- affidabilità della rete
- architetture distribuite
- ripristino rapido

Adeguamento per un professionista o uno studio associato

Processi e procedure

Applicazione misure di sicurezza informatiche

Misure di ripristino

Misure di sicurezza	Applicabilità allo Studio
Politiche di back-up	Applicazione domestica o automatizzata diversificata in relazione all'utilizzo e alla conservazione delle banche dati.
Continuità operativa e Disaster recovery	Applicazione a tutto il sistema informativo

Empowerment dell'utente

- Le soluzioni tecnologiche non riescono da sole a garantire la sicurezza dei sistemi, ma deve essere posta attenzione all'adozione di procedure organizzative volte alla formazione, all'aggiornamento e alla sensibilizzazione, per promuovere quei comportamenti corretti che possano prevenire malfunzionamenti e intrusioni
- corretta gestione delle credenziali di autenticazione, l'attenzione al *phishing* e alle altre tecniche di *social engineering*, attenzione alle wi-fi aperte, la cifratura dei dispositivi, la cancellazione sicura dei dati, evitare di lasciare il proprio computer in disponibilità di terzi, evitare di lasciare stampe incustodite, consapevolezza delle tracce delle attività online (regolamento informatico interno).

Adeguamento per un professionista o uno studio associato

Processi e procedure

Formazione del personale

Premesso che tutte le persone che effettuano operazioni di trattamento devono essere debitamente istruite e formate sui compiti e responsabilità nell'ambito delle operazioni di trattamento dei dati personali, è necessario che il Titolare (Studio Associato) preveda un piano di formazione specifico in relazione alle mansioni svolte ed esercitate dal dipendente.

Il piano di formazione per ciascun dipendente deve avere le seguenti caratteristiche:

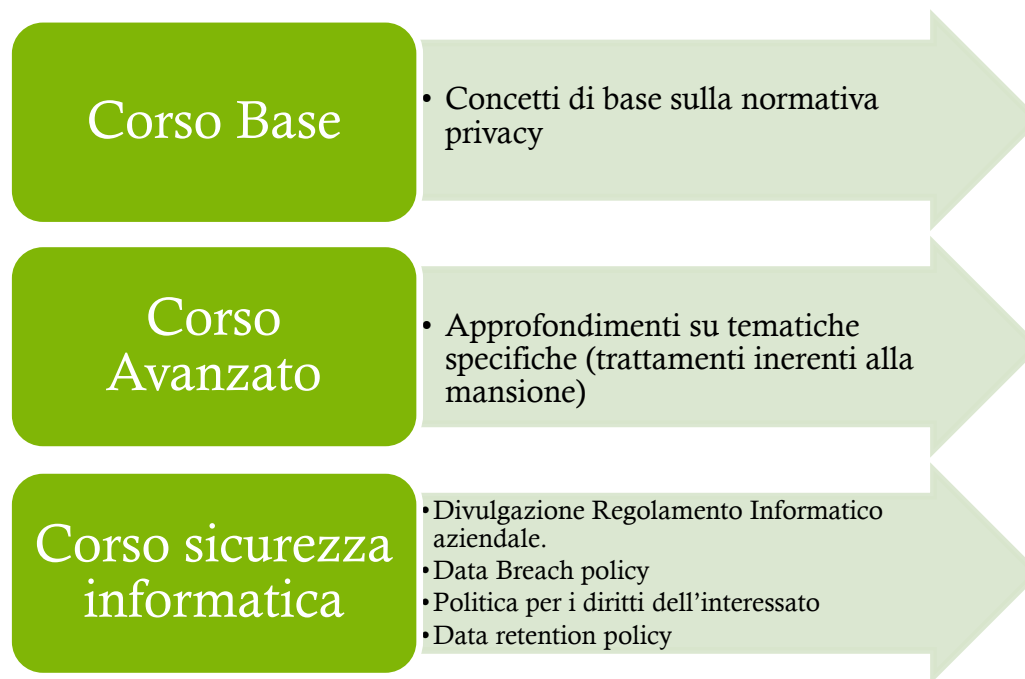
- Specifico, ovvero che corrisponda alla tipologia di mansione svolta.
- Appropriato, ovvero che sia affine alle tipologie di trattamenti svolti.
- Permanente, ovvero che preveda una programmazione temporale ed un aggiornamento periodico.
- Documentato, ovvero che siano annotati i corsi di formazioni in apposito registro.
- Efficace, ovvero che preveda una fase di verifica dell'apprendimento del dipendente.

Adeguamento per un professionista o uno studio associato

Processi e procedure

Formazione del personale

Come si può strutturare un buon piano di formazione del personale?



Contatti



- ✓ Dott. Andrea Cecchetti: andrea.cecchetti@smprivacy.com
andrea.cecchetti@cecchettialbani.com
- ✓ Avv. Fabio Righi: fabio.righi@smprivacy.com