



ANDREA OMAR BIANCO

GDPR

PER I PROFESSIONISTI

PROCEDURE COVID-19 E GREEN PASS



**PRONTO
GRAFILL**

Clicca e richiedi di essere contattato
per informazioni e promozioni

  **WEBAPP INCLUSA**
CON AGGIORNAMENTO AUTOMATICO



Andrea Omar Bianco

GDPR PER I PROFESSIONISTI – PROCEDURE COVID-19 E GREEN PASS

Ed. I (11-2021)

ISBN 13 978-88-277-0290-1

EAN 9 788827 702901

Collana **COME FARE PER** (81)



Licenza d'uso da leggere attentamente
prima di attivare la WebApp o il Software incluso

Usa un QR Code Reader
oppure collegati al link <https://grafill.it/licenza>

Per assistenza tecnica sui prodotti Grafill aprire un ticket su <https://www.supporto.grafill.it>

L'assistenza è gratuita per 365 giorni dall'acquisto ed è limitata all'installazione e all'avvio del prodotto, a condizione che la configurazione hardware dell'utente rispetti i requisiti richiesti.

© **GRAFILL S.r.l.** Via Principe di Palagonia, 87/91 - 90145 Palermo

Telefono 091/6823069 - Fax 091/6823313 - Internet <http://www.grafill.it> - E-Mail grafill@grafill.it

**CONTATTI
IMMEDIATI**



Pronto GRAFILL
Tel. 091 6823069



Chiamami
chiamami.grafill.it



Whatsapp
grafill.it/whatsapp



Messenger
grafill.it/messenger



Telegram
grafill.it/telegram

Edizione destinata in via prioritaria ad essere ceduta nell'ambito di rapporti associativi.

Tutti i diritti di traduzione, di memorizzazione elettronica e di riproduzione sono riservati. Nessuna parte di questa pubblicazione può essere riprodotta in alcuna forma, compresi i microfilm e le copie fotostatiche, né memorizzata tramite alcun mezzo, senza il permesso scritto dell'Editore. Ogni riproduzione non autorizzata sarà perseguita a norma di legge. Nomi e marchi citati sono generalmente depositati o registrati dalle rispettive case produttrici.



**PRONTO
GRAFILL**

**CLICCA per maggiori informazioni
... e per te uno SCONTO SPECIALE**

SOMMARIO

INTRODUZIONE	p.	7
1. Svolgo la mia professione da solo!.....	"	7
2. La precedente normativa?.....	"	7
3. E se facessi orecchie da mercante?	"	7
4. Fornitori	"	8
5. Tipologia di dati	"	9
1. COSA SAPERE	"	11
1.1. Brevi cenni sulle novità introdotte dal GDPR	"	11
1.2. Organigramma	"	12
1.2.1. Il Titolare del trattamento	"	12
1.2.2. Contitolare del trattamento.....	"	12
1.2.3. Esempi di contitolarità professionale	"	14
1.2.4. Responsabile del trattamento	"	15
1.2.5. Responsabile interno od esterno?.....	"	15
1.2.6. Sub-responsabile	"	17
1.2.7. Autorizzato al trattamento	"	17
1.2.8. Il danno risarcibile, responsabilità solidali, la rivalsa e il diritto al risarcimento.....	"	19
1.3. Rischi connessi al trattamento	"	20
1.3.1. Trattamento di dati suscettibili di danni fisici, materiali o morali	"	20
1.3.2. Furto di identità.....	"	21
1.4. Misure di sicurezza.....	"	21
1.5. Il decreto legislativo 10 agosto 2018, n. 101	"	24
1.5.1. Nuove fattispecie di trattamento illecito.....	"	25
2. COSA FARE	"	26
2.1. Introduzione	"	26
2.2. Verifica del consenso e dei dati acquisiti antecedentemente alla riforma	"	27

2.3.	Modulistica da presentare al cliente.....	p.	28
2.3.1.	Esempio di informativa e consenso	"	30
2.4.	Regolarizzazione delle figure interne ed esterne dello studio	"	32
2.4.1.	Esempio di nomina autorizzato.....	"	32
2.4.2.	Esempio di nomina responsabile esterno	"	35
2.4.3.	Esempio di accordo	"	39
2.5.	Gestione dei fascicoli	"	41
2.6.	Misure, protocolli di sicurezza da adottare e valutazione dei rischi	"	41
2.6.1.	Accesso ai dati.....	"	41
2.6.2.	Cancellazione dei dati	"	42
2.6.3.	Misure di sicurezza idonee per il cartaceo: procedure di custodia atti e documenti.....	"	42
2.6.4.	Misure di Sicurezza elettroniche	"	42
2.6.5.	Misure fisiche e organizzative	"	44
2.6.6.	Sicurezza	"	47
2.6.7.	Email.....	"	48
2.6.8.	Esempio di piano disaster recovery	"	48
2.6.9.	Schema di valutazione dei rischi.....	"	49
2.7.	Predisporre un registro delle attività di trattamento	"	52
2.7.1.	Esempio di registro	"	53
2.7.2.	Sito professionale	"	54
2.7.3.	Esempio di privacy policy e cookies.....	"	57
2.8.	Cancellazione e smaltimento del materiale cartaceo ed elettronico.....	"	67
2.9.	Istruzioni al personale.....	"	69
2.9.1.	Esempio di accordo di riservatezza	"	69
2.9.2.	Regole tecniche sulla cancellazione sicura dei dati	"	70
2.9.3.	Scheda informativa sulla cancellazione (G.U.R.I. n. 287 del 2008)	"	71
2.10.	Formazione.....	"	76
2.10.1.	Esempio di programma di formazione	"	77
2.10.2.	Esempio di test di valutazione	"	78
3.	COVID-19 E PRIVACY	"	80
3.1.	Premessa.....	"	80
3.2.	Interventi normativi	"	80
3.3.	Documentazione privacy da aggiornare	"	86
3.3.1.	Esempi di clausole per le informative	"	86
3.3.2.	Esempi di clausole per nomine di autorizzato	"	87
3.3.3.	Esempio di aggiornamento del trattamento sul registro.....	"	88

3.4.	Smart Working sicuro e Formazione.....	p.	88
3.5.	Bibliografia	"	90
4.	GREEN PASS E PRIVACY	"	92
5.	CONTENUTI E ATTIVAZIONE DELLA WEBAPP	"	95
5.1.	Contenuti della WebApp.....	"	95
5.2.	Requisiti hardware e software	"	95
5.3.	Attivazione della WebApp	"	95



INTRODUZIONE

Svolgere la propria professione diventa sempre più difficile! Un'ennesima incombenza normativa colpisce i Professionisti.

È il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, noto con il diminutivo di GDPR o RGPD.

Dal 25 di maggio 2018, tutte le attività che raccolgono o trattano dati personali saranno costrette a conformarsi. La speranza di proroghe è vana. L'obiettivo è quello di scoraggiare gli abusi, i trafficanti di dati, l'approccio menefreghista nonché superficiale che fino alla riforma è stato perpetrato.

La normativa introdotta, mira alla difesa di un bene a cui pochi prestano attenzione, la privacy. Questo testo, vi consentirà di avere un valido supporto per gestire tutte le incombenze richieste quotidianamente sub materia.

1. Svolgo la mia professione da solo!

La normativa non prevede esenzioni e non tiene conto della strutturazione interna del professionista. Se possedete un titolo professionale senza esercitare allora potete chiudere questo libro.

2. La precedente normativa?

Il decreto legislativo 30 giugno 2003, n. 196¹, è stato integrato dall'entrata in vigore della nuova normativa europea. Grazie al decreto legislativo 10 agosto 2018, n. 101², il Governo ha conciliato la decaduta legislazione con la nuova normativa.

3. E se facessi orecchie da mercante?

Far finta di nulla sarebbe molto semplice. Chi penserebbe mai di denunciarmi? Il cliente fornisce la propria autorizzazione e non ha strumenti adatti per comprendere

¹ Decreto legislativo 30 giugno 2003, n. 196, recante «Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)». Pubblicato sulla Gazzetta Ufficiale 29 luglio 2003, n. 174 – Suppl. Ord. n. 123.

² Decreto legislativo 10 agosto 2018, n. 101, recante «Codice in materia di protezione dei dati personali». Pubblicato sulla Gazzetta Ufficiale 4 settembre 2018, n. 205.

a fondo ciò che sottopongo alla sua attenzione. Pende completamente dalle mie labbra. Figurarsi poi se qualcuno verrà mai a casa mia per controllare i dati raccolti!

Niente di più errato.

Sebbene sia difficile che il cliente possa essere parte attiva nella segnalazione di una eventuale violazione (in quanto ciò presupporrebbe la conoscenza di quest'ultimo dei propri diritti, nonché, la consapevolezza dei doveri del professionista e della normativa in quanto tale) questa possibilità non può dirsi remota. A tal proposito, è opportuno considerare che il cliente potrebbe essere un professionista avente un buon livello di conoscenza della materia in oggetto. Ciò, senza mai dimenticare la macchina dello Stato che, in situazioni di difficoltà potrebbe strumentalizzare la normativa per fare cassa.

Infine, lo stesso Garante potrebbe rivolgere degli avvertimenti al Titolare del Trattamento o al Responsabile del trattamento sulla circostanza che l'attività svolta possa aver violato il GDPR, così da conformare i trattamenti alle disposizioni normative, specificandone tempi e modi.

Dunque, cosa accadrebbe se mancasse l'adeguamento?

L'articolo 83 e seguenti del GDPR disciplinano le ipotesi nelle quali è prevista l'applicazione di sanzioni amministrative, pecuniarie e/o penali.

Le prime, possono raggiungere i 10 milioni di euro o, se superiore, il 2% del fatturato mondiale. Ad esempio, nei casi di:

- violazione delle condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione;
- trattamento illecito di dati personali che non richiede l'identificazione dell'interessato;
- mancata o errata notificazione e/o comunicazione di un data *breach* all'Autorità nazionale competente;
- violazione dell'obbligo di nomina del DPO;
- mancata applicazione di misure di sicurezza.

L'importo delle **sanzioni amministrative pecuniarie** può salire fino a 20 milioni di euro, o alternativamente, sino al 4% del fatturato mondiale dell'impresa nelle ipotesi di:

- inosservanza di un ordine, di una limitazione provvisoria o definitiva concernente un trattamento, imposti da un'Autorità nazionale competente;
- trasferimento illecito *cross-border* di dati personali ad un destinatario in un Paese terzo.

4. Fornitori

Un altro aspetto importante riguarda il rapporto con le organizzazioni che vengono pagate per svolgere attività connesse al trattamento dei dati.

La normativa UE pone le stesse responsabilità del titolare in capo a tutti coloro i quali, su vostro incarico, collaborano al trattamento dei dati: consulente finanziario, web master, medico del lavoro, RSPP, dipendenti, collaboratori di studio, fornitori di servizi, domiciliatari, ecc..

COSA SAPERE

1.1. Brevi cenni sulle novità introdotte dal GDPR

Il GDPR rivoluziona il modo in cui la *privacy* viene affrontata dalle singole realtà di tutta Europa, disciplinandola come mai prima d'ora ed istituendo un quadro formativo incentrato sui doveri e sulla responsabilizzazione del Titolare del trattamento.

Ad essere stato introdotto è il **principio di *accountability*** che comprende la definizione delle responsabilità all'interno delle singole organizzazioni.

Il **Titolare del trattamento**, ovvero il massimo **responsabile della tutela della *privacy***, è tenuto al rispetto dei **principi previsti dal GDPR**, comprovandoli attraverso una serie di strumenti indicati dalla nuova normativa. Ciò, è possibile attraverso una valutazione dei rischi e degli impatti antecedente all'avvio del trattamento di dati personali, nonché ad una progettazione strutturata della tutela della *privacy* stessa.

La riforma, richiede lo sviluppo di ulteriori **misure e tecniche organizzative** per comprovare l'adeguatezza dei propri sistemi come pure delle proprie pratiche, al fine di escludere, in caso di una violazione dei dati, una eventuale responsabilità.

Il GDPR introduce quindi due concetti chiave:

- 1) *Privacy by design*;
- 2) *Privacy by default*.

Il primo si riferisce alla necessità di progettare misure di sicurezza e *privacy* adeguate alle nuove esigenze e normative.

Il secondo invece alla capacità di disegnare misure di sicurezza e *privacy* per default, considerandole come un prerequisito fondamentale per il normale funzionamento dei sistemi informativi aziendali.

Ad essere ulteriormente evidenziati sono infine i **principi di liceità del trattamento**, trattamento possibile previa autorizzazione dell'interessato all'utilizzo dei propri dati personali, ma anche di **adeguatezza, pertinenza e non eccedenza dei dati** rispetto alle finalità per cui vengono raccolti e trattati. La trasparenza in tal senso diventa fondamentale, come anche l'assoluto **rispetto della *privacy*** di ogni singolo individuo coinvolto. Sicché, i sistemi, si fanno più trasparenti, maggiormente strutturati e specifici ma, soprattutto, a norma.

La presenza di una figura responsabile, che garantisca la tutela della *privacy*, non esclude che debba essere dimostrata la conoscenza e il rispetto della normativa. Tale adeguamento dovrà, dunque, essere provato attraverso una adeguata documentazione inter-

na nonché attraverso una regolarizzazione conforme dei rapporti professionali e il possesso di qualifiche e certificazioni ufficiali (per chi intenda intraprendere la professione di *Consulente Privacy*). Queste ultime, possono essere conseguite attraverso un corso dedicato all'aggiornamento riguardo la GDPR in aggiunta ad una sana esperienza sul campo.

1.2. Organigramma

Le figure chiavi indicate e disciplinate dal GDPR sono da ricondursi al Titolare (contitolare) e quindi il professionista/i, il Responsabile del trattamento che nella maggior parte dei casi è esterno con tutti gli eventuali Sub-Responsabili nominati da quest'ultimo, il **DPO/RPD** (difficilmente nominato perché sulla scorta della struttura dei professionisti non è obbligatoria la designazione) e gli autorizzati/incaricati dal trattamento dei dati.

La presenza di tutte queste figure dipende dalle dimensioni dello studio.

1.2.1. Il Titolare del trattamento

Il professionista è sempre il Titolare del trattamento cioè colui il quale singolarmente o insieme ad altri professionisti, chiamati e nominati eventualmente Contitolari, scelgono le finalità e modalità di trattamento dei dati personali.

Nell'espletamento di questo potere il professionista deve avere piena e libera autonomia, in particolare per:

- valutare *ab origine* quali dati sia necessario acquisire;
- determinare le finalità del trattamento;
- adottare tutte le misure tecniche e organizzative adeguate per garantire il trattamento dei soli dati necessari ad ogni specifica finalità di trattamento;
- predisporre politiche interne (protocolli) conformi alla sua organizzazione e al Regolamento;
- dimostrare, in caso di controllo, che il trattamento è conforme al Regolamento (principio di *Accountability*) e di aver adottato misure tecniche e organizzative efficaci ed adeguate per proteggere i dati acquisiti.

1.2.2. Contitolare del trattamento

«La figura del contitolare del trattamento è prevista all'art. 26 "Contitolari del trattamento" GDPR, il quale precisa che i contitolari possono anche essere più di due. Gli stessi, inoltre, devono determinare congiuntamente le finalità e mezzi del trattamento (si veda Gruppo di lavoro articolo 29, Parere 1/2010 – WP 169).

Si ravvisa dunque la necessità di una codecisione in merito alle finalità (perché) ed ai mezzi (come) di un determinato trattamento.

Tramite un accordo fra le parti, i contitolari hanno l'obbligo di determinare, in modo trasparente, le proprie responsabilità e i propri compiti sull'osservanza degli obblighi de-

COSA FARE

2.1. Introduzione

In questo capitolo si cercherà di dare delle linee guida al fine di garantire una conformità valida dello studio del professionista ai dettati normativi.

Prima di iniziare, il professionista deve porsi delle domande, ossia:

- 1) *«Ho verificato se i dati dei miei clienti in mio possesso acquisiti prima dell'entrata in vigore della normativa europea sono stati acquisiti nel rispetto del vecchio Codice privacy e se sono stati superati i termini di conservazione?»*
- 2) *Ho predisposto tutta la modulistica per procedere, durante il primo incontro con il Cliente, alla raccolta dei dati fornendo allo stesso una informativa completa, semplice e chiara?*
- 3) *Ho organizzato le mie attività in modo da raccogliere e trattare solo ed esclusivamente dati necessari o utili in vista dell'espletamento del mandato professionale ricevuto?*
- 4) *Ho organizzato la conservazione dei documenti relativi alle varie pratiche in modo da averne sempre, al momento giusto, la disponibilità ed in modo che i dati siano accessibili al solo personale autorizzato?*
- 5) *Ho nominato e adeguatamente istruito i miei collaboratori e dipendenti?*
- 6) *Ho formalizzato mediante apposita nomina i rapporti con i professionisti ai quali mi rivolgo per la gestione e lo sviluppo delle attività dello studio?*
- 7) *Detengo e aggiorno regolarmente i miei Registri da Titolare, da Responsabile Esterno o in caso da Domiciliatario?*
- 8) *I miei PC sono protetti dalle minacce esterne?*
- 9) *Dispongo, in caso di bisogno, di un tecnico-informatico di fiducia al quale rivolgermi per la soluzione di specifici problemi?*
- 10) *Provvedo ad eseguire un salvataggio integrale (backup) di tutti i dati su i PC per lo meno 1 volta alla settimana?*
- 11) *Ho definito un tempo di conservazione dei dati personali in linea con le finalità dei trattamenti.*
- 12) *Mi sono preoccupato della sicurezza fisica dello studio, ossia adottare misure o cautele atte ragionevolmente a prevenire accessi indesiderati e azioni concretatesi nella lesione della riservatezza, disponibilità, integrità delle banche dati?*

- 13) *Quando devo rottamare PC, Notebook e altri strumenti elettronici utilizzati per le attività dello studio, mi assicuro che la dismissione avvenga nel rispetto della esigenza di protezione dei dati?*
- 14) *Portatili e altri strumenti informatici rimovibili sono utilizzati al di fuori dello studio in modo da minimizzare i rischi di perdita accidentale, sottrazione fraudolenta e similari?¹».*

Se la risposta ad ogni domanda è positiva allora possiamo affermare che lo studio è effettivamente adeguato al Regolamento. Nel caso in cui manchi anche una delle risposte in oggetto si può affermare, a seconda della domanda o che non si è adeguati o che vi sia un alto rischio di violazione del dato per il quale è necessario intervenire.

2.2. Verifica del consenso e dei dati acquisiti antecedentemente alla riforma

Il professionista come prima incombenza deve verificare di essere in possesso di un consenso e che quest'ultimo sia stato acquisito in modo valido.

Considerando l'art. 43, n. 9, altre disposizioni del Codice: artt. 18, 20, possiamo dire che il garante attribuisce essenzialmente la valida base giuridica del trattamento del consenso ottenuto prima della data di entrata in vigore del Regolamento europeo purché sia stato raccolto con modalità tali per cui risulti «*esplicito*» (se riferito a dati sensibili e a decisioni basate su trattamenti automatizzati), «*libero, specifico, informato*» e «*manifestato attraverso dichiarazione o azione positiva inequivocabile*» (se riferito a dati ordinari).

In sintesi il professionista deve verificare di aver fornito e ottenuto dal suo cliente o tramite un informativa ad hoc o tramite un consenso all'interno di un altro documento (ad es. il mandato, un contratto di servizio, ecc.) un documento che rispetti i dettami del D.Lgs. n. 196/2003. In questo caso dovrà fornire un **supplemento** di informativa con le nuove informazioni richieste in base alle norme e alla piena trasparenza (vedi l'art. 5, comma 1, lettera a)), offrendo contestualmente agli interessati la possibilità di **revocare** il consenso originariamente fornito e naturalmente specificando le eventuali conseguenze di tale revoca.

Ipotizzandone la mancanza o l'inadeguatezza delle modalità il Professionista obbligatoriamente dovrà richiedere ai suoi clienti, seguendo le nuove indicazioni e presentando un formato informativo tale da ottenere dai vecchi clienti un legittimo consenso, l'autorizzazione al trattamento dei loro dati. In tal guisa, non sorgono problemi se il cliente è reperibile ed ancora seguito dallo studio perché l'acquisizione del Consenso sarà indubbiamente facile.

Nel caso in cui l'assistito non fosse più cliente occorrerà richiedere il consenso per i dati per i quali il professionista è tenuto per legge alla conservazione. In caso di irreperibilità lasciare sempre traccia del tentativo di regolarizzazione del rapporto sotto il profilo *privacy*, mediante ricevuta della raccomandata AR, una email, pec, un fax, ecc., così da

¹ Decalogo a cura dell'Avv. Paolo Marini, Altatex 2018.

COVID-19 E PRIVACY

3.1. Premessa

L'emergenza *Covid-19*, oltre ad incidere sul piano sanitario ed economico, ha determinato per le autorità e i datori di lavoro l'obbligo di adottare una serie di misure per il corretto rilevamento della malattia e limitare il più possibile i contagi.

Ciò si è tradotto in una serie di attività che coinvolgono il trattamento dei dati personali imponendo al Titolare del trattamento di adeguare la modulistica e prevedere nuove misure.

3.2. Interventi normativi

Il Garante, di fronte all'emergenza sanitaria e alle varie richieste di chiarimento sul trattamento dei dati in merito, è intervenuto pubblicando, il 2 marzo 2020, il Comunicato riportato a seguire:

«L'Ufficio sta ricevendo numerosi quesiti da parte di soggetti pubblici e privati in merito alla possibilità di raccogliere, all'atto della registrazione di visitatori e utenti, informazioni circa la presenza di sintomi da Coronavirus e notizie sugli ultimi spostamenti, come misura di prevenzione dal contagio. Analogamente, datori di lavoro pubblici e privati hanno chiesto al Garante la possibilità di acquisire una "autodichiarazione" da parte dei dipendenti in ordine all'assenza di sintomi influenzali, e vicende relative alla sfera privata.

Al riguardo, si segnala che la normativa d'urgenza adottata nelle ultime settimane prevede che chiunque negli ultimi 14 gg abbia soggiornato nelle zone a rischio epidemiologico, nonché nei comuni individuati dalle più recenti disposizioni normative, debba comunicarlo alla azienda sanitaria territoriale, anche per il tramite del medico di base, che provvederà agli accertamenti previsti come, ad esempio, l'isolamento fiduciario.

I datori di lavoro devono invece astenersi dal raccogliere, a priori e in modo sistematico e generalizzato, anche attraverso specifiche richieste al singolo lavoratore o indagini non consentite, informazioni sulla presenza di eventuali sintomi influenzali del lavoratore e dei suoi contatti più stretti o comunque rientranti nella sfera extra lavorativa.

La finalità di prevenzione dalla diffusione del Coronavirus deve infatti essere svolta da soggetti che istituzionalmente esercitano queste funzioni in modo qualificato.

GREEN PASS E PRIVACY

I limiti e i presupposti del potere di accertamento dell'identità del titolare delle certificazioni verdi, nei contesti nei quali sia richiesto il possesso di tali attestazioni è il dilemma più comune.

Per quanto di competenza, tuttavia, non può che rilevarsi come l'art. 9-*bis*, comma 4, secondo periodo, del D.L. 22 aprile 2021, n. 52, introdotto dall'art. 3 del D.L. 23 luglio 2021, n. 105, preveda ai fini della regolamentazione delle modalità di esecuzione della verifica delle certificazioni verdi l'applicazione, anche nelle nuove ipotesi di ostensione introdotte dal D.L. n. 105, della disciplina procedurale prevista dal D.P.C.M. attuativo dell'art. 9, comma 10, del D.L. n. 52/2021, convertito, con modificazioni, dalla legge 17 giugno 2021, n. 87. Tale disciplina procedurale (oggi riconducibile al D.P.C.M. 17 giugno 2021) comprende, del resto – oltre la regolamentazione degli specifici canali digitali funzionali alla lettura della certificazione verde – anche gli obblighi di verifica dell'identità del titolare della stessa, con le modalità e alle condizioni di cui all'art. 13, comma 4, del citato D.P.C.M..

Tra le garanzie previste da tale decreto è, del resto, compresa anche l'esclusione della raccolta, da parte dei soggetti verificatori, dei dati dell'intestatario della certificazione, in qualunque forma (art. 13, comma 5, del suddetto D.P.C.M.).

Entro questi termini, pertanto, e nei sensi di cui al combinato disposto degli artt. 9-*bis*, comma 4, secondo periodo, del D.L. n. 52/2021 e 13, comma 4 del citato D.P.C.M., è consentito il trattamento dei dati personali consistente nella verifica, da parte dei soggetti di cui all'art. 13, comma 2, dell'identità dell'intestatario della certificazione verde, mediante richiesta di esibizione di un documento di identità.

Sicché può dirsi che si hanno 2 fasi tra di loro distinte:

- 1) la verifica della validità del *Green Pass* attraverso l'App *VerificaC19*, utilizzabile su uno smartphone, che può operare tranquillamente offline in quanto, si dichiara, non trasmette alcun dato;
- 2) la verifica dell'identità del soggetto al fine di riscontrare la coincidenza dei dati presenti sul *Green Pass* attraverso l'esposizione di un documento di riconoscimento.

Prendendo in considerazione il controllo dell'identità del soggetto non si pone alcun problema di violazione della normativa privacy poiché viene effettuato un controllo meramente apodittico dell'identità del soggetto e privo di possibili oggettivi riscontri; dove non si procede nemmeno alla raccolta o altro trattamento di dati personali.

CONTENUTI E ATTIVAZIONE DELLA WEBAPP

5.1. Contenuti della WebApp

- **Modelli GDPR:** Informativa sul trattamento dei dati personali; Informativa sul trattamento dei dati personali (Dipendenti); Informativa sul trattamento dei dati personali (Fornitori); Lettera di nomina ad autorizzato al trattamento dei dati personali (Dipendente); Lettera di nomina ad autorizzato al trattamento dei dati personali (Medico del lavoro); Nomina a responsabile esterno del trattamento (Buste paga); Registro delle attività di trattamento (Studi professionali).
- **Atti legislativi in materia di privacy** (Regolamento (UE) 2016/679 del 27 aprile 2016 e D.Lgs. n. 101 del 10 agosto 2018).
- **Speciale Coronavirus** – Normativa consultabile attraverso un motore di ricerca e con aggiornamenti automatici per 365 giorni dall'attivazione della WebApp.

5.2. Requisiti hardware e software

- Dispositivi con MS Windows, Mac OS X, Linux, iOS o Android;
- Accesso ad internet e browser web con Javascript attivo;
- Software per la gestione di documenti Office e PDF.

5.3. Attivazione della WebApp

- Collegarsi al seguente indirizzo internet:

https://www.grafill.it/pass/0290_1.php

- Accedere al **Profilo utente Grafill** oppure crearne uno su www.grafill.it;
- Cliccare sul pulsante **[G-CLOUD]**;
- Cliccare sul pulsante **[Vai alla WebApp]** a fianco del prodotto acquistato;
- Fare il *login* usando le stesse credenziali di accesso al **Profilo utente Grafill**;
- Accedere alla WebApp abbinata alla presente pubblicazione cliccando sulla relativa immagine di copertina presente nello scaffale **Le mie App**.

