

**Informativa privacy ai sensi degli artt. 13 e 14  
del Regolamento EU 679/2016  
Verifica possesso certificazione verde (Green Pass)**

### 1. Premessa

E' necessario ricordare che:

- è **dato personale** qualunque informazione capace di identificare – direttamente oppure indirettamente (cioè anche utilizzando ulteriori informazioni) - una persona fisica, il cd. **interessato**;
- si parla di **trattamento di dati personali** in relazione a 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;
- il **Titolare** del trattamento è il soggetto (anche pubblico) che utilizza tali dati per proprie finalità individuando i mezzi (cioè le modalità di realizzazione, sia da un punto di vista tecnico che organizzativo) con cui effettuare il trattamento.

Affinché un trattamento di dati sia lecito deve rispettare alcune condizioni, presupposti e finalità previsti e consentiti dalla vigente normativa in materia di protezione dei dati personali, i cui riferimenti fondamentali sono attualmente i seguenti:

- *Regolamento generale 2016/679/UE relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati ...* (di seguito: Regolamento Generale);
- *D.Lgs. 30 giugno 2003, n. 196 Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 ...* (di seguito: Codice).

Le **informazioni** (anche: **informativa**) sul trattamento sono un diritto dell'interessato ed un obbligo per il titolare del trattamento. In breve, qualora un titolare deve trattare dati che si riferiscono ad una persona fisica – cioè dati personali – deve preventivamente informare questi sugli scopi del trattamento, la relativa base giuridica, le tipologie di dati trattati, i relativi tempi di conservazione, le modalità del trattamento ecc., declinando una serie di elementi analiticamente previsti e prescritti dagli artt. 13 (dati personali raccolti presso l'interessato) e 14 (dati personali non raccolti presso l'interessato) del Regolamento Generale.

Le presenti **informazioni** sul trattamento fanno riferimento tanto all'art. 13 del Regolamento Generale che anche all'art. 14, in quanto per la verifica, pur se effettuata utilizzando



informazioni (riassunte nel QR code) messe a disposizione dall'interessato, si accede a dati precedente raccolti dal Ministero della Salute.

## **2. Contesto del trattamento**

Il presente documento riguarda il trattamento di dati personali necessario per adempiere alle prescrizioni del D.L. 127/2021 *Misure urgenti per assicurare lo svolgimento in sicurezza del lavoro pubblico e privato mediante l'estensione dell'ambito applicativo della certificazione verde COVID-19 e il rafforzamento del sistema di screening*, nonché del DPCM 12 ottobre 2021 *Adozione delle linee guida in materia di condotta delle pubbliche amministrazioni per l'applicazione della disciplina in materia di obbligo di possesso e di esibizione della certificazione verde COVID-19 da parte del personale*.

Ai sensi di tali disposizioni, dal 15 ottobre 2021 e fino al 31 dicembre 2021, termine di cessazione dello stato di emergenza, al fine di prevenire la diffusione dell'infezione da SARS-CoV-2, al personale delle amministrazioni pubbliche è fatto obbligo, ai fini dell'accesso ai luoghi di lavoro, di *possedere e di esibire*, su richiesta, la certificazione verde COVID-19 (in via residuale, nelle more del rilascio e dell'eventuale aggiornamento delle certificazioni verdi Covid19 da parte della piattaforma nazionale DGC – Digital Green Certificate - i soggetti interessati possono avvalersi dei documenti rilasciati, in formato cartaceo o digitale, dalle strutture sanitarie pubbliche e private, dalle farmacie, dai laboratori di analisi, dai medici di medicina generale e dai pediatri di libera scelta che attestano o refertano una delle condizioni di cui al comma 2, lettere a), b) e c), dell'art 9 del decreto legge n. 52 del 2021); tale obbligo si applica altresì a tutti i soggetti (pubblici o privati) che svolgano, a qualsiasi titolo, la propria attività lavorativa (come anche di formazione o di volontariato) presso le amministrazioni pubbliche; non si applicano invece ai soggetti esenti dalla campagna vaccinale sulla base di idonea certificazione medica. La verifica del personale delle amministrazioni pubbliche viene effettuata dal datore di lavoro, tanto al momento dell'accesso ai luoghi di lavoro che, se non possibile, successivamente a campione, individuando con atto formale i soggetti incaricati dell'accertamento e della contestazione delle violazioni degli obblighi. Relativamente agli altri soggetti interessati, la verifica è effettuata tanto dai rispettivi datori di lavoro che da quelli delle amministrazioni ove prestano la loro attività.

L'accertamento e quanto ad esso consegue comportano ovviamente un trattamento di dati personali, circa il quale il presente documento di "informazioni sul trattamento" rende appunto disponibili all'interessato gli elementi informativi prescritti dalla vigente normativa in materia di protezione dei dati personali.

## **3. Soggetti interessati**

Le presenti informazioni riguardano tanto i dipendenti dell'Azienda che tutti i soggetti che, svolgano, a qualsiasi titolo, la propria attività lavorativa o di formazione o di volontariato presso l'Azienda stessa.

## **4. Tipologie di dati trattati**

Il Regolamento Generale, dopo aver offerto all'art. 4 1) la nozione di dato personale (vedi il § 1), specifica poi, che il dato personale può ricondursi alle *categorie particolari di dati personali* di cui all'art. 9 (dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, dati genetici, dati



biometrici, dati relativi alla salute, dati relativi alla vita sessuale o all'orientamento sessuale della persona) o ai *dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza* di cui all'art. 10; vi sono poi ovviamente dati che non appartengono a tali categorie, e che si definiscono complessivamente *dati comuni*. Ne segue che possono individuarsi tre categorie di dati personali:

- le categorie particolari di dati personali
- i dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza
- i dati comuni

Ai fini del trattamento oggetto della presente informativa, sono trattati i seguenti dati:

- QR code;
- dalla lettura del QR code: cognome, nome, data di nascita, nonché esito della verifica;
- dal documento di identità, in caso in caso di richiesta di identificazione dell'interessato da parte del verificatore: i dati anagrafici in esso riportati;
- dati sanitari contenuti nella documentazione sanitaria di cui al § 2;
- nominativo e matricola (nominativo, codice fiscale ed azienda/ente di appartenenza o riferimento per i soggetti esterni) della persona fisica non in possesso della certificazione verde o non in grado di esibirla, per gli adempimenti conseguenti.

Come qualificare, tra le tipologie sopra richiamate, tali dati? Ciò è fondamentale, in quanto un trattamento di dati è lecito in riferimento a norme diverse a seconda, oltre che dello scopo del trattamento, appunto delle tipologie di dati in esso ricompresi.

I dati personali relativi al possesso della certificazione possono senz'altro essere qualificati come dati rientranti nelle categorie "particolari" di dati personali, ovvero dati relativi alla salute di cui all'art. 9 del Regolamento Generale; ciò in quanto il possesso della certificazione verde rimanda a prestazioni sanitarie (vaccinazione o tampone) o ad una patologia sofferta (appunto l'infezione da COVID).

L'accesso al QR code, se positivo, si risolve dunque in un trattamento di dati afferenti alle categorie particolari, ovvero di dati relativi alla salute.

Lo stesso, ovviamente, per l'accesso alla documentazione sanitaria di cui al § 2.

Per quanto riguarda invece il dato relativo al mancato possesso della certificazione verde, esso potrebbe certo ricondursi agli orientamenti di carattere politico o filosofico di cui all'art. 9 del Regolamento Generale: in generale, però, tale mancato possesso potrebbe anche essere dovuto al fatto di non aver scaricato o stampato il certificato, di non essere in grado di esibirlo per dimenticanza e per problemi tecnici, ecc.; da questo punto di vista le relative informazioni sarebbero riconducibili a dati personali che non rientrano tra le categorie particolari di dati di cui all'art. 9 (né certo a quelli relativi alle condanne penali e ai reati o a connesse misure di sicurezza di cui all'art. 10 del Regolamento Generale stesso): sono perciò qualificabili come dati cd. "comuni".



L'accesso al QR code, se negativo, o il mancato accesso ad esso per impossibilità di esibirlo, si risolve dunque in un trattamento di dati comuni.

### **5. Finalità del trattamento**

Il Titolare del trattamento può lecitamente trattare dati personali solo quando il trattamento ha una specifica base giuridica: cioè, in riferimento ad un ente pubblico, quando è funzionale ad attività che sono ricomprese tra le proprie finalità istituzionali (o non sono comunque con esse incompatibili) e soddisfa alcune condizioni generali, nel rispetto della vigente normativa.

Le attività di cui alle presenti informazioni comportano un trattamento di dati che ha diverse finalità lecite (in una attività possono coesistere diverse finalità del trattamento); il trattamento è dunque effettuato:

- per motivi di interesse pubblico nella sanità pubblica ai sensi dell'art. 9 par. 2 lettera i del Regolamento Generale (categorie particolari di dati);
- per adempiere ad un obbligo legale, ai sensi dell'art. 6 paragrafo 1 lettera c del Regolamento Generale (dati comuni);
- per motivi di interesse pubblico rilevante, ai sensi dell'art. 6 paragrafo 1 lettera e (dati comuni) e dell'art. 9 par. 2 lettera g del Regolamento Generale (categorie particolari di dati).
- affinché il datore di lavoro possa assolvere agli obblighi in materia di diritto del lavoro, ai sensi dell'art. 9 par. 2 lettera b del Regolamento Generale (categorie particolari di dati).

I trattamenti di dati comuni necessari per adempiere ad un obbligo legale, ai sensi dell'art. 6 paragrafo 1 lettera c) e per motivi di interesse pubblico rilevante, ai sensi dell'art. 6 paragrafo 1 lettera e) del Regolamento Generale sono leciti se previsti, ai sensi dell'art. 2-ter, da una norma di legge o, nei casi previsti dalla legge, di regolamento, o comunque se necessari per l'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri.

I motivi di interesse pubblico rilevante vengono appunto in causa in riferimento ai trattamenti di dati effettuati dagli enti pubblici per le proprie finalità istituzionali; essi sono relativi a scopi di carattere in senso lato amministrativo che esauriscono (es. gestione del rapporto di lavoro) o supportano (es. attività medica) una attività istituzionale che comporta il trattamento di dati personali.

I trattamenti di categorie particolari di dati per motivi di interesse pubblico rilevante sono leciti, quando riguardano categorie particolari di dati, ai sensi dell'art. 2 sexies del D.Lgs. 196/2003 "qualora siano previsti ... nell'ordinamento interno, da disposizioni di legge o, nei casi previsti dalla legge, di regolamento che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato".



Ciò significa che quando un ente pubblico tratta dati particolari (ad es. dati relativi alla salute) per le proprie finalità istituzionali, occorre verificare se, non solo la finalità in generale, ma la stessa specifica operazione di trattamento che si intende effettuare sia appunto puntualmente prevista da una disposizione di legge o, nei casi previsti dalla legge, di regolamento.

La disposizione in questione, nel nostro caso, è in ultima analisi, il medesimo D.L. 127/2021.

Il conferimento dei dati, in quanto necessario per le finalità lecite sopra richiamate, non richiede il consenso dell'interessato.

## **6. Operazioni effettuate e modalità del trattamento**

La protezione dei dati personali si informa ad un generale principio di minimizzazione: i dati devono cioè essere trattati nel rispetto dei principi di pertinenza, completezza e non eccedenza. Inoltre, devono essere trattati in osservanza dei principi di liceità, correttezza e trasparenza, previsti dalla legge, e in modo tale da garantirne la sicurezza e tutelare la massima riservatezza dell'interessato.

Sui dati che vengono trattati per verificare il possesso (o non possesso) della certificazione verde, vengono eseguite, indicativamente, le seguenti operazioni di trattamento, tra quelle previste nella definizione richiamata in § 1: *accesso, registrazione, uso, consultazione, conservazione, comunicazione*.

La verifica delle certificazioni verdi COVID-19 è effettuata mediante la lettura del codice a barre bidimensionale (QR code), stampato o presente nello smartphone dell'interessato, attraverso l'utilizzo esclusivo da parte di un addetto autorizzato dell'applicazione mobile denominata VerificaC19, sviluppata dal Ministero della Salute per il tramite di SOGEL e installata nel dispositivo aziendale (smartphone o tablet).

L'applicazione VerificaC19 consente unicamente il processo di verifica dell'autenticità, validità e integrità delle certificazioni verdi COVID-19, senza rendere visibili le informazioni che ne hanno determinato l'emissione (secondo le disposizioni contenute nell'Allegato B, par. 4 d.P.C.M. 17 giugno 2021 dove sono indicate – come previsto dall'art. 9, co. 10 del decreto-legge 22 aprile 2021, n. 52 - le specifiche tecniche per assicurare l'interoperabilità tra le certificazioni verdi COVID-19 e la Piattaforma nazionale DGC, nonché tra questa e le analoghe piattaforme istituite negli altri Stati membri dell'Unione europea, tramite il Gateway europeo).

La verifica si svolge dunque ordinariamente “qui e adesso” (pur se è possibile, in alcuni ambiti, richiedere che il mancato possesso del certificato sia comunicato al datore di lavoro non oltre 48 ore prima di un termine prefissato); in particolare, i dati relativi ai termini di validità della certificazione (che potrebbero essere utili ad evitare di dover effettuare la verifica per ogni accesso ai luoghi di lavoro, ma che indirettamente possono indicare a quale titolo l'interessato possiede la certificazione) non possono essere acceduti o registrati.

I dati connessi alla verifica positiva vengono “usati” per permettere l'accesso al luogo di lavoro (tanto del dipendente che del collaboratore esterno).

Una operazione di registrazione è legittima per due scopi. Si richiama, al punto 1.2 del DPCM 12 ottobre 2021, la seguente prescrizione:

In osservanza alla disciplina in materia di trattamento dei dati personali, non è comunque consentita la raccolta dei dati dell'intestatario in alcuna forma, salvo quelli strettamente necessari all'applicazione delle misure previste dagli articoli .... 9 quinquies, commi 6 e ss. ...".

I commi richiamati fanno riferimento a:

- comunicazione del dipendente di non essere in possesso della certificazione verde (comma 6);
- verifica che il dipendente, all'eccesso al luogo di lavoro, non è in possesso della certificazione verde (comma 6);
- sanzione del dipendente che si trovi nelle condizioni di cui ai due punti precedenti con l'assenza ingiustificata (comma 6);
- sanzione del dipendente che accede al luogo di lavoro in violazione degli obblighi sulla certificazione verde con procedimento disciplinare (comma 7);
- comunicazione al Prefetto dell'accesso al luogo di lavoro in violazione degli obblighi sulla certificazione verde per l'irrogazione della sanzione da euro 600 a 1500 (commi 8 e 9).

In breve, possono essere registrati e conservati i dati personali necessari a documentare e gestire le situazioni di cui ai punti precedenti.

Ciò significa, all'opposto, che non è possibile raccogliere dati personali relativi alla effettuazione di verifiche positive, ma soltanto quelli riferite alle verifiche non positive; ciò anche nel caso di verifiche a campione, per attestare le quali si potranno raccogliere solo dati numerici relativamente ai controlli effettuati.

Qualora l'interessato (dipendente dell'azienda o altro soggetto) non sia in possesso della certificazione verde, gli deve essere vietato l'accesso al luogo di lavoro. L'operazione di trattamento effettuata è appunto quella definita come "uso": l'evidenza del mancato possesso viene usata, utilizzata per vietare l'accesso al luogo di lavoro.

Nel caso mancato adempimento, si danno due casi:

- il dipendente rifiuta la verifica;
- la verifica effettuata con la app VerificaC19 non è positiva.

Nel primo caso, occorre registrare il nominativo del dipendente per poter dare evidenza del suo rifiuto, con le conseguenze normativamente previste.

Nel secondo caso, è possibile, oltre che registrare i dati personali del dipendente, conservare il relativo screen shot.

Una comunicazione di dati, in particolare, è prevista in almeno due situazioni.



La sanzione di cui all'art. 4 del D.L. 25 marzo 2020, n. 19 così come convertito con modificazioni dalla L. 22 maggio 2020, n. 35 (pagamento di una somma da euro 400 a euro 1.500), ai sensi dell'art. 8 del D.L. 127/2021, è irrogata dal Prefetto, e gli atti relativi alla violazione gli devono essere comunicati.

Inoltre, qualora il dipendente esterno sia stato trovato non in possesso della certificazione verde, di ciò deve essere data evidenza al suo datore di lavoro.

Le operazioni eseguite possono essere effettuate con procedure informatizzate (quindi i dati sono trattati su supporti informatici, ad esempio gli applicativi aziendali, in particolare quello per la gestione del personale, cfr. § successivo) che con supporti cartacei.

### **7. Conservazione dei dati personali**

I dati sono conservati per il tempo previsto dalla vigente normativa; in particolare, relativamente alla situazione di assenza ingiustificata viene inserito nel sistema di gestione delle presenze un codice specifico che viene conservato, così come i cartellini personali in cui è ricompreso, per 10 anni.

### **8. Trasferimento Extra UE dei dati personali**

I dati non saranno oggetto di trattamento in paesi fuori dall'Unione Europea.

### **9. Esercizio dei diritti**

L'interessato ha diritto, se lo desidera, di:

- accedere ai dati personali che lo riguardano;
- chiederne la rettifica, l'integrazione e, ove applicabile, la cancellazione (la cancellazione dei dati non è prevista laddove il trattamento sia necessario per l'esecuzione di un compito di interesse pubblico: anche in questi casi, è comunque possibile la cancellazione di dati non essenziali rispetto agli obblighi di documentazione prescritti);
- chiedere, ove applicabile, la limitazione del trattamento (cioè la temporanea sottoposizione dei dati, in casi particolari tassativamente elencati all'art. 18 del Regolamento Generale, alla sola operazione di conservazione, in attesa di verifiche da effettuarsi oppure per assicurare particolari pretese dell'interessato).
- opporsi al trattamento dei dati personali.

Le istanze relative all'esercizio di tali diritti potranno essere presentate al Responsabile per la protezione dei dati personali o al Titolare del trattamento agli indirizzi mail sotto indicati

Infine, si ritenga che il trattamento dei dati personali avvenga in violazione di quanto previsto dalle vigenti normative, si può proporre reclamo al Garante, come previsto dall'art. 77 del Regolamento Generale adire le opportune sedi giudiziarie (art. 79 del Regolamento Generale).



## **10. Dati di contatto**

Titolare del trattamento dei dati è l'Azienda Ospedaliero-Universitaria Careggi, con sede legale in L.go Brambilla 3 50134 Firenze.

Rappresentante Legale: Direttore Generale pro tempore, tel.0557949501, e-mail [segreteriaadg@aou-careggi.toscana.it](mailto:segreteriaadg@aou-careggi.toscana.it) [aoucareggi@pec.it](mailto:aoucareggi@pec.it)

Responsabile per la protezione dei dati personali, tel.0557979067 cell. 3666823917, e-mail: [rpd@aou-careggi.toscana.it](mailto:rpd@aou-careggi.toscana.it)

Autorità di controllo: Garante per la protezione dei dati personali, [www.garanteprivacy.it](http://www.garanteprivacy.it), e-mail [garante@gpdp.it](mailto:garante@gpdp.it), centralino tel. 06696771