PRIVACY

Passaporto vaccinale e GDPR: il parere delle istituzioni europee

Il parere dello European Data Protection Board e dello European Data Protection Supervisor sul passaporto vaccinale indica che i lavori sono a buon punto ma, specie su valutazione dei rischi e misure di sicurezza per la protezione dei dati personali, servono ulteriori chiarimenti e proposte della Commissione Europea

16 Apr 2021

G Adriano Garofalo
Studio De Berti Jacchia Franchini Forlani

Il 6 aprile lo **European Data Protection Board** (EDPB) e lo **European Data Protection Supervisor** (EDPS) hanno pubblicato un parere condiviso sulla proposta di regolamento inerente al Digital Green Certificate o "**passaporto vaccinale**" pubblicata dalla Commissione il 17 marzo, la cui introduzione ci permetterà di viaggiare liberamente all'interno dell'Unione Europea e di lasciare alle spalle le limitazioni al libero movimento delle persone.

L'avvento di questo certificato è, senza dubbio, molto atteso, tuttavia, considerate la mole e la natura dei **dati personali** coinvolti, nonché i potenziali rischi per i **diritti e le libertà fondamentali** dei cittadini europei, è necessario fare i conti con le evidenti difficoltà che possono caratterizzare la definizione di tale regolamento alla luce, soprattutto, dei principi sanciti dal Regolamento (UE) 2016/679 (GDPR).

Indice degli argomenti

Passaporto vaccinale: le indicazioni di EDPB ed EDPS

In base a quanto affermato nel Parere, la proposta dovrebbe essere integrata ai fini di una migliore e più precisa definizione delle finalità per cui il Digital Green Certificate sarà introdotto, fermo restando che la finalità primaria è quella di garantire la **libertà di movimento tra gli Stati membri** in conformità alla Carta dei Diritti Fondamentali dell'Unione Europea.

E-mail aziendale

Selezionando questa casella, confermo di voler ricevere comunicazioni di marketing e informazioni su prodotti, servizi ed eventi da OpenText. Sono consapevole di poter annullare la mia iscrizione in qualsiasi momento. Per ulteriori dettagli su come OpenText condivida, protegga, conservi e trasmetta i dati personali consulti: OpenText Privacy Policy. Le nostre cookie policy possono essere consultate qui.

SCARICA ORA

La ratio di tale raccomandazione risiede nella necessità di salvaguardare i cittadini dalla possibilità di essere discriminati: ad esempio, gli Stati membri potrebbero far sì che il Digital Green Certificate sia un requisito necessario per entrare in negozi, ristoranti, luoghi di culto, palestre o, addirittura, identificarlo quale requisito per essere assunti o potersi recare presso il luogo di lavoro.

Infatti, l'EDPB e l'EDPS ritengono che, qualora gli Stati membri cerchino di utilizzare il Digital Green Certificate per tali scopi ulteriori rispetto a quello dichiarato nella Proposta, si potrebbe incorrere in conseguenze e rischi collaterali per i diritti fondamentali dei cittadini europei e sottolineano che **l'ulteriore utilizzo del Digital Green Certificate, effettuato in base alla normativa nazionale, non dovrebbe mai portare legalmente o de facto a discriminazioni sulla base dell'essere stati (o meno) vaccinati**.

Per questo motivo sottolineano che **eventuali tali ulteriori utilizzi dovranno avvenire in maniera compatibile con la finalità primaria** sopra citata e **nel pieno rispetto delle normative europee** e, in particolare, dei principi di pertinenza, necessità, proporzionalità del trattamento.

Gli Stati membri che ricorrono ad ulteriori utilizzi del certificato dovranno regolarli in maniera molto precisa, prevedendo misure rafforzate e specifiche a tutela delle libertà e dei diritti fondamentali delle persone, decise in seguito ad una valutazione dei rischi per tali libertà e diritti, vietando qualsiasi conservazione dei dati, ove possibile.

La normativa nazionale dovrà indicare con precisione le caratteristiche del trattamento, ivi incluse, in particolare, la base giuridica, la finalità, le categorie di soggetti coinvolti nel trattamento e le misure adottate per prevenire un utilizzo abusivo del certificato.

L'Unione Europea dovrebbe controllare l'operato degli Stati membri e, pertanto, EDPB ed EDPS suggeriscono l'istituzione di un meccanismo per il monitoraggio sul loro uso del certificato.

In sintesi, gli Stati membri potranno sfruttare il Digital Green Certificate per scopi ulteriori che siano compatibili con quelli stabiliti dalla Commissione Europea, ma, considerati i rischi per la privacy dei cittadini ed il pericolo concreto che questi ultimi possano essere discriminati, dovranno attenersi scrupolosamente a quanto stabilito dalla legislazione europea, ivi inclusi il Regolamento sul Digital Green Certificate, il GDPR e la Carta dei Diritti Fondamentali dell'Unione Europea.

Alcuni specifici rilievi dell'EDPB e dell'EDPS

Minimizzazione dei dati

L'EDPB e l'EDPS sottolineano come sia apprezzabile che la

Proposta sia stata complessivamente redatta tenendo conto del principio fondamentale secondo cui, data la finalità che si intende perseguire, è necessario limitare al minimo i dati personali trattati, tuttavia, hanno rilevato che l'Allegato I alla Proposta, che definisce le categorie e i campi che, una volta compilati, conterranno i dati personali che saranno trattati nell'ambito del Digital Green Certificate, non sia sufficientemente chiaro ed esaustivo nel delineare le ragioni per cui è necessario trattare i dati che saranno indicati in ciascuno degli specifici campi.

Periodo di conservazione dei dati

Il Parere evidenzia come la Proposta non chiarisca il periodo di validità del Digital Green Certificate e che ciò, conseguentemente, comporti una definizione altrettanto incerta del periodo di conservazione dei dati personali oggetto del certificato.

L'EDPB e l'EDPS hanno, pertanto, richiesto che la Proposta definisca, ove possibile, dei precisi tempi di conservazione o che, alternativamente, stabilisca i criteri in base al quale determinare tali periodi di conservazione.

Limitazione della finalità

EDPB ed EDPS hanno rilevato che il campo "patologia o agente dal quale il cittadino è guarito" dovrebbe essere compilato limitandosi a inserire il Covid19, varianti incluse, senza lasciar spazio a differenti interpretazioni.

Infatti, il certificato non deve contenere indicazione di ulteriori

patologie che sono al di fuori del perimetro delle finalità per cui il Digital Green Certificate sarà istituito, le quali ineriscono esclusivamente il Covid19.

Misure di sicurezza

È interessante notare come l'EDPB e l'EDPS, oltre a richiedere che la Proposta venga integrata richiamando espressamente la necessità di proteggere i dati personali con misure di sicurezza adeguate rispetto ai rischi per la privacy degli interessati (come previsto dall'art. 32 del GDPR), invitino la Commissione Europea a specificare le misure di sicurezza che obbligatoriamente dovranno essere adottate.

L'EDPB e l'EDPS, quindi, derogano parzialmente il risk-based approach che caratterizza il predetto art. 32, in base al quale il titolare o responsabile del trattamento deve valutare autonomamente il rischio del trattamento e, di conseguenza, implementare misure di sicurezza adeguate per proteggere i dati personali.

Il Parere suggerisce, invece, che ciascun titolare o responsabile dovrà implementare contestualmente sia le misure di sicurezza obbligatorie per legge sia quelle individuate in base ad una valutazione risk based; ciò, da un lato, rappresenta un aspetto molto particolare e un interessante spunto per riflessioni più approfondite sul risk-based approach che costituisce una delle anime del GDPR, dall'altro, suona come un campanello d'allarme, apparendo come la dimostrazione dell'essere di fronte ad uno dei

trattamenti di dati personali più rischiosi mai effettuati per la privacy dei cittadini europei e sul quale, come sottolineato nel Parere, ad oggi non è stata effettuata alcuna valutazione d'impatto ex art. 35 del GDPR.

Diritti degli interessati, trasparenza e ruoli del trattamento

Il Parere sottolinea come sia necessario definire con precisione il ruolo dei soggetti coinvolti nel trattamento dei dati personali.

In particolare, è importante che la Proposta sia estremamente chiara con riferimento a tale definizione, poiché dovrebbe essere istituito un elenco pubblico di tutti i soggetti che tratteranno i dati personali in qualità di titolari, responsabili e destinatari.

La redazione e pubblicazione di questo elenco consentirebbe ai cittadini di conoscere agevolmente l'identità del soggetto cui possono rivolgersi per esercitare i propri diritti in materia di protezione dei dati personali.

A tal fine, inoltre, il Parere sottolinea l'importanza dell'effettiva applicazione del principio della trasparenza, che dovrà trovare riscontro in un'adeguata informativa agli interessati.

Trasferimento di dati al di fuori dello Spazio Economico Europeo ("SEE")

In base al considerando 39 della Proposta non è escluso che i dati personali possano essere trasferiti al di fuori del SEE. A tal proposito, considerati i rischi ulteriori che caratterizzano il trattamento in caso di trasferimento di dati extra SEE, il Parere

evidenzia la necessità di chiarire esplicitamente se e quando sono previsti tali trasferimenti di dati personali e di definire misure di garanzia idonee ad assicurare che i dati personali, anche se trasferiti al di fuori del SEE, saranno utilizzati solo ed esclusivamente per le finalità indicate dalla Commissione Europea e specificate nella Proposta.

Conclusioni

Complessivamente lo stato dei lavori sembra a buon punto anche se, soprattutto con riferimento alla valutazione dei rischi e alla determinazione delle misure di sicurezza per la protezione dei dati personali, sarà necessario attendere ulteriori chiarimenti e proposte ad opera della Commissione Europea.

Pur sollecitando una maggiore precisione relativa ad alcuni elementi chiave della Proposta, il Parere non manca di sottolinearne, in numerose occasioni, gli aspetti positivi dal punto di vista della protezione dei dati personali, il che è in controtendenza rispetto ad alcuni precedenti pareri congiunti di EDPB ed EDPS, come, ad esempio, l'opinione congiunta sulla proposta di Data Governance Act.

Alla luce di quanto sopra, riteniamo di poter concludere con una nota di ottimismo, confidando che il giorno in cui si potrà tornare a spostarci liberamente non sia lontano.

SAP GRC - Dall'IT alle Operations al Legal, proteggi il tuo patrimonio aziendale!

Legal

Manifatturiero/Produzione

Leggi l'informativa sulla privacy

E-mail

E-mail aziendale

☐ Consente l'invio di comunicazioni promozionali inerenti i prodotti e servizi di soggetti terzi rispetto alle Contitolari che appartengono al ramo manifatturiero, di servizi (in particolare ICT) e di commercio, con modalità di contatto automatizzate e tradizionali da parte dei terzi medesimi, a cui vengono comunicati i dati.

SCARICA IL WHITE PAPER

Personaggi