Il ‘Sistema di Allerta Covid-19’ nazionale è partito con l’app Immuni, dopo l’autorizzazione del Garante Privacy. Pubblicate anche le modalità tecniche per il coinvolgimento del Sistema Tessera Sanitaria

Author : Sergio Guida

Date : 22 Giugno 2020

Dal 15 giugno l’App Immuni è utilizzabile in tutta Italia e ci si augura che presto venga scaricata dal maggior numero possibile di persone, in quanto strumento prezioso nella strategia globale di lotta alla pandemia.

Per attuare gli strumenti di *contact tracing*[1] secondo le indicazioni fornite dal nostro Garante per la Privacy e dalle Autorità europee, in un *continuum* ideale e valoriale, un requisito fondamentale era rappresentato da una fonte normativa che ne sancisse l’assoluta necessità, sicché in data 30 aprile 2020, sono state approvate[2] le "*misure urgenti per l'introduzione del sistema di allerta Covid-19*", in particolare al Capo II, art. 6, dove viene descritto il “**Sistema di allerta Covid-19**”.

Il comma 1 stabilisce che *“al solo fine di allertare le persone che siano entrate in contatto stretto con soggetti risultati positivi e tutelarne la salute attraverso le previste misure di prevenzione nell'ambito delle misure di sanità pubblica legate all'emergenza COVID-19, é istituita una **piattaforma unica nazionale** per la gestione del sistema di allerta dei soggetti che, a tal fine, hanno installato, su base volontaria, un'apposita applicazione sui dispositivi di telefonia mobile”.*

Il titolare del trattamento è il Ministero della Salute, che si coordina, sentito il Ministro per gli affari regionali e le autonomie, anche ai sensi dell'articolo 28 del Regolamento (UE) 2016/679 (GDPR), con i soggetti operanti nel Servizio nazionale della protezione civile, nonché con l'Istituto superiore di sanità e, anche per il tramite del **Sistema Tessera Sanitaria**, con le strutture pubbliche e private accreditate del Servizio sanitario nazionale, *“nel rispetto delle relative competenze istituzionali in materia sanitaria connessa all'emergenza epidemiologica da COVID 19, per gli ulteriori adempimenti necessari alla gestione del sistema di allerta e per l'adozione di correlate misure di sanità pubblica e di cura”*.
Le modalità operative del sistema di allerta tramite la piattaforma informatica sono complementari alle ordinarie modalità in uso nell'ambito del Servizio sanitario nazionale (cd.

‘*tracciamento manuale dei contatti’*).

In ottemperanza alle prescrizioni del Regolamento (UE) 2016/679, il Ministero della salute:

- dopo una valutazione di impatto, effettuata ai sensi dell'art.35,
- ha adottato misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato ai rischi elevati per i diritti e le libertà' degli interessati,
- sentito il Garante per la protezione dei dati personali ai sensi dell'art.36, par. 5, e dell'articolo 2-quinquiesdecies del ‘Codice in materia di protezione dei dati personali’[3].

Era infatti necessario assicurare, in particolare, che:

a) gli utenti ricevessero, prima dell'attivazione dell'app, informazioni chiare e trasparenti, ai sensi degli artt.13 e 14, al fine di raggiungere una piena consapevolezza, in particolare, sulle finalità e sulle operazioni di trattamento, sulle tecniche di pseudonimizzazione utilizzate e sui tempi di conservazione dei dati;
b) per impostazione predefinita, in conformità all'art.25, i dati personali raccolti fossero esclusivamente quelli necessari ad avvisare gli utenti dell'applicazione di rientrare tra i contatti stretti di altri utenti accertati positivi al COVID-19 (individuati secondo criteri stabiliti dal Ministero della salute), nonché ad agevolare l'eventuale assistenza sanitaria in loro favore;
c) il trattamento effettuato per allertare i contatti fosse basato sul trattamento di dati di prossimità dei dispositivi, resi anonimi oppure, ove ciò non sia possibile, pseudonimizzati; *“è esclusa in ogni caso la geo-localizzazione dei singoli utenti”*;
d) fossero garantite su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento nonché misure adeguate ad evitare il rischio di reidentificazione degli interessati cui si riferiscono i dati pseudonimizzati oggetto di trattamento;
e) i dati relativi ai contatti stretti fossero conservati, anche nei dispositivi mobili degli utenti, per il periodo strettamente necessario al trattamento, la cui durata é stabilita dal Ministero della salute e specificata nell'ambito delle presenti misure; i dati fossero infine cancellati in modo automatico alla scadenza del termine;
f) i diritti degli interessati (artt. 15- 22) potessero venire esercitati anche con modalità semplificate.

I dati raccolti attraverso l'app non possono essere trattati per finalità diverse da quelle sopra indicate, salva la possibilità di utilizzo in forma aggregata o comunque anonima, per soli fini di sanità pubblica, profilassi, statistici o di ricerca scientifica, ai sensi degli artt. 5, paragrafo 1, lettera a) e 9, paragrafo 2, lettere i) e j), del Regolamento (UE) 2016/679.

Viene espressamente ribadita la **volontarietà** dell’utilizzo: *“il mancato utilizzo dell'applicazione non comporta alcuna conseguenza pregiudizievole ed é assicurato il rispetto del principio di parità di trattamento”.*

La piattaforma informatica *“è di titolarità pubblica ed è realizzata dal Commissario Straordinario per l’attuazione e il coordinamento delle misure di contenimento e contrasto dell’emergenza epidemiologica Covid-19”*. Utilizza solo infrastrutture pubbliche situate all'interno dei confini

nazionali ed è gestita esclusivamente dalla società pubblica Sogei SpA. Il codice sorgente è stato sviluppato per la presidenza del Consiglio dei ministri da Bending Spoons SpA ed è rilasciato sotto licenza GNU Affero General Public License (versione 3). L'utilizzo dell'App e della piattaforma, nonché ogni trattamento di dati personali dovranno essere interrotti alla data di cessazione dello stato di emergenza disposto con delibera del Consiglio dei ministri del 31 gennaio 2020, e comunque non oltre il 31 dicembre 2020, ed entro la medesima data tutti i dati personali trattati dovranno essere cancellati o resi definitivamente anonimi.

In data 1 giugno 2020, il Garante per la protezione dei dati personali ha autorizzato il Ministero della salute ad avviare il trattamento relativo al "Sistema di allerta Covid-19" (app "Immuni")[4], sicché da pari data l'app è disponibile sugli *store* digitali di Apple e Google.

Come si legge nel Provvedimento, sulla base della valutazione d'impatto effettuata dal Ministero, il trattamento di dati personali effettuato nell'ambito del Sistema *"può essere considerato proporzionato, essendo state previste misure volte a garantire in misura sufficiente il rispetto dei diritti e le libertà degli interessati, che attenuano i rischi che potrebbero derivare da trattamento".*

Tuttavia, anche a causa della complessità del sistema e del numero dei soggetti coinvolti, **il Garante ha voluto indicare una serie di misure**, volte a rafforzare la sicurezza dei dati degli utenti dell'app; in particolare, l'Autorità ha disposto che, utilizzando anche il periodo di test che dall'8 giugno ha riguardato quattro regioni (Abruzzo, Liguria, Marche e Puglia):

- gli utenti fossero informati adeguatamente in ordine al funzionamento dell'algoritmo di calcolo utilizzato per la valutazione del rischio di esposizione al contagio;
- fossero portati a conoscenza del fatto che il sistema potrebbe generare notifiche di esposizione che non sempre riflettono un'effettiva condizione di rischio;
- avessero inoltre la possibilità di disattivare temporaneamente l'App, attraverso una funzione facilmente accessibile nella schermata principale;
- fosse anche garantita la trasparenza del trattamento a fini statistico-epidemiologici dei dati raccolti e individuate modalità adeguate a proteggerli, evitando ogni forma di riassociazione a soggetti identificabili e adottando idonee misure di sicurezza e tecniche di anonimizzazione;
- venissero introdotte misure volte ad assicurare il tracciamento delle operazioni compiute dagli amministratori di sistema sui sistemi operativi, sulla rete e sulle basi dati;
- la conservazione degli indirizzi Ip dei cellulari venisse commisurata ai tempi strettamente necessari per il rilevamento di anomalie e di attacchi;
- venissero adottate misure tecniche e organizzative per mitigare i rischi derivanti da "falsi positivi";
- particolare attenzione fosse dedicata all'informativa e al messaggio di allerta, tenendo altresì conto del fatto che è previsto l'uso del Sistema anche da parte di minori ultra quattordicenni.

Il Garante ha sottolineato infine che il trattamento di dati personali raccolti attraverso l'app *"da parte di soggetti non autorizzati può determinare un trattamento di dati personali illecito, eventualmente anche sotto il profilo penale".*

Dal canto suo, il 3 giugno 2020 il Ministero dell'Economia e delle Finanze è intervenuto a indicare le “modalità tecniche per il coinvolgimento del ‘**Sistema Tessera Sanitaria**’ ai fini dell'attuazione delle misure di prevenzione nell'ambito delle misure di sanità' pubblica legate all'emergenza COVID-19”[5].

Il Sistema TS (di cui è titolare il Ministero dell'economia e delle finanze) rende disponibili all'operatore sanitario (l'operatore del Dipartimento di prevenzione della ASL autorizzato ad accedere al Sistema TS per la trasmissione al Sistema di allerta Covid-19 dei dati raccolti mediante l’app), anche tramite «SAR» (il Sistema di accoglienza regionale), le funzionalità per la trasmissione dei dati[6], secondo le seguenti modalità.

In caso di esito positivo di un tampone, l'operatore sanitario contatta il paziente per effettuare l'indagine epidemiologica, che prevede anche la verifica dell'installazione dell'App Immuni: se il paziente l’ha installata, gli sarà richiesto di aprirla e di utilizzare la funzione di generazione del codice OTP (*One time password* di durata temporale limitata). Il paziente comunica i 10 caratteri del codice OTP all'operatore sanitario e attende l'autorizzazione a procedere con l'*upload* delle proprie TEK (*Temporary exposure key*, chiave crittografica casuale generata da un telefono cellulare o altro dispositivo «mobile» dotato dell'App).

L'operatore sanitario, secondo le modalità descritte nell'Allegato A del decreto, accede al Sistema TS e, in virtù del particolare profilo attribuito, inserisce i dati forniti dal paziente concernenti:

Messaggio di richiesta

Campo	Descrizione	Obbligatorio
Codice OTP	Codice One Time Password	SI
Data inizio sintomi	Data di inizio dei sintomi	SI

Il Sistema TS invia i dati al server di *backend* del Sistema di allerta Covid-19:

Messaggio di risposta

Campo	Descrizione	Fonte
Identificativo transazione	Identificativo alfanumerico della transazione, generato dal sistema	Sistema TS
Data-ora	Data-ora-minuti-secondi-millisecondi in cui si e' conclusa la transazione	Sistema TS
Esito	Esito della transazione	Backend App Immuni

Di seguito evidenzio alcuni dei punti di maggiore interesse - in ottica *data protection & privacy* - relativi alle modalità tecniche di trasmissione da parte degli operatori sanitari dei dati alla componente di *backend,* descritte appunto nell'Allegato A del decreto MEF.

Accesso al servizio

Le possibilità di accesso al servizio da parte dell'operatore sanitario sono riassunte nella seguente tabella, che indica gli utenti che possono accedere al sistema TS attraverso sistemi software con interfacce web o *web services*, oppure per il tramite di sistemi regionali (SAR):

ID	Utente	Modalita'	Autenticazione	Note
1	Operatore sanitario che accede tramite SAR	Web service tramite SAR	Autenticazione a 2 fattori, CNS, CIE, SPID	L'operatore sanitario si connette al sistema regionale che a sua volta invoca il servizio tramite client applicativo. Certificato di autenticazione rilasciato dal Sistema TS. Il codice fiscale dell'operatore viene trasmesso come campo applicativo nel tracciato. Il sistema regionale deve garantire i requisiti minimi di sicurezza adottati dal Sistema TS in termini di autenticazione forte, nel tracciato viene dichiarata la tipologia di autenticazione: 2 fattori, CNS, CIE, SPID.

				L'operatore sanitario invoca il servizio tramite software gestionale. Credenziali di autenticazione rilasciate dal Sistema TS.
2	Operatore sanitario	Web service tramite software gestionale	TS-CNS oppure CNS oppure basic authentication (ID utente e password) con pincode come fattore di autenticazione	
				L'operatore sanitario invoca il servizio tramite interfaccia web. Credenziali di autenticazione rilasciate dal Sistema TS.
3	Operatore sanitario	Applicazione web	TS-CNS oppure CNS oppure basic authentication (ID utente e password) con pincode come fattore di autenticazione	

Registrazione degli accessi applicativi e tempi di conservazione

Il servizio non costituisce né alimenta alcuna banca dati contenuta nel Sistema TS, in quanto la sua finalità é la trasmissione dei dati al *backend* dall'app. Il sistema registra unicamente gli accessi all'applicazione e l'esito dell'operazione, e inserisce i dati dell'accesso in un archivio dedicato. In nessun caso sono tracciati i dati applicativi (OTP, data inizio sintomi), né su banca dati né su file di log. I log degli accessi così descritti sono conservati per dodici mesi.

Misure di sicurezza

Infrastruttura fisica

L'infrastruttura fisica é realizzata dal Ministero dell'economia e delle finanze attraverso l'utilizzo dell'infrastruttura del Sistema tessera sanitaria. I locali sono sottoposti a videosorveglianza continua e sono protetti da qualsiasi intervento di personale esterno. L'accesso ai locali avviene secondo una documentata procedura, prestabilita dal titolare del trattamento, che prevede l'identificazione delle persone che accedono e la registrazione degli orari di ingresso e di uscita di tali persone.

Registrazione degli utenti ed assegnazione degli strumenti di sicurezza

L’infrastruttura di *Identity* e *Access Management* censisce direttamente le utenze, accogliendo

flussi di autenticazione e di autorizzazione, per l'assegnazione dei certificati *client* di autenticazione, delle credenziali di autenticazione e delle risorse autorizzative. Il certificato viene emesso con un sistema di **crittografia asimmetrica** a chiave pubblica/privata. Il sistema effettua la gestione completa del certificato di autenticazione: assegnazione, ri-emissione alla scadenza, revoca.

La gestione dei profili di autorizzazione é effettuata sempre dagli amministratori di sicurezza delle ASL: *“a tutti gli operatori sanitari che devono essere autorizzati viene assegnata una risorsa di autorizzazione creata e dedicata appositamente al servizio descritto dal presente decreto. Gli amministratori di sicurezza si autenticano con le credenziali in* basic authentication. *Entro sessanta giorni dalla data di adozione del decreto saranno dotati di strumenti di autenticazione forte. La gestione degli amministratori di sicurezza delle ASL é effettuata dall'Amministratore centrale della sicurezza. L'Amministratore centrale della sicurezza é nominato tra gli incaricati del trattamento”.*

Sistemi e servizi di backup e disaster recovery

Non sono previsti sistemi e servizi di *backup* e *disaster recovery* per i log di accesso in quanto non necessari per le finalità di trattamento dei dati del servizio. Tali sistemi non sono previsti nemmeno per i dati: infatti, poiché il sistema non prevede una banca dati e registra unicamente gli accessi al servizio, l’eventuale perdita delle informazioni registrate non pregiudicherebbe l'utilizzo né l'efficienza del servizio, in quanto il codice OTP ha durata limitata, non è in alcun modo riconducibile all'interessato, e comunque può essere rigenerato in qualunque momento dal dispositivo «mobile». È unicamente previsto il backup dei sistemi.

Accesso ai sistemi

L'infrastruttura dispone di sistemi di tracciamento degli accessi ai sistemi informatici di supporto come base dati, server web e infrastrutture a supporto del servizio.

L'accesso alla base dati avviene tramite utenze nominali e il sistema di tracciamento registra (su appositi log) le seguenti informazioni: identificativo univoco dell'utenza che accede, data e ora di login, logout e login falliti, postazione di lavoro utilizzata per l'accesso (IP client), tipo di operazione eseguita sui dati (ad esclusione delle risposte alle *query*).

Per ogni accesso ai sistemi operativi, ai sistemi di rete, al software di base e ai sistemi complessi (anche da parte degli amministratori di sistema), il sistema di tracciamento registra (su appositi log) le seguenti informazioni: identificativo univoco dell'utenza che accede, data e ora di login, logout e login falliti, postazione di lavoro utilizzata per l'accesso (IP client).

I log prodotti dai sistemi di tracciamento infrastrutturali sono soggetti a **monitoraggio costante** allo scopo di individuare eventuali anomalie inerenti alla sicurezza (accessi anomali, operazioni anomale, ecc.) e di valutare l'efficacia delle misure implementate.

I log di accesso degli amministratori di sistema e degli incaricati sono protetti da eventuali tentativi di alterazione e dispongono di un sistema di verifica della loro integrità. I log relativi agli

accessi e alle operazioni effettuate sui sistemi operativi, sulla rete, sul software di base e sui sistemi complessi sono conservati per dodici mesi.

Sin dalla sua attivazione, secondo gli ultimi aggiornamenti, l'app Immuni è stata scaricata da **2,5 milioni di persone**. Se ne auspica la sua più ampia diffusione, in quanto è uno strumento fondamentale nella lotta alla pandemia, non solo perché consente di affinare sempre più i dati epidemiologici, statistici e di ricerca scientifica, ma soprattutto per prevenire 'attivamente' il contagio massivo: in definitiva, *"più persone la scaricano, maggiore sarà la sua efficacia"*, come è stato detto e ripetuto da più parti.

Note

[1] Per ampi dettagli scientifici, tecnici e giuridici, si rinvia al White Paper a cura di Sergio Guida "*Un Framework per il Contact Tracing in Italia tra esigenze scientifiche, possibilità tecnologiche e rispetto di Diritti e Liberta' Individuali in termini di Data Protection*", in corso di pubblicazione.

[2] Con il Decreto Legge n. 28 "*Misure urgenti per la funzionalità' dei sistemi di intercettazioni di conversazioni e comunicazioni, ulteriori misure urgenti in materia di ordinamento penitenziario, nonché disposizioni integrative e di coordinamento in materia di giustizia civile, amministrativa e contabile e misure urgenti per l'introduzione del sistema di allerta Covid-19*", (GU n.111 del 30-4-2020).

[3] È il "*Codice Privacy*", di cui al decreto legislativo 30 giugno 2003, n. 196 integrato con le modifiche introdotte dal Decreto Legislativo 10 agosto 2018, n.101, 2018 n. 101, concernente «*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*».

[4] Con il *Provvedimento di autorizzazione al trattamento dei dati personali effettuato attraverso il Sistema di allerta Covid-19 - App Immuni* [doc. web n. 9356568], GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, Registro dei provvedimenti, n. 95 del 1° giugno 2020.

[5] È il decreto ministeriale 3 giugno 2020, *Modalità tecniche per il coinvolgimento del Sistema tessera sanitaria ai fini dell'attuazione delle misure di prevenzione nell'ambito delle misure di sanità pubblica legate all'emergenza COVID-19* (20A03083) (GU n.144 del 8-6-2020).

[6] Cfr. *"Il Ministero della salute, in qualità di titolare del trattamento ai sensi dell'art. 6, comma 1 del decreto-legge 30 aprile 2020, n. 28, ha designato il Ministero dell'economia e delle finanze quale responsabile esterno del trattamento dei dati di cui al presente decreto. La valutazione di impatto dei trattamenti effettuati nell'ambito del Sistema tessera sanitaria di cui al presente decreto è riportata nel documento di valutazione di impatto di cui all'art. 6, comma 2 del decreto-legge 30 aprile 2020, n. 28".*

Articolo a cura di **Sergio Guida**