Ordinanza ingiunzione nei confronti di Istituto Nazionale Assicurazione Infortuni sul Lavoro - 28 aprile 2022 [9771184]

VEDI ANCHE NEWSLETTER DEL 30 MAGGIO 2022

[doc. web n. 9771184]

Ordinanza ingiunzione nei confronti di Istituto Nazionale Assicurazione Infortuni sul Lavoro - 28 aprile 2022

Registro dei provvedimenti
n. 147 del 28 aprile 2022

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, alla quale hanno preso parte la prof.ssa Ginevra Cerrina Feroni, vicepresidente, il dott. Agostino Ghiglia e l'avv. Guido Scorza, componenti e il cons. Fabio Mattei, segretario generale;

VISTO il 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" (di seguito, "Regolamento");

VISTO il d.lgs. 30 giugno 2003, n. 196 recante "Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al 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 (di seguito "Codice");

VISTO il Regolamento n. 1/2019 concernente le procedure interne aventi rilevanza esterna, finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati al Garante per la protezione dei dati personali, approvato con deliberazione n. 98 del 4 aprile 2019, pubblicato in G.U. n. 106 dell'8 maggio 2019 e in www.gpdp.it, doc. web n. 9107633 (di seguito "Regolamento del Garante n. 1/2019");

Vista la documentazione in atti;

Viste le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del Regolamento del Garante n. 1/2000 sull'organizzazione e il funzionamento dell'ufficio del Garante per la protezione dei dati personali, doc. web n. 1098801;

Relatore l'avv. Guido Scorza;

PREMESSO

1. Premessa.

Il XX, il XX e il XX, l'Istituto Nazionale Assicurazione Infortuni sul Lavoro (di seguito, "INAIL" o "Istituto") ha notificato al Garante, ai sensi dell'art. 33 del Regolamento, tre diverse violazioni dei dati personali, verificatesi tra il 2019 e il 2020, che hanno riguardato il servizio online denominato "Sportello Virtuale Lavoratori" (di seguito, "Sportello Virtuale" o "SVL") - che fornisce una serie di servizi rivolti agli utenti lavoratori - e che hanno comportato la visualizzazione, da parte di soggetti terzi, in differenti giornate, di pratiche di infortunio e malattia professionale di altri utenti.

Lo Sportello Virtuale consente, in particolare, ai cittadini vittime di infortunio del lavoro o di malattia professionale, di visualizzare lo stato delle proprie pratiche aperte presso INAIL nonché i provvedimenti emanati dall'Istituto. Sebbene i dati strutturati trattati non siano riconducibili a categorie particolari, i provvedimenti scaricabili dall'utente contengono, di solito, anche informazioni sullo stato di salute. Gli utenti registrati al portale con il profilo "Cittadino con credenziali dispositive" (SPID, PIN Inps in federazione e credenziali INAIL rilasciate allo sportello) sono circa 400.000 (v. nota del XX, p. 1). Tali credenziali consentono l'accesso al portale dell'Istituto che espone una serie di servizi, oltre a quello oggetto di violazione. L'utente può visualizzare solo le pratiche di infortunio o malattia professionale associate al proprio codice fiscale e non sono previste operazioni dispositive.

2. Le violazioni di dati personali.

Più nel dettaglio, sulla base delle dichiarazioni rese dall'Istituto, sia in sede di notifica delle violazioni dei dati personali, sia in risposta alle successive richieste di informazioni effettuate dall'Ufficio, risulta che, tra maggio 2019 e aprile 2020, alcuni utenti hanno avuto la possibilità di visualizzare dati personali, anche relativi alla salute, di altri interessati (anch'essi utenti del servizio).

In particolare, il XX l'Istituto ha notificato al Garante una violazione dei dati personali relativa alla visualizzazione, da parte di un soggetto, in due giornate differenti, tramite lo Sportello Virtuale, di pratiche di infortunio e/o malattia professionale relative ad altri due interessati. Al riguardo, l'Istituto ha dichiarato che tali eventi sarebbero probabilmente attribuibili a una non meglio specificata "configurazione delle infrastrutture software e middleware", ipotizzando che si sia trattato "di una situazione contingente o quantomeno molto rara" e che "nonostante tutte le consultazioni di pratiche nel servizio di cui trattasi siano tracciate, l'anomalia sia tale da non lasciare informazioni nel sistema di logging" (v. nota del XX; v. anche notifica del XX).

Al fine di porre rimedio alla violazione dei dati personali, l'Istituto ha proceduto a sospendere il servizio "SVL" e ad adottare, prima di ripristinarne l'operatività, misure tecniche e organizzative volte a prevenire simili violazioni future (cfr. nota del XX). Ha precisato, inoltre, di aver informato le due persone interessate dall'episodio di violazione, fornendo al Garante copia della comunicazione inviata il XX (v. nota del XX).

Successivamente, in data XX, l'Istituto ha notificato al Garante una seconda violazione dei dati personali, avvenuta in data 22 ottobre 2019, precisando che:

> "il giorno XX una signora (madre di un lavoratore assistito) segnala via email che dopo l'accesso ai servizi on-line di INAIL usando le credenziali del figlio, ha visualizzato pratiche appartenenti ad altre persone (lei pensava omonimi del figlio). L'utente non fornisce evidenza (es. screenshot) dei dati visualizzati ma ci comunica di aver avuto accesso a pratiche non di competenza del figlio senza però dati identificativi riconducibili ad altri interessati" (v. nota del XX, p. 4);
>
> "lo Sportello Virtuale Lavoratori ha mostrato una schermata contenente dati di riepilogo di prestazioni erroneamente associate al nominativo del lavoratore senza però dati identificativi delle altre persone interessate alle prestazioni" (v. nota del XX, p. 7);

sono state avviate le opportune verifiche, al fine di constatarne la sussistenza e determinare l'effettivo rischio;

le analisi preliminari hanno evidenziato che "le informazioni personali mostrate dall'applicativo in riferimento allo stesso nominativo non sono effettivamente afferenti a pratiche di un eventuale utente omonimo ma a pratiche di altri utenti non identificabili";

gli ulteriori dettagli ottenuti dall'utente, insieme alle evidenze delle analisi effettuate, hanno consentito all'INAIL di venire a conoscenza della violazione dei dati personali il giorno 27 novembre 2019; è stato comunque "escluso che i dati mostrati fossero riferiti ad utenti omonimi o identificabili" (v. nota del XX, p. 7);

"dai dettagli ricevuti e dall'assenza di altre segnalazioni si ipotizza che si tratti degli effetti di una situazione contingente o quantomeno molto rara. La visualizzazione di dati personali e sensibili da parte di altre persone, pur appartenenti anch'esse alla categoria degli infortunati o tecnopatici, costituisce indubbiamente una violazione del diritto alla riservatezza. Il danno che il singolo potrebbe aver avuto da tale esposizione, data la episodicità e casualità dell'evento, nonché la ristretta popolazione che avrebbe potuto visualizzare i dati, sembra modesto, pur configurandosi indubbiamente una lesione alla sfera dei diritti" (v. nota del XX, p. 1);

"la violazione dei dati personali ha coinvolto complessivamente sei interessati "non identificabili" e ha riguardato, in particolare, il "tipo di pratica (malattia professionale o infortunio); iban e somme prestazioni erogate; stato di lavorazione della pratica" (v. nota del XX, p. 7).

Infine, in data 24 aprile 2020, l'Istituto ha notificato al Garante una terza violazione dei dati personali – che ha coinvolto sempre lo Sportello Virtuale – a seguito di una segnalazione di un utente che "nella sera di Mercoledì 22 Aprile 2020, tra le 21:00 e le 21:50, aprendo la sua posizione INAIL, ha visualizzato i vari provvedimenti con i relativi dati personali di utenti delle sedi di La Spezia e Palermo, per i quali fornisce due file PDF e degli screenshot associati" (v. nota del XX, p. 7). In particolare, l'Istituto ha rappresentato che:

- la violazione ha riguardato "dati relativi ad infortuni e/o malattia professionale: nome cognome, tipo di pratica (malattia professionale o infortunio); informazioni stato e avanzamento pratica" riferiti a due interessati e che la stessa è stata determinata da un "errore di processo che ha comportato la presenza in esercizio della versione errata dell'applicativo" (v. nota del XX, pp. 5 e 7);

- "la gravità della violazione è alta in quanto è possibile scaricare la documentazione in formato PDF contenente informazioni e dati personali particolari di altri utenti" (v. nota del XX, p. 9);

- ha provveduto a comunicare la violazione dei dati personali agli interessati coinvolti, fornendo copia della comunicazione inviata (v. nota del XX, pp. 4 e 5).

3. Le misure tecniche e organizzative adottate.

Per quanto attiene alle misure tecniche e organizzative adottate per porre rimedio alla violazione dei dati personali, l'Istituto ha rappresentato che, a seguito della violazione notificata il 29 novembre 2019 e per attenuarne i possibili effetti negativi nei confronti degli interessati, erano state intraprese – anche a seguito della violazione dei dati personali notificata il 16 maggio 2019 – le seguenti iniziative:

- "ripetere i test di sicurezza avvalendosi di criteri e strumenti di verifica aggiornati […]";

- “introdurre ulteriori meccanismi di logging poiché si era rilevato che, nonostante tutte le consultazioni di pratiche nel servizio di cui trattasi siano tracciate, l’anomalia era tale da non lasciare informazioni nel sistema di logging […];

- “attivare per il servizio SVL un monitoraggio particolarmente analitico al fine di comprendere le cause del problema, qualora esso dovesse ripresentarsi, fermo restando che l’anomalia sarebbe neutralizzata dall’ulteriore controllo di seguito indicato […]”;

- “in aggiunta ai controlli sulla manipolazione delle sessioni utente già implementati sui servizi dell’Istituto, introdurre un modulo centralizzato che esegua verifiche di congruenza fra le informazioni di sessione, i cookie di sessione e l’IP di provenienza delle richieste, consentendo anche un innalzamento del livello di tracking” (v. nota del XX, p. 2);

- a valle di tali interventi, “tuttavia un errore di processo ha comportato la presenza in esercizio della versione errata dell'applicativo, determinando la successiva violazione di cui alla comunicazione notificata il 24 aprile 2020” e “dal momento del caricamento della versione corretta dell’applicativo i log di cui sopra non hanno rilevato ulteriori istanze della problematica e pertanto, dai dati disponibili ad oggi, la portata della violazione e il coinvolgimento degli interessati si considera limitato a quanto comunicato all’Autorità” (v. nota del XX, p. 3).

Per quanto attiene alle misure tecniche e organizzative adottate per prevenire simili violazioni dei dati personali in futuro, l’Istituto ha dichiarato che, oltre alle misure sopra descritte, avrebbe effettuato anche “verifiche e attività di audit al fine di ottimizzare il processo di deploy. Nel dettaglio una specifica iniziativa di audit è già stata annunciata dal responsabile dell’Ufficio competente ai fini di fornire l'informativa necessaria all'Autorità Garante per la protezione dei dati personali in riferimento ad una segnalazione di data breach avvenuta per l'applicativo "Sportello Virtuale dei Lavoratori", che avrà la finalità di identificare le possibili cause che hanno generato la suddetta violazione ed identificare le possibili azioni di miglioramento al fine di evitare il ripetersi dell’evento” (v. nota del XX, p. 3).

4. L’attività istruttoria

In riscontro a una richiesta formulata dall’Ufficio del Garante (v. nota del XX, in atti), l’Istituto ha:

fornito il report contenente le risultanze emerse dall’esecuzione delle attività di audit interno in merito all’evento avvenuto in data 22 aprile 2020 sullo Sportello Virtuale;

precisato di aver contattato gli utenti che hanno avuto accesso ai dati di terzi al fine di richiedere “maggiori specifiche circa il determinarsi dell’anomalia e fornire verbalmente le indicazioni per prevenire trattamenti dei dati non consentiti (es. utilizzi illeciti, comunicazione a terzi o diffusione)”, chiedendo altresì “di cancellare quanto prima i dati ricevuti erroneamente senza farne ulteriore e improprio utilizzo”;

predisposto a tal fine un modello di comunicazione, da fornire a eventuali soggetti terzi cui dovessero in futuro essere trasmessi dati personali in modo improprio, comprensiva delle indicazioni per prevenire trattamenti di dati non consentiti (v. nota XX, p. 2);

fornito i dati statistici relativi all’utilizzo del servizio “SVL” a partire da marzo 2020 (di regola circa 10.000 accessi/mese), evidenziando come “nei mesi precedenti, a causa dei predetti eventi di data breach e le successive disattivazioni delle funzionalità coinvolte nella problematica al fine di annullare l’esposizione al rischio degli interessati, i dati non forniscono indicazioni significative dell’andamento e del volume di utilizzo del servizio” (v. nota XX p. 3).

Con nota del XX (prot. n. XX), l’Ufficio, sulla base degli elementi acquisiti dalle verifiche compiute

e dei fatti emersi a seguito dell'attività istruttoria, ha notificato all'Istituto, ai sensi dell'art. 166, comma 5, del Codice, l'avvio del procedimento per l'adozione dei provvedimenti di cui all'art. 58, par. 2, del Regolamento, avente a oggetto le presunte violazioni degli artt. 5, par. 1, lett. a) e f), 6, par. 1, lett. e), 9, par. 2, lett. g), e 32 del Regolamento, nonché 2-ter e 2-sexies del Codice nel testo antecedente alle modifiche apportate dal d.l. 8 ottobre 2021, n. 139, applicabile al caso di specie.

Con la medesima nota, l'Istituto è stato invitato a produrre al Garante scritti difensivi o documenti ovvero a chiedere di essere sentito dall'Autorità (art. 166, commi 6 e 7, del Codice, nonché art. 18, comma 1, dalla l. 24 novembre 1981, n. 689).

Con nota del XX, l'Istituto ha presentato la propria memoria difensiva, dichiarando, in particolare, che:

- "complessivamente le […] violazioni hanno determinato: la visualizzazione di dati personali di n.8 persone (primo e secondo evento di violazione); la visualizzazione e il download in formato PDF di dati personali di n. 2 persone (terzo evento di violazione)";

- "INAIL ha subito riconosciuto a tali eventi un livello di gravità alto, provvedendo a mettere in campo una serie di ulteriori contromisure di sicurezza volte alla riduzione dell'impatto e della futura probabilità di accadimento. INAIL ha tempestivamente notificato le predette violazioni dei dati personali all'Autorità e ha prontamente informato gli interessati coinvolti nelle violazioni";

- "[…] le incidentali visualizzazioni di pratiche personali da parte di soggetti terzi risultano avvenute a seguito di un incidente. Pertanto, nel trattarsi di un evento per definizione fuori controllo ed esulante dalla volontà del Titolare, non può esistere un supporto normativo al riguardo";

- "[…] l'applicazione di contromisure di sicurezza allo stato dell'arte non garantisce che non si verifichino mai problemi o incidenti; la sicurezza è infatti materia complessa, non completamente controllabile ed in continua evoluzione. Ne consegue che il verificarsi di un incidente non è sufficiente a dimostrare che la pianificazione e la progettazione delle contromisure non fosse adeguata rispetto allo stato dell'arte. A tal proposito si rappresenta che non vi sono contromisure di sicurezza derivanti dall'analisi del rischio che siano state identificate ma non implementate, né tantomeno domini di sicurezza non considerati";

- "in particolare, […] l'Istituto: opera secondo processi, utilizzando il framework ITIL V3 quale schema di riferimento; dispone di un proprio Sistema di Gestione della Sicurezza delle Informazioni (SGSI), certificato ISO27001 già a partire dal 2017; ha messo in atto misure tecniche e organizzative di sicurezza a protezione dei dati personali che tratta in ragione della propria missione istituzionale";

- "l'Istituto opera secondo le previsioni del Sistema di Gestione della Sicurezza delle Informazioni (SGSI) certificato ISO27001 risultando ad oggi tra le poche pubbliche amministrazioni ad aver raggiunto questo obiettivo";

- "il servizio SVL di cui trattasi si è avvalso e si avvale delle stesse contromisure preventive e correttive di sistemi quali quello per i finanziamenti ISI alle imprese o quello per la gestione delle denunce di infortunio, i quali sono da più di tre anni certificati ai sensi dello standard ISO-27001 e rientra nel più generale perimetro di certificazione legato al "Data Center" dell'Istituto";

- "a livello di processo INAIL utilizza, nella propria definizione del modello dei processi, il framework ITIL V3 quale schema di riferimento, finalizzato a offrire indicazioni per

l’erogazione di Servizi IT di qualità”;

- “pertanto, “il sistema SVL è stato, come le altre applicazioni INAIL, sottoposto a collaudi funzionali, collaudi di stress, prove di accessibilità e verifiche di sicurezza prima di ogni rilascio in produzione, [e] gestito in esercizio nel rispetto delle stesse procedure operative applicate per i servizi certificati secondo la norma ISO-27001, in un ambiente protetto da intrusioni e costantemente monitorato, dal punto di vista della sicurezza, dal Security Operations Center”;

- “la causa tecnica degli episodi è, a tutt'oggi, ignota, ne è mai stato possibile replicare i malfunzionamenti in un ambiente controllato, neanche simulando elevati carichi operativi. Si ritiene che la causa possa risiedere in comportamenti non documentati delle piattaforme software acquistate da INAIL (sistemi operativi, application server, ecc.), tra l’altro inseriti in una filiera complessa con forti probabilità che la causa sia in uno dei sistemi della filiera, per le quali l’Istituto non può che limitarsi ad applicare regolarmente le patch correttive distribuite dai relativi fornitori”;

- “la sequenza dei tre incidenti che hanno coinvolto il servizio SVL non dimostra quindi l'assenza di contromisure adeguate, ma il verificarsi di una risposta immediata e coerente con le previsioni del Sistema di Gestione della Sicurezza INAIL, anche se l’effetto finale è stato in parte vanificato da un errore operativo (peraltro anch’esso prontamente corretto)”;

- “il primo incidente è stato dovuto a cause non indentificate e si è presentato nonostante il sistema avesse superato, come illustrato, approfonditi controlli di sicurezza nonché meccanismi di patch management e vulnerability assessment e fosse protetto […] da appositi servizi di autenticazione e autorizzazione, oltre che da sistemi IPS, WAF, Firewall di rete, host IPS, antivirus e antimalware. Come misura atta a scongiurare ulteriori criticità si è provveduto alla sospensione delle funzionalità del servizio in oggetto. A valle delle analisi effettuate, non riuscendo a replicare in ambiente di laboratorio l’evento che ha determinato la violazione e quindi definire azioni specifiche, considerando anche la scarsa probabilità di accadimento, si è optato per mettere in campo controlli aggiuntivi sul codice fiscale dell’utente di cui vengono visualizzate le informazioni”;

- “il secondo incidente è avvenuto a valle della riabilitazione delle funzionalità di SVL, comunque protetto dalle misure di sicurezza tecniche e organizzative illustrate […], con la stessa imprevedibilità del primo incidente. Tuttavia, seguito del secondo incidente, furono introdotti nell'applicazione ulteriori controlli straordinari, comprendenti una tracciatura più granulare delle azioni applicativa al fine di identificare eventuali nuove occorrenze dell’evento, ma anche di bloccare immediatamente il funzionamento del sistema laddove l'errore si dovesse verificare”;

- “il terzo incidente avvenne a causa di un errore umano legato al processo di rilascio in ambiente di esercizio, che ha comportato la presenza in esercizio di una versione errata dell’applicativo. Il processo di avvio in produzione negli ambienti INAIL è codificato e collaudato da anni e prevede verifiche ex post dell’avvenuta transizione dei servizi nell’ambiente di esercizio. Nel caso in questione, purtroppo, un errore operativo nella fase di rilascio in produzione, impedì la pubblicazione in esercizio della versione comprensiva dei nuovi controlli aggiuntivi utili a eludere l’anomalia”.

In occasione dell’audizione, richiesta ai sensi dell’art. 166, comma 6, del Codice e tenutasi in data XX, l’Istituto, ha dichiarato, in particolare, che:

- “l’Istituto ha adottato un sistema di gestione della sicurezza delle informazioni e opera secondo processi e procedure definite; negli ultimi 3 anni l’Istituto ha ottenuto e mantenuto le certificazioni ISO 27001, ISO 9001 e ISO 20000”;

- “la Direzione centrale dell'organizzazione digitale si occupa dello sviluppo e della gestione dei servizi digitali dell’Istituto rivolti a utenti interni ed esterni, provvedendo anche a individuare e adottare misure tecniche e organizzative volte a garantire la sicurezza delle informazioni e la protezione dei dati personali”;

- “ogni servizio applicativo, prima di essere rilasciato in produzione viene sottoposto a una serie di test (prestazionali, di sicurezza, qualità statica del codice e accessibilità) che vengono effettuati da un’unità organizzativa distinta rispetto a quella che si occupa dello sviluppo; inoltre, anche il rilascio in esercizio è effettuato da un’apposita unità organizzativa; ogni attività è tracciata mediante un sistema di ticketing”;

- “oltre al monitoraggio tecnico dei servizi, la gestione degli incidenti e dei problemi è affidata a una specifica unità organizzativa che adotta metodologia ITIL”;

- “la vicenda oggetto del presente procedimento inizia nell’aprile 2019 quando un utente segnala che, accedendo allo SVL, era riuscito a visualizzare le pratiche di altri due soggetti; in quella circostanza, l’accesso allo SVL è stato tempestivamente sospeso e sono stati effettuati diversi test, anche prestazionali, volti a replicare l’evento segnalato; è stato inoltre analizzato il codice sorgente, senza riscontrare bug applicativi; l’ipotesi più accreditata è che l’incidente possa essere connesso alla gestione delle sessioni applicative sui web server che erogano il servizio; dopo aver introdotto uno specifico controllo applicativo straordinario (per verificare che le pratiche presenti nella lista visualizzata dall’utente fossero riferite all’utente autenticato), lo SVL è stato riattivato nell’autunno 2019”;

- “successivamente, a novembre 2019, un nuovo utente ha segnalato che, accedendo allo SVL, era riuscito a visualizzare pratiche riferite ad altri sei soggetti; in particolare, l’utente, pur visualizzando un elenco di pratiche di sua competenza, selezionandole accedeva a pratiche contenenti dati di altri soggetti; anche in tale occasione l’accesso allo SVL è stato sospeso al fine di accertare le cause dell’incidente; lo SVL è stato riattivato nella primavera 2020 a seguito dell’introduzione di un nuovo controllo applicativo volto a verificare che i dati presenti nelle pratiche accedute dall’utente fossero riferite all’utente autenticato”;

- “ad aprile 2020, l’Istituto ha ricevuto una nuova segnalazione da parte di un utente che riusciva a visualizzare pratiche di altri due soggetti; in tale occasione è stato accertato che la causa era di natura non tecnica ma organizzativa, in quanto la componente software che conteneva il controllo applicativo introdotto a seguito della seconda segnalazione non era stata rilasciata in esercizio per un disguido; è stato condotto un audit che ha raccomandato l’adozione di un cruscotto di monitoraggio dei ticket che rimangono nello stesso stato per troppo tempo, al fine di prevenire il verificarsi di simili problematiche in futuro”;

- “da quel momento non si è più verificata alcuna anomalia, come si evince dai log prodotti dallo SVL e dal fatto che non sono pervenute segnalazioni da parte di utenti né sono stati lamentati disservizi su altri canali (es. social network)”;

- “la tutela dei dati personali è esplicitamente richiamata anche nella politica generale della sicurezza del SGSI, la cui attuazione è attestata dalle citate certificazioni ISO”;

- “il livello di adeguatezza delle misure di sicurezza IT adottate dall’Istituto è attestato anche dal rating che BitSight ha attribuito all’Istituto, che è uno dei più elevati in Italia”;

- “le politiche adottate dall’Istituto sono conformi ai principi della sicurezza in profondità, della separazione dei ruoli e del miglioramento continuo”;

- “sistemi informativi dell’Istituto si sono sempre distinti per la loro efficienza e la costante manutenzione”;

- “l’Istituto ha adottato misure tecniche e organizzative tempestive per limitare le conseguenze negative per gli interessati coinvolti e, in ossequio ai principi di buona fede e correttezza, ha cooperato con l’Autorità nel corso del presente procedimento”;

- “l’Istituto ritiene che i trattamenti in esame siano riconducibili alle funzioni istituzionali dell’Ente e la visualizzazione da parte di ciascun utente dei propri dati personali è non solo lecita, ma anche necessaria a consentire la consultazione delle pratiche che lo riguardano gestite dall’Istituto; le violazioni dei dati personali in esame sono frutto di eventi accidentali, non caratterizzati da dolo o da colpa”.

5. Esito dell’attività istruttoria

5.1. La normativa in materia di protezione dei dati personali.

La disciplina di protezione dei dati personali prevede che il trattamento di dati personali da parte di soggetti pubblici può essere effettuato solo se necessario “per adempiere un obbligo legale al quale è soggetto il titolare del trattamento” oppure “per l’esecuzione di un compito di interesse pubblico o connesso all’esercizio di pubblici poteri di cui è investito il titolare del trattamento” (art. 6, par. 1, lett. c) ed e) del Regolamento).

La disciplina nazionale ha introdotto, inoltre, disposizioni più specifiche per adeguare l’applicazione delle norme del Regolamento, determinando, con maggiore precisione, requisiti specifici per il trattamento e altre misure atte a garantire un trattamento lecito e corretto (art. 6, par. 2, del Regolamento) e, in tale ambito, ha previsto che le operazioni di trattamento, e tra queste la “comunicazione” e la “diffusione” di dati personali, sono ammesse solo quando previste da una norma di legge o, nei casi previsti dalla legge, di regolamento (art. 2-ter, commi 1 e 3, del Codice).

Con riguardo alle categorie particolari di dati personali, inclusi quelli relativi alla salute (in merito ai quali è previsto un generale divieto di trattamento, a eccezione dei casi indicati all’art. 9, par. 2 del Regolamento e, comunque un regime di maggiore garanzia rispetto alle altre tipologie di dati, in particolare, per effetto dell’art. 9, par. 4, nonché dell’art. 2-septies del Codice), il trattamento è consentito ove “necessario per motivi di interesse pubblico rilevante sulla base del diritto dell’Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l’essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell’interessato” (art. 9, par. 2, lett. g), del Regolamento). Il legislatore nazionale ha definito “rilevante” l’interesse pubblico per il trattamento “effettuato da soggetti che svolgono compiti di interesse pubblico o connessi all’esercizio di pubblici poteri” nelle materie indicate, seppur in modo non esaustivo, dall’art. 2-sexies del Codice, stabilendo che i relativi trattamenti “sono ammessi qualora siano previsti dal diritto dell'Unione europea ovvero, 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”.

Il titolare del trattamento è tenuto a rispettare i principi di “liceità, correttezza e trasparenza”, “limitazione delle finalità”, “minimizzazione dei dati”, “esattezza”, “limitazione della conservazione” e “integrità e riservatezza”, nonché di “responsabilizzazione” (art. 5 del Regolamento).

Il titolare deve, in particolare, assicurare che i dati siano “trattati in maniera da garantire un’adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali” (art. 5, par. 1, lett. f), del Regolamento). Conformemente al predetto principio di “integrità e riservatezza”, il titolare del trattamento è tenuto a mettere in atto misure

tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio, “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”; nel valutare l'adeguato livello di sicurezza, si deve tener conto, in particolare, “dei rischi presentati dal trattamento che derivano in particolare dalla […] divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati” (art. 32 del Regolamento; cfr. anche considerando n. 83).

5.2. La comunicazione di dati personali

All’esito dell’istruttoria, è emerso che - fatta eccezione per la violazione del 29 novembre 2019, che non ha riguardato dati personali di interessati identificabili – nell’ambito delle violazioni dei dati personali notificate il 16 maggio 2019 e il 24 aprile 2020, alcuni utenti del Servizio hanno avuto la possibilità di visualizzare dati personali, anche relativi alla salute in quanto relativi a infortuni o a malattie professionali, di altri utenti (in particolare: nome, cognome, tipo di pratica – es. malattia professionale o infortunio –, informazioni su stato e avanzamento pratica).

Ciò, ha determinato, nell’ambito di trattamenti riconducibili allo svolgimento di compiti di interesse pubblico dell’Istituto, accessi non autorizzati a dati personali di terzi (utenti diversi), anche relativi alla salute (art. 4, punto 10), del Regolamento) che configurano comunicazioni dei dati personali, in violazione degli artt. 5, par. 1, lett. a), 6, par. 1, lett. e), e 9, par. 2, lett. g), del Regolamento, nonché degli artt. 2-ter e 2-sexies del Codice (nel testo antecedente alle modifiche apportate dal d.l. 8 ottobre 2021, n. 139, applicabile al caso di specie).
5.3. La sicurezza del trattamento.

Nel corso dell’istruttoria è emerso che, per quanto attiene alle violazioni dei dati personali notificate il 16 maggio 2019 e il 24 aprile 2020, il malfunzionamento sarebbe stato riconducibile, rispettivamente, a una non meglio specificata “configurazione delle infrastrutture software e middleware” e a un “errore di processo che ha comportato la presenza in esercizio della versione errata dell'applicativo”.

Al riguardo, occorre evidenziare che il titolare del trattamento è tenuto ad adottare adeguate misure tecniche e organizzative per assicurare su base permanente la riservatezza dei dati trattati, nonché l’integrità dei sistemi e dei servizi di trattamento e che, in ogni caso, deve adottare procedure “per testare, verificare e valutare regolarmente l’efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento” (cfr. art. 32, par. 1, lett. b) e d), del Regolamento).

L’Istituto ha documentato nel corso dell’istruttoria di aver adottato un sistema di gestione della sicurezza delle informazioni e di operare secondo processi e procedure, basate sul framework ITIL V3, che prevedono, tra l’altro, che ogni servizio, prima di essere rilasciato in esercizio viene sottoposto a una serie di verifiche (prestazionali, di sicurezza, qualità statica del codice e accessibilità) effettuate da un’unità organizzativa distinta rispetto a quella che si occupa delle attività di sviluppo. Tuttavia, ciò non ha impedito il verificarsi degli incidenti di sicurezza alla base delle violazioni in esame e non ha consentito, nei primi due casi, di individuarne le cause.

Peraltro, in riferimento al terzo incidente di sicurezza, come documentato e confermato dallo stesso titolare, la violazione è stata invece determinata da un “errore umano” intervenuto nel processo di rilascio in ambiente di esercizio, che è, comunque, riconducibile alla sfera di responsabilità del titolare.
Per tali ragioni, si ritiene che, al momento in cui si sono verificate le violazioni dei dati personali notificate il 16 maggio 2019 e il 24 aprile 2020, l’Istituto non avesse adottato misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato ai rischi presentati dal trattamento, determinando in tal modo le premesse delle violazioni di dati personali sopra

richiamate, in violazione degli artt. 5, par. 1, lett. f) e 32 del Regolamento.

6. Conclusioni.

Alla luce delle valutazioni sopra richiamate, si rileva che le dichiarazioni rese dal titolare del trattamento nel corso dell'istruttoria della cui veridicità si può essere chiamati a rispondere ai sensi dell'art. 168 del Codice , seppure meritevoli di considerazione, non consentono di superare i rilievi notificati dall'Ufficio con l'atto di avvio del procedimento e risultano insufficienti a consentire l'archiviazione del presente procedimento, non ricorrendo, peraltro, alcuno dei casi previsti dall'art. 11 del Regolamento del Garante n. 1/2019.

Si confermano, pertanto, le valutazioni preliminari dell'Ufficio e si rileva l'illiceità del trattamento di dati personali effettuato dall'Istituto, che ha comportato l'accesso non autorizzato da parte di soggetti diversi dagli interessati ai dati personali, anche relativi alla salute, di altri utenti, in maniera non conforme ai principi di "liceità, correttezza e trasparenza" e di "integrità e riservatezza", in assenza di un idoneo presupposto normativo e in assenza di misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio presentato dal trattamento, e, pertanto, in violazione degli artt. 5, par. 1, lett. a) e f), 6, par. 1, lett. e), 9, par. 2, lett. g), e 32 del Regolamento, nonché 2-ter e 2-sexies del Codice, nel testo antecedente alle modifiche apportate dal d.l. 8 ottobre 2021, n. 139, applicabile al caso di specie.

La violazione delle predette disposizioni rende applicabile la sanzione amministrativa prevista dall'art. 83, par. 5, del Regolamento, ai sensi degli artt. 58, par. 2, lett. i), e 83, par. 3, del Regolamento medesimo, come richiamato anche dall'art. 166, comma 2, del Codice.

In tale quadro, considerando, in ogni caso, che la condotta ha esaurito i suoi effetti, non ricorrono i presupposti per l'adozione di ulteriori misure correttive di cui all'art. 58, par. 2, del Regolamento.

7. Adozione dell'ordinanza ingiunzione per l'applicazione della sanzione amministrativa pecuniaria e delle sanzioni accessorie (artt. 58, par. 2, lett. i e 83 del Regolamento; art. 166, comma 7, del Codice).

Il Garante, ai sensi degli artt. 58, par. 2, lett. i) e 83 del Regolamento nonché dell'art. 166 del Codice, ha il potere di "infliggere una sanzione amministrativa pecuniaria ai sensi dell'articolo 83, in aggiunta alle [altre] misure [correttive] di cui al presente paragrafo, o in luogo di tali misure, in funzione delle circostanze di ogni singolo caso" e, in tale quadro, "il Collegio [del Garante] adotta l'ordinanza ingiunzione, con la quale dispone altresì in ordine all'applicazione della sanzione amministrativa accessoria della sua pubblicazione, per intero o per estratto, sul sito web del Garante ai sensi dell'articolo 166, comma 7, del Codice" (art. 16, comma 1, del Regolamento del Garante n. 1/2019).

Al riguardo, tenuto conto dell'art. 83, par. 3, del Regolamento, nel caso di specie la violazione delle disposizioni citate è soggetta all'applicazione della sanzione amministrativa pecuniaria prevista dall'art. 83, par. 5, del Regolamento, come richiamato anche dall'art. 166, comma 2, del Codice

La predetta sanzione amministrativa pecuniaria inflitta, in funzione delle circostanze di ogni singolo caso, va determinata nell'ammontare tenendo in debito conto gli elementi previsti dall'art. 83, par. 2, del Regolamento.

In relazione ai predetti elementi è stato considerato che gli incidenti di sicurezza in questione - ancorché isolati e riguardanti un numero esiguo di interessati- , sono riconducibili alla sfera di responsabilità dell'Istituto le cui rilevanti competenze istituzionali - fra cui l'assicurazione obbligatoria contro gli infortuni sul lavoro e le malattie professionali- richiedono un elevato grado di responsabilizzazione (c.d. accountability), al fine di garantire la sicurezza del trattamento che ha a

oggetto anche informazioni riconducibili alla salute di un numero elevato di interessati, spesso vulnerabili, considerata la platea di soggetti a cui si rivolgono i servizi offerti.

Di contro, si è tenuto in considerazione che le violazioni dei dati personali hanno riguardato un numero limitato di interessati (inferiore a dieci) e che, almeno in un caso, l'incidente è stato determinato da un "errore umano"; che l'Istituto ha tempestivamente notificato le predette violazioni dei dati personali all'Autorità e ha prontamente informato gli interessati coinvolti nelle violazioni, in conformità agli artt. 33 e 34 del Regolamento, adottando da ultimo, misure ritenute adeguate per porre rimedio alle violazioni e attenuarne i possibili effetti negativi nei confronti degli interessati. L'Istituto ha inoltre prestato, anche con l'ausilio del proprio Responsabile della protezione dei dati, una particolare collaborazione nel corso dell'istruttoria, provvedendo ad adottare misure tecniche e organizzative volte a conformare i trattamenti in corso alla disciplina in materia di protezione dei dati personali, nel rispetto del principio di responsabilizzazione. Non risultano, infine, precedenti violazioni pertinenti commesse dal titolare del trattamento o precedenti provvedimenti di cui all'art. 58 del Regolamento.

In ragione dei suddetti elementi, valutati nel loro complesso, si ritiene di determinare l'ammontare della sanzione pecuniaria nella misura di euro 50.000 (cinquantamila) per la violazione degli artt. 5, par. 1, lett. a) e f), 6, par. 1, lett. e), 9, par. 2, lett. g), e 32 del Regolamento, nonché 2-ter e 2-sexies del Codice, quale sanzione amministrativa pecuniaria ritenuta, ai sensi dell'art. 83, paragrafo 1, del Regolamento, effettiva, proporzionata e dissuasiva.

Tenuto conto dalla natura dei dati trattati e la rilevanza dei servizi offerti dall'Istituto sul territorio nazionale si ritiene, altresì, che debba applicarsi la sanzione accessoria della pubblicazione sul sito del Garante del presente provvedimento, prevista dall'art. 166, comma 7 del Codice e art. 16 del Regolamento del Garante n. 1/2019.

Si ritiene, infine, che ricorrano i presupposti di cui all'art. 17 del Regolamento n. 1/2019.

TUTTO CIÒ PREMESSO IL GARANTE

ai sensi dell'art. 57, par. 1, lett. a), del Regolamento, dichiara illecita la condotta tenuta dall'Istituto, descritta nei termini di cui in motivazione, consistente nella violazione degli artt. 5, par. 1, lett. a) e f), 6, par. 1, lett. e), 9, par. 2, lett. g), e 32 del Regolamento, nonché 2-ter e 2-sexies del Codice, nei termini di cui in motivazione;

ORDINA

ai sensi degli artt. 58, par. 2, lett. i) e 83 del Regolamento, nonché dell'art. 166 del Codice, all'Istituto Nazionale Assicurazione Infortuni sul Lavoro, in persona del legale rappresentante pro-tempore, con sede legale in Via IV Novembre, 144 - 00198 Roma (RM), C.F. 01165400589, di pagare la somma di euro 50.000 (cinquantamila) a titolo di sanzione amministrativa pecuniaria per le violazioni indicate in motivazione. Si rappresenta che il contravventore, ai sensi dell'art. 166, comma 8, del Codice, ha facoltà di definire la controversia mediante pagamento, entro il termine di 30 giorni, di un importo pari alla metà della sanzione comminata;

INGIUNGE

al predetto Istituto Nazionale Assicurazione Infortuni sul Lavoro, in caso di mancata definizione della controversia ai sensi dell'art. 166, comma 8, del Codice, di pagare la somma di euro 50.000 (cinquantamila) secondo le modalità indicate in allegato, entro 30 giorni dalla notificazione del presente provvedimento, pena l'adozione dei conseguenti atti esecutivi a norma dall'art. 27 della l. n. 689/1981.

DISPONE

- la pubblicazione del presente provvedimento sul sito web del Garante ai sensi dell'art. 166, comma 7, del Codice (v. art. 16 del Regolamento del Garante n. 1/2019);

- l'annotazione del presente provvedimento nel registro interno dell'Autorità, previsto dall'art. 57, par. 1, lett. u), del Regolamento, delle violazioni e delle misure adottate in conformità all'art. 58, par. 2, del Regolamento (v. art. 17 del Regolamento n. 1/2019).

Ai sensi degli artt. 78 del Regolamento, 152 del Codice e 10 del d.lgs. n. 150/2011, avverso il presente provvedimento è possibile proporre ricorso dinnanzi all'autorità giudiziaria ordinaria, a pena di inammissibilità, entro trenta giorni dalla data di comunicazione del provvedimento stesso ovvero entro sessanta giorni se il ricorrente risiede all'estero.

Roma, 28 aprile 2022

IL VICEPRESIDENTE
Cerrina Feroni

IL RELATORE
Scorza

IL SEGRETARIO GENERALE
Mattei