Ordinanza ingiunzione nei confronti di Aeroporto Guglielmo Marconi di Bologna S.p.a. - 10 giugno 2021 [9685922]

- VEDI ANCHE NEWSLETTER DEL 2 AGOSTO 2021

[doc. web n. 9685922]

Ordinanza ingiunzione nei confronti di Aeroporto Guglielmo Marconi di Bologna S.p.a. - 10 giugno 2021

Registro dei provvedimenti
n. 235 del 10 giugno 2021

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, alla quale hanno preso parte il prof. Pasquale Stanzione, presidente, 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 del n. 98 del 4/4/2019, pubblicato in G.U. n. 106 dell'8/5/2019 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 la prof.ssa Ginevra Cerrina Feroni;

PREMESSO

1. Premessa.

Nell'ambito di un ciclo di attività ispettive, avente a oggetto le principali funzionalità di alcuni tra gli applicativi per l'acquisizione e gestione delle segnalazioni di illeciti più diffusamente impiegati dai datori di lavoro pubblici e privati nel quadro della disciplina in materia di segnalazione di condotte illecite (c.d. whistleblowing), sono stati effettuati specifici accertamenti nei confronti delle società Aeroporto Guglielmo Marconi di Bologna S.p.a. (di seguito "Società" o "AdB"; v. verbali delle operazioni compiute del XX) e aiComply S.r.l. (di seguito "Fornitore", v. verbale delle operazioni compiute del XX), che fornisce e gestisce per conto della Società l'applicativo denominato "WB Confidential". Ciò anche alla luce di quanto disposto, con riguardo all'attività ispettiva di iniziativa curata dall'Ufficio del Garante, con deliberazioni del 12 settembre 2019, doc. web n. 9147297, del 6 febbraio 2020, doc. web n. 9269607, e del 1° ottobre 2020, doc. web n. 9468750.

2. L'attività istruttoria.

All'esito dell'istruttoria, stante la particolare complessità dei profili di natura tecnologica emersi nel corso dell'istruttoria (cfr. relazione tecnica del XX, prot. n. XX), è emerso che:

- il titolare del trattamento – società di capitali a partecipazione pubblica per circa il 45% del capitale sociale e quotata nei mercati regolamentati, unico gestore dell'aeroporto di Bologna, in quanto concessionario di pubblico servizio fino al 28 dicembre 2044 in virtù di una convenzione con l'Ente nazionale per l'aviazione civile (ENAC) – ha adottato un modello di organizzazione, gestione e controllo ai sensi del d.lgs. n. 231/2001 che, con l'entrata in vigore della l. n. 179/2017, è stato integrato e aggiornato con una specifica "policy whistleblowing", impiegando l'applicativo "WB Confidential";

- l'applicativo è reso disponibile dal Fornitore in modalità SaaS (Software as a Service), per l'acquisizione e la gestione delle segnalazioni di condotte illecite. A tal fine il rapporto con il Fornitore, quale responsabile del trattamento, è stato regolamentato ai sensi dell'art. 28 del Regolamento (v. verbale del XX, spec. all. 10 - atto di designazione);

- la Società rende disponibile un'informativa ai sensi del Regolamento "ai soggetti segnalanti in fase di invio di una segnalazione mediante l'applicativo WB Confidential, raggiungibile all'indirizzo web http://whistleblowing.bologna-airport.it/". La stessa informativa "è resa disponibile nella sezione informativa del medesimo applicativo, unitamente alla Policy Whistleblowing e al Manuale utente per l'utilizzo dell'applicativo" (v. verbale del XX, p. 4) anche a beneficio degli interessati che potrebbero essere menzionati all'interno delle segnalazioni ricevute dalla Società;

- "l'invio delle segnalazioni [è consentito] sia da parte dei dipendenti che da parte di altri soggetti portatori d'interesse. Le segnalazioni possono essere presentate in forma anonima o nominativa mediante l'ausilio dell'applicativo WB Confidential o in forma nominativa mediante l'utilizzo di caselle di posta elettronica dedicate, come previsto dalla Policy whistleblowing. In entrambi i casi, l'unico soggetto autorizzato a trattare i dati delle segnalazioni, accedendo all'applicativo o alle citate caselle di posta elettronica, è [… il] responsabile della funzione aziendale di Internal Audit [… che], quando accede all'applicativo, non ha la visibilità dei dati identificativi del segnalante che sono separati, a livello logico, dal contenuto della segnalazione. Solo in determinate ipotesi, stabilite nella Policy Whistleblowing, [… il responsabile] può venirne a conoscenza previa espressa richiesta alla società aiComply S.r.l." (v. verbale del XX, p. 5);

- "a seguito dell'invio di una segnalazione nominativa, l'applicativo rilascia al segnalante delle credenziali di autenticazione (username e password), che lo stesso può utilizzare per accedere all'applicativo e seguire l'andamento della segnalazione nonché effettuare un'integrazione, anche su richiesta del Responsabile della funzione Internal Audit. Nel caso di segnalazione anonima, è necessario accedere all'applicativo con credenziali di

autenticazione dedicate, riportate nel Manuale utente". Come per le segnalazioni nominative, "vengono rilasciate al segnalante delle ulteriori credenziali di autenticazione (username e password)" (v. verbale del XX, p. 4);

- inoltre, "al momento della ricezione di una segnalazione mediante l'applicativo [... il responsabile] riceve un'email di notifica sulla propria casella di posta elettronica. In base alla fattispecie oggetto di segnalazione, […] valuta il coinvolgimento del Comitato Etico ed Anticorruzione o dell'Organismo di Vigilanza, avendo cura di rimuovere, se del caso, gli elementi da cui sia possibile, anche indirettamente, risalire all'identità del segnalante. In talune circostanze, anche l'identità del segnalato può essere omessa. Qualora ne ricorrano i presupposti, la segnalazione viene inoltrata anche al Direttore Generale e/o ai Responsabili di altre funzioni aziendali, al Responsabile delle risorse umane per i profili disciplinari e/o all'Autorità Giudiziaria nel caso di fatti penalmente rilevanti" e in ogni caso "l'identità del segnalante può resa nota ai predetti soggetti solo nei casi" previsti dalla legge di settore (v. verbale del XX, p. 5);

- la Società "dispone di un unico account per l'accesso all'applicativo, assegnato al [… responsabile], a cui sono assegnati i privilegi di gestione delle segnalazioni ricevute"; inoltre, come verificato nel corso degli accertamenti, "in presenza di una segnalazione nominativa, il responsabile non è abilitato alla visualizzazione dei dati identificativi del segnalante" e che "ad ogni segnalazione è assegnato un codice identificativo (denominato "ID Ticket") con formato del tipo "SA-WB00000042" o "SN-WB00000052", dove le lettere "SA" o "SN" indicano rispettivamente il carattere anonimo o nominativo della segnalazione mentre le cifre rappresentano il numero progressivo assegnato alla segnalazione";

- nel corso delle verifiche è stata riscontrata la presenza sull'applicativo di due segnalazioni anonime di cui una archiviata (v. verbale del XX, p. 5);

- il trattamento è "censito nel registro tenuto ai sensi dell'art. 30 del Regolamento";

- la Società ha dichiarato di non aver ritenuto che fosse necessario effettuare una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35 del Regolamento, "tenuto conto anche dell'esiguo numero dei dati trattati e degli interessati coinvolti dal trattamento in questione" (v. verbale del XX, p. 2);

- è stato verificato che l'applicativo, esposto su rete Internet, non utilizza un protocollo di rete sicuro (quale il protocollo https) per il trasporto dei dati e la Società ha sul punto rappresentato di aver avviato valutazioni circa "l'opportunità di mettere in atto tale misura a garanzia della riservatezza e dell'integrità dei dati trasmessi su rete pubblica" (v. verbale del XX p. 3);

- con riguardo alle modalità di navigazione in Internet da parte dei dipendenti che sono connessi alla rete aziendale, con particolare riguardo alla navigazione sull'applicativo "WB Confidential", la Società ha rappresentato che "l'accesso alla rete pubblica avviene mediante sistemi firewall di nuova generazione, che consentono di configurare specifiche regole di navigazione in Internet, anche in ragione del ruolo delle diverse funzioni e mansioni svolte dai singoli dipendenti […e] che tali sistemi firewall memorizzano in appositi file di log le operazioni di navigazione effettuate, il cui termine di conservazione è fissato in 90 giorni, precisando che non sono state previste specifiche cautele al fine di non effettuare la registrazione delle operazioni di navigazione sull'applicativo WB Confidential" (v. verbale del XX, p. 3).

Nel corso degli accertamenti effettuati presso il Fornitore (v. verbale del XX, pp. 2 e ss.) è emerso che:

- lo stesso offre un'"attività di manutenzione specialistica, sia a livello sistemistico che a livello applicativo, in relazione all'applicativo [… "WB Confidential"] avvale[ndosi] sia di personale interno che di personale esterno di altre due società: Agic Technology S.r.l. e A1Tech S.r.l.";

- "A1Tech svolge attività di gestione sistemistica dell'infrastruttura IT del servizio offerto ad AdB, mentre Agic Technology svolge principalmente attività di manutenzione e di assistenza specialistica sull'applicativo", precisando che "nessuna delle predette società è stata designata sub-responsabile del trattamento che AiComply svolge per conto di AdB";

- l'applicativo "WB Confidential" "è stato progettato, a partire dal 2010 circa, per l'acquisizione e la gestione delle segnalazioni di condotte illecite da parte di soggetti pubblici e di istituti finanziari. L'effettiva commercializzazione dell'applicativo è avvenuta a partire dal 2015 circa";

- "l'applicativo è reso disponibile nella sua versione standard ma, a richiesta dei clienti, può essere personalizzato definendo, ad esempio, una diversa classificazione degli stati di lavorazione delle segnalazioni e delle tipologie di condotte segnalabili nonché abilitando segnalazioni non solo nominative, ma anche anonime";

- con riguardo ai trattamenti effettuati per conto della Società, "le segnalazioni sono gestite da uno o più soggetti del cliente a cui è attribuito un profilo di autorizzazione denominato "Responsabile" che consente di ricevere le segnalazioni, di trattarle, di interloquire con i segnalanti mediante l'applicativo, di cambiare lo stato della lavorazione delle segnalazioni nonché di chiudere e, se del caso, di riaprire le segnalazioni", evidenziando che "l'applicativo prevede un ulteriore profilo di autorizzazione denominato "System Administrator" a cui sono associati i massimi privilegi amministrativi per la gestione e configurazione dell'applicativo. I soggetti a cui è attribuito tale profilo di autorizzazione possono eseguire qualsiasi operazione";

- "i soggetti con il profilo di autorizzazione di "Responsabile" non hanno i privilegi per cancellare le segnalazioni presenti sull'applicativo, ancorché la loro lavorazione risulti conclusa. Tale operazione può essere effettuata, su esplicita richiesta del cliente, con procedura manuale, del tutto eccezionale, eseguita dai soggetti con il profilo "System Administrator"", precisando che "la cancellazione di una segnalazione non è consentita per impostazione predefinita ma richiede una temporanea disabilitazione di tale limitazione. Dopo aver effettuato tale operazione, è possibile cancellare manualmente i dati presenti in tre distinte tabelle contenenti la segnalazione, i dati del segnalante e i dati di accoppiamento dell'una agli altri. Tale cancellazione non è tuttavia definitiva in quanto le segnalazioni così cancellate confluiscono in un c.d. "Cestino" per un periodo di ulteriori trenta giorni, al termine dei quali le segnalazioni vengono in automatico cancellate definitivamente";

- "l'applicativo è esposto su rete pubblica e che la raggiungibilità delle singole istanze dello stesso riservate all'acquisizione e alla gestione delle segnalazioni di competenza di ciascun cliente (titolare del trattamento) è limitata ai soli indirizzi IP pubblici comunicati da ciascun cliente. Con riferimento all'istanza dell'applicativo riservata ad AdB, […] la stessa è raggiungibile da qualsiasi indirizzo IP per soddisfare la specifica richiesta di AdB di consentire l'invio di segnalazioni al di fuori della rete intranet aziendale, anche da parte di altri soggetti, portatori di interesse, esterni alla stessa";

- "le istanze dell'applicativo WB Confidential utilizzano per la trasmissione in rete dei dati il protocollo http (hypertext transfer protocol)", precisando che "sono in corso specifiche iniziative per migrare le attuali istanze dell'applicativo dal protocollo http al protocollo https";

- con riguardo all'utilizzo di strumenti di crittografia per la conservazione delle segnalazioni, "i dati memorizzati sul database non sono cifrati".
Con successiva nota del XX, la Società ha fornito "copia dei file di log generati dai sistemi firewall – che permettono la navigazione in internet, accedendo alla rete aziendale – relativi agli accessi effettuati all'applicativo WB Confidential, dal 1° febbraio al 15 aprile 2019", evidenziando come "l'estrazione non abbia riscontrato registrazioni di log antecedenti il 1 febbraio 2019". Con la medesima nota, sono state fornite ulteriori informazioni e documentazione relativa agli interventi aggiuntivi effettuati al fine di "potenziare le misure di sicurezza adottate a tutela dei diritti e delle libertà degli interessati [… e] a garanzia della tutela dell'identità dei soggetti segnalanti condotte illecite", tra i quali, in particolare:

- la modifica della "configurazione del proprio firewall, al fine di prevedere una regola specifica per il traffico destinato al server WB Confidential" (v. relazione tecnica allegata alla nota del XX);

- "l'abilitazione di un protocollo di trasmissione dati sicuro (certificato SSL) da e per la piattaforma WB Confidential";

- "l'implementazione di una nuova funzionalità della piattaforma WB Confidential […] che consente al Gestore delle segnalazioni di archiviare le segnalazioni" che in tal modo non saranno "più visibili al Gestore, sebbene recuperabili a mezzo di specifico intervento dell'Amministratore di Sistema di aiComply s.r.l., su richiesta del Gestore medesimo".

Con nota dell'XX (prot. n. XX, l'Ufficio, sulla base degli elementi acquisiti, ha notificato alla Società, 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, invitando il predetto titolare del trattamento 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 legge n. 689 del 24 novembre 1981).

Con la nota sopra menzionata, l'Ufficio ha rilevato che la Società ha posto in essere trattamenti di dati personali di dipendenti e altri interessati, mediante l'utilizzo dell'applicativo per l'acquisizione e gestione delle segnalazioni illecite, in maniera non conforme ai principi di "integrità e riservatezza", della "protezione dei dati fin dalla progettazione" e della "protezione dei dati per impostazione predefinita", in violazione degli artt. 5, par. 1, lett. f), e 25 del Regolamento; in assenza di misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato ai rischi presentati dal trattamento, in violazione dell'art. 32 del Regolamento; non avendo effettuato una valutazione di impatto sulla protezione dei dati, in violazione dell'art. 35 del Regolamento.

Con nota del XX il titolare ha fatto pervenire le proprie memorie difensive, "manifestando la […] volontà di cooperare con […l'] Autorità al fine di rimuovere i vizi contestati", allegando la documentazione necessaria a comprovare le misure a tal fine adottate con riguardo ai trattamenti in corso nei confronti della generalità dei dipendenti, e precisando, tra l'altro, che:

- "il trend di crescita, registratosi nell'ultima decade, è stato purtroppo bruscamente arrestato dai drammatici effetti prodotti sul comparto aviation dal diffondersi su scala mondiale del virus SARS-COVID-19. La crisi scaturita non ha, infatti, alcun precedente storico […]. I dati di questi primi mesi del 2021 non sono di certo più rassicuranti in termini di ripresa […]. Anche dal punto di vista economico i ricavi ed i risultati di AdB sono rilevantemente diminuiti subendo il crollo del traffico e la drammatica situazione delle compagnie aeree e degli aeroporti […]";

- "alla data del 25 maggio 2018 lo scenario giuridico di riferimento era tutt'altro che maturo e ben definito. Nelle more delle evoluzioni legislative che si sono – via via – susseguite nel

tempo fino ai giorni odierni, AdB nell'aprile 2019 risultava […] avere posto in essere […] gli adempimenti necessari per la conformità ai principi della normativa e in linea con le modalità previste dalle regolamentazioni attuative all'epoca vigenti";

- "nell'aprile 2019 […] ci si trovava ancora in un periodo di prima attuazione della normativa e che la maggior parte degli […] interventi chiarificatori sono successivi a tale periodo ed alla specifica epoca dell'ispezione condotta presso lo scalo, come, ex pluris, nel caso dell'intervento dell'Autorità Garante con provvedimento del 4 dicembre 2019 n. 9215763 in relazione ai trattamenti di Wistleblowing. Restavano, invece, valide le valutazioni che i titolari e responsabili erano chiamati ad effettuare alla luce dei principi richiamati dalla normativa (Es. art. 35 GDPR e WP n. 248 del 4 aprile 2017) e in ottica risk based";

- "AdB provvedeva immediatamente a porre in essere gli adempimenti […]. La pro-attività di AdB […] dovrebbe essere valutata positivamente nel contesto generale delle contestazioni, in quanto rappresenta da un lato, la forte volontà di AdB a collaborare in ottica costruttiva e migliorativa sulle tematiche descritte e dall'altro, dimostra la buona fede circa l'attuazione di adempimenti normativi complessi in un'epoca storica-giuridica prematura sotto alcuni punti di vista e, senza dubbio, in fase di assestamento per le aziende che, come AdB, presentano delle loro caratteristiche tipiche di settore. […]";

- "in data XX comunicava all'Autorità Garante di aver provveduto ad eseguire la valutazione di impatto e ad adottare le misure tecniche ed organizzative […]. Le ispezioni dell'Autorità Garante rappresentano anche un momento di confronto con il Titolare e, soprattutto in un periodo di incertezze normative o con pochi […] precedenti giurisprudenziali, possono – e così è stato per AdB – supportare i medesimi titolari o responsabili a mettere delle solide basi giuridiche ad un modello di gestione costruito secondo i principi della buona fede e dell'ordinaria diligenza, nonché a migliorare le misure tecniche ed organizzative adottate sulla scorta di analisi del rischio condotte sulla scorta degli elementi normativi e regolamentari di riferimento . Ciò non dovrebbe essere valutato dal Garante con disfavore, al contrario, dovrebbe essere un elemento di positiva considerazione di un atteggiamento collaborativo come quello dimostrato da AdB e costruttivo, secondo il medesimo principio dell'accountability del Titolare, per una disciplina giuridica applicabile al contesto specifico";

- "conscia delle linee guida di mercato che suggeriscono l'implementazione di un protocollo per la comunicazione sicura https, relativamente all'applicativo "WB Confidential" AdB ha valutato di utilizzare il semplice protocollo http per diverse ragioni, evidenziate dall'analisi dei rischi per i diritti e le libertà degli interessati ed a tutela dell'anonimato del segnalante, basandosi soprattutto sui seguenti elementi: a. Servizio attivo dal 2015 al 2019 che ha ricevuto 3 segnalazioni (di cui nessuna nel periodo 25/05/2018 – 16/04/2019), generando quindi pochissime transazioni a bassissimo volume di traffico, peraltro estremamente complesse da identificare nel mezzo di tutto il traffico telematico che transita sulla rete di AdB, […]; b. Scarsa utilità per fornitori o terzi non autorizzati che volessero intraprendere azioni malevoli sulla rete di AdB al fine di ottenere informazioni utili o poter propagare ulteriormente un accesso abusivo ai sistemi; c. Probabilità estremamente bassa di minacce quali phishing, o altre minacce simili, disinnescate dalla possibilità di verificare l'autenticità del sito. Non solo sarebbe scarsa la redemption (numero di possibili vittime che raggirate si trasformano in vittime reali) di mail tese a far collegare possibili utenti al sito, ma le utenze AdB effettivamente attive sono di un solo utente Responsabile Internal Audit, estremamente consapevole circa l'uso dello strumento";

- "in fase di attivazione del servizio veniva chiesto al fornitore aiComply, di fornire una valutazione di merito all'opportunità di attivare il protocollo https a fronte della loro esperienza commerciale e di una maggior conoscenza dello stato dell'arte nonché del generale andamento di mercato su tali sistemi […]. Orbene, dietro suggerimento del fornitore

e considerata la rassicurazione fornita sul tema, lo stesso non riteneva necessaria tale misure suppletiva, […]. Ferma l'analisi dei rischi effettuata in coerenza con gli obblighi posti in capo al Titolare del trattamento, AdB si è affidata alla competenza e affidabilità rivestita dal fornitore […]";

- a seguito dell'attività ispettiva "AdB […] ha rivalutato l'analisi e adottato lo strumento https entro i 10 giorni successivi dall'ispezione, per cui tale misura risulta attiva dal 16 Aprile 2019 […]";

- "relativamente alla presunta mancanza di protocolli di cifratura delle informazioni memorizzate nel database, anche in questo caso si deve evidenziare parimenti che all'atto dell'adozione della piattaforma "WB Confidential" l'interpretazione della normativa e delle regolamentazioni vigenti, non avevano condotto il Titolare a ravvedere una necessità di adottare la misura della crittografia, poiché applicabile ed adeguata nei casi di fattispecie caratterizzate da ampi volumi di dati e/o in differenti ambiti soggettivi […]";

- "L'accesso al database era precluso a tutto il personale tecnico e non di AdB e riservato esclusivamente ai tecnici incaricati del fornitore aiComply, che non avevano alcun interesse nel consultare tali dati né a comunicarli o diffonderli";

- "L'implementazione di tale funzionalità richiedeva l'acquisto di una funzionalità aggiuntiva […]. Tale importo sarebbe stato un costo di attuazione ragionevolmente sproporzionato rispetto [… al costo complessivo del servizio]";

- "Eventuali accessi da parte di terzi non autorizzati sarebbero comunque avvenuti rispetto ad un sistema contenente 3 segnalazioni tra il 2015 ed il 2019, scarsamente utilizzabili sia a fini economici (es. richiesta di riscatto o rivendita sul mercato), sia al fine di perpetrare ulteriori attacchi ad AdB o altri stakeholder parte del suo ecosistema";

- "per completezza di informazione, giova segnalare che il fornitore aiComply ha nel frattempo proposto ad AdB, a seguito del passaggio dei loro servizi alla piattaforma cloud Microsoft Azure, l'adozione di una metodologia di cifratura adeguata e sostenibile per la scrivente, anche in considerazione dei costi di attuazione, tanto più in una situazione di crisi del comparto aereo senza precedenti e di dipendenti in cassa integrazione. Tale soluzione tecnica potrebbe, dunque, essere implementata dal corrente anno, laddove il contratto di fornitura con l'attuale fornitore fosse rinnovato";

- "pur confermando che ai fini di prevenzione degli attacchi e monitoraggio della rete, i firewall tenevano traccia nei log delle informazioni di accesso alla piattaforma "WB Confidential", si segnalano i seguenti elementi: a. Tali log impediscono di conoscere quale azione sia stata compiuta sulla piattaforma (es. distinguere chi ha scaricato il manuale o chi ha fatto una segnalazione anonima o nominativa o chi ha solo letto l'informativa privacy). b. Tali log sono in numero talmente esiguo da richiedere una conservazione su un lungo periodo, una analisi specifica al fine di identificare, tra tutti i log, quelli specifici di accesso a "WB confidential", operazione fattibile solo da parte di qualcuno a conoscenza della piattaforma nello specifico; circa i rischi collegati a collaboratori, fornitori o terzi non autorizzati si rimanda al punto 1 e a tutte le analisi svolte circa i rischi rappresentati da tali attori nonché alle contromisure in essere. L'analisi fatta, quindi, dimostra come, anche nel 2015, quando il GDPR non era in vigore e nel 2018 dopo la sua applicabilità, siano stati rispettati i principi della data protection by design e by default in osservanza dell'art 25. Con il medesimo spirito di collaborazione e arricchimento della metodologia in uso, si segnala che AdB ha provveduto a configurare [… una nuova] misura tecnica ed organizzativa", configurando i sistemi firewall in modo da non registrare nei log il traffico destinato all'applicativo "WB Confidential";

- “nell’ambito dell’analisi del rischio rilevava la necessità di effettuare la valutazione di impatto ai sensi dell’art. 35 GDPR relativamente al trattamento [… in esame …]. Orbene, considerato l’esiguo numero dei dati trattati e degli interessati coinvolti dal trattamento in questione, considerato inoltre che tra i criteri indicati dal WP29 n. 248 del 4 aprile 2017 solo uno di questi risulta pienamente sussistente (la vulnerabilità dei soggetti coinvolti nel trattamento), AdB ha considerato il trattamento con un grado di rischio “non elevato” e, per tale motivo, ha ritenuto non necessario procedere alla valutazione di impatto sin dal 25 maggio 2018, ma di monitorare il rischio sotteso al trattamento de quo l’andamento del trattamento e rivalutarlo in sede di aggiornamento del registro (annuale). […]”;

- “la valutazione dei criteri sopra riportati ha orientato AdB nella rilevazione del rischio sotteso al trattamento, non tanto con riferimento alla necessarietà di effettuare la DPIA […], ma con riferimento alla necessità di effettuarla con priorità rispetto ad altri trattamenti. Conseguentemente, nelle scelte e nelle valutazioni di AdB si era comunque tenuto conto, in via generale, della delicatezza del trattamento atteso tuttavia che in linea di principio, lo stesso WP29 ritiene che quanto maggiore è il numero dei criteri soddisfatti da un determinato trattamento, tanto maggiore è la probabilità che esso presenti un rischio elevato per i diritti e le libertà degli interessati e, quindi, che si renda necessaria una DPIA indipendentemente dalle misure che il titolare prevede di adottare. In altre termini, fermo quanto sopra indicato, si chiede […all’]Autorità di rivalutare la censura effettuata in ordine alla violazione dell’art. 35 GDPR, in quanto come descritto AdB aveva effettuato tutte le valutazioni necessarie nel rispetto dell’art. 35 GDPR e nel rispetto delle indicazioni prescritte dal WP29 e di tenere conto della pianificazione effettuata secondo una logica di rischiosità relativa al trattamento de quo ai fini della completa esecuzione degli adempimenti previsti dalla normativa. Ciò è dimostrato anche dalla proattività con cui AdB ha […] in stretto coordinamento con l’Autorità Garante ha posto in essere la DPIA […]”.

In data 16 aprile 2021 si è, inoltre, svolta l’audizione richiesta dalla Società, ai sensi dell’art. 166, comma 6, del Codice, in occasione della quale, nel confermare quanto già dichiarato in sede di memorie difensive, è stato rappresentato, tra l’altro, che:

- “la Società ha sempre approcciato la materia della protezione dei dati personali con grande attenzione, adottando nuove tecnologie, dotandosi di un modello organizzativo privacy e svolgendo, tra l’altro, un’analisi dei rischi con riguardo ai diversi trattamenti effettuati”;

- “il livello di compliance della Società è stato evidenziato anche in sede degli accertamenti ispettivi, a seguito dei quali la Società ha proattivamente inteso adottare, nei giorni immediatamente successivi ai predetti accertamenti, una serie di ulteriori misure tecniche volte a innalzare ulteriormente il livello di conformità alle disposizioni del Regolamento e del Codice ed effettuando una valutazione di impatto sulla protezione dei dati per i trattamenti relativi al whistleblowing”;

- “la Società ha dimostrato di aver adottato un approccio basato sul principio di data protection by design, che è stato applicato anche ai trattamenti relativi al whistleblowing, per i quali era stata effettuata una valutazione dei rischi, potenziali ed effettivi, per gli interessati; valutazione che ha tenuto conto del numero esiguo delle segnalazioni whistleblowing acquisite e trattate, del limitato numero di interessati coinvolti, delle categorie di dati personali trattati (che non includevano dati appartenenti a categorie particolari) nonché del contesto di riferimento, anche con riguardo alle soluzioni tecnologiche all’epoca disponibili sul mercato e al generale quadro applicativo di riferimento”;

- “le scelte adottate dalla Società in materia di protezione dei dati personali sono sempre state ispirate al rispetto dei principi di proporzionalità, necessità e liceità dei trattamenti”.

3. Esito dell'attività istruttoria.

La disciplina in materia di tutela del dipendente che segnala illeciti e la disciplina in materia di protezione dei dati personali (c.d. whistleblowing) - originariamente prevista solo per i soggetti pubblici (cfr. art. 54-bis del d.lgs. 30 marzo 2001, n. 165, introdotto dall'art. 1, comma 51, della l. n. 190/2012) - è stata integrata e modificata dalla l. 30 novembre 2017, n. 179 ("Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato"), che ha introdotto una nuova disciplina in materia di whistleblowing riferita ai soggetti privati, integrando la normativa in materia di "responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica" (cfr. art. 2 della l. n. 179/2017 che ha aggiunto il comma 2-bis all'art. 6 del d.lgs. 8 giugno 2001, n. 231).

Il quadro normativo sopra richiamato prevede, più in generale, misure volte a proteggere la divulgazione dell'identità del segnalante, allo scopo di prevenire principalmente l'adozione di misure discriminatorie nei confronti dello stesso.

In questo ambito, i trattamenti di dati personali effettuati dai soggetti obbligati possono essere considerati necessari per adempiere a un obbligo legale al quale è soggetto il titolare del trattamento (artt. 6, par. 1, lett. c), 9, par. 2, lett. b), e 10 del Regolamento).

Per tali ragioni, la disciplina di settore sopra richiamata, che prevede trattamenti dei dati del dipendente che segnala illeciti, deve essere considerata come una delle "norme più specifiche per assicurare la protezione dei diritti e delle libertà con riguardo al trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro" previste dall'art. 88, par. 1, del Regolamento (cfr. provv. 4 dicembre 2019, doc. web n. 9215763, parere del Garante sullo schema di "Linee guida in materia di tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza in ragione di un rapporto di lavoro, ai sensi dell'art. 54-bis del d.lgs. 165/2001 (c.d. whistleblowing)" di ANAC).

In tale quadro, il titolare del trattamento è comunque tenuto a rispettare i principi in materia di protezione dei dati (art. 5 del Regolamento) e i dati devono inoltre essere "trattati in maniera da garantire un'adeguata sicurezza" degli stessi, "compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali" (artt. 5, par. 1, lett. f), del Regolamento).

Il titolare, nell'ambito della necessaria individuazione delle misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato agli specifici rischi derivanti dai trattamenti in esame (artt. 24, 25 e 32 del Regolamento), può ricorrere a un responsabile per lo svolgimento di alcune attività di trattamento cui impartisce specifiche istruzioni (cons. 81, artt. 4, punto 8), e 28 del Regolamento) e deve definire il proprio modello di gestione delle segnalazioni in conformità ai principi della "protezione dei dati fin dalla progettazione" e della "protezione per impostazione predefinita", tenuto conto anche delle osservazioni presentate al riguardo dal responsabile della protezione dei dati (RPD).

3.1. Mancato utilizzo di tecniche crittografiche per il trasporto e la conservazione dei dati

Nel corso dell'istruttoria è emerso che l'accesso all'applicativo "WB Confidential" per l'acquisizione e la gestione delle segnalazioni di illeciti avveniva mediante il protocollo http (hypertext transfer protocol), ossia un protocollo di rete che non garantisce l'integrità e la riservatezza dei dati scambiati tra il browser dell'utente e il server che ospita l'applicativo in questione, e non consente agli utenti di verificare l'autenticità del sito web con il quale stanno interagendo.

Al riguardo, tenuto conto della natura dei dati scambiati e degli elevati rischi derivanti dalla loro

possibile acquisizione da parte di terzi, si ritiene che la modalità di accesso all'applicativo in questione non possa essere considerata una misura idonea a garantire un adeguato livello di sicurezza.

Sebbene, nel corso dell'istruttoria, la Società abbia rappresentato di non aver, in un primo momento, ritenuto necessario adottare un protocollo di rete sicuro (quale il protocollo https) sulla base delle assicurazioni del Fornitore e in ragione del limitato numero di segnalazioni ricevute ("pochissime transazioni a bassissimo volume di traffico"), della "scarsa utilità", per eventuali terzi, delle informazioni contenute nelle segnalazioni acquisite mediante l'applicativo e della "probabilità estremamente bassa di minacce quali phishing […] disinnescate dalla possibilità di verificare l'autenticità del sito", si osserva che, in ogni caso, il titolare del trattamento deve mettere in atto misure tecniche e organizzative adeguate tenuto conto dello stato dell'arte, dei costi di attuazione, della natura, dell'ambito di applicazione, del contesto, delle finalità e dei rischi connessi al trattamento.

Con riferimento alla conservazione dei dati relativi alle segnalazioni acquisite mediante l'applicativo "WB Confidential", nel corso dell'istruttoria è emerso che lo stesso non prevede la cifratura dei dati personali (dati identificativi del segnalante, informazioni relative alla segnalazione nonché eventuale documentazione allegata) conservati nel relativo database. Tale misura era stata raccomandata dall'ANAC fin dal 2015 in relazione all'acquisizione e gestione delle segnalazioni di condotte illecite (cfr. le raccomandazioni sull'utilizzo di "strumenti di crittografia end-to-end per i contenuti delle segnalazioni e dell'eventuale documentazione allegata", Linee guida in materia di tutela del dipendente pubblico che segnala illeciti (c.d. whistleblower), adottate con determinazione n. 6 del 28 aprile 2015).

Al riguardo, la Società ha rappresentato, tra l'altro, di aver ritenuto originariamente di non dover "adottare la misura della crittografia, poiché applicabile ed adeguata nei casi di fattispecie caratterizzate da ampi volumi di dati e/o in differenti ambiti soggettivi", poiché "l'accesso al database [… era] riservato esclusivamente ai tecnici incaricati del fornitore aiComply, che non avevano alcun interesse nel consultare tali dati né a comunicarli o diffonderli" e in quanto "l'implementazione di tale funzionalità richiedeva l'acquisto di una funzionalità aggiuntiva [… con] un costo di attuazione ragionevolmente sproporzionato rispetto [al costo complessivo del servizio]".

Le argomentazioni difensive della Società, in relazione alla mancata adozione di misure per la cifratura dei dati sia nel trasporto che nella conservazione, seppur tenute in debita considerazione ai fini del presente provvedimento, non sono però sufficienti a escludere completamente la responsabilità del titolare del trattamento con riguardo agli obblighi derivanti dalla disciplina in materia di protezione dei dati personali (cfr. art. 24 e 32 del Regolamento). Ciò anche in ragione del fatto che il titolare è il soggetto sul quale ricadono le decisioni circa le finalità e le modalità del trattamento dei dati personali degli interessati e che ha una "responsabilità generale" sui trattamenti posti in essere (v. art. 5, par. 2, c.d. principio di "accountability", e 24 del Regolamento), anche con riferimento alla predisposizione di misure tecniche e organizzative che soddisfino i requisiti del Regolamento sotto il profilo della sicurezza (artt. 24 e 32 del Regolamento), anche quando talune operazioni di trattamento siano poste in essere da un responsabile per suo conto (cfr. le recenti decisioni del Garante relative anche al ruolo e alle connesse responsabilità del titolare e del responsabile del trattamento, provv. 17 settembre 2020, nn. 160 e 161, doc. web nn. 9461168 e 9461321, provv. 11 febbraio 2021, n. 49, doc. web n. 9562852, nonché provv. 17 dicembre 2020, nn. 280, 281 e 282, doc. web nn. 9524175, 9525315 e 9525337).

Per tali ragioni, il mancato utilizzo di strumenti di crittografia per il trasporto e la conservazione dei dati non risulta conforme alle disposizioni di cui all'art. 5, par. 1, lett. f), e all'art. 32 del Regolamento che, al suo par. 1, lett. a), individua espressamente la cifratura come una delle

possibili misure di sicurezza idonee a garantire un livello di sicurezza adeguato al rischio (v. anche cons. 83 del Regolamento nella parte in cui prevede che "il titolare del trattamento […] dovrebbe valutare i rischi inerenti al trattamento e attuare misure per limitare tali rischi, quali la cifratura").

Inoltre, si osserva che, in base al principio della "protezione dei dati fin dalla progettazione" (art. 25, par. 1, del Regolamento), il titolare del trattamento deve adottare misure tecniche e organizzative adeguate ad attuare i principi di protezione dei dati (art. 5 del Regolamento) e deve integrare nel trattamento le necessarie garanzie per soddisfare i requisiti del Regolamento e tutelare i diritti e le libertà degli interessati. Tale obbligo si estende anche ai trattamenti svolti per mezzo di un responsabile del trattamento. Infatti, le operazioni di trattamento effettuate da un responsabile dovrebbero essere regolarmente esaminate e valutate dal titolare per garantire che continuino a rispettare i principi e permettano al titolare di adempiere gli obblighi previsti dal Regolamento (cfr. "Linee guida 4/2019 sull'articolo 25 Protezione dei dati fin dalla progettazione e per impostazione predefinita", adottate il 20 ottobre 2020 dal Comitato europeo per la protezione dei dati, spec. punti 7 e 39). Pertanto, la mancata adozione delle predette misure – volte ad attuare i principi di protezione dei dati e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del Regolamento – si pone anche in contrasto con il principio della "protezione dei dati fin dalla progettazione" di cui all'art. 25, par. 1, del Regolamento.

Per tali ragioni si conclude che, fino all'adozione delle nuove misure con le quali la Società ha provveduto a garantire la protezione dei dati sia nella fase di trasporto che in quella di conservazione, il trattamento posto in essere mediante l'applicativo in questione è avvenuto in violazione degli artt. 5, par. 1, lett. f), 25, par. 1, e 32 del Regolamento.

3.2. Tracciamento degli accessi all'applicativo "WB Confidential".

Nel corso dell'istruttoria è stato constatato che l'accesso all'applicativo "WB Confidential" da parte dei dipendenti della Società con postazioni di lavoro o dispositivi personali connessi alla rete aziendale era mediato da apparati "firewall di nuova generazione, che consentono di configurare specifiche regole di navigazione in Internet, anche in ragione del ruolo delle diverse funzioni e mansioni svolte dai singoli dipendenti". Tali apparati "memorizza[va]no in appositi file di log le operazioni di navigazione effettuate, il cui termine di conservazione è fissato in 90 giorni", ivi comprese le connessioni all'applicativo "WB Confidential".

Come risulta dalla documentazione acquisita nel corso degli accertamenti ispettivi, i log generati dai predetti apparati firewall contenevano, tra gli altri, l'indirizzo IP del dispositivo utilizzato per la connessione all'applicativo "WB Confidential" e, "in virtù dell'integrazione del firewall con Active Directory", la username del soggetto che stava effettuando tale connessione.

Al riguardo, la Società ha precisato che nei predetti log non risultano presenti "informazioni circa gli accessi specifici alle diverse sezioni del sito (pagine .aspx), quindi non è possibile conoscere a quale pagina specifica è stato fatto accesso (es. segnalazione anonima, segnalazione nominativa, FAQ, Normativa, …)", evidenziando che "date le informazioni generate e memorizzate dal firewall e le competenze specifiche sul funzionamento dei componenti della piattaforma posseduti dal Titolare, risulta altamente improbabile, se non "impossibile", identificare tra gli eventuali visitatori eventuali segnalanti" (v. relazione tecnica allegata alla nota del XX, p. 4).

Nel prendere atto che "per maggior prudenza e garanzia della tutela dell'identità del segnalante, [… la Società] ha ritenuto adeguato far modificare la configurazione del proprio firewall, al fine di prevedere una regola specifica per il traffico destinato al server WB Confidential" e che "la nuova regola, attiva dal 15.04.2019 impone che non venga generata alcuna informazione di log per tutti gli accessi diretti alla piattaforma WB Confidential" (v. relazione tecnica allegata alla nota del XX, p. 4), si rileva, tuttavia, che, diversamente da quanto sostenuto dalla Società, la registrazione e la conservazione, nei log degli apparati firewall, delle informazioni relative alle connessioni

all'applicativo "WB Confidential" avrebbe potuto consentire la tracciabilità dei soggetti che utilizzavano l'applicativo, ivi inclusi i segnalanti. Ciò, considerato proprio l'esiguo numero di connessioni all'applicativo in questione, che rendeva quindi inefficaci le altre misure adottate per tutelare la riservatezza dell'identità dei segnalanti come richiesto dalla disciplina di settore, ponendosi in contrasto con le disposizioni di cui all'art. 5, par. 1, lett. f), e all'art. 32 del Regolamento.

Al riguardo, non rileva, ai fini della valutazione complessiva del rispetto degli obblighi di sicurezza del trattamento, quanto evidenziato dalla Società in ordine al fatto che i log non consentivano di conoscere la specifica azione compiuta dagli utenti sull'applicativo e che sarebbe stata necessaria una "analisi specifica al fine di identificare, tra tutti i log, quelli specifici di accesso a "WB confidential"".

In tale quadro, peraltro, il titolare del trattamento, oltre a rispettare il principio della "protezione dei dati fin dalla progettazione" (art. 25, par. 1, del Regolamento) – adottando misure tecniche e organizzative adeguate ad attuare i principi di protezione dei dati (art. 5 del Regolamento) e integrando nel trattamento le necessarie garanzie per soddisfare i requisiti del Regolamento e tutelare i diritti e le libertà degli interessati – deve anche, in conformità al principio della "protezione dei dati per impostazione predefinita" (art. 25, par. 2, del Regolamento), effettuare scelte tali da garantire che venga effettuato, per impostazione predefinita, solo il trattamento strettamente necessario per conseguire una specifica e lecita finalità. Ciò comporta quindi che, per impostazione predefinita, il titolare del trattamento non deve raccogliere dati personali che non sono necessari per la specifica finalità del trattamento (cfr. "Linee guida 4/2019 sull'articolo 25 Protezione dei dati fin dalla progettazione e per impostazione predefinita", adottate il 20 ottobre 2020 dal Comitato europeo per la protezione dei dati, spec. punti 42, 44 e 49).

Come recentemente messo in evidenza dal Garante (cfr., in particolare, con riguardo al trattamento di dati di utenti e dipendenti mediante un sistema di prenotazione di servizi allo sportello, provv. 17 dicembre 2020, n. 282, doc. web n. 9525337, ma già provv. 7 marzo 2019, n. 81, doc. web n. 9121890), il titolare del trattamento, anche quando utilizza prodotti o servizi realizzati da terzi, deve verificare, anche avvalendosi del supporto del responsabile della protezione dei dati ove nominato, la conformità ai principi applicabili al trattamento dei dati (art. 5 del Regolamento) adottando, nel rispetto del principio di responsabilizzazione, le opportune misure tecniche e organizzative e impartendo le necessarie istruzioni al fornitore del servizio (cfr. artt. 5, par. 2, 24, 25 e 32 del Regolamento).

In tale prospettiva, il titolare del trattamento deve eseguire una valutazione dei rischi e accertarsi che siano disattivate le funzioni che non hanno una base giuridica, non sono compatibili con le finalità del trattamento, ovvero si pongono in contrasto con specifiche norme di settore previste dall'ordinamento (v., in particolare, la disciplina in materia di whistleblowing, ma anche le norme nazionali e di maggior tutela per gli interessati con riguardo ai trattamenti in ambito lavorativo, art. 88 del Regolamento in relazione agli artt. 113 e 114 del Codice; sotto tale ultimo profilo, con riguardo a operazioni di tracciamento delle connessioni a siti Internet da parte di dipendenti, v. da ultimo provv. 13 maggio 2021, n. 190, in corso di pubblicazione).

La mancata adozione delle necessarie misure a tutela degli interessati con riguardo al tracciamento degli accessi all'applicativo "WB Confidential" si pone pertanto in contrasto anche con i principi della "protezione dei dati fin dalla progettazione" e della "protezione dei dati per impostazione predefinita" di cui all'art. 25 del Regolamento.

Per tali ragioni, si ritiene che la registrazione e la conservazione, all'interno dei log degli apparati firewall, di informazioni direttamente identificative degli utenti dell'applicativo "WB Confidential" è stata posta in essere, fino al momento in cui la Società ha provveduto ad adottare specifiche misure a tutela degli interessati volte a non registrare più nei log dei sistemi firewall gli accessi

all’applicativo in questione, in violazione degli artt. 5, par. 1, lett. f), 25 e 32 del Regolamento.

3.3. Mancata esecuzione di una valutazione d’impatto sulla protezione dei dati.

Come risulta dalle evidenze istruttorie in atti, il trattamento dei dati personali degli interessati è stato effettuato in assenza di una preliminare valutazione d’impatto sulla protezione dei dati in ragione “dell’esiguo numero dei dati trattati e degli interessati coinvolti dal trattamento in questione” (cfr. verbale 2 aprile 2019, p. 2).

Al riguardo, si ritiene che il trattamento dei dati personali mediante i sistemi di acquisizione e gestione delle segnalazioni di presunte condotte illecite – in ragione della particolare delicatezza delle informazioni trattate, nonché degli elevati rischi, in termini di possibili effetti ritorsivi e discriminatori, anche indiretti, per il segnalante, la cui identità è protetta da uno specifico regime di garanzia e riservatezza previsto dalla normativa di settore (tanto a livello nazionale quanto a livello europeo, cfr., da ultimo, la direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio del 23 ottobre 2019 riguardante la protezione delle persone che segnalano violazioni del diritto dell’Unione) – presenti rischi specifici per i diritti e le libertà degli interessati.

Ciò, anche considerata, la “vulnerabilità” degli interessati (soggetti segnalanti e segnalati) nel contesto lavorativo (cfr. artt. 35 e 88, par. 2, del Regolamento; “Linee guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del Regolamento 2016/679”, WP 248 del 4 aprile 2017; v., da ultimo, provv. 4 dicembre 2019, doc. web n. 9215763, con il quale il Garante ha reso il parere ad ANAC sullo schema di "Linee guida in materia di tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza in ragione di un rapporto di lavoro, ai sensi dell’art. 54-bis del d.lgs. 165/2001 (c.d. whistleblowing)", ove espressamente si fa rinvio “ai principali adempimenti previsti dalla normativa in materia di protezione dei dati personali (artt. 13, 14, 30, 35 e 36 del Regolamento), anche tenuto conto degli specifici rischi per i diritti e le libertà degli interessati nel contesto lavorativo”).

Nel prendere atto che, a seguito degli approfondimenti svolti dalla Società, la stessa ha effettuato, seppur tardivamente, una valutazione d’impatto sulla protezione dei dati ai sensi dell’art. 35 del Regolamento (cfr. nota del XX, p. 1, e “Privacy Impact Assessment” allegato) si deve concludere che, comunque, fino alla data di predisposizione della stessa (aprile 2019), il trattamento è stato effettuato in assenza di una valutazione d’impatto necessaria a individuare misure specifiche per attenuare i rischi derivanti dal trattamento, in violazione dell’art. 35 del Regolamento. Tuttavia, tenuto conto della fase di prima applicazione del Regolamento e del Codice in cui è avvenuto il trattamento oggetto della presente istruttoria, delle incertezze derivanti dal quadro giuridico in evoluzione, e del fatto che specifici chiarimenti sul punto sono stati forniti dal Garante nell’ambito del citato parere reso ad ANAC il 4 dicembre 2019, cioè successivamente all’effettuazione delle attività ispettive presso la Società, si ritiene di non dover procedere, sul punto, all'applicazione di una sanzione amministrativa, anche ai sensi dell’art. 22, comma 13, del d.lgs. 10 agosto 2018, n. 101.

4. Conclusioni.

Alla luce delle valutazioni sopra richiamate, si rileva che le dichiarazioni rese dal titolare del trattamento negli scritti difensivi della cui veridicità si può essere chiamati a rispondere ai sensi dell’art. 168 del Codice seppure meritevoli di considerazione e indicative della piena collaborazione del titolare del trattamento al fine di attenuare i rischi del trattamento, rispetto alla situazione presente all’atto dell’avvio dell’istruttoria, non consentono tuttavia di superare i rilievi notificati dall’Ufficio con l’atto di avvio del procedimento e risultano quindi 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.

Per la determinazione della norma applicabile, sotto il profilo temporale, deve essere richiamato, in particolare, il principio di legalità di cui all'art. 1, comma 2, della l. n. 689/1981, ai sensi del quale le leggi che prevedono sanzioni amministrative si applicano soltanto nei casi e nei tempi in esse considerati. Ciò determina l'obbligo di prendere in considerazione le disposizioni vigenti al momento della commessa violazione, che nel caso in esame – data la natura permanente degli illeciti contestati – deve essere individuato nell'atto di cessazione della condotta illecita. Nel prendere atto che il titolare del trattamento ha, nel corso dell'istruttoria, provveduto a conformare il trattamento ai principi del Regolamento, ad adottare misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio presentato dal trattamento, nonché a effettuare una specifica valutazione d'impatto sulla protezione dei dati, si ritiene che, stante la cessazione dei trattamenti illeciti avvenuta successivamente alla data in cui il Regolamento è divenuto applicabile (cfr. nota del XX, nella quale si dà conto delle varie iniziative assunte dal titolare per porre rimedio alle violazioni contestate), il Regolamento e il Codice costituiscano la normativa alla luce della quale valutare i trattamenti in questione.

Si confermano pertanto le valutazioni preliminari dell'Ufficio e si rileva l'illiceità del trattamento di dati personali effettuato dalla Società in quanto esso è avvenuto in maniera non conforme ai principi generali di "protezione dei dati fin dalla progettazione" e della "protezione dei dati per impostazione predefinita", in violazione degli artt. 5, par. 1, lett. f), 25, 32 e 35 del Regolamento.

La violazione delle predette disposizioni rende inoltre applicabile la sanzione amministrativa ai sensi degli artt. 58, par. 2, lett. i), e 83, parr. 4 e 5, del Regolamento.
In tale quadro, considerando che la condotta ha esaurito i suoi effetti, non ricorrono invece i presupposti per l'adozione di misure correttive, di cui all'art. 58, par. 2, del Regolamento.

5. 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 stessa sanzione amministrativa pecuniaria prevista dall'art. 83, par. 5, del Regolamento.
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.

Ai fini dell'applicazione della sanzione sono stati considerati la natura, l'oggetto e la finalità del trattamento la cui disciplina di settore prevede, a tutela dell'interessato, un elevato grado di riservatezza con specifico riguardo all'identità dello stesso.

Di contro, è stato considerato che il trattamento ha, in concreto, riguardato un numero esiguo di interessati (tra soggetti segnalati e segnalanti) in ragione del limitato numero di segnalazioni presenti nell'applicativo utilizzato per l'acquisizione e la gestione delle segnalazioni di condotte illecite. Inoltre, il titolare del trattamento ha prestato una particolare collaborazione nel corso dell'istruttoria provvedendo ad adottare, già a seguito dell'attività ispettiva condotta dall'Ufficio e

con l'ausilio del responsabile della protezione dei dati, 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. Sono state altresì tenute in considerazione le ripercussioni economiche sul comparto in cui opera il titolare del trattamento per effetto del diffondersi su scala mondiale del virus SARS-CoV-2.

Non risultano, inoltre, precedenti violazioni 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 40.000,00 (quarantamila) per la violazione degli artt. 5, par. 1, lett. f), 25 e 32 del Regolamento. Nella quantificazione della sanzione il Garante ha tenuto della fase di prima applicazione delle disposizioni sanzionatorie, ai sensi dell'art. 22, comma 13, del d. lgs. 10 agosto 2018, n. 101, con particolare riguardo alla violazione dell'art. 35 del Regolamento.

Tenuto conto della particolare delicatezza dei dati illecitamente trattati, 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 dall'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

rileva l'illiceità del trattamento effettuato da Aeroporto Guglielmo Marconi di Bologna S.p.a. per la violazione degli artt. 5, par. 1, lett. f), 25, 32 e 35 del Regolamento, nei termini di cui in motivazione;

ORDINA

ad Aeroporto Guglielmo Marconi di Bologna S.p.a., in persona del legale rappresentante pro-tempore, con sede legale in Bologna, via Triumvirato, n. 84, C.F./P.IVA 03145140376, ai sensi degli artt. 58, par. 2, lett. i), e 83, par. 5, del Regolamento, di pagare la somma di euro 40.000,00 (quarantamila) 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 trenta giorni, di un importo pari alla metà della sanzione comminata;

INGIUNGE

ad Aeroporto Guglielmo Marconi di Bologna S.p.a. di pagare la somma di euro 40.000,00 (quarantamila) in caso di mancata definizione della controversia ai sensi dell'art. 166, comma 8, del Codice, secondo le modalità indicate in allegato, entro trenta giorni dalla notifica 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;

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.

Ai sensi dell’art. 78 del Regolamento, degli artt. 152 del Codice e 10 del d.lgs. 1° settembre 2011, n. 150, 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, 10 giugno 2021

IL PRESIDENTE
Stanzione

IL RELATORE
Cerrina Feroni

IL SEGRETARIO GENERALE
Mattei