GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Provvedimento correttivo e sanzionatorio nei confronti di Università degli studi di Roma “La Sapienza” - 23 gennaio 2020 [9269618]

VEDI ANCHE Newsletter del 18 febbraio 2020

[doc. web n. 9269618]

Provvedimento correttivo e sanzionatorio nei confronti di Università degli studi di Roma “La Sapienza” - 23 gennaio 2020

Registro dei provvedimenti
n. 17 del 23 gennaio 2020

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del dott. Antonello Soro, presidente, della dott.ssa Augusta Iannini, vicepresidente, della prof.ssa Licia Califano e della dott.ssa Giovanna Bianchi Clerici, componenti e del dott. Giuseppe Busia, 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, in www.gpdp.it, doc. web n. 1098801;

Relatore il dott. Antonello Soro;

PREMESSO

1. La violazione dei dati personali.

Con nota del 14 dicembre 2018 (prot. n. 37333), l’Università degli studi di Roma “La Sapienza” ha notificato al Garante, ai sensi dell’art. 33 del Regolamento, l’avvenuta diffusione di dati personali trattati per il tramite della piattaforma che l’Ateneo, all’epoca dei

fatti, utilizzava per l'acquisizione e la gestione delle segnalazioni di illeciti da parte dei propri dipendenti e di soggetti terzi, nell'ambito della disciplina del c.d. whistleblowing. In particolare l'Ateneo ha notificato la "dispersione di dati personali comuni (nome, indirizzo e-mail) relativi a 2 segnalanti tramite la piattaforma whistleblowing (fornita dalla Società Agic Technology srl) su motori di ricerca" (v. nota del 14 dicembre 2018, p. 1).

2. L'attività istruttoria.

In riscontro alle specifiche richieste formulate dall'Ufficio, l'Ateneo (cfr. note del 9 gennaio 2019, prot. n. 800 e dell'8 febbraio 2019, prot. n. 4492) ha fornito specifici elementi al fine di consentire una compiuta ricostruzione del fatto.

a) che la "pubblicazione sul web dell'elenco dei soggetti che hanno aperto segnalazioni riservate contenute nell'applicativo" di condotte illecite ha dato luogo anche alla indicizzazione delle pagine web in questione da parte di motori di ricerca web (v. allegato 1 alla nota del 9 gennaio 2019, p. 1);

b) di essere "venut[o] a conoscenza della dispersione dei dati il 12.12.2018" (v. nota del 9 gennaio 2019, p. 1) e di aver notificato la violazione dei dati personali al Garante entro le 72 ore dal momento in cui ne è venuto a conoscenza;

c) che "i dati personali accidentalmente dispersi sono riferiti ad un dipendente tecnico-amministrativo e ad una studentessa dell'Ateneo" (v. nota del 9 gennaio 2019, p. 1);

d) che "i dati personali […] interessati dal data breach sono stati i seguenti: nome; cognome; struttura/sede; telefono; e-mail; data segnalazione" (v. documento tecnico sull'architettura informatica del 6 febbraio 2019, p. 4) mentre "il contenuto delle segnalazioni non è stato in alcun modo reso accessibile a soggetti non autorizzati" (v. allegato 1 alla nota del 9 gennaio 2019, p. 1);

e) di aver comunicato la violazione dei dati personali ai due interessati coinvolti il 30 gennaio 2019. A tal proposito l'Ateneo ha rappresentato che "[…] tenuto conto della presenza delle copie dei dati (divenuti pubblici) memorizzati all'interno dei server di indicizzazione delle pagine web (es. google) nonostante il blocco dell'accesso al portale on-line (primo intervento d'urgenza) si è ritenuto, anche per motivi puramente prudenziali, di effettuare la comunicazione ai suddetti interessati" (v. nota dell'8 febbraio 2019, pp. 1-2);

f) di aver coinvolto il Centro InfoSapienza per la sospensione dell'applicativo whistleblowing e la cancellazione da alcuni motori di ricerca delle copie cache delle pagine web che riportavano tali dati. Sul punto l'Ateneo ha in particolare specificato di aver "provveduto ad oscurare la pagina alle ore 15.55 dello stesso giorno" in cui è venuto a conoscenza della violazione (v. documento tecnico sull'architettura informatica del 6 febbraio 2019, p. 4), evidenziando che "successivamente alla protezione del dominio interessato, il Centro Infosapienza ha effettuato una prima analisi dei risultati indicizzati da Google" e che "da questa ricerca si è potuto notare come la totalità delle pagine coinvolte nel data breach contenessero nel titolo la […] stringa Segnalazioni Nominative Riservate" (v. relazione tecnica sulla risoluzione dell'indicizzazione Google del 28 gennaio 2019, p. 3);

g) di aver inizialmente richiesto a Google la rimozione dei singoli contenuti indicizzati – e in alcuni casi conservati in copie cache – mediante lo strumento denominato "Remove outdated content", rappresentando che "tuttavia, questo strumento si è rivelato inefficiente per la rimozione di molteplici pagine dinamiche. Infatti, a seguito della rimozione dei primi URL segnalati, la problematica riscontrata evidenziava come fossero presenti ancora le medesime pagine tra i risultati Google, aventi semplicemente i valori dei parametri GET differenti rispetto all'URL inizialmente rimosso" (v. relazione tecnica sulla risoluzione dell'indicizzazione Google del 28 gennaio 2019, p. 4)

h) di aver quindi "provveduto a segnalare l'intera directory http://segnalazioni.uniroma1.it", […] ottenendo la rimozione completa dei risultati associati a Whistleblowing" (v. relazione tecnica sulla risoluzione dell'indicizzazione Google del 28 gennaio 2019, p. 5).

i) di essersi adoperato per "segnalare la rimozione dell'intero sito web anche su Bing, e di riflesso su Yahoo, appartenente sempre a Microsoft e operante con lo stesso motore di Bing" (v. relazione tecnica sulla risoluzione dell'indicizzazione Google del 28 gennaio 2019, p. 6).

Con nota del 15 aprile 2019 (prot. n. 12891), l'Ufficio, sulla base degli elementi acquisiti, anche attraverso la documentazione inviata e dei fatti emersi nel corso dell'attività istruttoria, ha notificato all'Ateneo, 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 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 24/11/1981).

In particolare l'Ufficio ha ritenuto che la violazione di dati personali che, seppur accidentale e tempestivamente notificata al Garante ai sensi dell'art. 33 del Regolamento, abbia determinato un trattamento di dati personali:

a) non conforme al rispetto dei principi di "liceità, correttezza e trasparenza", in violazione dell'art. 5, par. 1, lett. a), del Regolamento;

b) in assenza di un idoneo presupposto normativo, in violazione dell'art. 2-ter, commi 1 e 3, del Codice e dell'art. 6, par. 1, lett. c) ed e), par. 2 e par. 3, lett. b), del Regolamento;

c) in violazione 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" ai sensi dell'art. 88, par. 1, del Regolamento in relazione all'art. 54-bis del d. lgs. 30 marzo 2001, n. 165;

d) in violazione dell'art. 32 del Regolamento, in assenza di adeguate misure tecniche e organizzative volte a garantire la riservatezza e l'integrità dei dati personali trattati mediante l'ausilio dell'applicativo.

Con nota del 17 maggio 2019 (prot. n. 17392) l'Ateneo ha fatto pervenire le proprie memorie difensive ove ha dichiarato che:

a) la violazione "risale ad un periodo antecedente (24.04.2018) alla data a decorrere dalla quale è divenuto applicabile il Regolamento", che quindi "non possono essere contestate a questa Amministrazione violazioni di disposizioni non applicabili all'atto della dispersione" e che inoltre trova applicazione al caso di specie l'art. 22, comma 13, del d.lgs. 101/2018 (cfr. nota del 17 maggio 2019, cit., pp. 1-2);

b) "risulta infondata l'assimilazione della fattispecie in oggetto – data breach che abbia comportato accidentalmente la divulgazione di dati – ad una diffusione di dati personali in assenza di un idoneo presupposto normativo" (cfr. cit., p. 2);

c) la contestazione relativa alla "mancata osservanza di norme vigenti e 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 [di cui all'art. 88, par. 1, del Regolamento in relazione all'art. 54-bis del d.lgs. n. 165/2001]" risulta infondata in quanto la stessa sarebbe "esclusivamente riconducibil[e] al solo asserito mancato apprestamento di adeguate misure tecniche e organizzative" (cfr. cit., p. 6);

d) "la causa del problema […] del sistema http://segnalazioni.uniroma1.it è legata a un aggiornamento e modifica obbligatoria (patch del sistema) delle impostazioni di sicurezza della piattaforma software Microsoft Sharepoint che ha interferito con l'applicativo e permesso la visualizzazione di alcune liste che risultavano nativamente non esposte (e quindi non indicizzabili dai motori di ricerca)" (cfr. cit., p. 7);

e) "il sistema di autenticazione informatica […] non è stato minimamente coinvolto nell'esposizione dei dati identificativi dei segnalanti, che invece è avvenuta attraverso la sovrascrittura accidentale dei permessi di accesso di una pagina web interna dell'applicativo" (cfr. cit., p. 7);

f) "la singola pagina erroneamente esposta […] era individuabile tramite motori di ricerca solamente utilizzando a tal fine specifiche parole chiave" e che ciò "era possibile […] immettendo il campo 'nome' ovvero 'data' di una delle due segnalazioni" (cfr. cit., p. 7);

g) "non può affermarsi che la diffusione è stata resa possibile da un sistema non efficace di autenticazione dal momento che solo l'RPCT o, a limite, i segnalanti medesimi erano in possesso delle informazioni per poter risalire al dato" (cfr. cit., p. 7);

h) con riguardo al “mancato utilizzo di strumenti di crittografia per il trasporto e la conservazione dei dati […], l’assenza del protocollo di rete HTTPS è risultata irrilevante ai fini dell’esfiltrazione dei dati in oggetto” e che tale misura non sarebbe “obbligatoria ma semplicemente suggerita ai sensi della normativa vigente” (cfr. cit., p. 8);

i) con riguardo al “non completo disaccoppiamento dei dati del segnalante dal contenuto della segnalazione”, tale contestazione risulterebbe infondata anche in ordine all’eventualità che “chiunque, purché in possesso di elementi informativi relativi al contenuto di una segnalazione e alla data della sua ricezione, [possa] risalire all’identità del segnalante” (cfr. cit., p. 8);

j) “i dati presenti nell’applicativo […] non corrispondono necessariamente ad indicazioni di ‘verità’, ben potendo […] corrispondere sia ad uno pseudonimo o a nomi di fantasia (ad es. ‘Paolino Paperino”) sia a nomi reali di persona che però non corrispondono all’effettiva identità del segnalante” (cfr. cit., p. 9).

3. Esito dell’attività istruttoria. Normativa applicabile.

In via preliminare si rappresenta che, seppure la violazione dei dati personali oggetto dell’istruttoria da parte di questa Autorità sia iniziata prima della data di piena applicazione del Regolamento (e in particolare, stando a quanto dichiarato, in data 24 aprile 2018), al fine della determinazione del quadro normativo applicabile sotto il profilo temporale deve essere richiamato il principio di legalità di cui all’art. 1, comma 2, della legge n. 689 del 24 novembre 1981 che, nel prevedere come «Le leggi che prevedono sanzioni amministrative si applicano soltanto nei casi e nei tempi in esse considerati», stabilisce la ricorrenza del principio del tempus regit actum. L’applicazione di tale principio determina, quindi, l’obbligo di prendere in considerazione le disposizioni vigenti al momento della commessa violazione. Nel caso in questione, la completa rimozione dei dati personali dalle pagine web e la sospensione dell’applicativo è avvenuta, successivamente al 12 dicembre 2018, data in cui l’Ateneo ha dichiarato di essere venuto a conoscenza della violazione (v. nota del 9 gennaio 2019, p. 1 e relazione tecnica sulla risoluzione dell’indicizzazione Google del 28 gennaio 2019, cit.). Pertanto, considerando la natura permanente dell’illecito, di carattere peraltro omissivo, la disciplina applicabile va individuata con riferimento a quella vigente alla data di perfezionamento della fattispecie, da ravvisarsi appunto nel momento della cessazione della condotta, verificatasi successivamente alla citata data del 12 dicembre 2018, allorquando trovavano già applicazione tanto il citato Regolamento, quanto la normativa interna di adeguamento (d.lgs. 101 del 2018).

3.1. La sicurezza del trattamento.

In base al Regolamento, i dati personali devono essere “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).

Al riguardo, l’art. 32 del Regolamento stabilisce che “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, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio” e che “nel valutare l’adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare […] dalla divulgazione non autorizzata […] di] dati personali trasmessi, conservati o comunque trattati”.

Nel corso dell’istruttoria l’Ateneo ha illustrato le misure adottate al fine di garantire la sicurezza del trattamento. In particolare, è emerso come l’applicativo whistleblowing utilizzato fosse un prodotto software disponibile sul mercato e che lo stesso non consentisse al titolare del trattamento di effettuare “personalizzazioni”. Come rappresentato dall’Ateneo, il Centro Infosapienza aveva fornito esclusivamente le macchine virtuali, secondo i prerequisiti indicati dal fornitore del software, all’interno delle quali il fornitore stesso aveva installato le componenti (DBMS e middleware SharePoint) necessarie al funzionamento dell’applicativo whistleblowing (v. documento tecnico sull’architettura informatica del 6 febbraio 2019, p. 4).

a. Le misure tecniche per il controllo degli accessi.

Sulla base della documentazione in atti, i dati identificativi dei segnalanti presenti in alcune delle pagine web dell’applicativo whistleblowing, erano indicizzati e liberamente rintracciabili in rete con l’ausilio di comuni motori di ricerca web da chiunque. Tale circostanza è comprovata dal fatto che tra i risultati di un’interrogazione effettuata tramite il motore di ricerca Google

con la stringa “inurl:segnalazioni.uniroma1.it” erano presenti pagine web contenenti i dati personali identificativi di taluni segnalanti, alcune delle quali erano presenti anche sotto forma di copia cache di Google (cfr. verbale di operazioni compiute del 14 gennaio 2019). Ciò consente ulteriormente di ritenere che, contrariamente a quanto rappresentato dall’Ateneo, non “solo l’RPCT o, a limite, i segnalanti medesimi erano in possesso delle informazioni per poter risalire al dato” (cfr. nota del 17 maggio 2019, p. 7), ma anche da chiunque mediante ricerche libere in Internet.

La reperibilità sul web di tali dati personali è indicativa del fatto che le pagine web in questione fossero esposte su rete pubblica in assenza di misure tecniche per il controllo accessi, che avrebbero consentito di limitare l’accesso ai soli soggetti autorizzati dotati di credenziali di autenticazione e di uno specifico profilo di autorizzazione, ciò in violazione dell’art. 32 del Regolamento.

Sebbene l’Ateneo abbia rappresentato, nelle memorie difensive, che “la causa del problema [… sarebbe] legata a un aggiornamento e modifica obbligatoria (patch del sistema) delle impostazioni di sicurezza della piattaforma software Microsoft Sharepoint” che avrebbe dato luogo ad una “sovrascrittura accidentale dei permessi di accesso” di alcune pagine web dell’applicativo whistleblowing, occorre evidenziare che, in ogni caso, il titolare del trattamento è tenuto ad adottare apposite procedure “per testare, verificare e valutare regolarmente l’efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento” (art. 32, par. 1, lett. d), del Regolamento). L’asserita riduzione dell’efficacia delle misure tecniche per il controllo accessi, che, stando a quanto dichiarato dall’Ateneo, sarebbe derivata dall’aggiornamento della piattaforma Microsoft Sharepoint, resta comunque riconducibile alla sfera di responsabilità del titolare del trattamento.

b. Le misure tecniche per il trasporto e la conservazione dei dati.

Nel corso dell’istruttoria è altresì emerso che l’accesso all’applicativo whistleblowing avveniva mediante l’indirizzo web “http://segnalazioni.uniroma1.it”. Il protocollo di rete “http” (hypertext transfer protocol) utilizzato per il trasporto dei dati non garantisce una comunicazione sicura sia in termini di riservatezza e integrità dei dati scambiati che di autenticità del sito web visualizzato.

Con riguardo all’applicativo in questione, tenuto conto della natura, dell’oggetto e della finalità del trattamento nonché dell’elevato rischio per i diritti e le libertà dei segnalanti, la soluzione adottata dall’Ateneo non può essere considerata una misura tecnica adeguata a garantire la riservatezza e l’integrità dei dati trattati nonché l’autenticità del sito web visualizzato da parte dei soggetti che lo utilizzano sia come canale di invio delle segnalazioni (dipendenti, studenti, ecc.) che come strumento di gestione delle stesse (RPCT ed eventuali suoi collaboratori).

Il mancato utilizzo di strumenti di crittografia per il trasporto dei dati si pone quindi in contrasto con l’art. 32 del Regolamento, che peraltro al par. 1, lett. a), individua espressamente la cifratura dei dati come una delle possibili misure di sicurezza idonea a garantire un livello di sicurezza adeguato al rischio (sul punto, cfr. anche il considerando 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” nonché con le raccomandazioni di ANAC sull’utilizzo di “strumenti di crittografia end-to-end per i contenuti delle segnalazioni e dell’eventuale documentazione allegata” contenute nelle Linee guida in materia di tutela del dipendente pubblico che segnala illeciti (c.d. whistleblower), adottate con delibera n. 6 del 28 aprile 2015. La necessità di adottare misure tecniche e organizzative per garantire la sicurezza, la riservatezza e l’integrità dei dati trattati nell’ambito delle procedure informatiche per la gestione delle segnalazioni, mediante protocolli sicuri di trasporto dei dati, è stato di recente ribadito dal Garante (cfr. Provvedimento n. 215 del 4 dicembre 2019, doc. web n. 9215763, recante il parere 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)”).

Da ultimo, si prende atto che, come emerge chiaramente dalla documentazione acquisita nel corso dell’istruttoria, l’Ateneo si è limitato a recepire le scelte progettuali dell’azienda che ha fornito l’applicativo whistleblowing che non prevedevano la cifratura dei dati personali (dati identificativi del segnalante, informazioni relative alla segnalazione nonché eventuale documentazione allegata) conservati nel database utilizzato dal medesimo applicativo, non adottando misure tecniche e organizzative adeguate a garantire la riservatezza e l’integrità dei dati personali trattati mediante l’ausilio dell’applicativo whistleblowing, in violazione dell’art. 32 del Regolamento.

3.2. Conclusioni.

Alla luce delle valutazioni sopra richiamate, tenuto conto delle 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 si rappresenta che gli elementi forniti dal titolare del trattamento nelle memorie difensive non consentono di superare i rilievi notificati dall'Ufficio con l'atto di avvio del procedimento, non ricorrendo peraltro alcuno dei casi previsti dall'art. 11 del Regolamento del Garante n. 1/2019.

Per tali ragioni si rileva l'illiceità del trattamento di dati personali effettuato dall'Università degli studi di Roma "La Sapienza", per aver, in particolare, omesso di adempiere agli obblighi di sicurezza imposti dall'art. 32 del Regolamento.

In tale quadro, considerando, in ogni caso, che la condotta ha esaurito i suoi effetti, e atteso che l'Ateneo ha dichiarato di aver provveduto a sospendere l'applicativo (v. nota dell'8 febbraio 2019, p. 1), non ricorrono i presupposti per l'adozione delle misure correttive di cui all'art. 58, par. 2, del Regolamento.

4. 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).

Ai sensi dell'art. 83, par. 3 del Regolamento, se in relazione allo stesso trattamento o a trattamenti collegati, un titolare o un responsabile del trattamento viola, con dolo o colpa, varie disposizioni del Regolamento, l'importo della sanzione amministrativa pecuniaria non supera l'importo applicabile per la violazione più grave.

Alla luce di quanto sopra, si ritiene di dover applicare la sanzione di cui all'art. 83, par. 4, lett. a) del Regolamento, in relazione al riscontrato omesso adempimento degli obblighi di sicurezza di cui all'art. 32 del Regolamento stesso, imputabile all'Ateneo

Il Garante, ai sensi 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).

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 considerata la particolare gravità delle condotte rispetto a trattamenti la cui disciplina di settore prevede, a tutela dell'interessato, un elevato grado di riservatezza, nonché l'intensità dell'elemento soggettivo (sub specie della gravità della negligenza), in ragione appunto della rilevante inadeguatezza degli accorgimenti adottati, sotto il profilo tecnico e organizzativo, al fine di soddisfare le esigenze di sicurezza e particolare riservatezza proprie della gestione dei dati nell'ambito delle procedure di whistleblowing (art. 83, par. 2, lett. b), d) e g) del Regolamento.

Di contro, ai sensi delle lettere a) e c) del citato art. 83, par. 2, è stato considerato che la violazione ha, in concreto, riguardato un numero esiguo di interessati (solo due) e si è tenuto conto anche delle misure correttive adottate tempestivamente volte all'eliminazione delle cause che hanno generato la condotta contestata, in particolare, attivandosi presso i motori di ricerca per ottenere la deindicizzazione e la rimozione delle copie cache delle pagine web dell'applicativo whistleblowing (cfr. le iniziative del titolare riportate nel par. 2 del presente provvedimento). E' stato inoltre considerato che l'Autorità è venuta a conoscenza della violazione a seguito della notifica da parte del titolare, il quale ha attivamente cooperato con l'Autorità nel corso della istruttoria e del presente procedimento, che non sono pervenute segnalazioni o reclami rispetto alla condotta oggetto del presente procedimento, né risultano precedenti violazioni pertinenti commesse dal titolare del trattamento o precedenti provvedimenti di cui all'art. 58 del Regolamento (art. 83, par. 2, lett. e), f), h), i), del Regolamento medesimo).

In ragione dei suddetti elementi, valutati nel loro complesso, si ritiene di determinare l'ammontare della sanzione pecuniaria - tenendo anche conto, ai sensi dell'art. 22, comma 13, del d. lgs. n. 101 del 2018, del contesto temporale in cui è stato realizzato l'illecito, - nella misura di euro 30.000 (trentamila) in particolare per la violazione dell'art. 32, del Regolamento quale sanzione amministrativa pecuniaria ritenuta, ai sensi dell'art. 83, par. 1, del Regolamento, effettiva, proporzionata e dissuasiva.

In tale contesto si ritiene altresì – anche in considerazione dell'invasività del trattamento contestato rispetto ai diritti fondamentali degli interessati, delle carenze riscontrate in relazione alla sicurezza dei sistemi informativi dell'Università, del particolare regime di riservatezza stabilito dalle disposizioni in materia di whistleblowing - che, ai sensi degli artt. 166, comma 7, del Codice, e 16, comma 1, del Regolamento del Garante n. 1/2019, si debba procedere alla pubblicazione del presente provvedimento sul sito web del Garante, a titolo di sanzione accessoria.

Si ravvisa peraltro la ricorrenza dei presupposti di cui all'art. 17 del Regolamento n. 1/2019 concernente le procedure interne aventi rilevanza esterna, finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati al Garante.

TUTTO CIÒ PREMESSO IL GARANTE

dichiara l'illiceità del trattamento di dati personali effettuato dall'Università degli studi di Roma "La Sapienza", nei termini di cui in motivazione.

ORDINA

all'Università degli studi di Roma "La Sapienza", con sede legale in Piazzale Aldo Moro 5, Roma CF 80209930587, in persona del legale rappresentante pro-tempore, di pagare la somma di euro 30.000,00 (trentamila) a titolo di sanzione amministrativa pecuniaria per la condotta indicata in motivazione, rappresentando che il contravventore, ai sensi dell'art. 166, comma 8, del Codice ha facoltà di definire la controversia, mediante il pagamento, entro il termine di trenta giorni, di un importo pari alla metà della sanzione irrogata.

INGIUNGE

alla predetta Università, in caso di mancata definizione della controversia ai sensi dell'art. 166, comma 8, del Codice, di pagare la somma di euro 30.000,00 (trentamila) 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 legge n. 689/1981.

DISPONE

ai sensi dell'art. 166, comma 7, del Codice, la pubblicazione per intero del presente provvedimento sul sito web del Garante, ravvisando altresì la ricorrenza dei presupposti di cui all'art. 17 del Regolamento n. 1/2019 concernente le procedure interne aventi rilevanza esterna, finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati al Garante.

Ai sensi dell'art. 78 del Regolamento, degli artt. 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, 23 gennaio 2020

IL PRESIDENTE
Soro

IL RELATORE
Soro

IL SEGRETARIO GENERALE
Busia