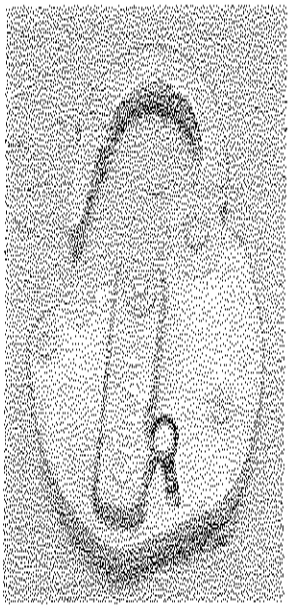
Istituto Comprensivo "Milani "
Terracina (LT)



Documento di Adozione delle Misure di Sicurezza nel trattamento dei dati personali

Predisposto ai sensi dell'art. 34
del Decreto Lgs. 196/2003 e del suo Allegato B
" Disciplinare Tecnico in materia di misure minime di sicurezza "

2017

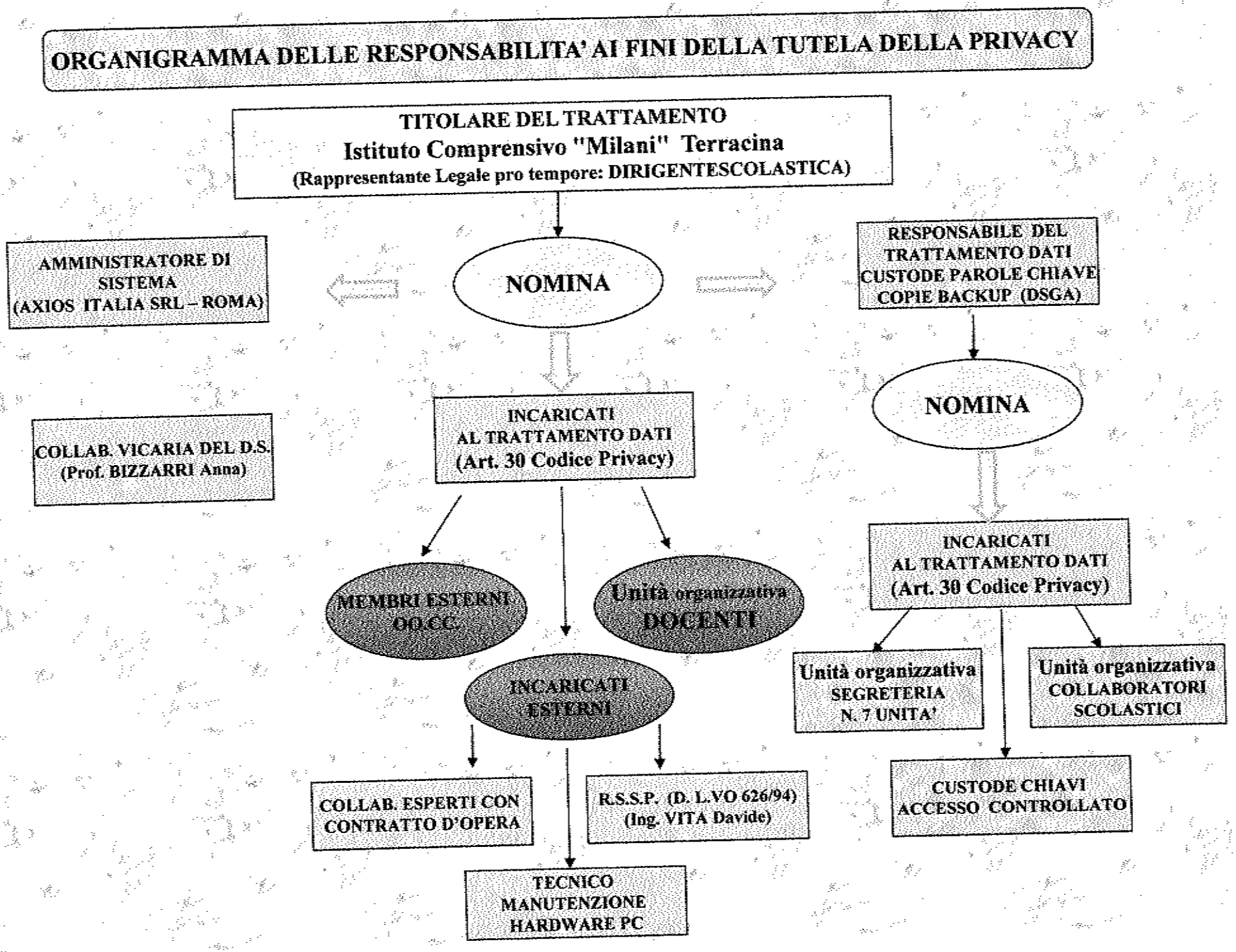
Documento conforme alle modifiche apportate dal
Decreto Legge 9 febbraio 2012, n. 5
"Disposizioni urgenti in materia di semplificazioni e di sviluppo"

Documento di Adozione delle Misure di sicurezza nel Trattamento dei dati personali

Documento conforme alle modifiche apportate dal Decreto legge 5/2012 – "Semplificazioni"

Anno 2017

ORGANIGRAMMA DELLE RESPONSABILITA' AI FINI DELLA TUTELA DELLA PRIVACY



PREMESSA

Il decreto-legge 9 febbraio 2012, n. 5, "**Disposizioni urgenti in materia di semplificazione e di sviluppo**", pubblicato nella GU 9 febbraio 2012, n. 33 all'art. 45 ha apportato semplificazioni anche in materia di dati personali.
La principale innovazione, in tale ambito, del provvedimento entrato in vigore il 10 febbraio 2012, è l'espressa abrogazione del punto 19 dell'Allegato B, nonché "*la lettera g) del comma 1 e il comma 1-bis dell'art. 34*" che comporta l'abolizione dell'obbligo di adozione, entro il 31 marzo di ogni anno, del Documento Programmatico Sicurezza.

Vediamo il provvedimento in dettaglio:

- Art. 45. Semplificazioni in materia di dati personali

1. Al decreto legislativo 30 giugno 2003, n. 196, sono apportate le seguenti modificazioni:
   a) all'articolo 21 dopo il comma 1 è inserito il seguente:
   «**1-bis. Il trattamento dei dati giudiziari è altresì consentito quando è effettuato in attuazione di protocolli d'intesa per la prevenzione e il contrasto dei fenomeni di criminalità organizzata stipulati con il Ministero dell'interno o con i suoi uffici periferici di cui all'articolo 15, comma 2, del decreto legislativo 30 luglio 1999, n. 300, che specificano la tipologia dei dati trattati e delle operazioni eseguibili.**»;
   b) all'articolo 27, comma 1, è aggiunto, in fine, il seguente periodo: "**Si applica quanto previsto dall'articolo 21, comma 1-bis.**";
   c) all'**articolo 34 è soppressa la lettera g)** del comma 1 ed è abrogato il comma 1-bis;
   d) nel disciplinare tecnico in materia di misure minime di sicurezza di cui all'**allegato B sono soppressi i paragrafi da 19 a 19.8 e 26.**

- Cosa è stato abrogato

- Il Decreto legislativo 30 giugno 2003, n. 196, "**Codice in materia di protezione dei dati personali**" all'**articolo 34** disciplina le ***"misure minime di sicurezza"*** da adottare nei "trattamenti" di dati con strumenti elettronici; la **lettera g** dell'articolo 34 richiedeva la "tenuta di un aggiornato **documento programmatico sulla sicurezza**" che dunque viene abrogato;
- Il **comma 1-bis** riguardava la possibilità per i soggetti che trattano soltanto dati personali non sensibili e che trattano come unici dati sensibili e giudiziari quelli relativi ai propri dipendenti e collaboratori (...) di **autocertificare** l'adozione delle misure di sicurezza invece di redigere il DPS.
- Il ***"Disciplinare tecnico in materia di misure minime di sicurezza"*** noto anche come ***allegato B*** al "Codice in materia di protezione dei dati personali" (artt. da 33 a 36 del Codice) riportava all'**articolo 19 (ora abrogato)** i contenuti obbligatori del DPS (elenco dei trattamenti eccetera ...) e all'**articolo 26** obbligava al titolare di riferire, nella relazione accompagnatoria del bilancio d'esercizio, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza (obbligo anch'esso decaduto).

Ciononostante, la succitata abrogazione normativa non determina in alcun modo l'esonero, per il titolare o per il responsabile del trattamento di dati, dall'obbligo di osservare le ***"Misure minime di sicurezza"***, infatti, permane l'integrale applicazione dell'art. 34 del Decreto Legislativo 196/03, nell'ipotesi di trattamento dei dati con strumenti elettronici.
In particolare, si dovrà tenere conto del fatto che ***"il trattamento di dati personali effettuato con strumenti elettronici"*** è consentito solo se sono adottate, nei modi previsti dal Disciplinare Tecnico contenuto nell'allegato B) le seguenti misure minime di sicurezza:

a) l'autenticazione informatica;

b) l' adozione di procedure di gestione delle credenziali di autenticazione;

c) l'utilizzazione di un sistema di autorizzazione;

d) l'aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici – provvedendo anche alla formazione degli stessi al fine di garantire l'effettiva protezione dei dati, nonché l'efficacia delle misure minime adottate;

e) la protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;

f) l'adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;

h) l'adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute.

Pertanto, si evidenzia come si ritiene necessario, per i soggetti di cui agli artt. 28 e 29 del D. L.vo 196/03, predisporre la redazione di un documento idoneo che descriva dettagliatamente l'organizzazione e le politiche di privacy adottate e che coincida nella logica con il DPS, senza però rispondere ai criteri imposti dal Garante della Privacy, e che attesti, quindi, il corretto adempimento delle misure minime previste dall'art. 34 e dall'Allegato B.

Permanendo, pertanto, le misure idonee (art. 31 del D. L.vo N. 193/03) da adottare in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, la relazione delinea il quadro delle misure di sicurezza, organizzative, fisiche e logistiche che saranno adottate in questa Istituzione scolastica relativamente al trattamento dei dati personali, per le rispettive competenze, da parte del dirigente Scolastico, del Direttore dei Servizi Generali e Amministrativi, degli Assistenti Amministrativi, del Personale Docente e dei Collaboratori Scolastici.

RIFERIMENTI NORMATIVI

- D. L.vo 30/06/2003 n. 196 – Codice in materia di protezione dei dati personali e Allegato B;
- D.M. 7/12/2006 n. 305 Regolamento recante identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate dal Ministero della Pubblica Istruzione;
- Prot. 45 del 7/03/2008 del Ministero della Pubblica Istruzione
- Decreto Legge del 9 febbraio 2012, n. 5 (cosiddetto Decreto "Semplificazioni")

OGGETTO E FINALITA' DEL DOCUMENTO

Il presente Documento, in ottemperanza a quanto disposto dal D. L.vo 196/2003, così come modificato all'art. 45 del Decreto "Semplificazioni" n. 5/2012, illustra le regole e le idonee strategie per la protezione dei dati personali trattati e quindi delle aree e dei locali interessati dalle misure di sicurezza dell'Istituto Comprensivo "MILANI" di Terracina.
Le Misure di Sicurezza, organizzative, fisiche, logistiche e logiche, adottate nel trattamento dei dati personali sono finalizzate a garantire "all'interessato" il rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.
Il tutto è disciplinato in modo da assicurare un elevato livello di tutela dei diritti e delle libertà, nel rispetto dei principi di semplificazione, armonizzazione ed efficacia delle modalità previste per il loro esercizio da parte degli interessati, nonché l'adempimento degli obblighi da parte del Titolare del trattamento (Art. 2 D. L.vo 196/2003).
- Il Titolare del Trattamento dei dati è l'Istituto Comprensivo "Milani" con sede in Terracina (LT), Codice fiscale n. 80003800598, il cui Rappresentante Legale pro-tempore è la Dirigente Scolastica prof.ssa Giuseppina Di Cretico, Codice fiscale DCRGPP63R62E472Z, che nel seguito del documento sarà indicata come "**Titolare**".
Il Responsabile del Trattamento dei dati, nella persona del sig. Giuseppe Sebastianelli, Codice fiscale SBSGPP56B17E472H, Direttore dei Servizi Generali ed Amministrativi, dipendente R. O. di questa Amministrazione nominato con lettera prot. N. 3380 FG/29 del 17/10/2008, ha collaborato alla stesura del presente documento firmandolo in calce insieme al Titolare.

Ai sensi dell'art. 1 del D. L.vo 196/2003 *"Chiunque ha diritto alla protezione dei dati personali che lo riguardano"*.
Tali dati riguardano:

- Tutto il personale che presta servizio presso l'Istituzione scolastica.
- Gli alunni che frequentano questa Istituzione scolastica.
- I genitori degli alunni o gli esercenti la potestà familiare per le notizie che trasmettono o portano a scuola.
- I fornitori.

In particolare, nel documento vengono definiti i criteri tecnici e organizzativi per:

- La protezione delle aree e dei locali interessati dalle misure di sicurezza, nonché le procedure per controllare l'accesso delle persone autorizzate ad accedere ai medesimi locali.
- I criteri e le procedure per assicurare l'integrità dei dati.
- I criteri e le procedure per la sicurezza e la trasmissione dei dati, cartacei e telematici.
- L'elaborazione di un piano di formazione per rendere edotti gli incaricati del trattamento dei rischi che incombono sui dati e dei modi per prevenire gli eventi dannosi.

CAMPO DI APPLICAZIONE

Il trattamento dei dati personali è funzionale al raggiungimento delle finalità di istruzione e di formazione in ambito scolastico, professionale e superiore con particolare riferimento a quelle svolte anche in forma integrata, ed è quindi di rilevante interesse pubblico, ai sensi degli art. 20 e 21 del D. L.vo 196/2003. Per le sue finalità istituzionali, l'Istituzione scolastica tratta dati personali, sia comuni che sensibili e giudiziari, di studenti, genitori, personale dipendente, collaboratori esterni e fornitori.
I trattamenti sono realizzati prevalentemente negli uffici di Presidenza e di Segreteria, nell'archivio della sede centrale, nelle aule scolastiche e nelle sale docenti.

I dati su supporto cartaceo sono conservati negli armadi chiusi a chiave degli uffici di segreteria, dell'ufficio del DSGA, nell'ufficio del Dirigente e nell'Archivio della sede centrale.
I dati acquisiti attraverso il Protocollo riservato e quelli relativi agli alunni disabili sono conservati nell'ufficio del Dirigente scolastico.
I docenti custodiscono i dati degli alunni in sala docenti che è chiusa a chiave.
I dati su supporto elettronico sono conservati negli archivi elettronici dei computer di tutti i servizi amministrativi e una copia degli stessi conservata nell'armadio di sicurezza della segreteria.

Tali dati si distinguono in:

- **DATI PERSONALI COMUNI**: dati anagrafici o identificativi delle persone, indirizzi, recapiti telefonici, codici fiscali, dati bancari, informazioni circa la composizione familiare, la professione esercitata da un determinato soggetto, la sua formazione, la sua carriera, ecc…

- **DATI SENSIBILI**: dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute, appartenenza a categorie protette, disabili, stato di gravidanza, vita sessuale, ecc…

- **DATI GIUDIZIARI**: provvedimenti sul casellario giudiziale, anagrafe delle sanzioni amministrative dipendenti da reato o dei relativi carichi pendenti, la qualità di imputato o indagato ai sensi degli Artt. 60 e 61 del Codice di Procedura Penale, avviso di garanzia, separazioni, affidamento dei figli, ecc…

1. Elenco dei trattamenti di dati personali (ex regola 19.1)

Poiché questo elenco rientra nell'organizzazione e nelle politiche di privacy adottate, anche se il paragrafo dell'Allegato B è stato soppresso, vengono fornite le informazioni essenziali in merito alla classificazione dei dati personali trattati e si precisano le modalità di trattamento dei dati effettuato dal Titolare, con l'indicazione della natura dei dati trattati e della struttura che operativamente effettua il trattamento.

- DATI TRATTATI DAI DOCENTI

Le banche dati cui ha accesso il singolo docente sono:
- Il registro personale [1]
- Gli elaborati

Le banche dati cui hanno accesso più docenti sono:
- Il registro di classe
- Il registro dei verbali del consiglio di classe o di interclasse
- La documentazione relativa alla programmazione didattica
- I documenti di valutazione
- La documentazione dello stato di handicap
- La corrispondenza con le famiglie
- La documentazione giustificativa delle assenze degli alunni (es. festività religiose, certificati medici, etc)

I dati trattati dai docenti sono nel loro insieme dati sensibili, ai sensi dell'art.4 del D. L.vo n.196 del 30 giugno 2003 comma 1 lett. b, c, d. Il trattamento dei dati da parte dei docenti (tenuta dei registri,

[1] Registro del singolo docente

modalità di compilazione dei documenti di valutazione, verbalizzazione, etc.) è definito puntualmente da norme di legge o regolamentari.

- **DATI TRATTATI DAL PERSONALE AMMINISTRATIVO**

Le banche dati su supporto cartaceo e/o informatizzato, contenenti dati personali, cui ha accesso il personale di segreteria, raggruppati in insiemi omogenei, sono:

- Fascicoli relativi al personale della scuola,
- Fascicoli alunni ed ex alunni
- Anagrafica fornitori
- Contratti e convenzioni
- Documentazione finanziaria e contabile
- Documentazione didattica trattata dai docenti per la conservazione
- Registro degli infortuni

- **DATI TRATTATI DAL DIRIGENTE SCOLASTICO**

Le banche dati di pertinenza del dirigente sono:

- Fascicoli del personale in servizio
- Verbali delle assemblee degli Organi Collegiali
- Programmazione relativa allo stato di disagio (handicap)
- Protocollo riservato
- Fascicoli del personale in prova

Tabella 1.1. Elenco dei trattamenti: informazioni di base

1		2	3	4	5
Identificativo del Trattamento		Natura dei dati trattati S G	Struttura di riferimento	Altre strutture concorrenti al trattamento	Descrizione degli strumenti utilizzati
Id.	Descrizione sintetica				
Tr.1	Selezione e reclutamento personale a Tempo indet. e determ. Gestione del rapporto di lavoro del personale.	S G	Ufficio del Dirigente Scolastico, DSGA e Segreteria Amm.va	Collaboratori del D.S., Collaboratori scolastici.	Documenti cartacei, registri e computers.
Tr.2	DIPENDENTI E ASSIMILATI : Gestione del contenzioso e procedimenti disciplinari	S G	Dirigente Scolastico, DSGA e Segreteria Amministrativa		Documenti cartacei e computers.
Tr.3	Organismi collegiali e Commissioni istituzionali	S	Dirigente Scolastico DSGA e Segreteria Amministrativa	Collaboratori del D. S., Docenti, Collab. scolastici, Membri esterni degli OO. CC.	Documenti cartacei e computers
Tr.4	Attività propedeutiche all' avvio dell'anno scolastico	S G	Dirigente Scolastico DSGA e Segreteria Amministrativa	Collaboratori del D.S., Docenti, Collab. Scolastici	Documenti cartacei, registri e computers
Tr.5	Attività educativa, didattica e formativa, di valutazione	S G	Dirigente Scolastico DSGA e Segreteria Amministrativa.	Collaboratori del Dir. Scol., Docenti, Collab. Scolastici, membri esterni degli OO. CC.	Documenti cartacei, registri e computers

Tr.6	Scuole non statali	S G	Dati non trattati nel ns. Istituto		Documenti cartacei e computers
Tr.7	Rapporti scuola – famiglie : gestione del contenzioso	S G	Dirigente Scolastico DSGA, Segreteria e Docenti.		Documenti cartacei e computers
Tr.8	Fornitori e clienti		Dirigente Scolastico DSGA e Segreteria Amministrativa	Collaboratori del D.S., Docenti nelle commissioni, Membri di OO.CC. Collab. scolastici,	Documenti cartacei e computers
Tr.9	Gestione finanziaria e contabile		Dirigente Scolastico DSGA e Segreteria Amministrativa	Collaboratori del D.S.G.A.	Documenti cartacei, registri e computers
Tr.10	Gestione Istituzionale		Dirigente Scolastico DSGA e Segreteria	Collaboratori del D.S.	Documenti cartacei, registro protocollo, e computers

Questa tabella indica trattamenti di dati sia cartacei che elettronici.

Il trattamento dei dati avviene attraverso modalità diverse: strumenti elettronici (n. 8 P.C. interni situati in 3 Uffici di segreteria, collegati in rete fra loro, con collegamenti alla rete Intranet e alla rete Internet, 1 Server (S01) collegato in rete.
Con riferimento alla gestione dei dati mediante rete ministeriale, l'Istituzione scolastica declina ogni responsabilità, operando come semplice utente, non essendo in grado di intervenire sulla gestione delle informazioni ivi contenute e gestite.

Con riferimento all'ubicazione fisica dei supporti di memorizzazione delle copie di sicurezza, l'Istituzione scolastica, tenendo conto dell'analisi di cui al punto 3, ha ritenuto di provvedere alla custodia dei supporti presso la segreteria, riservandone l'accesso al D.S.G.A. Giuseppe Sebastianelli.

2. Distribuzione dei compiti e delle responsabilità (ex regola 19.2)

Tabella 2.1. Strutture preposte ai trattamenti e attribuzione delle responsabilità.

Il decreto legislativo n.196 del 30 giugno 2003 sulla protezione dei dati personali individua all'art. 4, i soggetti che sono coinvolti nel trattamento dei dati personali:

- IL TITOLARE DEL TRATTAMENTO DEI DATI PERSONALI

Il Titolare del trattamento è il soggetto che, nel raccogliere i dati personali decide come ed in base a quali finalità (ad esempio per il rapporto di lavoro, per una finalità didattica, etc.) effettuerà il trattamento dei dati raccolti. Pertanto, ai sensi di legge, l'Istituzione scolastica, rappresentata dal Dirigente scolastico (art.28 D. L.vo n.196 del 30 giugno 2003) è "Titolare" dei dati personali da essa trattati con l'ausilio di mezzi informatici e cartacei.
Il Titolare, **quindi,** è la persona fisica e giuridica che ha la responsabilità finale ed assume decisioni fondamentali riferite al trattamento dei dati personali.

- IL RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI

In base a quanto disposto dell'art.29 comma 2 del D. L.vo n.196/2003
"*Il responsabile, se designato, deve essere nominato fra i soggetti che, per esperienza, capacità ed affidabilità, forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo della sicurezza*".

Il Dirigente scolastico ha individuato come Responsabile per il trattamento dei dati che riguardano in modo specifico i servizi di segreteria e il personale ausiliario, il Direttore dei Servizi Generali ed Amministrativi Giuseppe Sebastianelli.

- GLI INCARICATI DEL TRATTAMENTO DEI DATI PERSONALI

L'Incaricato è la persona fisica che materialmente provvede al trattamento dei dati, secondo le istruzioni impartite dal titolare o dal responsabile. Nella scuola i soggetti designati al trattamento dei dati sono i docenti, il personale amministrativo, i collaboratori scolastici e i membri del Consiglio d'istituto.
- Il **Docente, interno ed esterno**, è da considerarsi, per la propria sfera di competenza, incaricato del trattamento e come tale è stato nominato mediante specifico atto che elenca puntualmente: categorie dei dati cui può avere accesso; tipologia di trattamento e vincoli specifici applicabili alla varie tipologie di dati; istruzioni in merito ai soggetti cui i dati possono essere comunicati o diffusi.
- Ogni **Assistente amministrativo** è stato nominato incaricato del trattamento con specifico atto, in base ai compiti che assolve nell'ufficio.
- I **Collaboratori scolastici,** trattando anche saltuariamente dati personali, sono stati incaricati con specifico atto.

- L'INTERESSATO

L'interessato è la persona fisica (persona giuridica, ente o associazione) a cui si riferiscono i dati personali oggetto di trattamento.

Questa parte del documento contiene quindi una mappa delle strutture con l'elenco dei trattamenti da esse effettuati. Per ogni struttura è definita sinteticamente l'organizzazione della stessa e le relative responsabilità.

- L'AMMINISTRATORE DI SISTEMA

Il Titolare dei Trattamenti, recependo la segnalazione del Garante Privacy: Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema – 27 novembre 2008, G.U. n. 300 del 24 dicembre 2008 ai sensi dell'art. 154, comma 1, in considerazione anche delle responsabilità, specie di ordine penale e civile (artt. 15 e 169 del Codice), che possono derivare in caso di incauta o inidonea designazione, ha provveduto alla formale nomina dell'amministratore di sistema quale figura professionale preposta alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti.

In pratica "l'amministratore di sistema" deve possedere quelle conoscenze tecniche per eseguire il salvataggio dei dati, per l'organizzazione dei flussi di rete, per la gestione dei supporti di memorizzazione, per intervenire sull'hardware. Quindi ha la possibilità di accedere a tutti i dati personali presenti nel sistema gestionale.

Tabella 2.1. Strutture preposte ai trattamenti.

1	2	3	4
Struttura:	Responsabile:	Trattamenti operati dalla struttura:	Compiti della struttura:
Dirigente Scolastico	Dirigente Scolastico	Tutti	Direzione generale di tutte le attività, gestione delle pratiche riservate
INCARICATI INTERNI, UNITA' ORGANIZZATIVE OMOGENEE:			
Collaboratrice Vicaria del DS	Dirigente Scolastico	Tutti (potenzialmente)	Collaborazione con il D. S. con deleghe parziali e sostituzione dello stesso in caso di assenza
Segreteria	D .S. G. A. Responsabile del trattamento	Tutti Tr .3 anche dati sindacali. In casi eccezionali: Tr.1, Tr.5 (dati sensibili).	Gestione amministrativa di tutte le pratiche, supporto al Dirigente Scolastico e al Corpo Docente
Corpo Docente	Dirigente Scolastico	Tr.3, Tr.4, Tr.5, Tr.7, Tr.8, Tr.9, Tr.10 Tr .3 anche dati sindacali. In casi eccezionali: Tr.1, Tr.5 (dati sensibili). Se membri di commissione Tr.2 (dati sensibili o giudiziari).	Insegnamento e attività integrative e collaterali, partecipazione alle scelte organizzative e di orientamento generale, partecipazione alla gestione di specifiche attività (Biblioteca, scelte degli acquisti, commissioni varie, ecc,)
Collaboratori Scol. (Personale ausiliario)	D. S. G. A. Responsabile del trattamento	Tutti, con attività di supporto. E limitatamente alle strette esigenze della funzione	Apertura e chiusura della sede, custodia e controllo, consegna e ricezione plichi e lettere, pulizia, assistenza a tutte le altre attività, gestione di dati comuni di alunni, docenti e familiari
Membri ESTERNI di Organi Collegiali	Dirigente Scolastico	Tr.3 e tutti gli altri (tranne Tr.6) limitatamente alle strette esigenze della funzione	Partecipazione alle attività gestionali e alle scelte organizzative e di orientamento generale, nonché al C.d.I. e alla G. E. , decisioni di tipo amministrativo, finanziario e regolamentare
INCARICATI INTERNI CON COMPITI SPECIFICI O ULTERIORI:			
Incaricato del Backup periodico e coordinatore del <Disaster recovery> e delle prove di ripristino	D. S. G. A. Responsabile dei trattamenti in questione	Tutti, ma limitatamente alla funzione.	Esegue il back-up periodico (anche settimanale) degli archivi informatici contenenti dati personali. Coordina l'impostazione del piano di recupero in caso di disastro informatico che comporti l'inagibilità del sistema o la perdita di dati personali. Coordina le prove obbligatorie di efficienza del back-up e di ripristino dei dati dalla copia di salvataggio.
Custode delle chiavi degli archivi ad	DSGA Responsabile	Tutti i trattamenti non informatici, ma limitatamente	E' l'unico detentore delle chiavi degli archivi ad accesso controllato e

accesso controllato. Vice-custode delle chiavi.	dei trattamenti in questione e l'Ass. Amm.vo incaricato che lo sostituisce.	alla funzione	consegna all'Incaricato autorizzato all'accesso a un certo archivio la relativa chiave; la riceve di ritorno non appena cessata l'attività. Il vice lo sostituisce in caso di assenza.
Custode delle passwords	DSGA Responsabile dei trattamenti in questione	Tutti i trattamenti informatici , ma limitatamente alla funzione	Gli Incaricati muniti di accesso al computer mediante password, ad ogni scadenza della password (3 o 6 mesi, a seconda dei casi) ricevono una busta chiusa contenente la password, da tenere a disposizione in caso di necessità di accesso agli archivi elettronici di quell'Incaricato quando è assente
R. L. S. (Rappresentante dei lavoratori per la Sicurezza)	Ins.te Cacciotti Maria Teresa	Consultazione di tutti i documenti e materiali informatici inerenti alla funzione e risultanti come diritto di conoscenza	Contributo all'applicazione normativa D. L.vo 626/1994 e norme collegate; gestione sicurezza sul posto di lavoro e nella scuola in generale; verifica
RESPONSABILI INTERNI DI TRATTAMENTO:			
RESPONSABILE DEI TRATTAMENTI: D.S.G.A.	Direttore dei Servizi Generali ed Amm.vi	Tutti i trattamenti, limitatamente alla gestione amministrativo-contabile e alla gestione delle attività del personale di segreteria e dei Collaboratori scolastici.	Gestione amministrativa di tutte le pratiche, supporto al Dirigente Scolastico e al Corpo Docente
INCARICATI ESTERNI:			
R.S.P.P. o Addetto al S.P.P. ai sensi del D. Lgs 626/1994	Ing. Vita Davide	Trattamenti relativi alla applicazione della normativa 626 o ad essa riferiti: *Trattamenti autorizzati: tutti i trattamenti informatici e non, rigorosamente nei limiti relativi alle funzioni.*	Applicazione normativa D. L.vo 626/1994 e norme collegate; gestione sicurezza sul posto di lavoro e nella scuola in generale
Incaricato Esterno Amministratore di Sistema	Axios Italia Service srl Roma	*Tutti i trattamenti informatici, rigorosamente nei limiti relativi alle funzioni*	Gestione sistema informatico per la gestione della segreteria scolastica
Docenti Esterni (Con Contratti di Prestazione d'opera occasionale) per le attività didattiche, educative e formative	Dirigente Scolastico	*Trattamenti non informatici:* Tr.5 - Attività educativa, didattica e formativa, rigorosamente nei limiti relativi alle funzioni.	Attività di insegnamento a favore degli alunni della scuola interessati ai progetti di Laboratorio Musicale e di potenziamento delle Lingue straniere.

3. Analisi dei rischi che incombono sui dati (ex regola 19.3)

3.1 SITUAZIONE ATTUALE

I dati che seguono sono relativi a una rilevazione effettuata nel mese di Gennaio 2017.

3.1.1. Plessi e loro collocazione

Sede principale	Indirizzo	Città/paese
Presidenza e uffici di segreteria	Via A. Olivetti n. 41	Terracina
Plesso di Scuola Primaria e Infanzia "Giovanni Paolo II "	Via De Angelis	Terracina
Plesso di Scuola Primaria e Infanzia "G. Manzi"	Via Zicchieri	Terracina
Plesso di scuola Primaria e Infanzia "Francesco Lama"	Via G. Leopardi	Terracina

3.1.2. Locali dove avviene il trattamento dei dati da parte del personale docente

- I locali in cui i docenti effettuano il trattamento dei dati coincidono con quelli adibiti all'attività didattica, allocati nella sede centrale dell'Istituto e nei plessi di Scuola primaria e Infanzia.
- Esistono, nei plessi, locali di pertinenza esclusiva del personale docente (sala insegnanti).
- Il trattamento dei dati da parte dei docenti avviene su supporti cartacei e informatici (Registro elettronico).
- Le banche dati contenenti documentazione didattica (registri personali e di classe) vengono consegnati all'inizio dell'anno scolastico dal Dirigente scolastico ai docenti, che provvedono alla loro compilazione, conservazione e custodia.
  I tablet utilizzati per il registro elettronico vengono consegnati all'inizio delle lezioni ai docenti dal collaboratore scolastico incaricato e dagli stessi ritirati al termine delle lezioni per essere custoditi nell'apposito armadio di sicurezza
- All'interno delle banche dati di cui si tratta vengono custoditi temporaneamente, in attesa di sistemazione nei fascicoli personali, i certificati medici degli alunni.
- Le banche dati contenenti documentazione didattica vengono consegnati dai docenti al personale di segreteria.
- I verbali dei Consigli di Classe e degli Organi collegiali, la programmazione didattica e tutta la documentazione per gli allievi portatori di handicap è custodita e conservata dal Dirigente Scolastico.

3.1.3 Locali dove avviene il trattamento effettuato dal Dirigente scolastico e dal personale Amministrativo

I locali interessati al trattamento dei dati da parte del personale di segreteria e da parte del Dirigente Scolastico sono ubicati nella sede principale dell'Istituto sita in via A. Olivetti n. 41 in Terracina.

3.1.4 Descrizione generale dell'edificio che ospita gli uffici della Presidenza e di Segreteria

L'edificio della sede centrale, situato in via A. Olivetti, n. 41 a Terracina, che ospita i locali dell'Istituto Comprensivo "Milani" presenta le seguenti caratteristiche:

Accesso	Via A. Olivetti, n. 41
Recinzione	Muretto con inferriata
Cortile/giardino esclusivo	Si
Parcheggi esclusivi	No
Cancelli esterni di accesso all'edificio	Si, con serratura
Illuminazione esterna e interna	Si
Piani interrati	Si (un piano)
Sistema generale di allarme	Si
Locali utilizzati da altri soggetti	Un locale, interno alla struttura ma esterno all'edificio scolastico, utilizzato dal custode.

3.1.5. Descrizione dei locali della Direzione e dei Servizi Amministrativi

I locali, posti nella sede centrale della Scuola, sono collocati al piano terra cui si accede dal cortile/giardino della scuola stessa.
Sul corridoio al piano terra si affacciano:

- Ala destra dell'edificio
    1. Presidenza (stanza S01)
    2. Locali adibiti all'attività amministrativa: Segreteria (stanze S02 - S03 – S04)
    3. Sala ricevimento genitori (stanza S05)
    4. Ufficio della docente Vicaria del Dirigente scolastico (stanza S06)
    5. Sala docenti (stanza S07)
- Ala sinistra dell'edificio
    5. Ufficio di prima accoglienza utenza (Stanza S08 dei Collaboratori scolastici)
    6. Archivio cartaceo storico posto al piano interrato (Stanza S09)

L'Archivio cartaceo principale (corrente) è posto al piano terra negli uffici di segreteria (Stanze S02, S03 e S04).

3.1.6 Descrizione generale dell'edificio che ospita il plesso di Scuola Primaria e Infanzia "G. Manzi" (ex 4° Circolo)

L'edificio, situato in via Zicchieri, presenta le seguenti caratteristiche:

Accesso	Via Zicchieri
Recinzione	Muretto con inferriata
Cortile	Si
Parcheggi esclusivi	Si
Cancelli esterni di accesso all'edificio	Si, con serratura
Illuminazione esterna e interna	Si
Piani interrati	No
Sistema generale di allarme	Si

- Piano Terra

Sul corridoio si affacciano:

1. Ufficio della ex Dirigenza (stanza S01)
2. Ufficio della ex Segreteria (stanza S02 – S03)
3. Sala docenti (stanza S04)
4. Stanze adibite ad aule e la sala mensa (S05)
5. Ex Archivio cartaceo corrente (S06)
6. Archivio cartaceo storico (S07)

3.1.7 Descrizione generale dell'edificio che ospita il plesso di Scuola Primaria e Infanzia " Giovanni Paolo II "

L'edificio, situato in via De Angelis, presenta le seguenti caratteristiche:

Accesso	Via De Angelis
Recinzione	Muretto con inferriata
Cortile	Si
Parcheggi esclusivi	Si
Cancelli esterni di accesso all'edificio	Si, con serratura
Illuminazione esterna e interna	Si
Piani interrati	No
Sistema generale di allarme	Si

- Piano Terra

Sul corridoio si affacciano:

1. Ufficio della ex Dirigenza (stanza S01)
2. Ufficio della ex Segreteria (stanza S02 – S03)
3. Sala docenti (stanza S04)
4. Stanze adibite ad aule e la sala mensa (S05)
5. Ex Archivio cartaceo corrente (S06)
6. Archivio cartaceo storico (S07)

3.1.8 Descrizione generale dell'edificio che ospita il plesso di Scuola Primaria e Infanzia " Francesco Lama "

L'edificio, situato in via Giacomo leopardi, presenta le seguenti caratteristiche:

Accesso	Via De Angelis
Recinzione	Muretto con inferriata
Cortile	Si
Parcheggi esclusivi	No
Cancelli esterni di accesso all'edificio	Si, con serratura
Illuminazione esterna e interna	Si
Piani interrati	No
Sistema generale di allarme	No (in fase di attuazione)

- Piano Terra

➢ Piano Terra

Sul corridoio si affacciano:

1. Ufficio della ex Dirigenza (stanza S01)
2. Ufficio della ex Segreteria (stanza S02)
3. Sala docenti (stanza S03)
4. Stanze adibite ad aule e la sala mensa (S04)

3.2. ANALISI DEI RISCHI CHE INCOMBONO SUI DATI

I rischi che in generale incombono sui dati possono riguardare:

① Dati trattati con materiale cartaceo
② I luoghi e i contenitori che custodiscono tali dati
③ I dati in forma elettronica

I Dati cartacei a rischio sono:

· Raccoglitori dei documenti contenuti nei fascicoli del personale;
· Schede personali degli alunni;
· Registri di classe, giornale dell'insegnante, di presenza;
· Registro dello stato del personale;
· Decreti e certificati sulle persone;
· Anagrafica fornitori;
· Contratti e convenzioni;
· Documentazione finanziaria e contabile;
· Registro infortuni personale e alunni;
· Moduli di iscrizione, istanze, ecc…

I dati informatici a rischio sono:

- Anagrafica del personale, degli alunni e dei fornitori;
- Documentazione finanziaria e contabile;
- Contratti personale esterno e supplente;
- Protocollo.

Gli eventi che possono generare danni e che comportano rischi per la sicurezza dei dati personali si distinguono in:

1. Comportamento degli operatori:

- Sottrazione di credenziali di autenticazione;
- Carenza di consapevolezza, disattenzione e incuria;
- Manomissioni e comportamenti sleali e fraudolenti.

2. Eventi relativi agli strumenti:

- Azione di **virus informatici o di programmi** suscettibili di recare danno;
- **Spamming, tecnica di sabotaggio o posta spazzatura**: vettore attraverso il quale si fanno circolare virus e codici maligni di ogni tipo con l'obiettivo di compromettere il funzionamento delle apparecchiature informatiche e rendere al contempo più difficile l'individuazione da

parte delle forze dell'ordine preposte al compito di garantire la sicurezza della società;
- **Hacker:** persona che utilizza la sua abilità informatica in modo fraudolento con lo scopo di elaborare un virus o penetrare in una rete informatica protetta;
- **Malfunzionamento**, indisponibilità o degrado degli strumenti;
- **Accessi esterni** non autorizzati;
- **Intercettazioni** di informazioni in rete.

3. Eventi relativi al contesto fisico-ambientale:

- Eventi distruttivi, naturali o artificiali nonché dolosi, accidentali o dovuti ad incuria;
- Accesso di estranei o persone non titolari di incarichi e responsabilità nel trattamento dei dati;
- Errori umani nella gestione della sicurezza fisica;
- Accessi esterni non autorizzati;
- Vandalismo e/o sottrazione di strumenti contenenti dati;
- Intercettazioni di informazioni in rete;
- Guasto a impianti elettrici, gruppi di continuità, sistemi di climatizzazione, ecc….

Tabella 3.2. Analisi dei rischi

In questa tabella sono evidenziati i principali eventi potenzialmente pericolosi per la sicurezza dei dati, con la valutazione delle conseguenze e della loro gravità, in correlazione con le misure previste:

1		2		3
Evento		Impatto sulla sicurezza dei dati		Misure d'azione
		Descrizione	Gravità stimata	
Comportamento degli operatori	Furto delle credenziali di autenticazione	Accesso non autorizzato al computer	Bassa	Istruzioni agli Incaricati, formazione, azione del "Custode delle Parole-chiave", controllo accesso ai locali chiusi a chiave quando non presidiati, divieto di accesso ai locali alle persone non autorizzate
	Carenza di consapevolezza, disattenzione o incuria	Le credenziali perdono la riservatezza o i dati riservati sono resi visibili	Bassa	Stesse misure d'azione adottate per il furto delle credenziali di autenticazione
	Comportamenti sleali o fraudolenti	Accesso per fini personali ai dati (che però sono poco appetibili), che vengono conosciuti da Incaricati che non ne hanno diritto	Bassa	Come precedente, inoltre: eventuale creazione di profili di autorizzazione diversificati e utilizzo cifratura per i rari files contenenti dati sensibili, giudiziari o particolari importanti.
	Errore materiale	Cancellazione o perdita di dati	Bassa (esiste copia cartacea di tutto)	Formazione degli incaricati, profilo di autorizzazione che non consente la formattazione dei dischi fissi o la

				cancellazione di files importanti.
Eventi relativi agli strumenti	Azione di *virus* informatici	Cancellazione dati, malfunzionamenti o blocco del sistema, trasmissione casuale di dati a indirizzi di posta elettronica memorizzati, confusione con incapacità di individuare dati utili	Alta	Regolare aggiornamento dell'antivirus e del software, con istruzioni agli incaricati e regolare monitoraggio di controllo sull'effettiva attuazione, istruzioni a individuare e prevenire le situazioni a rischio
	Spamming (posta indesiderata e disturbante) o altre tecniche di sabotaggio	Confusione con rischio di non individuazione di messaggi utili o di loro cancellazione per errore.	Medio/alta	Formazione degli Incaricati a riconoscere i messaggi di disturbo e a gestire le regole di assegnazione delle e-mail alle varie cartelle
	Malfunzionamento, indisponibilità o degrado degli strumenti	Malfunzionamenti o blocco del sistema	Media	Manutenzione programmata, formazione ad individuare i sintomi di malfunzionamento per un rapido intervento, piano di back-up - Disaster Recovery e di continuità operativa
	Accessi esterni telematici non autorizzati	Visione indebita di dati o sabotaggio	**Bassa** (dati non appetibili il cui valore si basa sul cartaceo originale)	Dispositivo Firewall
	Intercettazione di informazioni in rete	Visione indebita di dati	Minima	Eventuale adozione di cifratura o firma elettronica per proteggere i dati più gravi (allo studio)
	Accessi non autorizzati a locali ad accesso ristretto	Sabotaggio delle macchine, con eventuale perdita di dati; accesso abusivo se le credenziali fossero lasciate disponibili	Sabotaggio: Bassa Altro: Bassa	Solidità degli infissi dei locali, chiusura a chiave quando non presidiati, allarme antifurto, disponibilità di estintori ad anidride carbonica per non danneggiare i computers, istruzioni a tutti gli operatori
Eventi relativi al contesto	Asportazione e furto di strumenti contenenti dati	Perdita di dati, rallentamento o blocco dell'attività per carenza di PC	Probabilità media, gravità alta	Come punto precedente Inoltre, regolare back-up dei dati, piano di back-up - Disaster Recovery e di continuità operativa
	Eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti ad incuria	Perdita di dati, rallentamento o blocco dell'attività per carenza di PC	Probabilità minima, gravità massima	Come punto precedente, allarme antincendio, inoltre sensibilizzazione e formazione del personale incaricato o

				di infiltrazioni d'acqua, incendio, inondazioni, terremoti (eseguita). Verifica della logistica degli apparecchi e del loro corretto posizionamento. Custodia dei dischi di back-up in armadio di sicurezza ignifugo
	Guasto ai sistemi complementari (impianto elettrico)	Perdita di dati e blocco del sistema	Bassa	Gruppo di continuità funzionanti, assistenza e manutenzione periodica.
	Guasto ai sistemi complementari (climatizzazione)	Surriscaldamento dei computers e in particolare della scheda madre o altre componenti, con possibilità di guasto	Bassa	Revisione regolare delle ventole interne e loro potenziamento. Verifica della logistica degli apparecchi e del loro corretto posizionamento.
	Errori umani nella gestione della sicurezza fisica.	Danni agli strumenti, con possibile perdita di dati e cattivo funzionamento.	Bassa	Formazione e sensibilizzazione di tutti gli Incaricati per il controllo. Verifica della logistica degli apparecchi e del loro corretto posizionamento.

4. Misure in essere e da adottare (ex regola 19.4)

Al fine di garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali rilevanti ai fini della loro custodia ed accessibilità, sono state adottate le seguenti misure di sicurezza:

- ✓ Individuazione e nomina del Responsabile del trattamento dei dati per l'accesso ai computer e per garantire tutte le misure di sicurezza necessarie alla conservazione e utilizzazione dei dati.
- ✓ Misure di prevenzione per eliminare gli eventuali incendi con adeguate modalità di gestione degli stessi.
- ✓ Individuazione dei locali e contenitori adeguati
- ✓ Regolamentazione con linee guida sia per il personale che per gli esterni nell'accesso ai locali e alle attrezzature che conservano dati, archivi e documentazione
- ✓ Attuazione di misure di protezione dei locali
- ✓ Periodico salvataggio dei dati informatici del server su unità rimovibili
- ✓ Verifica periodica della funzionalità e dell'efficienza delle misure di protezione e delle strutture operative che ne hanno la responsabilità.
- ✓ Installazione di dispositivo Firewall al fine di impedire ingressi di pirati o intercettazioni sulla rete informatica di questa istituzione scolastica con la configurazione di password e impostazioni di tutte le misure di sicurezza necessarie.

✓ Installazione di Antivirus per la protezione dei dati dall'attacco di virus informatici

4.1 PROTEZIONE DELLE AREE E DEI LOCALI

La sicurezza di aree e locali ha il compito di prevenire accessi fisici non autorizzati, danni o interferenze nello svolgimento dei servizi. Le contromisure attuate si riferiscono alla protezione perimetrale dei siti, ai controlli fisici all'accesso, alla sicurezza degli archivi e delle attrezzature informatiche rispetto ai danneggiamenti accidentali o intenzionali, alla protezione fisica dei supporti.

- Contro i rischi d'intrusione i locali della sede centrale sono dotati di impianto d'allarme a sensori infrarossi, attivabile mediante digitazione di un codice consegnato al collaboratore scolastico incaricato del trattamento e custode della scuola. L'attivazione dell'allarme viene disposta al termine dell'orario di lavoro.

- Per garantire la sicurezza delle aree in cui i dati sono trattati elettronicamente, sono state introdotte sui personal computer password di BIOS per accedere al sistema e password di rete per accedere alle aree specifiche del programma AXIOS che contengono i dati personali e sensibili relativi agli alunni, al personale, al bilancio e alle retribuzioni.

- Le aree contenenti dati in supporto cartaceo (archivio e armadi contenenti documentazioni contabili dei dipendenti e degli alunni) sono ubicate in modo tale che ciascun addetto possa rilevare a vista e impedire il tentativo di accesso da parte di persone estranee.

- Sono state impartite disposizioni affinché, in assenza del personale, le stanze rimangano chiuse e le chiavi siano custodite dal personale collaboratore scolastico in servizio addetto alla vigilanza. L'ubicazione negli uffici di segreteria di stampanti ed apparecchio telefax tradizionale non consente ad estranei di leggere od asportare eventualmente documenti non ancora prelevati dal personale.

- Tutti i plessi sono dotate di impianto elettrico a norma e di appositi estintori, controllati e periodicamente sostituiti.

4.2 PROTEZIONE INTEGRITA' DEI DATI

Le norme applicate per garantire la sicurezza e l'integrità dei dati sono le seguenti:

- **Computer e supporti informatici:**

- I computer, inclusi i server, risultano tutti sollevati da terra, in modo da evitare eventuali danni dovuti ad allagamenti; sono collegati a gruppi di continuità che consentono di escludere la perdita di dati derivanti da sbalzi di tensione o interruzione di corrente elettrica.
- L'integrità dei dati è inoltre garantita da idonee procedure di salvataggio periodico (backup) che consistono nell'utilizzo dell'apposito software di backup del programma di gestione amministrativa e contabile (il quale crea una copia compressa dei dati, archiviandoli in una apposita cartella del server stesso) e di un masterizzatore DVD, che consente il salvataggio degli archivi anche su disco DVD registrabile.
- Le copie di back up sono adeguatamente conservate a cura del Responsabile del Trattamento dati nell'armadio di sicurezza collocato nell'ufficio del DSGA che ne garantisce la protezione da:
  - agenti chimici
  - fonti di calore
  - campi magnetici
  - intrusione ed atti vandalici, furto
  - incendio
  - allagamento

L'accesso ai supporti utilizzati per il back up dei dati è limitato
· al Titolare del trattamento (Dirigente Scolastico)
· al Responsabile del trattamento della sicurezza dei dati (DSGA)
· all'Amministratore di Sistema (Società AXIOS Italia)
· agli Incaricati al trattamento (Assistenti amministrativi)

- L'introduzione di password all'accensione del personal computer e di password per l'accesso in rete determina un soddisfacente livello di protezione dei dati contenuti nei PC.
L'introduzione delle password inibisce ad estranei l'uso dei personal computer, attraverso i quali si accede alla posta elettronica.
- Al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita degli stessi a causa di virus informatici, i computer sono dotati di programma antivirus aggiornato annualmente e che consente di rilevare immediatamente all'apertura di un file la presenza di virus.

• **Supporti cartacei:**
Relativamente ai supporti cartacei sono state impartite dettagliate istruzioni al personale al momento dell'affidamento dell'incarico e nel corso degli interventi di formazione.

4.3 MISURE SPECIFICHE PER I DATI PERSONALI IDONEI A RIVELARE LO STATO DI SALUTE.

Questa istituzione tratta, occasionalmente, dati personali che rivelano lo stato di salute del personale, docente ed ATA e degli alunni esclusivamente per finalità previste dalla legge.
Secondo quanto prescritto dall'art.22 comma 7 del D. L.vo n.196/2003 i dati idonei a rivelare lo stato di salute "*sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo*".
Riguardo al trattamento senza l'ausilio di strumenti elettronici, dei dati di cui trattasi, si stabilisce quanto segue:

a) Dati riguardanti il personale docente ed a.t.a.

I dati consistono essenzialmente in certificati medici telematici.
Dopo la ricezione e protocollazione vengono inseriti nei relativi fascicoli personali, dove sono conservati all'interno di una busta chiusa recante l'indicazione del contenuto separatamente dagli altri documenti.

b) Dati riguardanti gli alunni

I dati consistono essenzialmente in certificati medici consegnati dai genitori ai docenti o al personale di segreteria, per scopi definiti da norme di legge (giustificazione assenze; esonero da attività di educazione fisica, necessità di particolari diete alimentari, etc).
Dopo la ricezione i dati vengono trattati e quindi custoditi in appositi contenitori chiusi.
I certificati riguardanti la necessità di particolari diete alimentari, possono in caso di necessità, essere comunicati al soggetto che espleta il servizio mensa previamente nominato responsabile esterno del trattamento da parte del titolare.

Tutti i dati contenuti in documentazione cartacea sono raccolti e conservati negli armadi di protezione dati situati nella Segreteria della Sede centrale dell'Istituto e negli armadi di protezione dati collocati negli uffici delle ex segreterie dei plessi staccati di Scuola Primaria e Infanzia.

5. Criteri e modalità di ripristino della disponibilità dei dati (ex regola 19.5)

I dati trattati dalla scuola in forma elettronica servono:

- a produrre documenti cartacei che sono conservati e che sono gli unici documenti ad avere valore legale
- ad elaborare dati provenienti da documenti cartacei che sono conservati e che sono gli unici documenti ad avere valore legale
- per produrre comunicazioni ad altri Enti (Tesoro, Ministero della Funzione Pubblica, MIUR, ecc.) e cessa la necessità di conservarli in forma elettronica non appena la comunicazione ha avuto effetto.
- per ricevere comunicazioni provenienti dall'esterno, delle quali di norma si fa immediatamente la copia cartacea, che viene poi conservata e che è l'unica ad avere valore legale. L'unica eccezione sono determinati allegati che non contengono dati personali e che non si ritiene utile stampare.

Al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita, è stata adottata una procedura di periodica esecuzione di copie di sicurezza dei dati trattati, eseguita settimanalmente dal D.S.G.A Giuseppe Sebastianelli.

Tutti i dati contenuti nel computer relativi alla gestione Alunni – Personale – Bilancio – Protocollo, vengono con periodicità settimanale, memorizzati su CD-RW riscrivibili, etichettati e depositati nell'armadio di sicurezza situato nella stanza del DSGA.
I documenti sono anche conservati in copia cartacea presso locali della scuola non accessibili a terzi.

Per il ripristino dei dati cartacei in seguito a distruzione o danneggiamento si potrà ricostruire copia dei documenti e atti in possesso degli interessati o di altri enti cui sono stati trasmessi con l'ausilio dei supporti informatici che ne costituiscono la parte più rilevante.

6. Pianificazione degli interventi formativi previsti (ex regola 19.6)

La formazione, che consente un miglioramento delle dinamiche lavorative in ambito privacy, rappresenta oggi una condizione indispensabile ed irrinunciabile sia per la Scuola che per ogni operatore che travalica il mero rispetto di un obbligo previsto per legge ed investe non solo l'ambito lavorativo ma anche quello personale di ognuno.

Affrontando la problematica della formazione con un corretto approccio organizzativo e metodologico, è stato possibile riscontrare fin da subito considerevoli vantaggi in termini di sicurezza e affidabilità dei sistemi informativi, di snellimento dei processi e delle procedure per la gestione documentale, di prevenzione di possibili reati informatici e trattamenti illeciti di dati personali.

Quindi, la formazione in ambito privacy è servita principalmente ad educare ognuno alla consapevolezza della propria libertà ed al suo esercizio e conseguentemente all'assunzione di responsabilità verso se stessi e verso gli altri.

Pertanto, considerata l'importanza di formare il personale sui pericoli e sulle responsabilità, civili e penali, derivanti da una cattiva custodia dei dati o da un loro illecito trattamento, l'istituto organizza una serie di interventi formativi e di aggiornamento degli incaricati del trattamento per renderli edotti dei rischi che incombono sui dati trattati e delle misure disponibili per prevenire eventi dannosi.

I corsi di autoformazione si svolgono con cadenza semestrale con l'ausilio di materiale informativo e con la proiezione di diapositive che diventano oggetto di discussione.
Alcune tematiche oggetto del percorso formativo sono:

- i rischi che incombono sui dati;
- le misure atte a prevenire la perdita, la manomissione o la sottomissione di dati personali;
- la responsabilità sui dati personali e sensibili;
- le modalità e gli strumenti per aggiornarsi alle Misure minime di sicurezza;
- le nuove indicazioni del Garante sul tema *La privacy a Scuola.*

In definitiva, quindi, nel concetto di "Formazione Privacy" sono comprese tutte quelle attività e interventi in materia di trattamento di dati personali finalizzati ad aumentare le competenze cognitive, operative e comportamentali di responsabili e incaricati dirette a correggere le errate abitudini operative, a riconoscere pericoli e condizioni potenziali che potrebbero determinare eventi indesiderati, a prevenire e a fronteggiare con efficacia eventuali emergenze.

DICHIARAZIONE FINALE

Il Dirigente Scolastico – Titolare del Trattamento dei dati – si impegna ad adottare, nella fase di graduale attuazione degli interventi previsti dalla normativa sulla tutela della privacy, ogni possibile misura destinata a salvaguardare la sicurezza dei dati personali, siano essi contenuti nei documenti cartacei che registrati mediante apparecchiature informatiche.
Tali misure riguarderanno gli aspetti organizzativi, logistici e procedurali miranti ad evitare con ogni mezzo qualsiasi incremento di rischi di distruzione o perdita, anche accidentale, dei dati oggetto di trattamento, di accesso non autorizzato o di trattamento non consentito.

Terracina, 22/03/2017

LA DIRIGENTE SCOLASTICA
Prof.ssa Giuseppina Di Cretico

Firma del Titolare _____

IL DIRETTORE DEI SS. GG. AA.
Geom. Giuseppe Sabastianelli

Firma del Responsabile _____

MINISTERO DELL'ISTRUZIONE, DELL'UNIVERSITÀ E DELLA RICERCA
Ufficio Scolastico Regionale per il Lazio
Istituto Comprensivo "Milani"- Terracina
Via Olivetti, 41 – 04019 Terracina (LT)

☎ 0773 725919; Fax. 0773 722388; ✉ ltic830001@istruzione.it; C.F.: 80003800598

Documento di Adozione delle Misure di sicurezza nel Trattamento dei dati personali

Documento conforme alle modifiche apportate dal Decreto legge 5/2012 – "Semplificazioni"

Aggiornamento Anno 2017

Allegati

ALLEGATO 1

Codice in materia di protezione dei dati personali
B. Disciplinare tecnico in materia di misure minime di sicurezza
(Artt. da 33 a 36 del Codice)

Trattamenti con strumenti elettronici
Modalità tecniche da adottare a cura del titolare, del responsabile ove designato e dell'incaricato, in caso di trattamento con strumenti elettronici:

Sistema di autenticazione informatica
1. Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.
2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.
3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.
4. Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.
5. La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.
6. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.
7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
8. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.
9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.
10. Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.
11. Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.

Sistema di autorizzazione
12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.
13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono

individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.
14. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

Altre misure di sicurezza

15. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.
16. I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-*quinquies* del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.
17. Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.
18. Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.

Documento programmatico sulla sicurezza

19. [soppresso] (1)

19.1. [soppresso](1)
19.2. [soppresso](1)
19.3. [soppresso](1)
19.4. [soppresso](1)
19.5. [soppresso](1)
19.6. [soppresso](1)
19.7. [soppresso](1)
19.8. [soppresso](1)

Ulteriori misure in caso di trattamento di dati sensibili o giudiziari

20. I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all'art. 615-*ter* del codice penale, mediante l'utilizzo di idonei strumenti elettronici.
21. Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.
22. I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.
23. Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.
24. Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi all'identità genetica sono trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato.

Misure di tutela e garanzia

25. Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria

struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.
26. [soppresso] (1)

Trattamenti senza l'ausilio di strumenti elettronici

Modalità tecniche da adottare a cura del titolare, del responsabile, ove designato, e dell'incaricato, in caso di trattamento con strumenti diversi da quelli elettronici:

27. Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.
28. Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.
29. L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.

(1) Paragrafi soppressi dall'art. 45, comma 1, lett. d), del decreto legge 9 febbraio 2012, n. 5, convertito, con modificazioni, dalla legge 4 aprile 2012, n. 35.

Per completezza, si riporta di seguito il testo dei paragrafi soppressi.

19. Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:

19.1. l'elenco dei trattamenti di dati personali;
19.2. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
19.3. l'analisi dei rischi che incombono sui dati;
19.4. le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonchè la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
19.5. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;
19.6. la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;
19.7. la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;
19.8. per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

26. Il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.

ALLEGATO 2 - *Disposizioni generali e Linee Guida*

Disposizioni generali

Tutto il personale dipendente interno dell'Istituto (Docenti, amministrativi e Collaboratori scolastici) e quanti vi operano a titolo diverso (collaboratori esperti esterni, membri esterni degli Organi Collegiali, ecc..) hanno l'assoluto divieto di diffondere notizie che devono restare segrete sia per quanto attiene i dati personali sia per i dati sensibili che hanno acquisito in virtù del loro ufficio.
Tutte le comunicazioni indirizzate agli uffici, ad altro personale della scuola e al dirigente scolastico debbono essere consegnate in busta chiusa al responsabile di sede o al protocollo della sede centrale. Non è consentito, se non espressamente autorizzato, l'utilizzo del fax, della posta elettronica e dei collegamenti alla rete internet per il trattamento dei dati personali.

Modalità operative per l'accesso e l'utilizzo del servizio Internet e del servizio di posta elettronica

Per accedere ai servizi informatici da una postazione di lavoro l'utente deve utilizzare un codice identificativo (id utente) e una parola chiave segreta (password).
Superato il sistema di autenticazione l'utente è collegato alla rete interna e ad internet senza ulteriori formalità.
L'utente, preso atto che la conoscenza della password da parte di terzi consente agli stessi l'accesso alla rete aziendale, l'utilizzo dei relativi servizi in nome dell'utente titolare e l'accesso ai dati cui il medesimo è abilitato, con possibilità di gestione degli stessi (ad es. visualizzazione di informazioni riservate, distruzione o modifica dei dati, lettura della propria posta elettronica, uso indebito di servizi ecc.), si impegna a:

- non cedere, una volta superata la fase di autenticazione, l'uso della propria stazione a personale non autorizzato.
- non lasciare incustodita ed accessibile la propria postazione una volta connesso al sistema con le proprie credenziali di autenticazione;
- conservare la password nella massima riservatezza e con la massima diligenza;
- mantenere la corretta configurazione del proprio computer non alterando le componenti hardware e software predisposte allo scopo, né installando ulteriori software non autorizzati;
- non salvare file audio, video e file non istituzionali di qualsiasi tipo nelle connessioni di rete su cui viene eseguito giornalmente il back-up.

L'installazione di software o la modifica della configurazioni, la configurazione dei servizi di accesso ad internet e di posta elettronica viene eseguita esclusivamente da personale specializzato incaricato dall'Amministrazione.
Di qualsiasi azione o attività svolta utilizzando il codice identificativo e/o la password assegnata è responsabile l'utente assegnatario del codice.
L'utente è civilmente responsabile di qualsiasi danno arrecato all'Istituto e all'internet provider e/o a terzi in dipendenza della mancata osservazione di quanto previsto dal disciplinare.
L'utente può essere chiamato a rispondere civilmente, oltre che per i propri fatti illeciti, anche per quelli commessi da chiunque utilizzi il suo codice identificativo e/o password, con particolare

riferimento all'immissione in rete di contenuti critici o idonei a offendere l'ordine pubblico o il buon costume così come definiti dalla giurisprudenza della Corte di Cassazione.
La violazione delle presenti disposizioni può comportare infine l'applicazione delle sanzioni disciplinari previste dal vigente Contratto Collettivo Nazionale di Lavoro – Comparto Scuola, rimanendo ferma ogni ulteriore forma di responsabilità penale.

- INTERNET

Tutti gli utenti cui è assegnata dall'Amministrazione una postazione di lavoro possono utilizzare internet, limitatamente ad una lista di siti istituzionali sicuri preventivamente individuati.

L'utilizzo ampio di internet, non limitato cioè alla lista di siti individuata come sopra, è autorizzato per ogni singolo utente dal Dirigente scolastico, previa richiesta adeguatamente motivata.
L'utente è direttamente responsabile dell'uso del servizio di accesso a internet, dei contenuti che vi ricerca, dei siti che contatta, delle informazioni che vi immette e delle modalità con cui opera.
Lo scarico di immagini, di file audio o musicali, di file video e in ogni casi di grandi quantità di dati in grado di degradare le prestazioni offerte dal servizio agli altri utenti può avvenire solo in casi eccezionali, su espressa autorizzazione del Dirigente scolastico.
All'utente non è consentito:
- servirsi o dar modo ad altri di servirsi della stazione di accesso a internet per attività non istituzionali, per attività poste in essere in violazione del diritto d'autore o altri diritti tutelati dalla normativa vigente;
- connettersi a siti che trasmettono programmi in streaming (come radio o TV via WEB)
- scaricare software dalla rete; eventuali necessità devono essere appositamente richieste al Dirigente scolastico;
- utilizzare internet provider diversi da quello ufficiale dell'Istituto e la connessione di stazioni di lavoro aziendali alle reti di tali provider con sistemi di connessione diversi (es. modem) da quello centralizzato;
- usare la rete in modo difforme da quanto previsto dal presente documento e dalle leggi penali, civili e amministrative in materia di disciplina dell'attività e dei servizi svolti sulla rete.

- POSTA ELETTRONICA

L'utilizzo del servizio di posta elettronica è consentito solo per ragioni di servizio agli utenti identificati con le modalità precedentemente illustrate.
All'utente non è consentito:
- utilizzare tecniche di "mail spamming" cioè di invio massiccio di comunicazioni a liste di distribuzione extra aziendali o di azioni equivalenti;
- utilizzare il servizio di posta elettronica per inoltrare appelli e petizioni (anche se possono sembrare veritieri e socialmente utili), giochi, scherzi e altre e–mail che non siano di lavoro;
- allegare al testo delle comunicazioni materiale potenzialmente insicuro (ad es. programmi, scripts, macro), così come file di dimensioni eccessive.

A nessuno è consentito creare account a nome e per conto dell'Istituto.

Linee Guida in materia di sicurezza

Istruzioni per gli Incaricati al Trattamento - Personale di Segreteria

Le misure operative da adottare per garantire la sicurezza dei dati personali sono le seguenti:

- Non lasciare floppy disk, cartelle o altri documenti a disposizione di estranei;
- Conservare i dati sensibili cartacei in armadi di sicurezza, ad accesso controllato o elettronici in files protetti da password;
- Non consentire l'accesso ai dati a soggetti non autorizzati;
- Riporre i supporti in modo ordinato negli appositi contenitori avendo cura di chiudere a chiave classificatori e armadi dove sono custoditi;
- Scegliere una password con le seguenti caratteristiche:
  1. originale, che non sia facilmente intuibile, evitando il nome proprio, il nome di congiunti, date di nascita e comunque riferimenti alla propria persona o lavoro facilmente ricostruibili;
  2. composta da otto caratteri e che contenga almeno un numero e un carattere speciale;
- curare la conservazione della propria password ed evitare di comunicarla ad altri;
  - cambiare periodicamente (almeno una volta ogni tre mesi) la propria password;
  - modificare prontamente (ove possibile) la password assegnata dal custode delle credenziali;
  - trascrivere su un biglietto chiuso in busta sigillata e controfirmata la nuova password e consegnarla al custode delle credenziali;
  - spegnere correttamente il computer al termine di ogni sessione di lavoro;
  - non abbandonare la propria postazione di lavoro per la pausa o altri motivi senza aver spento la postazione di lavoro o aver inserito uno screen saver con password;
  - comunicare tempestivamente al Titolare o al Responsabile qualunque anomalia riscontrata nel funzionamento del computer;
  - non riutilizzare i supporti informatici utilizzati per il trattamento di dati sensibili per altri trattamenti;
  - non gestire informazioni su più archivi ove non sia strettamente necessario e comunque curarne l'aggiornamento in modo organico;
  - utilizzare le seguenti regole per la posta elettronica:
    1. non aprire documenti di cui non sia certa la provenienza;
    2. non aprire direttamente gli allegati ma salvarli su disco e controllarne il contenuto con un antivirus;
    3. inviare messaggi di posta solo se espressamente autorizzati dal Responsabile;
    4. controllare accuratamente l'indirizzo dei destinatario prima di inviare dati personali

Si allega al presente documento l'art.4 relativo alle definizioni dei termini utilizzati nel codice

Art. 4. Definizioni

1. Ai fini del presente codice si intende per:

a) "**Trattamento**", qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo,

l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;

b) "**Dato personale**", qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

c) "**Dati identificativi**", i dati personali che permettono l'identificazione diretta dell'interessato;

d) "**Dati sensibili**", i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;

e) "**Dati giudiziari**", i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;

f) "**Titolare**", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;

g) "**Responsabile**", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;

h) "**Incaricati**", le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;

i) "**Interessato**", la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;

l) "**Comunicazione**", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

m) "**Diffusione**", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

n) "**Dato anonimo**", il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;

o) "**Blocco**", la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;

p) "**Banca di dati**", qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;

q) "**Garante**", l'autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675.

2. Ai fini del presente codice si intende, inoltre, per:

a) "**Comunicazione elettronica**", ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile;

b) "**Chiamata**", la connessione istituita da un servizio telefonico accessibile al pubblico, che consente la comunicazione bidirezionale in tempo reale;

c) "**Reti di comunicazione elettronica**", i sistemi di trasmissione, le apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, incluse le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;

d) "**Rete pubblica di comunicazioni**", una rete di comunicazioni elettroniche utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico;

e) "**Servizio di comunicazione elettronica**", i servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, nei limiti previsti dall'articolo 2, lettera c), della direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002;

f) "**Abbonato**", qualunque persona fisica, persona giuridica, ente o associazione parte di un contratto con un fornitore di servizi di comunicazione elettronica accessibili al pubblico per la fornitura ditali servizi, o comunque destinatario di tali servizi tramite schede prepagate;

g) "**Utente**", qualsiasi persona fisica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata;

h) "**Dati relativi al traffico**", qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione;

i) "**Dati relativi all'ubicazione**", ogni dato trattato in una rete di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico;

l) "**Servizio a valore aggiunto**", il servizio che richiede il trattamento dei dati relativi al traffico o dei dati relativi all'ubicazione diversi dai dati relativi al traffico, oltre a quanto è necessario per la trasmissione di una comunicazione o della relativa fatturazione;

m) "**Posta elettronica**", messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza.

3. Si intende, altresì, per:

a) "**Misure minime**", il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31;

b) "**Strumenti elettronici**", gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;

c) "**Autenticazione informatica**", l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;

d) "**Credenziali di autenticazione**", i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;

e) "**Parola chiave**", componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;

f) "**Profilo di autorizzazione**", l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonchè i trattamenti ad essa consentiti;

g) "**Sistema di autorizzazione**", l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

4. Ai fini del presente codice si intende per:

a) "**Scopi storici**", le finalità di studio, indagine, ricerca e documentazione di figure, fatti e circostanze del passato;

b) "**Scopi statistici**", le finalità di indagine statistica o di produzione di risultati statistici, anche a mezzo di sistemi informativi statistici;

c) "**Scopi scientifici**", le finalità di studio e di indagine sistematica finalizzata allo sviluppo delle conoscenze scientifiche in uno specifico settore.

Istruzioni per gli Incaricati al Trattamento - Personale Collaboratore Scolastico

Le misure operative da adottare per garantire la sicurezza dei dati personali sono le seguenti:

A) **Collaboratore scolastico adibito al servizio ai piani**

1) Accertarsi che al termine delle lezioni non restino incustoditi i seguenti documenti, segnalandone tempestivamente l'eventuale presenza al responsabile di sede e provvedendo temporaneamente alla loro custodia:

- ☐ Registro personale dei docenti / Registro elettronico
- ☐ Certificati medici e qualunque altro documento contenente dati personali o sensibili eventualmente esibiti dagli alunni a giustificazione delle assenze (consegnare in Segreteria – Ufficio Didattica)
- ☐ Qualsiasi documento contenente dati personali o sensibili dei docenti (consegnare in Segreteria – Ufficio Personale)

2) Verificare la corretta funzionalità dei meccanismi di chiusura di armadi che custodiscono dati personali , segnalando tempestivamente al responsabile di sede eventuali anomalie.

3) Procedere alla chiusura dell'edificio scolastico accertandosi che tutte le misure di protezione dei locali siano state attivate. (chiusura uffici, archivi e inserimento allarme anti-intrusione)

B) **Collaboratore scolastico adibito al servizio di supporto alla segreteria**

1) Effettuare esclusivamente copie fotostatiche di documenti per i quali si è autorizzati.
2) Non lasciare a disposizione di estranei fotocopie inutilizzate o incomplete di documenti che contengono dati personali o sensibili ma accertarsi che vengano sempre distrutte.
3) Non lasciare incustodito il registro contenente gli indirizzi e i recapiti telefonici del personale e non annotarne il contenuto sui fogli di lavoro.
4) Non abbandonare la postazione di lavoro per la pausa o altro motivo senza aver provveduto a custodire in luogo sicuro i documenti trattati.
5) Non consentire che estranei possano accedere ai documenti dell'ufficio o leggere documenti contenenti dati personali o sensibili.

6) Segnalare tempestivamente al Responsabile del trattamento la presenza di documenti incustoditi e provvedere temporaneamente alla loro custodia.
7) Procedere alla chiusura dei locali non utilizzati in caso di assenza del personale.
8) Procedere alla chiusura dei locali di segreteria accertandosi che siano state attivate tutte le misure di protezione e che le chiavi delle stanze siano depositate negli appositi contenitori.
9) Attenersi alle direttive ricevute e non effettuare operazioni per le quali non si è stati espressamente autorizzati dal Responsabile o dal Titolare.

Istruzioni per gli Incaricati al Trattamento - Personale Docente e collaboratori del Dirigente Scolastico.

Le misure operative da adottare per garantire la sicurezza dei dati personali trattati su materiale cartaceo e supporti elettronici sono le seguenti:

- Il Registro di Classe, il Registro dei verbali del consiglio di classe o di interclasse vanno custoditi negli armadi di sicurezza della Presidenza e dell'Ufficio della Segreteria Didattica;
- I documenti di valutazione, la documentazione relativa alla programmazione didattica e quella sullo stato di disabilità vanno custoditi nell'Armadio di sicurezza della Presidenza;
- La Certificazione medica degli allievi e la corrispondenza con le famiglie vanno consegnati al personale amministrativo della segreteria didattica che provvederà a inserirla nei fascicoli personali degli alunni contenenti dati comuni o sensibili e custoditi negli armadi di sicurezza della Segreteria Didattica;
- Il Registro personale ed elettronico va consegnato al collaboratore scolastico incaricato che provvederà alla loro sistemazione e messa in carico nell'apposito armadio di sicurezza nella sala docenti.
- Tutte le comunicazioni indirizzate agli uffici, ad altro personale della scuola e al Dirigente Scolastico devono essere consegnate in busta chiusa al responsabile di sede o all'Ufficio Protocollo della sede centrale. Non è consentito, se non espressamente autorizzato, l'utilizzo del fax, della posta elettronica e dei collegamenti alla rete internet per il trattamento dei dati personali.
- I Docenti sono tenuti a conservare la documentazione relativa alla classe e agli alunni nella sala docenti.
- È fatto divieto portare fuori dalla scuola i documenti di cui sopra. Il fiduciario di plesso avrà cura di verificare che, alla fine delle lezioni o delle attività collegiali, l'aula sia chiusa a chiave.

Una copia delle chiavi sarà depositata nell'ufficio della presidenza.

Istruzioni operative per i docenti che utilizzano l'aula di informatica (nel caso di trattamento di dati personali) e per il responsabile dell'aula di informatica:

Istruzioni operative per l'utilizzo del personal computer:

- Non lasciare floppy disk, cartelle o altri documenti a disposizione di estranei;
- Non consentire l'accesso ai dati a soggetti non autorizzati;
- Riporre i supporti in modo ordinato negli appositi contenitori e chiudere a chiave i classificatori e gli armadi dove sono custoditi;
- Scegliere una password con le seguenti caratteristiche:
  1. **originale**, che non sia facilmente intuibile, evitando il nome proprio, il nome di congiunti, date di nascita e comunque riferimenti alla propria persona o lavoro facilmente ricostruibili;

2. **composta da otto caratteri** e che contenga almeno un numero e un carattere speciale
- curare la conservazione della propria password ed evitare di comunicarla ad altri;
- cambiare periodicamente (almeno una volta ogni tre mesi) la propria password;
- modificare prontamente (ove possibile) la password assegnata dal custode delle credenziali;
- trascrivere su un biglietto chiuso in busta sigillata e controfirmata la nuova password e consegnarla al custode delle credenziali;
- spegnere correttamente il computer al termine di ogni sessione di lavoro;
- non abbandonare la propria postazione di lavoro senza aver spento la postazione di lavoro o aver inserito uno screen saver con password;
- comunicare tempestivamente al Titolare o al Responsabile qualunque anomalia riscontrata nel funzionamento del computer;
- utilizzare le seguenti regole per la posta elettronica:
    1. non aprire documenti di cui non sia certa la provenienza
    2. non aprire direttamente gli allegati ma salvarli su disco e controllarne il contenuto con un antivirus
    3. controllare accuratamente l'indirizzo dei destinatario prima di inviare dati personali

Il laboratorio di informatica è finalizzato:

- ad attività didattiche con intere classi o gruppi di alunni;
- a corsi di formazione\aggiornamento\ricerca per i docenti e il personale ATA.
- Tutti gli insegnanti sono responsabili del laboratorio di informatica e degli altri computer presenti nei vari plessi. I docenti assicurano il corretto uso dei sistemi, dei programmi, di Internet, della tenuta in ordine di tutto il materiale hardware e software. Tra i loro compiti quello di vigilare sul corretto uso della rete Internet affinché si escluda la possibilità di collegamento a siti web dal contenuto non adeguato.
- Gli alunni saranno sempre accompagnati da un insegnante e, in nessuna circostanza, sarà consentito loro l'accesso al laboratorio senza la presenza di un docente.
  Tutti i docenti dovranno osservare scrupolosamente le indicazioni per un corretto uso del laboratorio.
  Al di fuori del normale orario di utilizzo, il laboratorio deve rimanere chiuso a chiave.

L'Istituto possiede un sito web accessibile da internet ove sono pubblicati i documenti prodotti dalla scuola.

DIRITTI DELL'INTERESSATO

L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, come pure l'aggiornamento, la rettifica o, quando vi ha interesse, l'integrazione dei dati. L'interessato ha altresì diritto di richiedere la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di Legge.
I dati saranno resi noti solo ai diretti interessati e a persone, enti e organismi che per Legge sono titolati a ricevere i dati stessi.
Qualunque trattamento di dati personali da parte di soggetti pubblici è consentito solo per lo svolgimento delle funzioni istituzionali. Pertanto, per adempiere ai doveri d'ufficio, a disposizioni normative, a precisi obblighi di circolari non si richiede il consenso dell'interessato nell'invio di dati a persone od organismi titolati per legge a ricevere i dati stessi.
I dati sensibili possono essere oggetto di trattamento solo con il consenso scritto dell'interessato.

Indice

ALLEGATO 3

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Versione pdf delle *"Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati"*
[doc. web n. 3134436]

LA TRASPARENZA DELLA PA SUI SITI WEB

Registro dei provvedimenti
n. 243 del 15 maggio 2014

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, in presenza del dott. Antonello Soro, presidente, della dott.ssa Augusta Iannini, vicepresidente, della dott.ssa Giovanna Bianchi Clerici e della prof.ssa Licia Califano, componenti, e del dott. Giuseppe Busia, segretario generale;

VISTA la direttiva del Parlamento europeo e del Consiglio 95/46/CE del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati;

VISTO il Codice in materia di protezione dei dati personali (d. lgs. 30 giugno 2003, n. 196, di seguito «Codice»);

CONSIDERATO il «*Parere del Garante su uno schema di decreto legislativo concernente il riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle P.a.*» del 7 febbraio 2013 (in *www.garanteprivacy.it*, doc. *web* n. 2243168);

VISTO il decreto legislativo 14 marzo 2013, n. 33 recante «*Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni*» (in G.U. 5 aprile 2013, n. 80);

VISTE le «*Linee guida in materia di trattamento di dati personali contenuti anche in atti e documenti amministrativi effettuato da soggetti pubblici per finalità di pubblicazione e diffusione sul web*» del 2 marzo 2011 (in G.U. 19 marzo 2011, n. 64, p. 32; in *www.garanteprivacy.it*, doc. *web* n. 1793203);

ESAMINATE le segnalazioni e i quesiti pervenuti in ordine al trattamento dei dati personali derivante dagli obblighi di pubblicazione di atti e informazioni nel *web* contenuti nel citato d. lgs. n. 33/2013;

RITENUTA l'opportunità di individuare un quadro organico e unitario di garanzie finalizzato a indicare apposite cautele in relazione alle ipotesi di diffusione di dati personali mediante la pubblicazione sui siti *web* da parte di organismi pubblici e in particolare di quelli chiamati a dare attuazione al d. lgs. n. 33/2013 attraverso l'adozione di nuove «*Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati*»;

CONSIDERATO che tali nuove Linee guida sono state elaborate come opportuno supporto fornito a tutti i soggetti pubblici e altri enti obbligati per favorire l'implementazione, sotto il profilo della protezione dei dati personali, delle numerose e complesse disposizioni normative che si sono succedute negli ultimi anni in materia di pubblicazione e di diffusione dei dati, specie con riguardo al conseguimento della finalità di trasparenza;

RILEVATO che il quadro legislativo e regolamentare incidente su tale materia andrà soggetto a ulteriori modificazioni, segnatamente in relazione alla necessità di recepire nell'ordinamento nazionale la nuova direttiva 2013/37/UE relativa al riutilizzo dell'informazione del settore pubblico, e che pertanto potranno essere adottate altre linee guida e provvedimenti anche sulla base di una leale collaborazione con le altre autorità competenti;

TENUTO CONTO delle osservazioni e dei riscontri ricevuti dal Dipartimento della funzione pubblica presso la Presidenza del Consiglio dei ministri, dall'Autorità nazionale anticorruzione e per la valutazione e la trasparenza delle amministrazioni pubbliche (già CIVIT e ora ANAC) e dall'Agenzia per l'Italia Digitale (AgID);

VISTA la documentazione in atti;

VISTE le osservazioni dell'Ufficio, formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore la prof.ssa Licia Califano;

DELIBERA

1) ai sensi dell'art. 154, comma 1, lett. *h*), del Codice di adottare le «*Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati*» contenute nel documento allegato che forma parte integrante della presente deliberazione;

2) che copia del presente provvedimento sia trasmessa al Ministero della giustizia-Ufficio pubblicazione leggi e decreti, per la sua pubblicazione sulla *Gazzetta Ufficiale* della Repubblica italiana.

Roma, 15 maggio 2014

IL PRESIDENTE

Soro

IL RELATORE

Califano

IL SEGRETARIO GENERALE

Busia

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

«Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul *web* da soggetti pubblici e da altri enti obbligati»

(Allegato alla deliberazione n. 243 del 15 maggio 2014)

SOMMARIO

INTRODUZIONE

OBBLIGHI DI PUBBLICITÀ

Le recenti modifiche legislative in materia di pubblicità e trasparenza della pubblica amministrazione (cfr. da ultimo il d. lgs. 14 marzo 2013, n. 33) hanno reso necessario un intervento del Garante diretto ad assicurare l'osservanza della disciplina in materia di protezione dei dati personali nell'adempimento degli obblighi di pubblicazione sul *web* previsti dalle disposizioni di riferimento.

Le presenti Linee guida hanno, pertanto, lo scopo di definire un quadro unitario di misure e accorgimenti volti a individuare opportune cautele che i soggetti pubblici, e gli altri soggetti parimenti destinatari delle norme vigenti, sono tenuti ad applicare nei casi in cui effettuano attività di diffusione di dati personali sui propri siti *web* istituzionali per finalità di trasparenza o per altre finalità di pubblicità dell'azione amministrativa. Pertanto, il presente provvedimento sostituisce le precedenti «*Linee guida in materia di trattamento di dati personali contenuti anche in atti e documenti amministrativi, effettuato da soggetti pubblici per finalità di pubblicazione e diffusione sul web*» del 2 marzo 2011 (doc. *web* n. 1793203).

Le nuove *Linee guida* sostituiscono le precedenti adottate dal Garante il 2 marzo 2011

In via preliminare, vanno distinte, considerato il profilo del diverso regime giuridico applicabile, le disposizioni che regolano gli obblighi di pubblicità dell'azione amministrativa per finalità di trasparenza da quelle che regolano forme di pubblicità per finalità diverse (ad es. pubblicità legale).

In particolare, gli obblighi di pubblicazione *online* di dati per finalità di «*trasparenza*» sono quelli indicati nel d. lgs. n. 33/2013 e nella normativa vigente in materia avente a oggetto le «*informazioni concernenti l'organizzazione e l'attività delle pubbliche amministrazioni, allo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche*». A tali obblighi si applicano le indicazioni contenute nella parte prima delle presenti Linee guida.

Obblighi di pubblicazione per finalità di trasparenza. Applicazione della parte prima delle *Linee guida*

Accanto a questi obblighi di pubblicazione permangono altri obblighi di pubblicità *online* di dati, informazioni e documenti della p.a. –contenuti in specifiche disposizioni di settore diverse da quelle approvate in materia di trasparenza– come, fra l'altro, quelli volti a far conoscere l'azione amministrativa in relazione al rispetto dei principi di legittimità e correttezza, o quelli atti a garantire la pubblicità legale degli atti amministrativi (ad es. pubblicità integrativa dell'efficacia, dichiarativa, notizia). Si pensi, a titolo meramente esemplificativo, alle pubblicazioni ufficiali dello Stato, alle

Obblighi di pubblicazione per altre finalità di pubblicità dell'azione amministrativa diverse dalla trasparenza. Applicazione della parte seconda delle *Linee guida*

pubblicazioni di deliberazioni, ordinanze e determinazioni sull'albo pretorio *online* degli enti locali (oppure su analoghi albi di altri enti, come ad esempio le Asl), alle pubblicazioni matrimoniali, alla pubblicazione degli atti concernenti il cambiamento del nome, alla pubblicazione della comunicazione di avviso deposito delle cartelle esattoriali a persone irreperibili, ai casi di pubblicazione dei ruoli annuali tributari dei consorzi di bonifica, alla pubblicazione dell'elenco dei giudici popolari di corte d'assise, *etc.*. A tali obblighi si riferiscono le indicazioni contenute nella parte seconda delle presenti Linee guida.

Bilanciamento fra la pubblicità e la trasparenza con la tutela dei dati personali

In tutti i casi, indipendentemente dalla finalità perseguita, laddove la pubblicazione *online* di dati, informazioni e documenti, comporti un trattamento di dati personali, devono essere opportunamente contemperate le esigenze di pubblicità e trasparenza con i diritti e le libertà fondamentali, nonché la dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali (art. 2 del Codice).

Sindacabilità da parte del Garante delle scelte di pubblicazione di dati personali e relativa sanzionabilità

In tale quadro, è opportuno evidenziare che le decisioni, assunte dalle amministrazioni pubbliche o dagli altri soggetti onerati, in ordine all'attuazione degli obblighi di pubblicità sui siti *web* istituzionali di informazioni, atti e documenti contenenti dati personali sono oggetto di sindacato da parte del Garante al fine di verificare che siano rispettati i principi in materia di protezione dei dati personali.

Si fa presente, altresì, che la diffusione di dati personali da parte dei soggetti pubblici effettuato in mancanza di idonei presupposti normativi è sanzionata ai sensi degli artt. 162, comma 2-*bis*, e 167 del Codice.

Inoltre, l'interessato che ritenga di aver subito un danno –anche non patrimoniale– in particolare per effetto della diffusione di dati personali, può far valere le proprie pretese risarcitorie, ove ne ricorrano i presupposti, davanti all'autorità giudiziaria ordinaria (art. 15 del Codice).

PARTE PRIMA

PUBBLICITÀ PER FINALITÀ DI TRASPARENZA

1. Principi e oggetto del "decreto trasparenza" (artt. 1, 2 e 3 del d. lgs. n. 33/2013)

Con il d. lgs. 14 marzo 2013 n. 33 intitolato «*Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni*» il legislatore –in attuazione della delega contenuta nella legge 6 novembre 2012, n. 190, recante: «*Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione*» (art. 1, commi 35 e 36)– ha disciplinato in maniera organica i casi di pubblicità per finalità di trasparenza mediante inserzione di dati, informazioni, atti e documenti sui siti *web* istituzionali dei soggetti obbligati.

A tal fine, nel capo I dedicato ai «*principi generali*», la trasparenza è definita come «*l'accessibilità totale delle informazioni concernenti l'organizzazione e l'attività delle pubbliche amministrazioni, allo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche*» (art. 1, comma 1).

Nel medesimo capo I è precisato che «*oggetto del decreto*» è l'individuazione degli obblighi di trasparenza «*concernenti l'organizzazione e l'attività delle pubbliche amministrazioni*» e che «*tutti i documenti, le informazioni e i dati oggetto di pubblicazione obbligatoria ai sensi della normativa vigente sono pubblici e chiunque ha diritto di conoscerli, di fruirne gratuitamente, e di utilizzarli e riutilizzarli ai sensi dell'articolo 7*» (art. 2, comma 1, e art. 3).

Si evidenzia, in proposito, che lo stesso legislatore, ai soli fini del campo di applicazione del decreto, definisce la «*pubblicazione*» come l'inserimento nei siti istituzionali delle pubbliche amministrazioni, in conformità alle specifiche e alle regole tecniche previste nell'allegato al decreto stesso, dei documenti, delle informazioni e dei dati «*concernenti l'organizzazione e l'attività delle pubbliche amministrazioni*» (art. 2, comma 2).

Gli obblighi di pubblicazione concernenti l'organizzazione e l'attività delle pubbliche amministrazioni per finalità di trasparenza

Da ciò si deduce che tutte le volte in cui nel d.lgs. n. 33/2013 è utilizzata la locuzione «*pubblicazione obbligatoria ai sensi della normativa vigente*» –cfr. artt. 3, 5, 7, 8, 9, 10, 41, 43, 45, 46 e 48– il riferimento è limitato agli «*obblighi di pubblicazione concernenti l'organizzazione e l'attività delle pubbliche amministrazioni*» contenuti oltre che nel d. lgs. n. 33/2013 anche in altre disposizioni normative aventi analoga finalità di tra-

sparenza, con esclusione degli obblighi di pubblicazione aventi finalità diverse.

La tipologia dei predetti obblighi di pubblicazione per finalità di trasparenza concernenti l'organizzazione e l'attività delle pubbliche amministrazioni è schematicamente riassunta nell'allegato al d. lgs. n. 33/2013 che individua la «*struttura delle informazioni sui siti istituzionali*»[1] e che precisa come la sezione dei siti istituzionali denominata «*Amministrazione trasparente*» deve essere organizzata in sotto-sezioni all'interno delle quali devono essere inseriti i documenti, le informazioni e i dati previsti dal decreto (art. 48 e Allegato al decreto legislativo).

Uno schema più particolareggiato degli obblighi di pubblicazione ai sensi della normativa vigente per finalità di trasparenza sopra descritti è contenuto poi nell'allegato n. 1 della delibera della CIVIT n. 50/2013 recante «*Linee guida per l'aggiornamento del Programma triennale per la trasparenza e l'integrità 2014-2016*» cui si rimanda[2].

Riferibilità delle disposizioni del d. lgs. n. 33/2013 ai soli dati oggetto di pubblicazione per finalità di trasparenza (esclusione di albo pretorio, pubblicazioni matrimoniali *etc.*)

Per tale motivo, come si è detto, devono ritenersi estranei all'oggetto del citato decreto legislativo tutti gli obblighi di pubblicazione previsti da altre disposizioni per finalità diverse da quelle di trasparenza, quali gli obblighi di pubblicazione a fini di pubblicità legale[3], pubblicità integrativa dell'efficacia, pubblicità dichiarativa o notizia (già illustrati in forma esemplificativa nell'«*Introduzione*» (pag. 4) e presi in considerazione nella parte seconda delle presenti Linee guida.

Si pensi, ad esempio –tra i diversi casi indicati– alle pubblicazioni matrimoniali, la cui affissione alla porta della casa comunale (e oggi sui siti *web* istituzionali dei comuni) è prevista per otto giorni (cfr. art. 55 del d.P.R. n. 396 del 3/11/2000). La pubblicazione dei dati personali dei nubendi assolve a una funzione che evidentemente esula dalle finalità di trasparenza previste dal d. lgs. n. 33/2013 e che è pienamente assolta con la semplice pubblicazione per la durata temporale prevista. Infatti, sarebbe irragionevole applicare a essi il regime di conoscibilità previsto dalla normativa sulla trasparenza (limiti temporali di permanenza sul *web*, indicizzazione, accesso civico, riutilizzo *etc.*).

Di conseguenza, tutte le ipotesi di pubblicità non riconducibili a finalità di trasparenza (cfr. gli esempi forniti nell'«*Introduzione*» alle presenti Linee guida), qualora comportino una diffusione di dati personali, sono escluse dall'oggetto del d. lgs. n. 33/2013 e dall'ambito di applicazione delle relative previsioni fra cui, in particolare, quelle relative all'accesso

[1] Ai sensi del d. lgs. n. 33/2013, l'allegato al decreto costituisce parte integrante dello stesso e può essere modificato solo con un d.P.C.M. sentito il Garante per la protezione dei dati personali, la Conferenza unificata, l'Agenzia Italia Digitale, la CIVIT (ora ANAC) e l'ISTAT (art. 48, comma 2).

[2] Documento reperibile in *http://www.civit.it/?p=8953*.

[3] Nello stesso d. lgs. n. 33/2013 si fa riferimento più volte a ipotesi di pubblicità legale per finalità diverse da quelle di trasparenza (cfr. artt. 19, comma 1, e 37, comma 1).

civico (art. 5), all'indicizzazione (art. 4 e 9), al riutilizzo (art. 7), alla durata dell'obbligo di pubblicazione (art. 8) e alla trasposizione dei dati in archivio (art. 9).

2. Limiti generali alla trasparenza (artt. 1 e 4 del d. lgs. n. 33/2013)

I principi e la disciplina di protezione dei dati personali – come peraltro previsto anche dagli artt. 1, comma 2, e 4 del d. lgs. n. 33/2013 (v. altresì art. 8, comma 3) – devono essere rispettati anche nell'attività di pubblicazione di dati sul *web* per finalità di trasparenza.

In merito, si rappresenta che «*dato personale*» è «*qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale*» (art. 4, comma 1, lett. *b)*, del Codice).

I soggetti pubblici possono diffondere dati personali per finalità di trasparenza solo per espressa disposizione di legge o di regolamento (art. 19, comma 3, del Codice)

Inoltre, la «*diffusione*» di dati personali –ossia «*il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione*» (art. 4, comma 1, lett. *m*) del Codice)– da parte dei «*soggetti pubblici*» è ammessa unicamente quando la stessa è prevista da una specifica norma di legge o di regolamento (art. 19, comma 3, del Codice). Pertanto, in relazione all'operazione di diffusione, occorre che le pubbliche amministrazioni, prima di mettere a disposizione sui propri siti *web* istituzionali informazioni, atti e documenti amministrativi (in forma integrale o per estratto, *ivi* compresi gli allegati) contenenti dati personali, verifichino che la normativa in materia di trasparenza preveda tale obbligo (artt. 4, comma 1, lett. *m)*, 19, comma 3 e 22, comma 11, del Codice).

Laddove l'amministrazione riscontri l'esistenza di un obbligo normativo che impone la pubblicazione dell'atto o del documento nel proprio sito *web* istituzionale è necessario selezionare i dati personali da inserire in tali atti e documenti, verificando, caso per caso, se ricorrono i presupposti per l'oscuramento di determinate informazioni.

Rispetto del principio di necessità

I soggetti pubblici, infatti, in conformità ai principi di protezione dei dati, sono tenuti a ridurre al minimo l'utilizzazione di dati personali e di dati identificativi[4] ed evitare il relativo trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante dati anonimi o altre modalità che permettano di identificare l'interessato solo in caso di necessità (c.d. "*principio di necessità*" di cui all'art. 3, comma 1, del Codice). Pertanto, anche in presenza degli obblighi di pubblicazione di atti o docu-

[4] Dati identificativi sono i «*dati personali che permettono l'identificazione diretta dell'interessato*» (cfr. art. 4, comma 1, lett. *c)*, del Codice).

menti contenuti nel d. lgs. n. 33/2013, i soggetti chiamati a darvi attuazione non possono comunque «*rendere [...] intelligibili i dati personali non pertinenti o, se sensibili o giudiziari, non indispensabili rispetto alle specifiche finalità di trasparenza della pubblicazione*» (art. 4, comma 4, del d. lgs. n. 33/2013).

È, quindi, consentita la diffusione dei soli dati personali la cui inclusione in atti e documenti da pubblicare sia realmente necessaria e proporzionata alla finalità di trasparenza perseguita nel caso concreto (c.d. "*principio di pertinenza e non eccedenza*" di cui all'art. 11, comma 1, lett. *d)*, del Codice). Di conseguenza, i dati personali che esulano da tale finalità non devono essere inseriti negli atti e nei documenti oggetto di pubblicazione *online*. In caso contrario, occorre provvedere, comunque, all'oscuramento delle informazioni che risultano eccedenti o non pertinenti.

Rispetto dei principi di pertinenza e non eccedenza

È, invece, sempre vietata la diffusione di dati idonei a rivelare lo «*stato di salute*» (art. 22, comma 8, del Codice) e «*la vita sessuale*» (art. 4, comma 6, del d. lgs. n. 33/2013).

Divieto di diffusione dei dati idonei a rivelare lo stato di salute e la vita sessuale

In particolare, con riferimento ai dati idonei a rivelare lo stato di salute degli interessati, è vietata la pubblicazione di qualsiasi informazione da cui si possa desumere, anche indirettamente, lo stato di malattia o l'esistenza di patologie dei soggetti interessati, compreso qualsiasi riferimento alle condizioni di invalidità, disabilità o handicap fisici e/o psichici[5] (art. 22, comma 8, del Codice).

Il procedimento di selezione dei dati personali che possono essere resi conoscibili *online* deve essere, inoltre, particolarmente accurato nei casi in cui tali informazioni sono idonee a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale («*dati sensibili*»), oppure nel caso di dati idonei a rivelare provvedimenti di cui all'art. 3, comma 1, lettere da *a*) a *o*) e da *r*) a *u*), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, nonché la qualità di imputato o di indagato («*dati giudiziari*») (art. 4, comma 1, lett. *d)* ed *e)*, del Codice).

Pubblicazione di dati sensibili e giudiziari solo se «indispensabili»

I dati sensibili e giudiziari, infatti, sono protetti da un quadro di garanzie particolarmente stringente che prevede la possibilità per i soggetti

[5] Sulla nozione di dato relativo alle condizioni di salute cfr. "*Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico*" del 14 giugno 2007, doc. *web* n. 1417809, punto 6.3; nonché, *ex pluribus*, i provvedimenti del Garante 27 giugno 2013, doc. *web* n. 2576686; 4 aprile 2013, doc. *web* n. 2460997; 4 aprile 2013, doc. *web* n. 2473879; 22 novembre 2012, doc. *web* n. 2194472; 29 novembre 2012, doc. *web* n. 2192671; 7 ottobre 2009, doc. *web* n. 1664456; 17 settembre 2009, doc. *web* n. 1658335; 25 giugno 2009, doc. *web* n. 1640102; 3 febbraio 2009, doc. *web* n. 1597590; 8 maggio 2008, doc. *web* n. 1521716; 18 gennaio 2007, doc. *web* n. 1382026; 7 luglio 2004, doc. *web* nn. 1068839 e 1068917; 27 febbraio 2002, doc. *web* n. 1063639. Nella giurisprudenza di legittimità v. Cass. civ., sez. I, 8/8/2013, n. 18980.

pubblici di diffondere tali informazioni solo nel caso in cui sia previsto da una espressa disposizione di legge e di trattarle solo nel caso in cui siano in concreto «*indispensabili*» per il perseguimento di una finalità di rilevante interesse pubblico come quella di trasparenza; ossia quando la stessa non può essere conseguita, caso per caso, mediante l'utilizzo di dati anonimi o di dati personali di natura diversa (art. 4, commi 2 e 4, del d. lgs. n. 33/2013 cit.; artt. 20, 21 e 22, con particolare riferimento ai commi 3, 5 e 11, e art. 68, comma 3, del Codice).

Pertanto, come rappresentato dal Garante nel parere del 7 febbraio 2013 (doc. *web* n. 2243168), gli enti pubblici sono tenuti a porre in essere la massima attenzione nella selezione dei dati personali da utilizzare, sin dalla fase di redazione degli atti e documenti soggetti a pubblicazione, in particolare quando vengano in considerazione dati sensibili. In proposito, può risultare utile non riportare queste informazioni nel testo dei provvedimenti pubblicati *online* (ad esempio nell'oggetto, nel contenuto, *etc.*), menzionandole solo negli atti a disposizione degli uffici (richiamati quale presupposto del provvedimento e consultabili solo da interessati e controinteressati), oppure indicare delicate situazioni di disagio personale solo sulla base di espressioni di carattere più generale o, se del caso, di codici numerici (cfr. par. 2 del parere citato).

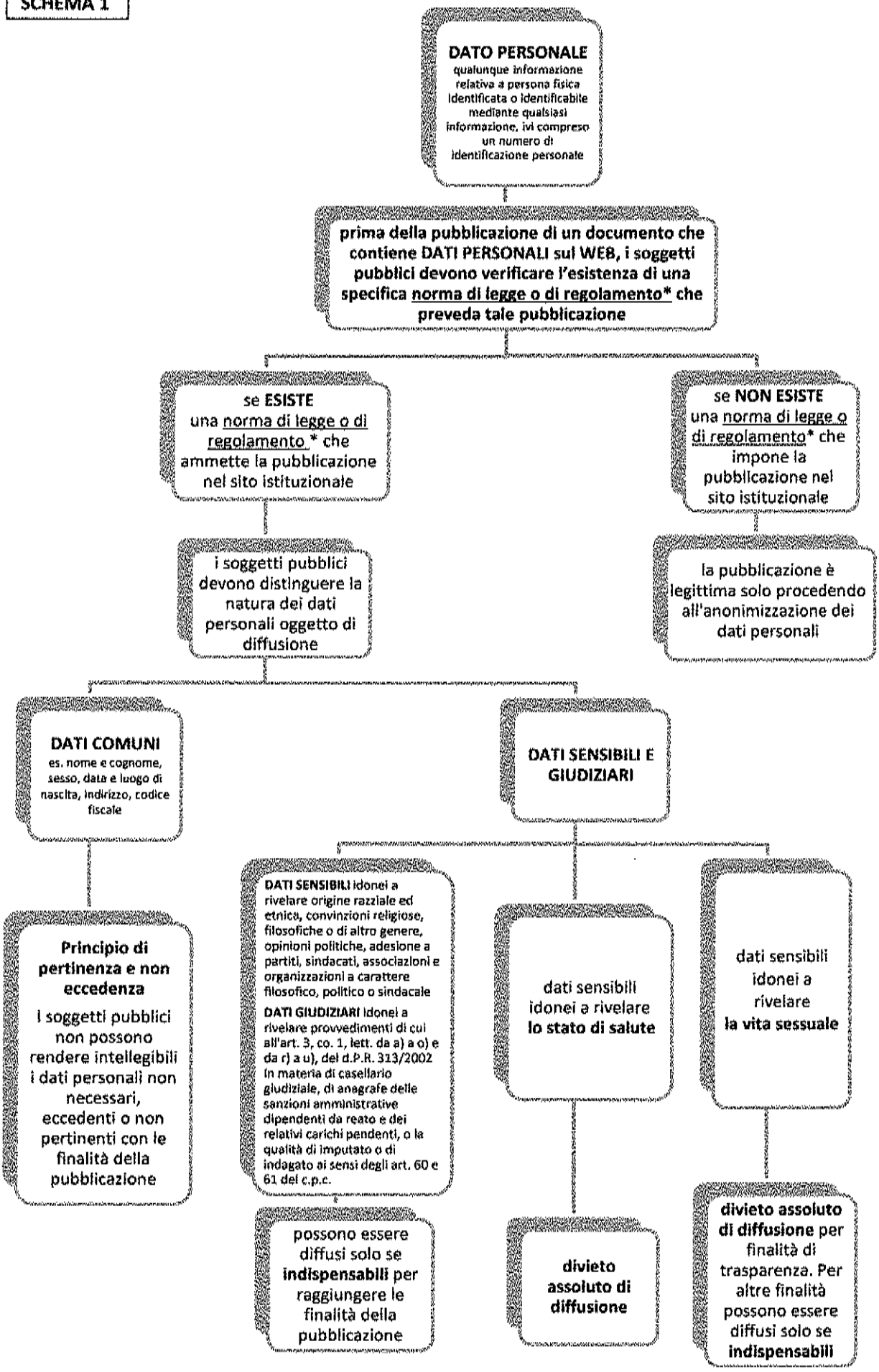
Deindicizzare dati sensibili e giudiziari

Effettuata, alla luce delle predette indicazioni, la previa valutazione circa i presupposti e l'indispensabilità della pubblicazione di dati sensibili e giudiziari, devono essere adottate idonee misure e accorgimenti tecnici volti ad evitare «*la indicizzazione e la rintracciabilità tramite i motori di ricerca web ed il loro riutilizzo*» (cfr. art. 4, comma 1 e art. 7 del d. lgs. n. 33/2013, tenendo altresì in considerazione le indicazioni fornite *infra* nei parr. 6 e 8 della presente parte ai quali si rimanda).

Rinvio allo schema 1 sotto riportato

Per esigenze di chiarezza espositiva, i limiti alla trasparenza sopradescritti sono sinteticamente rappresentati nello schema 1 sotto riportato.

SCHEMA 1



* N.B. Si precisa che la diffusione di dati comuni è ammessa solo se prevista da una norma di legge o di regolamento, mentre la diffusione di dati sensibili o giudiziari è ammessa se prevista espressamente solo da una norma di legge.

3. Pubblicazione di dati personali ulteriori (art. 4, comma 3, del d. lgs. n. 33/2013)

Dati ulteriori: obbligo di anonimizzazione dei dati la cui pubblicazione non è prevista dal d. lgs n. 33/2013 o da altra specifica disposizione di legge o di regolamento

Le pubbliche amministrazioni non sono libere di diffondere «*dati personali*» ulteriori, non individuati dal d. lgs. n. 33/2013 o da altra specifica norma di legge o di regolamento (art. 19, comma 3, del Codice).

L'eventuale pubblicazione di dati, informazioni e documenti, che non si ha l'obbligo di pubblicare, è legittima solo «*procedendo alla anonimizzazione dei dati personali eventualmente presenti*» (art. 4, comma 3, del d. lgs. n. 33/2013).

In proposito, si evidenzia che la prassi seguita da alcune amministrazioni di sostituire il nome e cognome dell'interessato con le sole iniziali è di per sé insufficiente ad anonimizzare i dati personali contenuti negli atti e documenti pubblicati *online*. Inoltre, il rischio di identificare l'interessato è tanto più probabile quando, fra l'altro, accanto alle iniziali del nome e cognome permangono ulteriori informazioni di contesto che rendono comunque identificabile l'interessato (si pensi, ad esempio, alle informazioni relative alla residenza oppure quando si possiede un doppio nome e/o un doppio cognome).

Per anonimizzare un dato non è sufficiente sostituire il nome e cognome dell'interessato con le relative iniziali

In molti casi, infatti, in particolari ambiti (ad es., per campioni di popolazioni di ridotte dimensioni), la pubblicazione *online* anche solo di alcuni dati –come la data di nascita, il sesso, la residenza, il domicilio, il codice di avviamento postale, il luogo di lavoro, il numero di telefono, la complessiva vicenda oggetto di pubblicazione, *etc.*– è sufficiente a individuare univocamente la persona cui le stesse si riferiscono e, dunque, a rendere tale soggetto identificabile mediante il collegamento con altre informazioni che possono anche essere nella disponibilità di terzi o ricavabili da altre fonti.

Per rendere effettivamente «*anonimi*»[6] i dati pubblicati *online* occorre, quindi, oscurare del tutto il nominativo e le altre informazioni riferite all'interessato che ne possono consentire l'identificazione anche *a posteriori*[7].

---

[6] Ai sensi del Codice «*dato anonimo*» è «*il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile*» (art. 4, comma 1, lett. *n*)).

[7] In proposito, va considerato che ottenere dati effettivamente 'anonimi' è sempre più difficile stante l'avanzare delle tecnologie informatiche e la crescente e diffusa mole di informazioni disponibili *online* e *offline* che aumenta progressivamente il rischio per gli interessati di essere re-identificati. Per un esame delle tecniche con cui anonimizzare i dati si rimanda al Parere del Gruppo Art. 29 n. 6/2013 su dati aperti e riutilizzo delle informazioni del settore pubblico, sez. VI (*http://www.garanteprivacy.it/documents/10160/2133805/WP207)*. Sul tema v. anche il codice di condotta «*Anonymisation: Managing data protection risk code of practice*» pubblicato dall'*Information Commissioner's Office* del Regno Unito nel novembre 2012 (*http://ico.org.uk/for_organisations/data_prot*

4. Qualità delle informazioni (art. 6 del d. lgs. n. 33/2013)

L'art. 6 del d. lgs. n. 33/2013 sancisce che «*Le pubbliche amministrazioni garantiscono la qualità delle informazioni riportate nei siti istituzionali nel rispetto degli obblighi di pubblicazione previsti dalla legge, assicurandone l'integrità, il costante aggiornamento, la completezza, la tempestività, la semplicità di consultazione, la comprensibilità, l'omogeneità, la facile accessibilità, nonché la conformità ai documenti originali in possesso dell'amministrazione, l'indicazione della loro provenienza e la riutilizzabilità secondo quanto previsto dall'articolo 7*» e che «*L'esigenza di assicurare adeguata qualità delle informazioni diffuse non può, in ogni caso, costituire motivo per l'omessa o ritardata pubblicazione dei dati, delle informazioni e dei documenti*».

Obbligo di pubblicazione di dati esatti, aggiornati e contestualizzati

Tale previsione deve essere interpretata anche alla luce dei principi in materia di protezione dei dati personali, per cui le pubbliche amministrazioni sono, altresì, tenute a mettere a disposizione soltanto dati personali esatti, aggiornati e contestualizzati (art. 11, comma 1, lett. *c)*, del Codice).

Le pubbliche amministrazioni titolari del trattamento devono, quindi, non solo controllare l'attualità delle informazioni pubblicate, ma anche modificarle o aggiornarle opportunamente, quando sia necessario all'esito di tale controllo e ogni volta che l'interessato ne richieda l'aggiornamento, la rettificazione oppure, quando vi abbia interesse, l'integrazione (art. 7, comma 3, lett. *a)*, del Codice).

5. Modalità di pubblicazione *online* dei dati personali (art. 7 del d. lgs. n. 33/2013)

L'art. 7 del d. lgs. n. 33/2013 prevede che «*I documenti, le informazioni e i dati oggetto di pubblicazione obbligatoria ai sensi della normativa vigente, resi disponibili anche a seguito dell'accesso civico di cui all'articolo 5, sono pubblicati in formato di tipo aperto ai sensi dell'articolo 68 del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, e sono riutilizzabili ai sensi del decreto legislativo 24 gennaio 2006, n. 36, del decreto legislativo 7 marzo 2005, n. 82, e del decreto legislativo 30 giugno 2003, n. 196, senza ulteriori restrizioni diverse dall'obbligo di citare la fonte e di rispettarne l'integrità*».

---

ection/topic_guides/~/media/documents/library/Data_Protection/Practical_application/anonymisation-codev2.pdf) e le Linee guida «*Gestion des risques vie privée*» della *Commission Nationale de l'Informatique et des Libertés* (CNIL) del giugno 2012 (in *http://www.cnil.fr/linstitution/actualite/article/article/les-guides-de-gestion-des-risques-sur-la-vie-privee-sont-disponibles-en-anglais/?tx_ttnews%5BbackPid%5D=91&cHash=fadc2817230d10784c18391f8fbc6082*). La questione relativa alle diverse tecniche di anonimizzazione disponibili è peraltro ancora all'attenzione del Gruppo Art. 29 il quale è in procinto di fornire specifiche indicazioni al riguardo.

La disposizione citata persegue, peraltro, lo scopo di non obbligare gli utenti a dotarsi di programmi proprietari o a pagamento per la fruizione –e, quindi, per la visualizzazione– dei *file* contenenti i dati oggetto di pubblicazione obbligatoria. Infatti, il «*formato di tipo aperto*» è «*un formato di dati reso pubblico, documentato esaustivamente e neutro rispetto agli strumenti tecnologici necessari per la fruizione dei dati stessi*» (art. 68, comma 3, lett. *a)*, del d. lgs. 7 marzo 2005, n. 82, Codice dell'amministrazione digitale-CAD)[8].

È necessario distinguere fra 'formato' di tipo aperto e 'dati' di tipo aperto

Con riferimento ai dati personali (dal novero dei quali sono esclusi i dati delle persone giuridiche, enti e associazioni non riconosciute, nonché i dati anonimi o aggregati; cfr. la definizione contenuta nell'art. 4, comma 1, lett. *b)*, del Codice), si rappresenta, quindi, che l'obbligo di pubblicazione in «*formato di tipo aperto*» non comporta che tali dati, pubblicati sui siti *web* istituzionali in ottemperanza agli obblighi di trasparenza, siano anche «*dati di tipo aperto*» nei termini definiti dal CAD[9].

Occorre, infatti, tenere distinto il concetto di «*formato di tipo aperto*» avente il significato sopra descritto, da quello di «*dato di tipo aperto*» che attiene, invece, più propriamente alla disponibilità unita alla riutilizzabilità del dato da parte di chiunque, anche per finalità commerciali e in formato disaggregato (art. 52, comma 2, e art. 68, comma 3, lett. *b)*, del CAD).

Da ciò consegue che i dati personali oggetto di pubblicazione obbligatoria non sono liberamente riutilizzabili da chiunque per qualsiasi ulteriore finalità, come meglio specificato nel paragrafo seguente.

---

[8] A mero titolo esemplificativo sono considerati *file* in formato aperto, fra gli altri, quelli dei *file* che nei sistemi *personal computer* sono usualmente registrati con estensione *txt*, *pdf*, *xml*. Sulla tipologia dei diversi «*formati di tipo aperto*» si rinvia alle citate «*Linee guida nazionali per la valorizzazione del patrimonio informativo pubblico*», par. 6.2, pagg. 51 ss.

[9] Ai sensi dell'art. 68, comma 3, lett *b*), del CAD sono «*dati di tipo aperto*» quei dati che presentano le seguenti tre caratteristiche:

«*1) sono disponibili secondo i termini di una licenza che ne permetta l'utilizzo da parte di chiunque, anche per finalità commerciali, in formato disaggregato;*

2) sono accessibili attraverso le tecnologie dell'informazione e della comunicazione, ivi comprese le reti telematiche pubbliche e private, in formati aperti ai sensi della lettera a), sono adatti all'utilizzo automatico da parte di programmi per elaboratori e sono provvisti dei relativi metadati;

3) sono resi disponibili gratuitamente attraverso le tecnologie dell'informazione e della comunicazione, ivi comprese le reti telematiche pubbliche e private, oppure sono resi disponibili ai costi marginali sostenuti per la loro riproduzione e divulgazione. L'Agenzia per l'Italia digitale deve stabilire, con propria deliberazione, i casi eccezionali, individuati secondo criteri oggettivi, trasparenti e verificabili, in cui essi sono resi disponibili a tariffe superiori ai costi marginali. In ogni caso, l'Agenzia, nel trattamento dei casi eccezionali individuati, si attiene alle indicazioni fornite dalla direttiva 2003/98/CE del Parlamento europeo e del Consiglio, del 17 novembre 2003, sul riutilizzo dell'informazione del settore pubblico, recepita con il decreto legislativo 24 gennaio 2006, n. 36».

6. Limiti al «*riutilizzo*» di dati personali (artt. 4 e 7 del d. lgs. n. 33/2013)

Limiti al riutilizzo dei dati personali pubblicati *online*

Gli artt. 4 e 7 del d. lgs. n. 33/2013 stabiliscono che il riutilizzo dei dati personali pubblicati è soggetto alle condizioni e ai limiti previsti dalla disciplina sulla protezione dei dati personali e dalle specifiche disposizioni del d. lgs. del 24 gennaio 2006 n. 36 di recepimento della direttiva 2003/98/CE sul riutilizzo dell'informazione del settore pubblico[10]. Tale direttiva è stata oggetto di recente revisione (v. direttiva 2013/37/UE entrata in vigore dopo l'approvazione del decreto legislativo sulla trasparenza[11]).

Con la modifica della predetta direttiva, l'Unione europea conferma il principio, da ritenersi ormai consolidato in ambito europeo[12], in base al quale il riutilizzo di tali documenti non deve pregiudicare il livello di tutela delle persone fisiche con riguardo al trattamento dei dati personali fissato dalle disposizioni di diritto europeo e nazionale in materia[13]. In particolare, le nuove disposizioni della direttiva introducono specifiche eccezioni al riutilizzo fondate sui principi di protezione dei dati, prevedendo che una serie di documenti del settore pubblico contenenti tale tipologia di informazioni siano sottratti al riuso anche qualora siano liberamente accessibili *online*[14].

Ciò significa che il principio generale del libero riutilizzo di documenti contenenti dati pubblici[15], stabilito dalla disciplina nazionale ed europea, riguarda essenzialmente documenti che non contengono dati perso-

---

[10] Direttiva 2003/98/CE del 17 novembre 2003 del Parlamento europeo e del Consiglio relativa al riutilizzo dell'informazione del settore pubblico.

[11] Direttiva 2013/37/UE del 26 giugno 2013 che modifica la direttiva 2003/98/CE del Parlamento europeo e del Consiglio relativa al riutilizzo dell'informazione del settore pubblico.

[12] Cfr., ad esempio, le indicazioni contenute nel documento «*Open Data Handbook*» dell'*Open Knowledge Foundation* (*http://opendatahandbook.org/pdf/OpenDataHandbook.pdf*), una fondazione non governativa che ha lo scopo di promuovere l'apertura dei contenuti e i dati aperti attraverso gruppi di lavoro internazionali (pag. 6).

[13] Art. 1, par. 4, dir. 2003/98/CE, come modificato dall'art. 1, par. 1, lett. *c*), dir. 2013/37/UE; cfr. art. 4, comma 1, lett. *a*), del d. lgs. n. 36/2006.

[14] Art. 1, par. 2, lett. *c-quater*) dir. 2003/98/CE, come modificato dall'art. 1, par. 1, lett. *a*), punto iii), dir. 2013/37/UE. V. anche Gruppo Art. 29, Parere n. 6/2013 cit., sez. V.

[15] Per dati pubblici si intendono dati conoscibili da chiunque (art. 1, comma 1, lett. *n*), del CAD), ma come, peraltro, specificato anche nelle *Linee guida nazionali per la valorizzazione del patrimonio informativo pubblico* dell'AgID, cit., par. 3.3, pag. 28 «*Il concetto di dato pubblico esclude, in linea generale, i dati personali per i quali trovano applicazione le norme del "Codice in materia di protezione dei dati personali" (i.e., D. lgs. n. 196/2003 e deliberazione n. 88/2011 dell'Autorità Garante per la protezione dei dati personali). Laddove, in un contesto informativo, il dato pubblico contiene riferimenti o è collegato a dati personali trova applicazione il comma 5 dell'articolo 2 del CAD "Le disposizioni del presente codice si applicano nel rispetto della disciplina rilevante in materia di trattamento dei dati personali e, in particolare, delle disposizioni del codice in materia di protezione dei dati personali approvato con decreto legislativo 30 giugno 2003, n. 196. I cittadini e le imprese hanno, comunque, diritto ad ottenere che il trattamento dei dati effettuato mediante l'uso di tecnologie telematiche sia conformato al rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato" o altre norme specifiche che consentono la pubblicazione di certe tipologie di informazioni, come ad esempio le norme sulla trasparenza come prima descritto (D. lgs. n. 33/2013)*».

nali oppure riguarda dati personali opportunamente aggregati e resi anonimi[16].

In altri termini, il semplice fatto che informazioni personali siano rese pubblicamente conoscibili *online* per finalità di trasparenza non comporta che le stesse siano liberamente riutilizzabili da chiunque e per qualsiasi scopo, bensì impone al soggetto chiamato a dare attuazione agli obblighi di pubblicazione sul proprio sito *web* istituzionale di determinare –qualora intenda rendere i dati riutilizzabili– se, per quali finalità e secondo quali limiti e condizioni eventuali utilizzi ulteriori dei dati personali resi pubblici possano ritenersi leciti alla luce del «*principio di finalità*» e degli altri principi di matrice europea in materia di protezione dei dati personali[17].

In particolare, in attuazione del principio di finalità di cui all'art. 11 del Codice, il riutilizzo dei dati personali conoscibili da chiunque sulla base delle previsioni del d. lgs. n. 33/2013 non può essere consentito "in termini incompatibili" con gli scopi originari per i quali i medesimi dati sono resi accessibili pubblicamente (art. 7 del d. lgs. n. 33/2013, art. 6, comma 1, lett. *b)*, direttiva 95/46/CE; art. 11, comma 1, lett. *b)*, del Codice)[18].

Opportunità di inserire specifici *alert* sui siti *web*

Pertanto, al fine di evitare di perdere il controllo sui dati personali pubblicati *online* in attuazione degli obblighi di trasparenza e di ridurre i rischi di loro usi indebiti, è quindi in primo luogo opportuno che le pubbliche amministrazioni e gli altri soggetti chiamati a dare attuazione agli obblighi di pubblicazione di cui al d. lgs. n. 33/2013 inseriscano nella sezione denominata «*Amministrazione trasparente*» dei propri siti *web* istituzionali un *alert* generale con cui si informi il pubblico che i dati personali pubblicati sono «*riutilizzabili solo alle condizioni previste dalla normativa vigente sul riuso dei dati pubblici (direttiva comunitaria 2003/98/CE e d. lgs. 36/2006 di recepimento della stessa), in termini compatibili con gli scopi per i quali sono stati raccolti e registrati, e nel rispetto della normativa in materia di protezione dei dati personali*».

Riutilizzo dei dati personali solo a seguito di una valutazione d'impatto *privacy*

Al riguardo, si rappresenta che una volta effettuata la pubblicazione *online* dei dati personali prevista dalla normativa in materia di trasparenza, il soggetto pubblico può rendere riutilizzabili tali dati o accogliere eventuali richieste di riutilizzo degli stessi da parte di terzi, solamente dopo avere effettuato una rigorosa valutazione d'impatto in materia di protezione dei dati, al fine di ridurre il rischio di perdere il controllo sulle medesime in-

[16] Cfr. Gruppo Art. 29, Parere n. 6/2013 cit., sez. VI e *Linee guida nazionali per la valorizzazione del patrimonio informativo pubblico dell'AgID*, cit., par. 3.3, pag. 28.

[17] Cfr. Parere del Garante del 7 febbraio 2013, doc. *web*. n. 2243168, par. 6; v. anche considerando n. 21 dir. 2003/98/CE e considerando n. 11 e n. 34, dir. 2013/37/UE; Corte di Giustizia UE, 16/12/2008, C-73/07, *Tietosuojavaltuutettu* v. *Satakunnan Markkinapörssi Oy and Satamedia Oy*, punto 48; Gruppo Art. 29, Parere n. 6/2013, cit., sez. IV.

[18] Per valutare se i dati personali pubblicamente disponibili *online* possono essere utilizzati per ulteriori scopi in termini compatibili con quelli originari, si vedano gli elementi condivisi in ambito europeo ed elaborati dal Gruppo Art. 29 nel Parere n. 3/2013 sul principio di limitazione della finalità (*http://www.garanteprivacy.it/documents/10160/2133805/WP203*).

formazioni o di dover far fronte a richieste di risarcimento del danno da parte degli interessati[19]. Tale valutazione deve essere volta a:

a) stabilire se è lecito, alla luce dell'esistenza di un presupposto normativo idoneo, che i dati personali pubblicamente accessibili sui siti *web* istituzionali possano essere riutilizzati da terzi e per scopi ulteriori (art. 11, comma 1, lett. *a)* e *b)*, del Codice)[20];

b) in caso di valutazione positiva, occorre poi verificare se l'utilizzo ulteriore di questi dati possa essere consentito:

- limitatamente ai dati rielaborati in forma anonima e aggregata, individuando il livello appropriato di aggregazione e la specifica tecnica di anonimizzazione da utilizzare sulla base di una ponderata valutazione del rischio di re-identificazione degli interessati oppure rispetto a tutti o soltanto ad alcuni dei dati personali resi pubblici (cfr. artt. 3 e 11, lett. *d)*, del Codice)[21];
- per qualsiasi scopo ulteriore o solo per taluni scopi determinati (art. 11, comma 1, lett. *b)*, del Codice)[22];
- secondo modalità di messa a disposizione *online* conformi ai principi di necessità, proporzionalità e pertinenza (artt. 3 e 11 del Codice)[23];
- a condizione che gli utilizzatori adottino modalità tecniche e rispettino specifici vincoli giuridici definiti in apposite licenze pre-

---

[19] Cfr. Gruppo Art. 29, Parere n. 6/2013, cit., sez. IV e VII.; v. anche i commenti del Garante europeo per la protezione dei dati in risposta alla consultazione pubblica avviata dalla Commissione europea sulle linee guida riguardanti le licenze *standard* raccomandate, i *set* di dati e l'imposizione di un corrispettivo in denaro per il riutilizzo, in attuazione del considerando n. 36 della dir. 2013/37/UE cit. (*https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2013/13-11-22_Comments_public_sector_EN.pdf*).

[20] Al riguardo, il mero rinvio alla disciplina generale sul riutilizzo dei dati pubblici (d. lgs. n. 36/2006 e dir. 2003/98/CE) non può costituire una base giuridica idonea a consentire il riutilizzo dei dati personali contenuti nei documenti degli organismi pubblici, essendo, invece, necessario verificare non solo se esiste una norma di settore che preveda specificamente la diffusione al pubblico di tali informazioni, ma anche se e in quali termini in base a tale previsione sia consentito qualsiasi ulteriore trattamento (v. art. 7 del d. lgs. n. 33/2013 e cfr. Gruppo Art. 29, Parere n. 6/2013, cit., specie sez. IV e par. 7.5, Parere n. 3/2013, cit., specie sez. III.2, e All. n. 2).

[21] Come detto, il tema della difficoltà di ottenere dati personali effettivamente 'anonimi' che impediscano la re-identificazione degli interessati è stato oggetto degli interventi di alcune autorità nazionali di protezione dei dati ed è attualmente all'attenzione del Gruppo ex Art. 29 (v. *supra* nota 7 e Parere del Gruppo Art. 29 n. 6/2013 cit., sez. VI).

[22] Ad esempio, per fini commerciali e/o non commerciali.

[23] Ciò sulla base di una rigorosa ponderazione dei rischi di utilizzi impropri e degli effetti negativi che possono derivare agli interessati, tenuto conto delle tipologie di informazioni oggetto di successivo trattamento, delle finalità per le quali esso può essere effettuato, delle categorie di potenziali utilizzatori e degli strumenti utilizzabili. Si fa riferimento in particolare all'adozione di accorgimenti tecnici e giuridici di messa a disposizione dei dati che garantiscano, fra l'altro, l'esattezza e l'aggiornamento delle informazioni rese disponibili, l'ulteriore utilizzo dei dati per finalità e con modalità compatibili con lo scopo iniziale della pubblicazione, la messa a disposizione dei dati per un periodo di tempo limitato e la loro tempestiva cancellazione una volta trascorso tale periodo, nonché l'esercizio dei diritti dell'interessato (compreso il diritto di chiederne la rettifica, l'aggiornamento o la cancellazione) riguardo ai dati personali resi disponibili per il riutilizzo (art. 6 della direttiva 95/46/CE; artt. 3 e 11, del Codice. Cfr. Gruppo Art. 29, Parere n. 6/2013, cit., sez. VII).

disposte al fine di individuare idonee cautele per tutelare i diritti degli interessati nei successivi trattamenti di dati a fini di riutilizzo[24].

All'interno del quadro generale delineato, è illecito, ad esempio, riutilizzare a fini di *marketing* o di propaganda elettorale i recapiti e gli indirizzi di posta elettronica del personale della p.a. oggetto di pubblicazione obbligatoria, in quanto tale ulteriore trattamento deve ritenersi incompatibile con le originarie finalità di trasparenza per le quali i dati sono resi pubblicamente disponibili. Lo scopo perseguito dalle disposizioni che impongono la pubblicazione dei dati del personale, infatti, seppure non espressamente indicato, è quello di aiutare i consociati a individuare i soggetti e i recapiti da contattare per presentare istanze o ottenere informazioni relative a procedimenti di competenza delle pubbliche amministrazioni (ad es., art. 35, d. lgs. n. 33/2013). Di conseguenza, il personale interessato, tenuto conto del contesto in cui i dati che lo riguardano sono stati raccolti, non potrebbe ragionevolmente prevedere che questi possano essere utilizzati per scopi non collegati alle proprie attività lavorative[25].

I dati personali pubblicati sul *web* per finalità di trasparenza non possono essere riutilizzati da terzi per qualsiasi finalità

In ogni caso, nella valutazione d'impatto sopra delineata, è necessario tener conto che, anche alla luce di un'intepretazione sistematica delle disposizioni del decreto sulla trasparenza, i dati personali sensibili e giudiziari sono espressamente esclusi dal riutilizzo (art. 4, comma 1, e art. 7 del d. lgs. n. 33/2013).

I dati sensibili e giudiziari non possono essere oggetto di riutilizzo

Va tenuto presente, inoltre, che non è ammesso l'incondizionato riutilizzo di dati personali oggetto di pubblicazione obbligatoria sulla base di mere licenze aperte che non pongano alcuna limitazione all'ulteriore trattamento dei dati[26]. Laddove, infatti, il soggetto che ha assolto gli obblighi di pubblicazione dei dati personali *online* voglia rendere gli stessi –dopo avere effettuato la predetta valutazione d'impatto *privacy*– anche riutilizzabili, è invece indispensabile che lo stesso predisponga sul proprio sito istituzionale licenze *standard*[27], in formato elettronico e rese facilmente conoscibili ai potenziali utilizzatori, le quali stabiliscano chiaramente le modalità di carattere giuridico e tecnico che presiedono al corretto riutilizzo di tali dati[28].

Non è consentito il riutilizzo di dati personali sulla base di semplici *«licenze aperte»*

---

[24] Le condizioni di riutilizzo cui si fa riferimento dovrebbero riguardare in particolare le questioni relative alle responsabilità in capo agli utilizzatori e alle modalità che garantiscono un uso corretto dei dati sotto il profilo del rispetto dei diritti delle persone cui questi si riferiscono. Cfr. art. 8, comma 2, d. lgs. n. 36/2006; v. anche art. 8 dir. 2003/98/CE così come modificato dall'art. 1, par. 8 della dir. 2013/37/UE e Gruppo Art. 29, Parere n. 6/2013 cit., sezioni VII e X.

[25] Cfr. Gruppo Art. 29, Parere n. 6/2013, cit., par. 7.6.

[26] Cfr. Gruppo Art. 29, Parere n. 6/2013, cit., par. 10.4.

[27] Sulle licenze *standard* si rinvia agli artt. 2, comma 1, lett. *h*), 5, comma 1, e 8, comma 1, del d. lgs. n. 36/2006; v. anche art. 8, della dir. 2003/98/CE così come modificato dall'art. 1, par. 8, della dir. 2013/37/UE.

[28] Tale esigenza è peraltro imprescindibile al fine di non ingenerare equivoci sulla legittimità del riutilizzo dei dati personali pubblicati *online*, stante la disposizione del Codice dell'amministrazione digi-

In proposito, per garantire il rispetto dei diritti degli interessati da parte degli utilizzatori, i termini delle licenze per il riutilizzo dovrebbero contenere una clausola di protezione dei dati sia quando il riuso riguardi dati personali, sia quando riguardi dati anonimi derivati da dati personali[29]. Nel primo caso, le condizioni di licenza dovrebbero indicare chiaramente le finalità e le modalità degli ulteriori trattamenti consentiti. Nel secondo caso tali condizioni dovrebbero, invece, vietare ai titolari delle licenze di re-identificare gli interessati e di assumere qualsiasi decisione o provvedimento che possa riguardarli individualmente sulla base dei dati personali così ottenuti, nonché prevedere in capo ai medesimi titolari l'obbligo di informare l'organismo pubblico nel caso in cui venisse rilevato che gli individui interessati possano essere o siano stati re-identificati[30].

Predisposizione di accorgimenti tecnici per ridurre il rischio di riutilizzo improprio di dati personali

Infine, dal punto vista tecnico, è importante considerare con attenzione quali accorgimenti tecnologici possono essere messi in atto per ridurre i rischi di usi impropri dei dati personali resi disponibili *online* e delle conseguenze negative che possono derivarne agli interessati. In questo quadro devono essere privilegiate modalità tecniche di messa a disposizione dei dati a fini di riutilizzo che consentano di controllare gli accessi a tali dati da parte degli utilizzatori e che impediscano la possibilità di scaricare o di duplicare in maniera massiva e incondizionata le informazioni rese disponibili, nonché l'indiscriminato utilizzo di *software* o programmi automatici[31].

---

tale in base alla quale, nel rispetto dalla disciplina in materia di trattamento dei dati personali (art. 2, comma 5, d. lgs. n. 82/2005), qualunque informazione o documento pubblicato dall'amministrazione con qualsiasi modalità, senza l'espressa adozione di una licenza, si intende rilasciato come «*dato di tipo aperto*», disponibile al riutilizzo gratuito da parte di chiunque, anche per finalità commerciali, e in formato aperto e disaggregato (artt. 52, comma 2, e 68, comma 3, *ivi*).

[29] Tali accorgimenti sono volti, nel primo caso, a evitare che i dati personali accessibili *online* siano riutilizzati in termini incompatibili con gli scopi originari e, nel secondo, a garantire che questi siano effettivamente utilizzati in forma anonima e aggregata.

[30] Cfr. Gruppo Art. 29, Parere n. 6/2013, cit., sez. X. Cfr. anche i sopra citati commenti del Garante europeo per la protezione dei dati in risposta alla consultazione pubblica avviata dalla Commissione europea sulle linee guida previste dal considerando n. 36 della dir. 2013/37/UE.

[31] A titolo esemplificativo, è possibile utilizzare a questo scopo sistemi di verifica '*captcha*' o interfacce personalizzate con funzionalità di accesso ai dati limitato (ad es., previa registrazione dell'utente oppure limitando le interrogazioni eseguibili sui *data base* accessibili *online* o la quantità e il tipo di dati ottenibili); oppure sistemi di *web publishing* e *Cms* (*Content management systems*) in grado di associare ai dati resi pubblici, anche mediante l'utilizzo di parole-chiave (meta-dati), regole di accesso e di utilizzo dei dati che consentono di regolarne la permanenza all'interno del sito istituzionale, consentendone anche la loro agevole rimozione, anche in forma automatica, al verificarsi di determinati eventi quali intervalli temporali o soglie di accessi *online*. In assenza di meccanismi automatizzati di gestione del termine di scadenza dei dati sul sito istituzionale, andrebbero inoltre previste procedure di verifica della validità temporale e del requisito di disponibilità al pubblico delle informazioni, da programmare con cadenza periodica o in seguito a un aggiornamento delle informazioni.

7. Durata degli obblighi di pubblicazione (artt. 8, 14, comma 2, 15, comma 4, del d. lgs. n. 33/2013)

Durata della pubblicazione

L'art. 8, comma 3, del d. lgs. n. 88/2013 prevede che i dati, le informazioni e i documenti oggetto di pubblicazione «*sono pubblicati per un periodo di 5 anni, decorrenti dal 1° gennaio dell'anno successivo a quello da cui decorre l'obbligo di pubblicazione, e comunque fino a che gli atti pubblicati producono i loro effetti, fatti salvi i diversi termini previsti dalla normativa in materia di trattamento dei dati personali e quanto previsto dagli articoli 14, comma 2, e 15, comma 4*».

Ai sensi di tale disposizione, dunque, il periodo di mantenimento di dati, informazioni e documenti sul *web* coincide in linea di massima con il termine di cinque anni.

Eccezioni alla durata quinquennale della pubblicazione

Sono tuttavia espressamente previste deroghe alla predetta durata temporale quinquennale:

a) nel caso in cui gli atti producono ancora i loro effetti alla scadenza dei cinque anni, con la conseguenza che gli stessi devono rimanere pubblicati fino alla cessazione della produzione degli effetti;

b) per alcuni dati e informazioni riguardanti i «*titolari di incarichi politici, di carattere elettivo o comunque di esercizio di poteri di indirizzo politico, di livello statale regionale e locale*» (art. 14, comma 2) e i «*titolari di incarichi dirigenziali e di collaborazione o consulenza*» che devono rimanere pubblicati *online* per i tre anni successivi dalla cessazione del mandato o dell'incarico (art. 15, comma 4);

c) nel caso in cui siano previsti «*diversi termini*» dalla normativa in materia di trattamento dei dati personali. In merito, si evidenzia come il Codice –che non prevede termini espliciti (come già evidenziato dal Garante nel parere del 7 febbraio 2013[32])– richiede espressamente che i dati personali devono essere «*conservati per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati*» e che l'interessato ha diritto di ottenere la cancellazione dei dati personali «*di cui non è necessaria la conservazione in relazione agli scopi per i quali sono stati raccolti o successivamente trattati*» (artt. 11, comma 1, lett. *e)*, e 7, comma 3, lett. *b)*, del Codice). Tali articoli recepiscono, peraltro, le identiche disposizioni contenute nella direttiva 95/46/CE relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali[33] le quali, in quanto tali, non possono essere derogate dalla disciplina nazionale in virtù del primato del diritto europeo. Da tale principio, inoltre, discende l'obbligo di interpretare il diritto nazionale

[32] Cfr. in particolare par. 7.

[33] Cfr. art. 6, par. 1, lett. *e*), e art. 12, par. 1, lett. *b*), dir. 95/46/CE.

in maniera conforme al diritto europeo[34] e, nello specifico, alle disposizioni direttamente applicabili che impongono il rispetto dei principi di pertinenza, necessità e proporzionalità, in base alle quali la pubblicazione di dati personali è consentita soltanto quando è al contempo necessaria e appropriata rispetto all'obiettivo perseguito e, in particolare, quando l'obiettivo perseguito non può essere realizzato in modo ugualmente efficace con modalità meno pregiudizievoli per la riservatezza degli interessati[35].

I dati personali pubblicati devono essere oscurati anche prima della scadenza dei cinque anni se sono cessate le finalità del trattamento

Per tale motivo, il Garante ritiene che laddove atti, documenti e informazioni, oggetto di pubblicazione obbligatoria per finalità di trasparenza, contengano dati personali, questi ultimi devono essere oscurati, anche prima del termine di cinque anni, quando sono stati raggiunti gli scopi per i quali essi sono stati resi pubblici e gli atti stessi hanno prodotto i loro effetti.

7.a. Le sezioni di «*archivio*» dei siti *web* istituzionali (art. 9, comma 2, del d. lgs. n. 33/2013)

L'art. 9, comma 2, del d. lgs. n. 33/2013 prevede che «*Alla scadenza del termine di durata dell'obbligo di pubblicazione di cui all'articolo 8, comma 3, i documenti, le informazioni e i dati sono comunque conservati e resi disponibili, con le modalità di cui all'articolo 6, all'interno di distinte sezioni del sito di archivio, collocate e debitamente segnalate nell'ambito della sezione "Amministrazione trasparente". I documenti possono essere trasferiti all'interno delle sezioni di archivio anche prima della scadenza del termine di cui all'articolo 8, comma 3*».

La disposizione richiamata richiede ai soggetti tenuti agli obblighi di pubblicazione di conservare e mettere a disposizione i documenti, le informazioni e i dati all'interno della sezione di archivio dei siti *web*, eventualmente anche prima che sia terminato il periodo di pubblicazione.

---

[34] Cfr., in particolare, *ex pluribus*, le sentenze della Corte di Giustizia CE, 10 aprile 1984, causa 14/83, *Von Colson e Kamann*, punto 26; 13 novembre 1990, C-106/89, *Marleasing*, punto 8; 16 dicembre 1993, causa C-334/92, *Wagner Miret*, punto 20; 25 febbraio 1999, causa C-131/97, *Carbonari*, punto 48; 5 ottobre 2004, C-397/01, *Pfeiffer*, punto 114; Corte di Giustizia CE, 29/1/2008, C-275/06, *Productores de Música de España-Promusicae*, punto 70.

[35] Cfr. art. 6, par. 1, lett. *c*), e art. 7, par.1, lett. *c*) e *d*), dir. 95/46/CE; artt. 3 e 11 del Codice. V. inoltre, Corte di Giustizia CE, 20/5/2003, cause riunite C-465/00, C-138/01 e C-139/01 e Corte Costituzionale austriaca 28 novembre 2003, KR 1/00-33 (in *http://www.vfgh.at/cms/vfgh-site/attachments/3/8/6/CH0006/CMS1108403943433/kr1-33-00.pdf*). Si ricorda che i principi di derivazione comunitaria richiamati soddisfano i requisiti dell'immediata applicabilità (cfr. la già citata sentenza della Corte di Giustizia CE, 20/5/2003, punti 98-100), con la conseguenza di obbligare, come già ricordato, non solo i giudici nazionali ma anche gli organi amministrativi a disapplicare la legislazione nazionale contrastante con la normativa comunitaria senza doverne attendere la rimozione in sede legislativa o per il tramite di impugnazioni di incostituzionalità (Corte cost. 11/7/1989, n 389; cfr. anche Corte di Giustizia 9 marzo 1978 causa C-106/77).

Con riferimento alla documentazione contenente dati personali, si precisa che la predetta ipotesi di "messa a disposizione" della documentazione nella sezione di archivio non comporta l'accesso e la conoscenza indiscriminata degli stessi una volta scaduti i diversi periodi di pubblicazione previsti dall'art. 8, comma 3, del d. lgs. n. 33/2013. Ciò perché, in caso contrario, si determinerebbe una diffusione *sine die* di dati personali *online* in violazione dei principi contenuti nella normativa europea come quello di proporzionalità descritto nel paragrafo precedente[36]. Inoltre, sempre ragionando *a contrario*, la formazione della sezione archivio si trasformerebbe in un mero trasferimento di documenti, informazioni e dati da una parte all'altra dello stesso sito *web* e all'interno, peraltro, della stessa sezione «*Amministrazione trasparente*».

Accesso selettivo alla documentazione trasferita nella sezione "archivio" del sito *web* istituzionale

Di conseguenza, per attuare le esigenze sottese alla prevista ipotesi di consultabilità di atti e documenti contenuti nella sezione archivio, non è in linea generale giustificato, alla luce del principio di proporzionalità, consentire, al di fuori dei casi espressamente previsti, l'accesso *online* libero e incondizionato alla consultazione di atti e documenti contenenti informazioni personali, specie se aventi natura sensibile, senza applicare criteri selettivi.

In tale quadro, bisogna, quindi, rendere disponibile la documentazione contenuta nelle sezioni di archivio secondo le regole sull'accessibilità degli "archivi"[37], individuando le condizioni di accesso e selezionando, a tal fine, anche preliminarmente, nell'ambito dei singoli atti e documenti, le informazioni da rendere consultabili. In tale prospettiva, si ritiene che le informazioni personali contenute in atti e documenti possano essere reperibili nelle sezioni di archivio, mediante modalità che ne garantiscano tra l'altro la «*semplicità di consultazione*» e la «*facile accessibilità*» (art. 6 del d. lgs. n. 33/2013)[38], attraverso, ad esempio, l'attribuzione alle persone che ne hanno fatto richiesta, nel rispetto delle predette regole, di una chiave personale di identificazione informatica secondo le regole stabilite in materia dal Codice dell'amministrazione digitale.

In alternativa, il Garante ritiene che è comunque possibile la libera consultazione da parte di chiunque della sezione di archivio a condizione che i soggetti destinatari degli obblighi di pubblicazione in materia di trasparenza adottino opportune misure a tutela degli interessati avendo cura di

In alternativa rendere anonimi i dati contenuti nella sezione "archivio" del sito *web* istituzionale

[36] Cfr. artt. 6, 7 e 12 dir. 95/46/CE cit. Sul punto, peraltro, la Corte di Giustizia dell'Unione europea (sent. 9/11/2010, cause riunite C-92/09 e C-93/09) ha dichiarato l'invalidità di un regolamento comunitario nella parte in cui imponeva la pubblicazione di dati personali di beneficiari di finanziamenti di fondi strutturali senza prevedere, fra l'altro, un limite temporale per la durata della stessa, commisurato ai periodi nel corso dei quali gli interessati hanno percepito gli aiuti.

[37] Cfr. artt. 124 ss., del d. lgs. 22/1/2004 n. 42. Al riguardo, vedi anche il *Codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi storici* (all. A.2 del Codice in materia di protezione dei dati personali, Provv. n. 8/P/2001 del 14 marzo 2001, in G.U. 5 aprile 2001, n. 80).

[38] Articolo espressamente richiamato dall'art. 9, comma 2, del d. lgs. n. 33/2013.

rendere anonimi i dati personali contenuti nella documentazione inserita in archivio, fermo restando il rispetto delle disposizioni normative sulla tenuta degli "archivi" sopra richiamate. Sulle misure e sugli accorgimenti necessari per l'anonimizzazione dei dati si rimanda alle indicazioni contenute *supra* in par. 3.

Per espressa previsione normativa, infine, i dati e le informazioni concernenti la situazione patrimoniale dei titolari di incarichi politici, di cui al citato art. 14, non devono essere trasferiti nelle sezioni di archivio dei siti *web* istituzionali alla scadenza del termine di pubblicazione (art. 14, comma 2, del d. lgs. n. 33/2013).

Eccezione al trasferimento dei dati in archivio (ad es., situazione patrimoniale dei titolari di incarichi di indirizzo politico)

8. Indicizzazione tramite motori di ricerca (art. 9, comma 1, del d. lgs. n. 33/2013)

L'art. 9 del d. lgs. n. 33/2013 stabilisce che «*Le amministrazioni non possono disporre filtri e altre soluzioni tecniche atte ad impedire ai motori di ricerca web di indicizzare ed effettuare ricerche all'interno della sezione "Amministrazione trasparente"*».

Si evidenzia che l'obbligo di indicizzazione nei motori generalisti durante il periodo di pubblicazione obbligatoria è limitato ai soli dati tassativamente individuati ai sensi delle disposizioni in materia di trasparenza da collocarsi nella «*sezione "Amministrazione trasparente"*», con esclusione di altri dati che si ha l'obbligo di pubblicare per altre finalità di pubblicità diverse da quelle di «*trasparenza*», come esposto nell'«*Introduzione*» e nella parte seconda delle presenti Linee guida.

Sono, fra l'altro, espressamente sottratti all'indicizzazione i dati sensibili e i dati giudiziari (art. 4, comma 1, d. lgs. n. 33/2013). Pertanto, i soggetti destinatari degli obblighi di pubblicazione previsti dal d. lgs. n. 33/2013 devono provvedere alla relativa deindicizzazione tramite –ad esempio– l'inserimento di *metatag noindex* e *noarchive* nelle intestazioni delle pagine *web* o alla codifica di regole di esclusione all'interno di uno specifico file di testo (il file *robots.txt*) posto sul *server* che ospita il sito *web* configurato in accordo al *Robot Exclusion Protocol* (avendo presente, comunque, come tali accorgimenti non sono immediatamente efficaci rispetto a contenuti già indicizzati da parte dei motori di ricerca Internet, la cui rimozione potrà avvenire secondo le modalità da ciascuno di questi previste)[39].

I dati sensibili e giudiziari non possono essere indicizzati

[39] Per approfondimenti, si consulti, a tal proposito, l'indirizzo *web*: *http://www.robotstxt.org/*.

9. Indicazioni per specifici obblighi di pubblicazione

9.a. Obblighi di pubblicazione dei *curricula* professionali (art. 10, comma 8, lett. *d)*, del d. lgs. n. 33/2013 *et al.*)

La disciplina in materia di trasparenza prevede di rendere visibile al pubblico, rispetto a taluni soggetti, informazioni personali concernenti il percorso di studi e le esperienze professionali rilevanti, nella forma del *curriculum* redatto in conformità al vigente modello europeo (art. 10, comma 8, lett. *d*)).

Le ipotesi previste riguardano, ad esempio, i *curricula* professionali dei titolari di incarichi di indirizzo politico (art. 14), dei titolari di incarichi amministrativi di vertice, dirigenziali e di collaborazione o consulenza (art. 15, comma 1, lett. *b*), nonché delle posizioni dirigenziali attribuite a persone –anche esterne alle pubbliche amministrazioni– individuate discrezionalmente dall'organo di indirizzo politico senza procedure pubbliche di selezione, di cui all'art. 1, commi 39 e 40, della legge 6 novembre 2012, n. 190 (art. 15, comma 5), dei componenti degli organismi indipendenti di valutazione (art. 10, comma 8, lett. *c*), nonché dei dirigenti in ambito sanitario come individuati dall'art. 41, commi 2 e 3.

Il riferimento del legislatore all'obbligo di pubblicazione del *curriculum* non può tuttavia comportare la diffusione di tutti i contenuti astrattamente previsti dal modello europeo (rispondendo taluni di essi alle diverse esigenze di favorire l'incontro tra domanda e offerta di lavoro in vista della valutazione di candidati oppure, nel corso del rapporto di lavoro, per l'assegnazione dell'interessato a nuovi incarichi o per selezioni concernenti la progressione di carriera), ma solo di quelli pertinenti rispetto alle finalità di trasparenza perseguite.

Evitare la pubblicazione di dati personali eccedenti e non pertinenti nel *curriculum* europeo

Prima di pubblicare sul sito istituzionale i *curricula*, il titolare del trattamento dovrà pertanto operare un'attenta selezione dei dati in essi contenuti, se del caso predisponendo modelli omogenei e impartendo opportune istruzioni agli interessati (che, in concreto, possono essere chiamati a predisporre il proprio *curriculum* in vista della sua pubblicazione per le menzionate finalità di trasparenza). In tale prospettiva, sono pertinenti le informazioni riguardanti i titoli di studio e professionali, le esperienze lavorative (ad es., gli incarichi ricoperti), nonché ulteriori informazioni di carattere professionale (si pensi alle conoscenze linguistiche oppure alle competenze nell'uso delle tecnologie, come pure alla partecipazione a convegni e seminari oppure alla redazione di pubblicazioni da parte dell'interessato). Non devono formare invece oggetto di pubblicazione dati eccedenti, quali

ad esempio i recapiti personali oppure il codice fiscale degli interessati, ciò anche al fine di ridurre il rischio di c.d. furti di identità[40].

Deve inoltre essere garantita agli interessati la possibilità di aggiornare periodicamente il proprio *curriculum* ai sensi dell'art. 7 del Codice[41] evidenziando gli elementi oggetto di aggiornamento.

9.b. Obblighi di pubblicazione della dichiarazione dei redditi dei componenti degli organi di indirizzo politico e dei loro familiari (art. 14 del d. lgs. n. 33/2013)

L'art. 14 del d. lgs. n 33/2013 prevede la pubblicazione delle «*dichiarazioni di cui all'articolo 2, della legge 5 luglio 1982, n. 441, nonché le attestazioni e dichiarazioni di cui agli articoli 3 e 4 della medesima legge, come modificata dal presente decreto, limitatamente al soggetto, al coniuge non separato e ai parenti entro il secondo grado, ove gli stessi vi consentano*»[42].

Evitare la pubblicazione di dati personali eccedenti e non pertinenti contenute nelle dichiarazioni dei redditi

Con riferimento all'obbligo di pubblicazione della dichiarazione dei redditi, la predetta disposizione deve essere coordinata con le altre disposizioni dello stesso d. lgs. n. 33/2013 (art. 4, comma 4), con i principi di pertinenza e non eccedenza (art. 11, comma 1, lett. *d)*, del Codice), nonché con le previsioni a tutela dei dati sensibili (art. 22 del Codice).

Pertanto, ai fini dell'adempimento del previsto obbligo di pubblicazione, risulta sufficiente pubblicare copia della dichiarazione dei redditi – dei componenti degli organi di indirizzo politico e, laddove vi acconsentano, del coniuge non separato e dei parenti entro il secondo grado– previo però oscuramento, a cura dell'interessato o del soggetto tenuto alla pubblicazione qualora il primo non vi abbia provveduto, delle informazioni eccedenti e non pertinenti rispetto alla ricostruzione della situazione patrimoniale degli interessati (quali, ad esempio, lo stato civile, il codice fiscale, la sottoscrizione, *etc.*), nonché di quelle dalle quali si possano desumere indirettamente dati di tipo sensibile, come, fra l'altro, le indicazioni relative a:

Esempi di informazioni eccedenti

- familiari a carico tra i quali possono essere indicati figli disabili;
- spese mediche e di assistenza per portatori di handicap o per determinate patologie;
- erogazioni liberali in denaro a favore dei movimenti e partiti politici;

[40] V. Provv. del Garante del 16 luglio 2009 in materia di «*Pubblica amministrazione: dirigenza e assenze e presenze del personale*» (doc. *web* n. 1639950), e circolare del Dipartimento della funzione pubblica presso la Presidenza del Consiglio dei Ministri n. 3/2009.

[41] *Ivi.*

[42] In relazione all'ambito soggettivo di applicazione di tale articolo si rimanda alle indicazioni contenute nella Delibera CIVIT n. 65/2013 in tema di «*Applicazione dell'art. 14 del d. lgs. n. 33/2013 – Obblighi di pubblicazione concernenti i componenti degli organi di indirizzo politico*» del 31 luglio 2013, in *http://www.civit.it/?p=9381*.

- erogazioni liberali in denaro a favore delle organizzazioni non lucrative di utilità sociale, delle iniziative umanitarie, religiose, o laiche, gestite da fondazioni, associazioni, comitati ed enti individuati con decreto del Presidente del Consiglio dei ministri nei paesi non appartenenti all'OCSE;
- contributi associativi versati dai soci alle società di mutuo soccorso che operano esclusivamente nei settori di cui all'art. 1 della l. 15 aprile 1886, n. 3818, al fine di assicurare ai soci medesimi un sussidio nei casi di malattia, di impotenza al lavoro o di vecchiaia, oppure, in caso di decesso, un aiuto alle loro famiglie;
- spese sostenute per i servizi di interpretariato dai soggetti riconosciuti sordomuti ai sensi della l. 26 maggio 1970, n. 381;
- erogazioni liberali in denaro a favore delle istituzioni religiose;
- scelta per la destinazione dell'otto per mille;
- scelta per la destinazione del cinque per mille.

Si ricorda che non possono essere pubblicati i dati personali del coniuge non separato e dei parenti entro il secondo grado che non abbiano prestato il consenso alla pubblicazione delle attestazioni e delle dichiarazioni di cui all'art. 14, comma 1, lett. *f*), del d. lgs. n. 33/2013.

Non possono essere pubblicati i dati personali del coniuge e dei parenti che non hanno prestato il relativo consenso

9.c. Obblighi di pubblicazione concernenti corrispettivi e compensi (artt. 15, 18 e 41, del d. lgs. n. 33/2013)

La disciplina in materia di trasparenza prevede che informazioni concernenti l'entità di corrispettivi e compensi percepiti da alcune tipologie di soggetti formino oggetto di pubblicazione secondo le modalità previste dal d. lgs. n. 33/2013. Tra questi ultimi sono annoverati, ad esempio, i titolari di incarichi amministrativi di vertice, dirigenziali e di collaborazione o consulenza (cfr. artt. 15 e 41, commi 2 e 3), nonché i dipendenti pubblici cui siano stati conferiti o autorizzati incarichi (art. 18).

Pertanto, ai fini dell'adempimento degli obblighi di pubblicazione, risulta proporzionato indicare il compenso complessivo percepito dai singoli soggetti interessati, determinato tenendo conto di tutte le componenti, anche variabili, della retribuzione. Non appare, invece, giustificato riprodurre sul *web* la versione integrale di documenti contabili, i dati di dettaglio risultanti dalle dichiarazioni fiscali oppure dai cedolini dello stipendio di ciascun lavoratore[43] come pure l'indicazione di altri dati eccedenti riferiti a

È sproporzionato riprodurre sul *web* la versione integrale di documenti contabili o i cedolini di pagamento

[43] V. *Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico* del 14 giugno 2007.

percettori di somme (quali, ad esempio, i recapiti individuali e le coordinate bancarie utilizzate per effettuare i pagamenti).

Non risulta inoltre giustificata la pubblicazione di informazioni relative alle dichiarazioni dei redditi dei dipendenti e dei loro familiari, ipotesi questa che la legge impone esclusivamente nei confronti dei componenti degli organi di indirizzo politico (art. 14, del d. lgs. n. 33/2013).

9.d. Obblighi di pubblicazione concernenti i provvedimenti amministrativi relativi a concorsi e prove selettive per l'assunzione del personale e progressioni di carriera (art. 23 del d. lgs. n. 33/2013)

L'art. 23 del d. lgs. n. 33/2013 prevede la pubblicazione obbligatoria di elenchi dei provvedimenti adottati dagli organi di indirizzo politico e dai dirigenti, tra i quali vanno menzionati i provvedimenti finali dei procedimenti relativi a concorsi e prove selettive per l'assunzione del personale e progressioni di carriera. In attuazione di tale disposizione, di questi provvedimenti devono essere pubblicati solo gli elementi di sintesi, indicati nel comma 2, quali il contenuto, l'oggetto, l'eventuale spesa prevista e gli estremi dei principali documenti contenuti nel fascicolo del procedimento. Con particolare riferimento ai provvedimenti finali adottati all'esito dell'espletamento di concorsi oppure di prove selettive non devono formare quindi oggetto di pubblicazione, in base alla disposizione in esame, gli atti nella loro veste integrale contenenti (anche in allegato), le graduatorie formate a conclusione del procedimento, né le informazioni comunque concernenti eventuali prove intermedie che preludono all'adozione dei provvedimenti finali (per i quali restano salve altre forme di conoscibilità previste dall'ordinamento: v. in merito, con riguardo alle forme di pubblicità delle graduatorie e degli altri atti riguardanti i concorsi, le prove selettive e le progressioni di carriera, le indicazioni contenute nel par. 3.b. della seconda parte delle presenti Linee guida).

Pubblicazione dei soli provvedimenti finali e rinvio alle indicazioni contenute nel par. 3.b. della seconda parte delle presenti *Linee guida*

9.e. Obblighi di pubblicazione degli atti di concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici e dell'elenco dei soggetti beneficiari (artt. 26 e 27 del d. lgs. n. 33/2013)

L'art. 26, comma 2, del d. lgs. n. 33/2013 stabilisce l'obbligo di pubblicazione degli atti di concessione «*delle sovvenzioni, contributi, sussidi ed ausili finanziari alle imprese, e comunque di vantaggi economici di qualunque genere a persone ed enti pubblici e privati ai sensi del citato articolo 12 della legge n. 241 del 1990, di importo superiore a mille euro*». Il comma 3 del medesimo articolo aggiunge che tale pubblicazione «*costitui-*

sce condizione legale di efficacia dei provvedimenti che dispongano concessioni e attribuzioni di importo complessivo superiore a mille euro nel corso dell'anno solare al medesimo beneficiario».

Per le predette pubblicazioni è prevista l'indicazione delle seguenti informazioni: a) il nome dell'impresa o dell'ente e i rispettivi dati fiscali o il nome di altro soggetto beneficiario; b) l'importo del vantaggio economico corrisposto; c) la norma o il titolo a base dell'attribuzione; d) l'ufficio e il funzionario o dirigente responsabile del relativo procedimento amministrativo; e) la modalità seguita per l'individuazione del beneficiario; f) il *link* al progetto selezionato e al *curriculum* del soggetto incaricato (art. 27, comma 1).

In tale quadro, lo stesso d. lgs. n. 33/2013 individua una serie di limiti all'obbligo di pubblicazione di atti di concessione di benefici economici comunque denominati.

Eccezioni all'obbligo di pubblicazione di dati di destinatari di benefici economici

Non possono, infatti, essere pubblicati i dati identificativi delle persone fisiche destinatarie dei provvedimenti di concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici, nonché gli elenchi dei relativi destinatari:

Divieto di diffusione dei dati personali di beneficiari di importi inferiore a mille euro nell'anno solare

a) di importo complessivo inferiore a mille euro nel corso dell'anno solare a favore del medesimo beneficiario[44];

b) di importo superiore a mille euro nel corso dell'anno solare a favore del medesimo beneficiario «*qualora da tali dati sia possibile ricavare informazioni relative allo stato di salute*» (art. 26, comma 4, d. lgs. n. 33/2013; nonché artt. 22, comma 8, e 68, comma 3, del Codice);

c) di importo superiore a mille euro nel corso dell'anno solare a favore del medesimo beneficiario «*qualora da tali dati sia possibile ricavare informazioni relative [...] alla situazione di disagio economico-sociale degli interessati*» (art. 26, comma 4, d. lgs. n. 33/2013).

Divieto di diffusione dei dati di beneficiari idonei a rivelare lo stato di salute e relativa casistica

Si ribadisce, con specifico riferimento alle informazioni idonee a rivelare lo stato di salute, che è vietata la diffusione di qualsiasi dato o informazione da cui si possa desumere lo stato di malattia o l'esistenza di patologie dei soggetti interessati, compreso qualsiasi riferimento alle condi-

[44] Cfr. sul punto la Delibera CIVIT n. 59/2013 in tema di «*Pubblicazione degli atti di concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche ed enti pubblici e privati (artt. 26 e 27, d. lgs. n. 33/2013)*» (in *http://www.civit.it/?p=9059*) che in proposito ha indicato: «*L'art. 26, c. 2, del d. lgs. n. 33/20013, inoltre, stabilisce che la pubblicazione è obbligatoria e condizione di efficacia solo per importi superiori a mille euro. In base a quanto stabilito dalla norma, questi sono da intendersi sia se erogati con un unico atto, sia con atti diversi ma che nel corso dell'anno solare superino il tetto dei mille euro nei confronti di un unico beneficiario. Ove, quindi, l'amministrazione abbia emanato più provvedimenti i quali, nell'arco dell'anno solare, hanno disposto la concessione di vantaggi economici a un medesimo soggetto, superando il tetto dei mille euro, l'importo del vantaggio economico corrisposto, di cui all'art. 27, c. 1, lett. b), del decreto, è da intendersi come la somma di tutte le erogazioni effettuate nel periodo di riferimento. In tali casi, l'amministrazione deve necessariamente pubblicare, come condizione legale di efficacia, l'atto che comporta il superamento della soglia dei mille euro, facendo peraltro riferimento anche alle pregresse attribuzioni che complessivamente hanno concorso al suddetto superamento della soglia*».

zioni di invalidità, disabilità o handicap fisici e/o psichici (cfr. *supra* par. 2). Si pensi, ad esempio, all'indicazione:

- della disposizione sulla base della quale ha avuto luogo l'erogazione del beneficio economico se da essa è possibile ricavare informazioni sullo stato di salute di una persona (si pensi all'indicazione "erogazione ai sensi della legge 104/1992" che, come noto, è la «*Legge-quadro per l'assistenza, l'integrazione sociale e i diritti delle persone handicappate*»);

- dei titoli dell'erogazione dei benefici (ad es., attribuzione di borse di studio a "soggetto portatore di handicap", o riconoscimento di buono sociale a favore di "anziano non autosufficiente" o con l'indicazione, insieme al dato anagrafico, delle specifiche patologie sofferte dal beneficiario);

- delle modalità e dei criteri di attribuzione del beneficio economico (ad es., punteggi attribuiti con l'indicazione degli "indici di autosufficienza nelle attività della vita quotidiana")[45];

- della destinazione dei contributi erogati (ad es., contributo per "ricovero in struttura sanitaria" o per "assistenza sanitaria").

Analogamente, è vietato riportare dati o informazioni da cui si può desumere la condizione di indigenza o di disagio sociale in cui versano gli interessati (art. 26, comma 4, del d. lgs. n. 33/2013).

Divieto di diffusione dei dati di beneficiari idonei a rivelare situazione di disagio economico-sociale degli interessati

Si tratta di un divieto funzionale alla tutela della dignità, dei diritti e delle libertà fondamentali dell'interessato (art. 2 del Codice), al fine di evitare che soggetti che si trovano in condizioni disagiate –economiche o sociali– soffrano l'imbarazzo della diffusione di tali informazioni, o possano essere sottoposti a conseguenze indesiderate, a causa della conoscenza da parte di terzi della particolare situazione personale. Si pensi, fra l'altro alle fasce deboli della popolazione (persone inserite in programmi di recupero e di reinserimento sociale, anziani, minori di età, *etc.*). Alla luce delle considerazioni sopra espresse, spetta agli enti destinatari degli obblighi di pubblicazione *online* contenuti nel d. lgs. n. 33/2013, in quanto titolari del trattamento, valutare, caso per caso, quando le informazioni contenute nei provvedimenti rivelino l'esistenza di una situazione di disagio economico o sociale in cui versa il destinatario del beneficio e non procedere, di conseguenza, alla pubblicazione dei dati identificativi del beneficiario o delle altre informazioni che possano consentirne l'identificazione. Tale decisione rimane comunque sindacabile da parte del Garante che assicura il rispetto dei predetti principi in materia di protezione dei dati personali.

Divieto di diffusione di dati personali non necessari, non pertinenti o eccedenti

In ogni modo, si evidenzia che i soggetti destinatari degli obblighi di pubblicazione contenuti nel d. lgs. n. 33/2013 sono tenuti, anche in tale ambito, al rispetto dei principi di necessità (art. 3, comma 1, del Codice),

[45] C.d. scala Adl o di Katz.

pertinenza e non eccedenza (art. 11, comma 1, lett. *d)*, del Codice), nonché delle disposizioni a tutela dei dati sensibili (art. 22 del Codice).

Non risulta, pertanto, giustificato diffondere, fra l'altro, dati quali, ad esempio, l'indirizzo di abitazione o la residenza, il codice fiscale di persone fisiche, le coordinate bancarie dove sono accreditati i contributi o i benefici economici (codici IBAN), la ripartizione degli assegnatari secondo le fasce dell'Indicatore della situazione economica equivalente-Isee, l'indicazione di analitiche situazioni reddituali, di condizioni di bisogno o di peculiari situazioni abitative, *etc.*.

Si evidenzia, inoltre, che il riutilizzo dei dati personali pubblicati ai sensi dei predetti artt. 26 e 27, non è libero, ma subordinato –come stabilito dallo stesso art. 7 del d. lgs. n. 33/2013– alle specifiche disposizioni di cui alla direttiva comunitaria 2003/98/CE e al d. lgs. n. 36 del 24 gennaio 2006 di recepimento della stessa, che non pregiudicano in alcun modo il livello di tutela delle persone con riguardo al trattamento dei dati personali (sul punto si rimanda alle indicazioni fornite *supra* nel par. 6).

Limiti al riutilizzo dei dati personali di soggetti destinatari di benefici economici

9.e.i. Albo dei beneficiari di provvidenze di natura economica (d.P.R. 7 aprile 2000, n. 118)

L'assolvimento degli obblighi di pubblicazione degli atti di concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici descritti nel paragrafo precedente deve essere coordinato con le disposizioni che regolano la predisposizione dell'albo dei beneficiari di provvidenze di natura economica (d.P.R. 7 aprile 2000, n. 118).

Coordinamento con gli obblighi previsti dal d.P.R. n. 118/2000

Per tale motivo –alla luce di un'interpretazione sistematica del quadro normativo emergente dalla recente novella in tema di trasparenza e al fine di non duplicare in capo alle pubbliche amministrazioni gli oneri di pubblicazione– deve ritenersi che l'adempimento delle prescrizioni contenute negli artt. 26 e 27 del d. lgs. n. 33/2013, con le relative modalità ed eccezioni descritte nel paragrafo precedente, assorbe gli obblighi previsti dagli artt. 1 e 2 del d.P.R. n. 118[46].

L'adempimento degli obblighi di pubblicazione contenuti negli artt. 26 e 27 del d. lgs. n. 33/2013 assorbe gli obblighi previsti per gli stessi soggetti dal d.P.R. n. 118/2000

Per gli stessi motivi, il Garante ritiene, inoltre, che i soggetti diversi dalle pubbliche amministrazioni[47] parimenti tenuti alla pubblicazione dell'albo dei beneficiari di provvidenze di natura economica ai sensi del d.P.R. n. 118/2000 devono comunque rispettare le medesime cautele ed eccezioni previste dagli artt. 26 e 27 descritte nel paragrafo precedente (ad

[46] Cfr. Delibera Civit n. 59/2013 in tema di «*Pubblicazione degli atti di concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche ed enti pubblici e privati (artt. 26 e 27, d.lgs. n. 33/2013)*», cit..

[47] Cfr. la definizione contenuta nell'art. 11 del d. lgs. n. 33/2013 che richiama l'art. 1, comma 2, del d. lgs. 30 marzo 2001, n. 165, e ss.mm..

es., divieto di pubblicazione dei dati identificativi dei soggetti beneficiari di importi inferiori a mille euro nell'anno solare, di informazioni idonee a rivelare lo stato di salute o la situazione di disagio economico-sociale degli interessati, di dati eccedenti o non pertinenti).

PARTE SECONDA

PUBBLICITÀ PER ALTRE FINALITÀ DELLA P.A.

1. Limiti alla diffusione di dati personali nella pubblicazione di atti e documenti sul *web* per finalità diverse dalla trasparenza

Obblighi di pubblicità dell'azione amministrativa pubblicazione per finalità diverse da quelle di trasparenza

Come illustrato nell'«*Introduzione*» alle presenti Linee guida, esistono casi e obblighi di pubblicità *online* di dati, informazioni e documenti della p.a., contenuti in specifiche disposizioni di settore diverse da quelle previste in materia di trasparenza, come, fra l'altro, quelli volti a far conoscere l'azione amministrativa in relazione al rispetto dei principi di legittimità e correttezza, o quelli necessari a garantire la pubblicità legale degli atti amministrativi (ad es., pubblicità integrativa dell'efficacia, dichiarativa, notizia).

Per un'elencazione non esaustiva degli obblighi di pubblicità che ricadono in tale categoria si rinvia agli esempi già illustrati nell'«*Introduzione*» alle presenti Linee guida.

Anche per tali fattispecie occorre –come già indicato per gli obblighi di pubblicità di dati personali per finalità di «*trasparenza*»– che le pubbliche amministrazioni, prima di mettere a disposizione sui propri siti *web* istituzionali atti e documenti amministrativi (in forma integrale o per estratto, ivi compresi gli allegati) contenenti dati personali, verifichino se la normativa di settore preveda espressamente tale obbligo (art. 4, comma 1, lett. *m)*, e art. 19, comma 3, del Codice, con riguardo ai dati comuni, nonché artt. 20, 21 e 22, comma 11, con riferimento ai dati sensibili e giudiziari).

Laddove l'amministrazione riscontri l'esistenza di un obbligo normativo che impone la pubblicazione dell'atto o del documento nel proprio sito *web* istituzionale è necessario selezionare i dati personali da inserire in tali atti e documenti, verificando, caso per caso, se ricorrono i presupposti per l'oscuramento di determinate informazioni.

Principio di necessità

Ciò pure in considerazione del fatto che, anche in tale ipotesi, i soggetti pubblici sono tenuti a ridurre al minimo l'utilizzazione di dati personali e di dati identificativi (art. 4, comma 1, lett *c)*, del Codice), ed evitare il relativo trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante dati anonimi o altre modalità che permettano di identificare l'interessato solo in caso di necessità (c.d. "*principio di necessità*" di cui all'art. 3, comma 1, del Codice).

Il rispetto dei principi di pertinenza e non eccedenza

Pertanto, anche in presenza di un obbligo di pubblicità è consentita la diffusione dei soli dati personali la cui inclusione in atti e documenti sia

realmente necessaria e proporzionata al raggiungimento delle finalità perseguite dall'atto (c.d. "*principio di pertinenza e non eccedenza*" di cui all'art. 11, comma 1, lett. *d)*, del Codice).

Il procedimento di selezione dei dati personali suscettibili di essere resi diffusi deve essere, inoltre, particolarmente accurato nei casi in cui tali informazioni sono idonee a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale, la vita sessuale («*dati sensibili*»), oppure nel caso di dati idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da *a*) a *o*) e da *r*) a *u*), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, nonché la qualità di imputato o di indagato («*dati giudiziari*») (art. 4, comma 1, lett. *d)* ed *e)*, del Codice).

Dati sensibili e giudiziari

I dati sensibili e giudiziari, infatti, sono protetti da un quadro di garanzie particolarmente stringente che prevede la possibilità per i soggetti pubblici di diffondere tali informazioni solo nel caso in cui sia previsto da una espressa disposizione di legge e di trattarle solo nel caso in cui siano in concreto «*indispensabili*» per svolgere l'attività istituzionale che non può essere adempiuta, caso per caso, mediante l'utilizzo di dati anonimi o di dati personali di natura diversa (artt. 22, in particolare commi 3, 5 e 11 e 68, comma 3, del Codice).

Resta, invece, del tutto vietata la diffusione di «*dati idonei a rivelare lo stato di salute*» (art. 22, comma 8, del Codice).

Divieto assoluto di diffusione di dati personali idonei a rivelare lo stato di salute

Ciò significa, di conseguenza, che è vietata la pubblicazione di qualsiasi informazione da cui si possa desumere lo stato di malattia o l'esistenza di patologie dei soggetti interessati, compreso qualsiasi riferimento alle condizioni di invalidità, disabilità o handicap fisici e/o psichici[48].

A tale scopo, fin dalla fase di redazione degli atti e dei documenti oggetto di pubblicazione, nel rispetto del principio di adeguata motivazione, non dovrebbero essere inseriti dati personali «eccedenti», «non pertinenti», «non indispensabili» (e, tantomeno, «vietati»). In caso contrario, occorre provvedere, comunque, al relativo oscuramento[49].

---

[48] Cfr. i provvedimenti del Garante citati *supra* in nota 5.

[49] In tal senso v. già il parere del Garante del 26 ottobre 1998, doc. *web* n. 30951; Provv.ti 17 aprile 2003, doc. *web* n. 1054640; 12 gennaio 2004, doc. *web* n. 1053395; 25 gennaio 2007, doc. *web* n. 1386836; 7 ottobre 2009, doc. *web* n. 1669620; 12 aprile 2012, doc. *web* n. 1896533; 1 agosto 2013, doc. *web* n. 2578588. Nella giurisprudenza di legittimità, in senso analogo, cfr. Cass. civ., sez. I, 20 luglio 2012, n. 12726, che ha confermato il Provvedimento del Garante del 9 dicembre 2003, doc. *web* n. 1054649; sulla necessità dell'osservanza del principio di proporzionalità (in occasione alla diffusione sull'albo pretorio di dati riferiti alle condizioni di salute dell'interessato) v. altresì Cass. civ., sez. I, 8 agosto 2013, n. 18980; Cass. civ., sez. I, 13 febbraio 2012, n. 2034.

Si pensi oltre al caso dei dati sensibili e giudiziari, a quelle informazioni delicate (come ad esempio agli atti adottati nel quadro dell'attività di assistenza e beneficenza, che comportano spesso la valutazione di circostanze e requisiti personali che attengono a situazioni di particolare disagio). Specie in tali casi –come già evidenziato con riferimento alla trasparenza (nel par. 2 della parte prima delle presenti Linee guida)– può risultare utile menzionare i predetti dati solo negli atti a disposizione negli uffici (richiamati quale presupposto della deliberazione e consultabili solo da interessati e controinteressati), oppure fare riferimento a delicate situazioni di disagio personale solo sulla base di espressioni di carattere più generale o, se del caso, di codici numerici [50].

Per esigenze di chiarezza espositiva, i limiti alla diffusione di dati personali sopradescritti sono sinteticamente rappresentati nello schema 1 riportato in calce al par. 2 della parte prima delle presenti Linee guida.

Rinvio allo schema 1 riportato in calce al par. 2 della parte prima delle *Linee guida*

2. Accorgimenti tecnici in relazione alle finalità perseguite

A fronte della messa a disposizione *online* di atti e documenti amministrativi contenenti dati personali per finalità di pubblicità dell'azione amministrativa, occorre assicurare forme corrette e proporzionate di conoscibilità di tali informazioni. A tal fine, è necessario impedire la loro indiscriminata e incondizionata reperibilità in Internet e garantire il rispetto dei principi di qualità ed esattezza dei dati, delimitando la durata della loro disponibilità *online*.

Le pubbliche amministrazioni sono tenute a individuare idonei accorgimenti tecnici per la protezione dei dati personali

2.a. Evitare l'indicizzazione nei motori di ricerca generalisti

Occorre evitare, ove possibile, la reperibilità dei dati personali da parte dei motori di ricerca esterni (ad es., *Google)*, stante il pericolo di decontestualizzazione del dato personale e la riorganizzazione delle informazioni restituite dal motore di ricerca secondo una logica di priorità di importanza del tutto sconosciuta, non conoscibile e non modificabile dall'utente.

Pertanto, è opportuno privilegiare funzionalità di ricerca interne al sito *web*, poiché in tal modo si assicurano accessi maggiormente selettivi e coerenti con le finalità di volta in volta sottese alla pubblicazione, garantendo, al contempo, la conoscibilità sui siti istituzionali delle informazioni che si intende mettere a disposizione[51].

Evitare l'indicizzazione nei motori di ricerca generalisti (ad es., *Google*)

[50] Cfr. par. 2 del citato Parere del Garante del 7 febbraio 2013, doc. *web*. n. 2243168.

[51] V. Provvedimento riguardante «*Motori di ricerca e provvedimenti di Autorità indipendenti: le misure necessarie a garantire il c.d. "diritto all'oblio"*» del 10 novembre 2004 (doc. *web* n. 1116068).

A tale scopo, alla luce dell'attuale meccanismo di funzionamento dei più diffusi motori di ricerca, in relazione ai dati personali di cui si intende limitare la diretta reperibilità *online* tramite tali strumenti, è possibile utilizzare regole di accesso convenzionali concordate nella comunità Internet.

Come già visto (cfr. parte prima, par. 8), si fa riferimento, a titolo esemplificativo, all'inserimento di *metatag noindex* e *noarchive* nelle intestazioni delle pagine *web* o alla codifica di regole di esclusione all'interno di uno specifico file di testo (il file *robots.txt*) posto sul *server* che ospita il sito *web* configurato in accordo al *Robot Exclusion Protocol* (avendo presente, comunque, come tali accorgimenti non sono immediatamente efficaci rispetto a contenuti già indicizzati da parte dei motori di ricerca Internet, la cui rimozione potrà avvenire secondo le modalità da ciascuno di questi previste)[52].

Come deindicizzare un documento

2.b. Tempi limitati e proporzionati di mantenimento della diffusione dei dati personali nel *web*

I soggetti pubblici sono tenuti ad assicurare il rispetto delle specifiche disposizioni di settore che individuano circoscritti periodi di tempo per la pubblicazione di atti e provvedimenti amministrativi contenenti dati personali, rendendoli accessibili sul proprio sito *web* solo per l'ambito temporale individuato dalle disposizioni normative di riferimento, anche per garantire il diritto all'oblio degli interessati (ad es., art. 124, del d. lgs. 18 agosto 2000, n. 267, riguardante la pubblicazione di deliberazioni sull'albo pretorio degli enti locali per quindici giorni consecutivi, su cui *infra* par. 3.a.).

È lecita la diffusione di dati personali solo entro il periodo di tempo previsto dalla normativa di riferimento

Nei casi in cui, invece, la disciplina di settore non stabilisce un limite temporale alla pubblicazione degli atti, vanno individuati –a cura delle amministrazioni pubbliche titolari del trattamento– congrui periodi di tempo entro i quali mantenerli *online*[53]. Tale lasso di tempo non può essere superiore al periodo ritenuto, caso per caso, necessario al raggiungimento degli scopi per i quali i dati personali stessi sono resi pubblici[54].

In mancanza di limiti temporali sanciti dalla disciplina di settore sono le pubbliche amministrazioni a dover individuare un termine

[52] Per approfondimenti, si consulti, a tal proposito, l'indirizzo *web*: *http://www.robotstxt.org/*.

[53] A titolo esemplificativo, è possibile utilizzare a questo scopo sistemi di *web publishing* e *Cms* (*Content management systems*) in grado di attribuire, anche mediante l'utilizzo di parole-chiave (metadati), un intervallo temporale di permanenza della documentazione all'interno del sito istituzionale, consentendone una sua agevole rimozione, anche in forma automatica. In assenza di meccanismi automatizzati di gestione del termine di scadenza della medesima documentazione, andrebbero inoltre previste procedure di verifica della validità temporale e del requisito di disponibilità al pubblico delle informazioni *ivi* contenute, da programmare con cadenza periodica o in seguito a un aggiornamento dell'informazione. Cfr. anche le *Linee guida per i siti web della PA* del Ministro per la pubblica amministrazione e l'innovazione redatte dall'allora DigitPa (ora AgID) ai sensi dell'art. 4 della Direttiva 8/2009 del Ministro per la pubblica amministrazione e l'innovazione del 26 novembre 2009 (in *http://www.funzionepubblica.gov.it/lazione-del-ministro/linee-guida-siti-web-pa/presentazione.aspx*).

[54] Cfr. Provv. Garante del 6 dicembre 2012, n. 384, doc. *web* n. 2223278.

Trascorsi i predetti periodi di tempo specificatamente individuati dalla normativa di settore o, in mancanza, dall'amministrazione, determinate notizie, documenti o sezioni del sito devono essere rimossi dal sito *web* oppure devono essere privati degli elementi identificativi degli interessati e delle altre informazioni che possano consentirne l'identificazione.

Resta salva la possibilità di consultare il documento completo, con i riferimenti in chiaro, tramite una rituale richiesta di accesso agli atti amministrativi presso gli uffici competenti, laddove esistano i presupposti previsti dalla l. 7 agosto 1990, n. 241.

2.c. Evitare la duplicazione massiva dei *file* contenenti dati personali

Le pubbliche amministrazioni devono predisporre opportune cautele per evitare la duplicazione massiva dei *file* contenenti dati personali

Devono essere adottate opportune cautele per ostacolare operazioni di duplicazione massiva dei *file* contenenti dati personali da parte degli utenti della rete, rinvenibili sui siti istituzionali delle amministrazioni pubbliche, mediante l'utilizzo di *software* o programmi automatici, al fine di ridurre il rischio di riproduzione e riutilizzo dei contenuti informativi in ambiti e contesti differenti.

A tale scopo si può fare ricorso ad accorgimenti consistenti, ad esempio, nell'uso di strumenti tecnologici in grado di riconoscere accessi che risultino anomali per la loro frequenza o perché realizzati tramite l'azione di strumenti automatizzati e non da persone: si può ricorrere in tal caso a sistemi di verifica '*captcha*'[55].

Gli accorgimenti che si intende utilizzare devono comunque essere conformi ai principi di fruibilità, di usabilità e di accessibilità dei siti istituzionali delle pubbliche amministrazioni, garantendo in particolare l'accessibilità alle informazioni riprodotte *online* anche alle persone disabili[56].

2.d. Dati personali esatti e aggiornati

Le pubbliche amministrazioni possono diffondere solo dati personali esatti e aggiornati

Per garantire la qualità dei dati personali trattati, le amministrazioni pubbliche, nel procedere alla divulgazione *online* nei casi previsti dalla disciplina di settore di dati e informazioni, sono tenute a mettere a disposizione soltanto dati personali esatti e aggiornati (art. 11, comma 1, lett. *c)*, del Codice).

---

[55] Sul punto, si rimanda alle precisazioni contenute *supra* in nota 31.

[56] V., al riguardo, art. 53 del CAD; v. anche d.P.R. 1 marzo 2005, n. 75 «*Regolamento di attuazione della l. 9 gennaio 2004, n. 4, per favorire l'accesso dei soggetti disabili agli strumenti informatici*» e d.m. 30 aprile 2008 «*Regole tecniche disciplinanti l'accessibilità agli strumenti didattici e formativi a favore degli alunni disabili*».

A tale fine, occorre adottare idonee misure per eliminare o ridurre il rischio di cancellazioni, modifiche, alterazioni o decontestualizzazioni delle informazioni e dei documenti resi disponibili tramite il proprio sito *web* istituzionale. Un utile accorgimento consiste, ad esempio, nell'indicazione, tra i dati di contesto riportati all'interno del contenuto informativo dei documenti[57], delle fonti attendibili per il reperimento dei medesimi documenti. Un ulteriore accorgimento la cui adozione potrà essere valutata dalle amministrazioni pubbliche titolari del trattamento, anche in relazione a specifiche categorie di documenti, è la sottoscrizione del documento pubblicato sul sito *web* con firma digitale[58] o altro accorgimento equivalente, in modo da garantirne l'autenticità e l'integrità.

Il rischio della decontestualizzazione è strettamente correlato alla possibilità che i contenuti informativi disponibili sul sito istituzionale sono accessibili mediante l'utilizzo di motori di ricerca esterni, oppure sono reperibili attraverso la consultazione di siti *web* dove sono ospitate copie dei medesimi contenuti informativi.

Pertanto, ogni *file* oggetto di pubblicazione sui siti *web* istituzionali, potendo essere letto in un altro ambito e in un momento successivo alla sua diffusione, dovrebbe prevedere l'inserimento dei "dati di contesto" (ad es., data di aggiornamento, periodo di validità, amministrazione, segnatura di protocollo o dell'albo).

3. Fattispecie esemplificative

3.a. Albo pretorio *online* degli enti locali

La disposizione di ordine generale sulla tenuta dell'albo pretorio negli enti locali è contenuta nel «*Testo unico delle leggi sull'ordinamento degli enti locali*», il quale sancisce che «*Tutte le deliberazioni del comune e della provincia sono pubblicate mediante affissione all'albo pretorio, nella sede dell'ente, per quindici giorni consecutivi, salvo specifiche disposizioni di legge*» e che «*Tutte le deliberazioni degli altri enti locali sono pubblicate mediante affissione all'albo pretorio del comune ove ha sede l'ente, per quindici giorni consecutivi, salvo specifiche disposizioni*» (art. 124, commi 1 e 2, del d. lgs. n. 267/2000).

Albo pretorio *online* degli enti locali: art. 124 del d. lgs. n. 267/2000

[57] V. la Delibera n. 105/2010 della CIVIT recante le «*Linee guida per la predisposizione del Programma triennale per la trasparenza e l'integrità (articolo 13, comma 6, lettera e, del decreto legislativo 27 ottobre 2009, n. 150)*», in *http://www.civit.it/wp-content/uploads/Delibera-n.105.20102.pdf*.

[58] Si rinvia, al riguardo, alle regole tecniche sulla firma digitale dettate da DigitPA (ora AgID) reperibili sul sito istituzionale dell'ente: *http://www.digitpa.gov.it/*.

Va aggiunto che, accanto a tale regola, nel corso del tempo si sono susseguite molteplici disposizioni di natura statale, regionale e locale che sanciscono a carico degli enti locali ulteriori obblighi di pubblicazione di atti e documenti nella bacheca dell'albo pretorio per periodi di tempo differenziati, producendo una frammentazione della disciplina in materia[59].

L'art. 32 della l. n. 69/2009

A seguito dell'entrata in vigore della riforma contenuta nella l. 18 giugno 2009, n. 69, recante «*Disposizioni per lo sviluppo economico, la semplificazione, la competitività nonché in materia di processo civile*», gli enti locali hanno provveduto all'istituzione dell'albo pretorio *online* al fine di adempiere agli obblighi di pubblicità legale dei propri atti.

La disciplina appena richiamata, infatti, senza abrogare le precedenti disposizioni in materia di tenuta dell'albo pretorio, ha sancito espressamente che «*a far data dal 1° gennaio 2010, gli obblighi di pubblicazione di atti e provvedimenti amministrativi aventi effetto di pubblicità legale si intendono assolti con la pubblicazione nei propri siti informatici da parte delle amministrazioni e degli enti pubblici obbligati*» e che «*a decorrere dal 1 gennaio 2011* [...] *le pubblicazioni effettuate in forma cartacea non hanno effetto di pubblicità legale*» (art. 32, commi 1 e 5). Dal 1° gennaio 2011, dunque, gli obblighi di pubblicità legale che gli enti locali assolvevano attraverso l'affissione all'albo pretorio sono sostituiti dalla pubblicazione della medesima documentazione nei rispettivi siti *web* istituzionali[60].

Lecita la diffusione di dati personali nell'albo pretorio *online* solo se prevista da una specifica norma di legge o di regolamento

Pertanto, l'amministrazione locale che ha intenzione di pubblicare sull'albo pretorio *online* un atto contenente dati personali (cfr. la definizione contenuta nell'art. 4, comma 1, lett. *b)*, del Codice) è tenuta a verificare, preliminarmente, per i dati comuni, l'esistenza di una norma di legge o di regolamento (ai sensi dell'art. 19, comma 3, del Codice) oppure, per i dati sensibili e giudiziari, di una norma di legge (ai sensi degli artt. 20, 21 e art.

[59] Cfr., a titolo esemplificativo, *ex pluribus*, l'affissione nell'albo del comune dell'avviso di deposito dell'atto da notificare a persona irreperibile in materia di accertamento delle imposte sui redditi (art. 60, comma 1, lett. *e)*, del d.P.R. 29 settembre 1973, n. 600); l'affissione all'albo comunale o provinciale della notizia dell'inadempienza alla diffida ad adempiere l'obbligo di pubblicità della situazione patrimoniale da parte degli amministratori locali (art. 14, comma 1, della legge 5 luglio 1982, n. 441); l'affissione nell'albo comunale da parte del segretario comunale dei dati relativi agli immobili e alle opere realizzati abusivamente, oggetto dei rapporti degli ufficiali e agenti di polizia giudiziaria e delle relative ordinanze di sospensione (art. 31, comma 7, del d.P.R. 6 giugno 2001, n. 380); l'affissione dell'avviso del sindaco contenente l'invito ai cittadini a presentare eventualmente ricorso contro le decisioni della Commissione elettorale comunale relative l'iscrizione nelle liste elettorali e dell'avviso del deposito presso la segreteria del comune dell'elenco revisionato degli elettori iscritti alle liste elettorali (art. 18, comma 1, e art. 32, comma 6, del d.P.R. 20 marzo 1967, n. 223); l'affissione all'albo pretorio del comune di una copia dell'elenco dei cittadini che, pur essendo compresi nelle liste elettorali, non avranno compiuto, nel primo giorno fissato per le elezioni, il diciottesimo anno di età redatta dalla commissione elettorale comunale (art. 33, comma 3, del d.P.R. n. 223/1967 cit.); l'affissione all'albo pretorio del comune dell'elenco dei giudici popolari di Corte di assise e di Corte di assise di appello (artt. 17 ss. della legge 10 aprile 1951, n. 287).

[60] Per una specifica delle caratteristiche dell'albo pretorio si rimanda alle indicazioni contenute nel *Vademecum* elaborato da DigitPA (ora AgID) del luglio 2011 intitolato «*Modalità di pubblicazione dei documenti nell'Albo online*», in *http://www.digitpa.gov.it/sites/default/files/VADEMECUM%202011_Modalita_pubblicazione_documenti_Albo_online.pdf*.

22, comma 11, del Codice) che le prescriva l'affissione di quell'atto all'albo pretorio.

Inoltre, anche alle pubblicazioni nell'albo pretorio *online* si applicano tutti i limiti previsti *supra* nel par. 1, della parte seconda, delle presenti Linee Guida (cfr. divieto di diffusione di dati idonei a rivelare lo stato di salute e cautele per gli altri dati sensibili e giudiziari; nonché divieto di diffondere dati personali non necessari, non pertinenti o eccedenti).

Il rispetto del principio di pertinenza e non eccedenza e le cautele per i dati sensibili e giudiziari: rinvio al par. 1 della parte seconda

Con specifico riferimento, inoltre, ai dati sensibili e giudiziari, gli enti locali devono agire nel rispetto del proprio regolamento sul trattamento dei dati sensibili e giudiziari adottato in conformità agli schemi tipo Anci, Upi e Uncem su cui il Garante ha già espresso parere favorevole, rispettivamente, il 21 settembre 2005, il 7 settembre 2005 e il 19 ottobre 2005 (v. doc. *web* n. 1174532, doc. *web* n. 1175684, doc. *web* n. 1182195).

Una volta trascorso il periodo temporale previsto dalle singole discipline per la pubblicazione degli atti e documenti nell'albo pretorio, gli enti locali non possono continuare a diffondere i dati personali in essi contenuti. In caso contrario, si determinerebbe, per il periodo eccedente la durata prevista dalla normativa di riferimento, una diffusione dei dati personali illecita perché non supportata da idonei presupposti normativi (art. 19, comma 3, del Codice). Ciò, salvo che gli stessi atti e documenti non debbano essere pubblicati in ottemperanza agli obblighi in materia di trasparenza (cfr. parte prima delle presenti Linee guida).

Lecita la diffusione dei dati personali solo entro il limite temporale previsto dalla normativa di riferimento

A tal proposito, ad esempio, la permanenza nel *web* di dati personali contenuti nelle deliberazioni degli enti locali oltre il termine di quindici giorni, previsto dall'art. 124 del citato d. lgs. n. 267/2000, può integrare una violazione del suddetto art. 19, comma 3, del Codice, laddove non esista un diverso parametro legislativo o regolamentare che preveda la relativa diffusione[61].

Nell'ipotesi in cui, invece, la normativa di riferimento non indichi la durata temporale dell'affissione all'albo, l'amministrazione deve comunque individuare un congruo periodo di tempo –non superiore al periodo ritenuto, caso per caso, necessario al raggiungimento dello scopo per il quale l'atto è stato adottato e i dati stessi sono stati resi pubblici– entro il quale i dati personali devono rimanere disponibili. Per i motivi esposti nell'«*Introduzione*» e nel par. 1 della parte prima delle presenti Linee guida alle pubblicazioni nell'albo pretorio *online* non si applica l'arco temporale dei cinque anni previsto per la pubblicità di dati e informazioni sui siti *web* istituzionali per finalità di trasparenza di cui all'art. 8 del d. lgs. n. 33/2013.

Archivi degli atti e della normativa degli enti locali

Pertanto –una volta trascorso il periodo di pubblicazione previsto dalle singole discipline di riferimento oppure, in mancanza, decorso il periodo di tempo individuato dalla stessa amministrazione– se gli enti locali

[61] Cfr. Provv. Garante del 23 febbraio 2012, doc. *web* n. 1876679.

vogliono continuare a mantenere nel proprio sito *web* istituzionale gli atti e i documenti pubblicati, ad esempio nelle sezioni dedicate agli archivi degli atti e/o della normativa dell'ente, devono apportare gli opportuni accorgimenti per la tutela dei dati personali. In tali casi, quindi, è necessario provvedere a oscurare nella documentazione pubblicata i dati e le informazioni idonei a identificare, anche in maniera indiretta, i soggetti interessati.

Evitare l'indicizzazione nei motori di ricerca generalisti dei dati personali contenuti negli atti pubblicati nell'albo pretorio *online*

Poiché, inoltre, la finalità perseguita mediante gli obblighi di pubblicazione nell'albo pretorio *online* riguarda atti e provvedimenti concernenti questioni rilevanti essenzialmente nell'ambito della collettività locale di riferimento, risulta sproporzionato, rispetto alla finalità di pubblicità, consentire l'indiscriminata reperibilità in rete dei dati personali contenuti in atti e provvedimenti amministrativi tramite i comuni motori di ricerca generalisti (ad es., *Google*). Pertanto, si consiglia alle amministrazioni pubbliche responsabili dell'inserzione degli atti nell'albo pretorio *online*, di adottare gli opportuni accorgimenti tecnici per evitare l'indicizzazione nei motori di ricerca generalisti della documentazione contenente dati personali e pubblicata sull'albo pretorio *online* dei siti istituzionali degli enti locali (sulle tecniche per deindicizzare si rinvia alle indicazioni contenute *supra* nel par. 2.a. della presente parte seconda).

3.b. Graduatorie

Resta fermo il regime di pubblicità previsto dalle singole norme di settore

Con riguardo alla pubblicità degli esiti delle prove concorsuali e delle graduatorie finali –nonché, nei casi (e con le modalità) previsti, dei risultati di prove intermedie– di concorsi e selezioni pubbliche e di altri procedimenti che prevedono la formazione di graduatorie, restano salve le normative di settore che ne regolano tempi e forme di pubblicità (ad es., affissione presso la sede dell'ente pubblico, pubblicazione nel bollettino dell'amministrazione o, per gli enti locali, all'albo pretorio)[62]. Tale regime di conoscibilità, come già rilevato in passato dal Garante[63], assolve alla funzione di rendere pubbliche le decisioni adottate dalla commissione esaminatrice e/o dall'ente pubblico procedente, anche al fine di consentire agli

[62] V. *Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico* del 14 giugno 2007, cit., punto 6.1. Cfr. art. 15, d.P.R. 9 maggio 1994, n. 487, in particolare commi 5, 6 e 6 *bis* e, più in generale, sulla pubblicità delle procedure di reclutamento del personale delle pubbliche amministrazioni, art. 35, comma 3, d. lgs. 30 marzo 2001, n. 165.

[63] Cfr. parr. 6.B.1 e 6.B.2, delle *Linee guida in materia di trattamento di dati personali contenuti anche in atti e documenti amministrativi, effettuato da soggetti pubblici per finalità di pubblicazione e diffusione sul web*, 2 marzo 2011 (già par. 6.1 delle *Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico*, 14 giugno 2007 e par. 10.2 delle *Linee guida in materia di trattamento di dati personali per finalità di pubblicazione e diffusione di atti e documenti di enti locali*, doc. *web* n. 1407101).

interessati l'attivazione delle forme di tutela dei propri diritti e di controllo della legittimità delle procedure concorsuali o selettive.

Anche a questo riguardo devono essere diffusi i soli dati pertinenti e non eccedenti riferiti agli interessati[64]. Non possono quindi formare oggetto di pubblicazione dati concernenti i recapiti degli interessati (si pensi alle utenze di telefonia fissa o mobile, l'indirizzo di residenza o di posta elettronica[65], il codice fiscale, l'indicatore Isee, il numero di figli disabili, i risultati di test psicoattitudinali o i titoli di studio), né quelli concernenti le condizioni di salute degli interessati (cfr. art. 22, comma 8, del Codice), ivi compresi i riferimenti a condizioni di invalidità, disabilità o handicap fisici e/o psichici[66].

Divieto di diffusione di dati concernenti la condizione di salute e legittimità della sola diffusione di dati pertinenti e non eccedenti

Come già rilevato in passato dal Garante[67], al fine di agevolare le modalità di consultazione delle graduatorie oggetto di pubblicazione in conformità alla disciplina di settore (per finalità diverse dalla trasparenza), le stesse possono altresì essere messe a disposizione degli interessati in aree ad accesso selezionato dei siti *web* istituzionali consentendo la consultazione degli esiti delle prove o del procedimento ai soli partecipanti alla procedura concorsuale o selettiva mediante l'attribuzione agli stessi di credenziali di autenticazione (ad es., *username* o *password*, numero di protocollo o altri estremi identificativi forniti dall'ente agli aventi diritto, oppure mediante utilizzo di dispositivi di autenticazione, quali la carta nazionale dei servizi).

---

[64] Cfr. Provv. 6 dicembre 2012, n. 384, doc. *web* n. 2223278.

[65] *Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico*, del 14 giugno 2007, cit., par. 6.1; Provv.ti 6 giugno 2013, n. 274, doc. *web* n. 2535862; del 6 giugno 2013, n. 275, doc. *web* n. 2536184; 6 giugno 2013, n. 276, doc. *web* n. 2536409.

[66] Cfr. già *Linee guida in materia di trattamento di dati personali contenuti anche in atti e documenti amministrativi, effettuato da soggetti pubblici per finalità di pubblicazione e diffusione sul web* (pubblicato in G.U. n. 64 del 19 marzo 2011, e doc. *web* n. 1793203; v. altresì, per fattispecie individuali, Provv.ti del 6 giugno 2013, n. 277, doc. *web* n. 2554965; 22 novembre 2012, doc. *web* n. 2194472; 29 novembre 2012, doc. *web* n. 2192671; 7 ottobre 2009, doc. web n. 1664456; 17 settembre 2009, doc. *web* n. 1658335; 25 giugno 2009, doc. *web* n. 1640102; 8 maggio 2008, doc. web n. 1521716; 18 gennaio 2007, doc. *web* n. 1382026; 27 febbraio 2002, doc. *web* n. 1063639.

[67] *Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico*, del 14 giugno 2007, cit., par. 6.1.