

AL33

POLICY - RAPPORTO TRA LA NORMATIVA COMUNITARIA E NAZIONALE SULLA PROTEZIONE DEI DATI PERSONALI E LA NORMATIVA NAZIONALE SULLA TRASPARENZA DELL'ATTIVITA' DI UNA PUBBLICA AMMINISTRAZIONE

AZIENDA SOCIO-SANITARIA TERRITORIALE RHODENSE, (P. IVA: 09323530965) (infra "ASST RHODENSE"), in persona del suo legale rappresentante pro tempore, con sede legale in Garbagnate Milanese (MI), viale Forlanini, 95, intende descrivere – in linea generale, e in un'ottica di "privacy by design" e di "privacy by default" ex art. 25¹ e Considerando n. 78)² del Regolamento UE n. 2016/679 (GDPR) – i principi tesi a regolamentare e a bilanciare il rapporto tra la normativa comunitaria e nazionale sulla protezione dei dati personali e la normativa nazionale volta a fornire trasparenza sull'attività ed organizzazione di una Pubblica Amministrazione (PA).

1. Principale quadro giuridico/normativo (di primo e di secondo livello) di riferimento:

- a. Art. 4 n. 1)³ del GDPR;
- b. Art. 6 paragrafo 1) lettere c) ed e)⁴ del GDPR;
- c. Art. 6 paragrafo 3)⁵ del GDPR;

¹ Art. 25 del GDPR: "Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità di trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate [...] volte ad attuare in modo efficace i principi di protezione dei dati [...]. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica".

² Considerando n. 78) del GDPR: "La tutela dei diritti e delle libertà delle persone fisiche relativamente al trattamento dei dati personali richiede l'adozione di misure tecniche e organizzative adeguate per garantire il rispetto delle disposizioni del presente regolamento. Al fine di poter dimostrare la conformità con il presente regolamento, il titolare del trattamento dovrebbe adottare politiche interne e attuare misure che soddisfino in particolare i principi della protezione dei dati fin dalla progettazione e della protezione dei dati di default. Tali misure potrebbero, tra l'altro, nel ridurre al minimo il trattamento dei dati personali, pseudonimizzare i dati personali il più presto possibile, offrire trasparenza per quanto riguarda le funzioni e il trattamento di dati personali, consentire all'interessato di controllare il trattamento dei dati e consentire al titolare del trattamento di creare e di migliorare caratteristiche di sicurezza. In fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, a far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati...".

³ Art. 4 n. 1) del GDPR: "dato personale": "qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale".

⁴ Art. 6 paragrafo 1) lettere c) ed e): "1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: c) il trattamento è necessario per adempiere a un obbligo legale al quale è soggetto il titolare del trattamento; [...] e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento".

⁵ Art. 6 paragrafo 3) del GDPR: "La base su cui si fonda il trattamento dei dati di cui al paragrafo 1, lettere c) ed e), deve essere stabilita: a) dal diritto dell'Unione; o b) dal diritto dello Stato membro cui è soggetto il titolare del trattamento. La finalità del trattamento è determinata in tale base giuridica o, per quanto riguarda il trattamento di cui al paragrafo 1, lettera e), è necessaria per l'esecuzione di un compito svolto nel pubblico interesse o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento. Tale base giuridica potrebbe contenere disposizioni specifiche per adeguare l'applicazione delle norme al presente regolamento, tra cui: le condizioni generali relative alla liceità del trattamento da parte del titolare del trattamento; le tipologie di dati oggetto del trattamento; gli interessati; i soggetti cui possono essere comunicati i dati personali e le finalità per cui sono comunicati; le limitazioni della finalità; i periodi di conservazione e le operazioni e procedure di trattamento, comprese le misure atte a garantire un trattamento lecito e corretto, quali quelle per altre specifiche situazioni di trattamento di cui al

- d. Art. 9 paragrafo 1)⁶, e paragrafo 2) lettera g)⁷ del GDPR;
- e. Art. 10⁸ del GDPR;
- f. Art. 2 ter⁹ del novellato D.lgs. n. 196/2003 (Codice Privacy);
- g. Art. 2 sexies commi 1) e 2)¹⁰ del Codice Privacy;
- h. Art. 2 septies comma 8)¹¹ del Codice Privacy;
- i. Corte Costituzionale, sentenza n. 20 del 21.2.2019;
- j. Corte di Giustizia dell'Unione Europea (CGUE), sentenza del 20.5.2003¹²;
- k. CGUE, sentenza del 9.11.2010¹³;
- l. D.Lgs. n. 33 del 14.3.2013, e s.m.i.;
- m. D.Lgs. n. 82 del 7.3.2005 (CAD: Codice dell'Amministrazione Digitale);
- n. ANAC, Delibera n. 1310 del 28.12.2016 ("Prime linee guida recanti indicazioni sull'attuazione degli obblighi di pubblicità, trasparenza e diffusione di informazioni contenute nel D.Lgs. 33/2013 come modificato dal D.Lgs. 97/2016");
- o. Garante Privacy italiano, Deliberazione "Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico" del 14.6.2007 (doc. web n. 1417809);

capo IX. Il diritto dell'Unione o degli Stati membri persegue un obiettivo di interesse pubblico ed è proporzionato all'obiettivo legittimo perseguito".

⁶ Art. 9 paragrafo 1) del GDPR: "E' vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona".

⁷ Art. 9 paragrafo 2) lettera g) del GDPR: "2. Il paragrafo 1 non si applica se si verifica uno dei seguenti casi: g) il trattamento è necessario per motivi di interesse pubblico sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato".

⁸ Art. 10 del GDPR: "Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica".

⁹ Art. 2 ter del Codice Privacy: "1. La base giuridica prevista dall'articolo 6, paragrafo 3, lettera b), del regolamento è costituita esclusivamente da una norma di legge o, nei casi previsti dalla legge, di regolamento. 2. La comunicazione fra titolari che effettuano trattamenti di dati personali, diversi da quelli ricompresi nelle particolari categorie di cui all'articolo 9 del Regolamento e di quelli relativi a condanne penali e reati di cui all'articolo 10 del Regolamento, per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri è ammessa se prevista ai sensi del comma 1. In mancanza di tale norma, la comunicazione è ammessa quando è comunque necessaria per lo svolgimento di compiti di interesse pubblico e lo svolgimento di funzioni istituzionali e può essere iniziata se è decorso il termine di quarantacinque giorni dalla relativa comunicazione al Garante, senza che lo stesso abbia adottato una diversa determinazione delle misure da adottarsi a garanzia degli interessati. 3. La diffusione e la comunicazione di dati personali, trattati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, a soggetti che intendono trattarli per altre finalità sono ammesse unicamente se previste ai sensi del comma 1. 4. Si intende per: a) "comunicazione", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate, ai sensi dell'articolo 2-quaterdecies, al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione; b) "diffusione", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione".

¹⁰ Art. 2 sexies commi 1) e 2) del Codice Privacy: "1. I trattamenti delle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, del Regolamento, necessari per motivi di interesse pubblico rilevante ai sensi del paragrafo 2, lettera g), del medesimo articolo, sono ammessi qualora siano previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o, nei casi previsti dalla legge, di regolamento che specificino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato. 2. Fermo quanto previsto dal comma 1, si considera rilevante l'interesse pubblico relativo a trattamenti effettuati da soggetti che svolgono compiti di interesse pubblico o connessi all'esercizio di pubblici poteri nelle seguenti materie: [...]"

¹¹ Art. 2 septies comma 8) del Codice Privacy: "I dati personali di cui al comma 1 [n.d.r.: i dati genetici, biometrici e relativi alla salute] non possono essere diffusi".

¹² Ha riunito i seguenti procedimenti: C-465/00; C-138/01; C-139/01.

¹³ Ha riunito i seguenti procedimenti: C-92/09; C-93/09.

- p. Garante Privacy italiano, Provvedimento “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” del 15.5.2014 (doc. web n. 3134436)¹⁴;
- q. Garante Privacy italiano, Provvedimento n. 377 del 25.6.2015 (doc. web n. 4166711).

2. Scopo.

La presente Policy ha lo scopo di definire un quadro unitario di misure e di accorgimenti volti ad individuare opportune cautele che un soggetto pubblico è tenuto ad applicare nel caso in cui effettua un’attività di diffusione di dati personali all’interno di un proprio sito internet istituzionale per finalità di trasparenza. A tal riguardo, occorre precisare, in via preliminare, che le esigenze di trasparenza devono essere temperate con i diritti e le libertà fondamentali, con particolare riferimento alla riservatezza, alla dignità ed identità dell’interessato e, di conseguenza, al diritto alla protezione dei dati personali.

AMMINISTRAZIONE TRASPARENTE¹⁵.

3. Principi e limiti.

Il D.Lgs. n. 33/2013 e s.m.i. ha disciplinato, in maniera organica, i casi di pubblicità per finalità di trasparenza¹⁶, mediante la pubblicazione¹⁷ di dati, informazioni, atti e documenti sui siti web istituzionali dei soggetti obbligati.

I principi e la disciplina di protezione dei dati personali – così come, peraltro, previsto anche dall’art. 1 comma 2) del D.Lgs. n. 33/2013 – devono essere rispettati anche nell’attività di pubblicazione di dati sul web per finalità di trasparenza. Nello specifico, la diffusione ex art. 2 ter comma 4) lettera b) del Codice Privacy dei dati personali da parte di un soggetto pubblico è ammessa unicamente quando la stessa è prevista da una specifica norma di legge o di regolamento: pertanto, in relazione all’operazione di diffusione, occorre che la pubblica amministrazione, 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, verifichi che la normativa in materia di trasparenza preveda tale obbligo.

Laddove la PA 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.

Il soggetto pubblico, infatti, in conformità ai principi di protezione dei dati, è tenuto a ridurre al minimo l’utilizzazione dei dati personali 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 (cfr. principio di “minimizzazione” ex art. 5 paragrafo 1) lettera c) del GDPR¹⁸).

¹⁴ Queste linee guida sono attualmente in corso di aggiornamento, sebbene ancora attuali nella loro parte sostanziale (cfr. dichiarazione, sul punto, espressa dal Garante Privacy italiano nel Provvedimento n. 296 del 22.7.2021, pag. 3 (doc. web n. 9697724).

¹⁵ Cfr. CGUE, sentenza del 9.11.2010, punto 68) (“Occorre ricordare che il principio di trasparenza è sancito dagli artt. 1 TUE e 10 TUE nonché dall’art. 15 TFUE. Esso consente una migliore partecipazione dei cittadini al processo decisionale e garantisce una maggiore legittimità, efficienza e responsabilità dell’amministrazione nei confronti dei cittadini in un sistema democratico”), punto 76) (“Quanto alla necessità della misura, si deve rammentare che l’obiettivo della pubblicazione in questione non può essere perseguito senza tener conto del fatto che esso deve essere conciliato con i diritti fondamentali sanciti dagli artt. 7 e 8 della Carta”), punto 77) (“...le deroghe e le limitazioni alla protezione dei dati personali devono operare entro i limiti dello stretto necessario”), e punto 85) (“...Si deve ricordare che le istituzioni, prima di divulgare informazioni riguardanti una persona fisica, devono soppesare l’interesse dell’Unione a garantire la trasparenza delle proprie azioni con la lesione dei diritti riconosciuti dagli artt. 7 e 8 della Carta. Orbene, non può riconoscersi alcuna automatica prevalenza dell’obiettivo di trasparenza sul diritto alla protezione dei dati personali...”).

¹⁶ Cfr. D.Lgs. n. 33 del 14.3.2013, artt. 1 comma 1) (“La trasparenza è intesa come accessibilità totale dei dati e documenti detenuti dalle pubbliche amministrazioni, allo scopo di tutelare i diritti dei cittadini, promuovere la partecipazione degli interessati all’attività amministrativa e favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull’utilizzo delle risorse pubbliche”).

¹⁷ Cfr. D.Lgs. n. 33 del 14.3.2013, art. 2 comma 2): “Ai fini del presente decreto, per pubblicazione si intende la pubblicazione, in conformità alle specifiche e alle regole tecniche di cui all’allegato A, nei siti istituzionali delle pubbliche amministrazioni dei documenti, delle informazioni e dei dati concernenti l’organizzazione e l’attività delle pubbliche amministrazioni, cui corrisponde il diritto di chiunque di accedere ai siti direttamente ed immediatamente, senza autenticazione ed identificazione”.

¹⁸ Cfr. Garante Privacy italiano, Provvedimento n. 73 del 25.2.2021 (doc. web n. 9574764): “Ciò è d’altronde confermato anche dal sistema di protezione dei dati personali contenuto nel RGPD, alla luce del quale è infatti previsto che il titolare del trattamento debba mettere “in atto misure tecniche ed organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità di trattamento (“privacy by design”) e debba essere “in grado di dimostrare” - alla luce del principio di “responsabilizzazione” (“accountability”) - di averlo fatto (artt. 5, par. 2; 24 e 25, par. 2, RGPD)”.

E' 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: 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.

Invece, è sempre vietata, ai sensi dell'art. 2 septies comma 8) del Codice Privacy, la diffusione dei dati genetici ex art. 4 n. 13)¹⁹ del GDPR, dati biometrici²⁰ ex art. 4 n. 14)²¹ del GDPR e dati personali relativi alla salute²² ex art. 4 n. 15)²³ e Considerando n. 35) del GDPR: 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.

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, oppure nel caso dei dati personali cd. giudiziari ex art. 10 del GDPR.

I descritti dati personali cd. particolari ovvero i dati personali cd. giudiziari sono, infatti, protetti da un quadro di garanzie particolarmente stringente che prevede la possibilità, per un soggetto pubblico, 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 un rilevante interesse pubblico, come, appunto, quello di trasparenza.

4. Pubblicazione di dati personali ulteriori.

La PA non è libera di diffondere dati personali ulteriori, non individuati dal D.Lgs. n. 33/2013 o da altra specifica norma di legge o di regolamento. L'eventuale pubblicazione di dati, informazioni e documenti, che non si ha l'obbligo di pubblicare, è legittimata soltanto procedendo all'anonimizzazione dei dati personali ivi presenti.

In proposito, giova evidenziare che la (diffusa) prassi 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 nei 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 il soggetto interessato (si pensi, ad esempio, alle informazioni relative alla residenza ovvero quando un soggetto possiede un doppio nome e/o cognome)²⁴.

5. Qualità delle informazioni.

¹⁹ Art. 4 n. 13) del GDPR: "dati genetici": "i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione".

²⁰ Art. 4 n. 14) del GDPR: "dati biometrici": "i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici".

²¹ Considerando n. 35) del GDPR: "Nei dati personali relativi alla salute dovrebbero rientrare tutti i dati riguardanti lo stato di salute dell'interessato che rivelino informazioni connesse allo stato di salute fisica o mentale passata, presente o futura dello stesso. Questi comprendono informazioni sulla persona fisica raccolte nel corso della sua registrazione al fine di ricevere servizi di assistenza sanitaria o della relativa prestazione di cui alla direttiva 2011/24/UE del Parlamento europeo e del Consiglio; un numero, un simbolo o un elemento specifico attribuito a una persona fisica per identificarla in modo univoco a fini sanitari; le informazioni risultanti da esami e controlli effettuati su una parte del corpo o una sostanza organica, compresi i dati genetici e i campioni biologici; e qualsiasi informazione riguardante, ad esempio, una malattia, una disabilità, il rischio di malattie, l'anamnesi medica, i trattamenti clinici o lo stato fisiologico o biomedico dell'interessato, indipendentemente dalla fonte, quale, ad esempio, un medico o altro operatore sanitario, un ospedale, un dispositivo medico o un test diagnostico in vitro".

²² Cfr. Garante Privacy, Provvedimento n. 68 del 25.2.2021 (doc. web n. 9567429): "Per quanto attiene alla circostanza che la determinazione in questione menzionasse solo l'assenza per malattia del reclamante, senza l'indicazione della diagnosi, si rileva che, secondo il costante orientamento del Garante, nella nozione di dato personale relativo alla salute "può rientrare anche una informazione relativa all'assenza dal servizio per malattia, indipendentemente dalla circostanza che sia contestualmente indicata esplicitamente la diagnosi" (cfr. Garante Privacy italiano, provvedimento n. 23 del 14.6.2007, n. 269 del 7.5.2015).

²³ Art. 4 n. 15) del GDPR: "dati relativi alla salute": "i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute".

²⁴ Per rendere effettivamente "anonimi" 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.

L'art. 6 del D.Lgs. n. 33/2013 sancisce espressamente 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".

Tale previsione deve essere interpretata anche alla luce dei principi in materia di protezione dei dati personali, per cui la PA è tenuta a mettere a disposizione soltanto i dati personali esatti ed aggiornati (cfr. art. 5 paragrafo 1) lettera d) del GDPR).

6. Durata degli obblighi di pubblicazione.

L'art. 8 comma 3) del D.Lgs. n. 33/2013 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.

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 o locale" (cfr. art. 14 comma 2) del D.Lgs. n. 33/2013) e "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 (cfr. art. 15 comma 4) del D.Lgs. n. 33/2013).

7. Pubblicazione di corrispettivi e di compensi.

La disciplina in materia di trasparenza prevede che le informazioni concernenti l'entità dei corrispettivi e dei 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 di collaborazione o consulenza (cfr. art. 15 del D.Lgs. n. 33/2013) nonché i dipendenti pubblici cui siano stati conferiti o autorizzati incarichi (cfr. art. 18 del D.Lgs. n. 33/2013).

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, come pure l'indicazione di altri dati eccedenti riferiti a percettori di somme (es. recapiti individuali e coordinate bancarie utilizzate per effettuare i pagamenti).

8. Pubblicazione degli atti di concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici e dell'elenco dei soggetti beneficiari.

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...", mentre il comma 3) del medesimo articolo aggiunge che tale pubblicazione "costituisce condizione legale di efficacia dei provvedimenti che dispongono concessioni e attribuzioni di importo complessivo superiore a mille euro nel corso dell'anno solare al medesimo beneficiario".

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. Infatti, non possono 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: (a) di importo complessivo inferiore a mille euro nel corso dell'anno solare a favore del medesimo beneficiario; (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" (cfr. art. 26 comma 4) del D.Lgs. n. 33/2013); (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" (cfr. art. 26 comma 4) del D.Lgs. n. 33/2013).

Si tratta di un divieto funzionale alla tutela della dignità, dei diritti e delle libertà fondamentali dell'interessato, 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 personale²⁵.

Nel rispetto dei principi cardine del GDPR, 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

²⁵ Cfr. Garante Privacy italiano, Provvedimento n. 296 del 22.7.2021 (doc. web n. 9697724).

economici (codice IBAN), la ripartizione degli assegnatari secondo le fasce Isee, l'indicazione di analitiche situazioni reddituali, di condizioni di bisogno o di peculiari situazioni abitative.

9. Bandi di concorso.

L'art. 19 del D.Lgs. n. 33/2013 dispone espressamente che: "1. Fermi restando gli altri obblighi di pubblicità legale, le pubbliche amministrazioni pubblicano i bandi di concorso per il reclutamento, a qualsiasi titolo, di personale presso l'amministrazione, nonché i criteri di valutazione della Commissione e le tracce delle prove scritte. 2. Le pubbliche amministrazioni pubblicano e tengono costantemente aggiornato l'elenco dei bandi di concorso".

Sul punto, il Garante Privacy italiano ha ricordato che "In relazione alla pubblicità degli esiti delle prove concorsuali e delle graduatorie finali di concorsi e selezioni pubbliche e di altri procedimenti che prevedono la formazione di graduatorie, questa Autorità fin dal 2014 ha evidenziato che sussistono "normative di settore che ne regolano tempi e forme di pubblicità (es. affissione presso la sede dell'ente pubblico, pubblicazione nel bollettino dell'amministrazione o, per gli enti locali, all'albo pretorio). Tale regime di conoscibilità, come già rilevato in passato dal Garante, assolve alla funzione di rendere pubbliche le decisioni adottate dalla commissione esaminatrice e/o dall'ente pubblico procedente, anche al fine di consentire agli 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. Non possono quindi formare oggetto di pubblicazione dati concernenti i recapiti degli interessati (quali fra l'altro) l'indirizzo di residenza o di posta elettronica..." (cfr. Garante Privacy italiano, Provvedimento n. 237 del 10.6.2021)²⁶.

10. Pubblicazione del curriculum vitae.

In vari passaggi, il D.Lgs. n. 33/2013 precisa alla PA l'onere di rendere visibile al pubblico, rispetto a taluni soggetti (es. incarico di collaborazione/consulenza), informazioni personali concernenti il percorso di studi e le esperienze professionali rilevanti, nella forma del curriculum vitae (CV), anche in formato europeo.

A tal riguardo, il Garante Privacy ha precisato che il riferimento del Legislatore all'obbligo di pubblicazione del CV non può, tuttavia, comportare la diffusione di tutti i contenuti astrattamente previsti all'interno del CV (in formato europeo), ma solo di quelli pertinenti rispetto alla finalità di trasparenza perseguita. Infatti, prima di pubblicare, sul sito istituzionale, un CV, la PA, in qualità di Titolare del trattamento, deve operare un'attenta selezione dei dati in essi contenuti, se del caso predisponendo modelli omogenei e impartendo opportune istruzioni ai soggetti interessati.

In tale prospettiva, sono pertinenti le informazioni riguardanti i titoli di studio e professionali, le esperienze lavorative, nonché ulteriori informazioni di carattere professionale (es. conoscenze linguistiche/tecnologiche); all'opposto, non possono, invece, formare oggetto di pubblicazione dati eccedenti, quali, ad esempio, i recapiti personali, il codice fiscale ovvero la firma autografa.

Garbagnate Milanese (MI), lì 16.6.2022 (data di ultimo aggiornamento).

AZIENDA SOCIO-SANITARIA TERRITORIALE RHODENSE

(in persona del suo legale rappresentante pro tempore)

²⁶ Cfr. Garante Privacy italiano, Provvedimento n. 154 del 3.9.2020 (doc. web n. 9468523): "Al riguardo, si evidenzia che la disciplina di settore applicabile al caso di specie contenuta nell'art. 15, comma 6-bis, del DPR 9/5/1994, n. 487 (Regolamento recante norme sull'accesso agli impieghi nelle pubbliche amministrazioni e le modalità di svolgimento dei concorsi, dei concorsi unici e delle altre forme di assunzione nei pubblici impieghi), dispone, in primo luogo, che siano pubblicate "nell'albo pretorio del relativo ente" le sole graduatorie definitive dei vincitori di concorso presso gli enti territoriali e non anche, come nella questione sottoposta all'attenzione del Garante, gli esiti delle prove intermedie o dei dati personali dei concorrenti non vincitori, non ammessi o che si sono ritirati".