UNIVERSITÀ DEL SALENTO

Ciclo di incontri seminariali
Adeguamento degli Atenei al GDPR e centralità della persona

Prof. Francesco Giacomo Viterbo
francesco.viterbo@unisalento.it

Lecce, 27 novembre 2020

GIORNATE DELLA TRASPARENZA 2020

Ciclo di seminari per la cultura della legalità, promossi nell'ambito del Piano Triennale di Prevenzione della Corruzione dell'Università del Salento 2020-2022

27 NOVEMBRE 2020 ORE 11.00

Adeguamento degli Atenei al Regolamento Europeo 2016/679 (GDPR) e centralità della persona

collegamento MS Teams: https://bit.ly/trasparenza1

Francesco Giacomo Viterbo
Delegato del Rettore alla Privacy, docente del Dipartimento di Scienze Giuridiche, Università del Salento

Introduce: *Gabriella Gianfrate*
Dirigente Ripartizione Tecnica e Tecnologica dell'Università del Salento

Prof. Francesco Giacomo Viterbo
francesco.viterbo@unisalento.it

Lecce, 27 novembre 2020

Il Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati e che abroga la Direttiva 95/46/CE (General Data Protection Regulation – GDPR) si inserisce nella

"**Strategia per il mercato unico digitale in Europa**" proposta dalla Commissione europea con la **Comunicazione del 6 maggio 2015** cui segue la **Comunicazione del 10 maggio 2017**

«Il mercato unico digitale è un mercato in cui è garantita la libera circolazione delle merci, delle persone, dei servizi e dei capitali e in cui, quale che sia la loro cittadinanza o nazionalità o il luogo di residenza, persone e imprese non incontrano ostacoli all'accesso e all'esercizio delle attività online in condizioni di concorrenza leale e potendo contare su un livello elevato di protezione dei consumatori e dei dati personali.»

Obiettivi:

- Aumentare fiducia e sicurezza nei servizi digitali e nella gestione dei dati personali: Le minacce informatiche costituiscono un problema che ignora le frontiere e che ha conseguenze negative per la nostra economia, i diritti fondamentali dei cittadini e la società nel suo complesso. Il numero sempre maggiore di reati (ad es., intercettazione dei dati, frode sui pagamenti online, usurpazione di identità, furto di segreti commerciali) determina pesanti perdite economiche. Spesso questi reati si traducono in interruzioni del servizio o in violazioni dei diritti fondamentali, e ne risulta minata la fiducia dei cittadini nelle attività online. Per quanto riguarda i dati personali e la difesa della vita privata, l'UE si è impegnata a rispettare i più elevati parametri di protezione garantiti dagli articoli 7 e 8 della Carta dei diritti fondamentali. Il regolamento generale sulla protezione dei dati rafforzerà la fiducia nei servizi digitali, perché dovrebbe tutelare le persone fisiche con riguardo al trattamento dei dati personali da parte di qualsiasi impresa che offra servizi sul mercato europeo.

- *Garantire la protezione della vita privata e dei dati personali in Internet*

Il **Regolamento (UE) 2016/679 - Regolamento generale sulla protezione dei dati (GDPR)** è uno strumento essenziale per salvaguardare il diritto fondamentale delle persone alla protezione dei dati personali nell'era digitale. Esso offre alle imprese regole semplificate, crea nuove opportunità imprenditoriali e incoraggia l'innovazione. Si applica a decorrere dal 25 maggio 2018.

⬇

Anche il sistema universitario si colloca nell'era digitale

Gli Atenei:
- erogano servizi digitali (es. DAD)

Prof. Francesco Giacomo Viterbo
francesco.viterbo@unisalento.it

Lecce, 27 novembre 2020

- gestiscono banche dati digitali e concorrono ad alimentare l'Anagrafe Nazionale Studenti gestita dal Miur
- si presentano all'esterno anche per il tramite del proprio portale online e gestiscono numerosi aspetti dei rapporti con gli studenti mediante il portale (es. iscrizioni)
- si avvalgono di algoritmi nella gestione di alcuni rapporti (es. personale)
- promuovono la ricerca scientifica attraverso l'impiego delle tecnologie digitali

⬇

Cosa si intende per: adeguamento di un Ateneo al GDPR?

A) A quali fonti normative occorre fare riferimento?

Fonti fino al 25 maggio 2018: Direttiva 95/46/CE – D.lgs. n. 196/2003 (codice privacy)

Fonti dopo il 25 maggio 2018:

- Regolamento UE 2016/679 (GDPR)
↓
Come applicare il GDPR? v. Le linee guida europee
↓
"Comitato europeo per la protezione dei dati" (EDPB)

- D.lgs. n. 196/2003 (codice privacy) come modificato dal d.lgs. 10 agosto 2018, n. 101 → perdita di centralità del codice privacy

- D.lgs. 18 maggio 2018, n. 5, che ha dato attuazione alla **Direttiva (UE) 2016/680 relativa alla protezione dei dati personali trattati a fini di contrasto in ambito penale**. Questa disciplina, che risponde a un bisogno crescente delle autorità degli Stati membri di trattare e scambiare dati nell'ambito della **lotta alla criminalità transnazionale e al terrorismo**, intende quindi tutelare il diritto delle persone, garantendo nel contempo un elevato livello di sicurezza pubblica

- Provvedimenti del Garante Privacy: es. del 5 giugno 2019, "**recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del d.lgs. 10 agosto 2018, n. 101**"; o il Provvedimento del 26 marzo 2020 - **"Didattica a distanza: prime indicazioni"**

Prof. Francesco Giacomo Viterbo
francesco.viterbo@unisalento.it

Lecce, 27 novembre 2020

⬇

B) Cosa si intende per dato personale? Art. 4, par. 1, n. 1, GDPR

DATO PERSONALE = qualsiasi informazione riguardante una persona fisica identificata o identificabile (c.d. interessato) – la nozione di «identificabilità» è poi meglio specificata nel senso che tale, cioè identificabile, è «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». Ne consegue che nell'ampia definizione appena richiamata è possibile ricomprendere una notevole quantità di dati generati durante le transazioni telematiche e durante la navigazione in Rete:

⬇

esempi: dati della carta d'identità (nome, cognome, foto, numero di matricola) – dati associati alle cose che utilizziamo o di cui siamo proprietari (numero di targa auto, numero cellulare) – altri identificativi online: (email, ora e durata degli accessi alla Rete, *password*, **indirizzo IP: anche dinamico? -** informazioni raccolte dai programmi informatici di *browsing*)

↓

Corte giust. UE 19 ottobre 2016 causa C-582/14 (*Breyer c. Repubblica Federale di Germania*)**: l'indirizzo IP dinamico deve ritenersi comunque dato personale in quanto permette l'identificabilità dell'utente** (intestatario del contratto di accesso) **attraverso l'incrocio con i dati raccolti dal provider**

CATEGORIE PARTICOLARI DI DATI PERSONALI (art. 9 GDPR)

dati che rivelano: origine razziale o etnica, convinzioni religiose o filosofiche, l'appartenenza sindacale: dati relativi allo status di rifugiato per la fruizione di esoneri e borse di studio

dati relativi alla salute (cons. 35): dati relativi agli studenti e/o a familiari diversamente abili, dati relativi allo stato di gravidanza

⬇

Cass. sez. un. 27 dicembre 2017 n. 30981: **il soggetto pubblico - Regione Campania - ed il soggetto persona giuridica privata - Banco di Napoli - sono tenuti, in qualità di titolari del trattamento dei dati personali del ricorrente, nel procedimento di riconoscimento, erogazione e concreto accredito dell'indennità ex lege n. 210 del 1992, ad occultare, mediante tecniche di cifratura o criptatura, il riferimento alla legge sopra indicata, in quanto rivelatore dello stato di salute del beneficiario dell'indennità. Le modalità organizzative, rimesse ai titolari del trattamento dei dati, devono essere dirette ad escludere il collegamento tra il dato sensibile e il soggetto beneficiario dell'indennità ed a limitare alle operazioni indispensabili ed ai soli addetti a tali specifiche operazioni la conoscenza del dato, celandone ai restanti componenti**

Prof. Francesco Giacomo Viterbo
francesco.viterbo@unisalento.it

Lecce, 27 novembre 2020

delle due organizzazioni complesse la decifrabilità ed, infine, conservando le medesime cautele nella comunicazione dei dati

dati relativi alla vita sessuale o all'orientamento sessuale
dati biometrici: es. impronte digitali
dati genetici: relativi al patrimonio genetico
dati relativi a condanne penali e reati (art. 10 GDPR)
⬇
aspetti più delicati e vulnerabili della persona

C) Cosa si intende per "trattamento" di dati personali?

↓

Art. 4, par. 1, n. 2, GDPR → Nozione molto ampia

⬇ ⬇

TRATTAMENTO = «qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione»

⬇

In ogni Ateneo sono trattati sistematicamente e su larga scala dati personali, incluse categorie particolari di dati *ex* art. 9 GDPR

In particolare, il Garante in un parere del 2005 ha identificato le seguenti **quattro macro-categorie di trattamenti**:

1 - Gestione del rapporto di lavoro del personale docente, dirigente, tecnico-amministrativo, dei collaboratori esterni e dei soggetti che intrattengono altri rapporti di lavoro diversi da quello subordinato;

2 - Attività di ricerca scientifica;

3 - Attività didattica e gestione delle iscrizioni e delle carriere degli studenti;

4 - Gestione del contenzioso giudiziale, stragiudiziale e attività di consulenza.

D) Principi applicabili al trattamento dei dati personali

↓

Art. 5 GDPR

Prof. Francesco Giacomo Viterbo
francesco.viterbo@unisalento.it

Lecce, 27 novembre 2020

↓

Principi	**Domande:**
a) Principi di liceità, correttezza e trasparenza	Qual è la base giuridica del trattamento? **(art. 6)**
b) Principio di limitazione della finalità	Per quale finalità il trattamento è effettuato?
c) Principio di minimizzazione dei dati	I dati trattati sono adeguati, pertinenti e limitati a quanto necessario?
d) Principio di esattezza	I dati trattati sono esatti? …occorre aggiornarli?
e) Principio di limitazione della conservazione	I dati per quanto tempo possono essere conservati?
f) Principio di integrità e riservatezza dei dati	Quali misure di sicurezza, tecniche e organizzative?
Principio di responsabilizzazione (artt. 24 ss.)	Chi ha la competenza/responsabilità?

Un punto essenziale della disciplina è: **la finalità del trattamento**.

È il Titolare del trattamento a determinare le finalità e i mezzi del trattamento

Principio di limitazione della finalità → Art. 5(1)(b) GDPR:
I dati personali sono raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo che non sia incompatibile con tali finalità

↓

test di compatibilità → in base ai criteri indicati dal "considerando" 50 e dall'art. 6(4) GDPR

Art. 5(1)(b) GDPR: Questa regola pone al titolare degli obblighi relativi a due momenti diversi:

- al momento della raccolta dei dati, il titolare deve specificare lo scopo del trattamento e informarne compiutamente l'interessato;
- al momento della organizzazione ed esecuzione dell'attività di trattamento, deve adottare modalità e mezzi non abusivi, cioè compatibili coerenti e adeguati allo scopo dichiarato e quindi al legittimo interesse perseguito.

Prof. Francesco Giacomo Viterbo
francesco.viterbo@unisalento.it

Lecce, 27 novembre 2020

Perché le finalità sono così importanti? Perché ciascuna finalità indica l'interesse che fa capo al titolare del trattamento, il valore cui l'attività di trattamento intende dare attuazione, in una parola: la funzione concreta del trattamento

↓

anche per le attività di trattamento si deve operare un controllo di liceità che impone di verificare che i dati personali non siano raccolti per scopi illeciti (es. per la commissione di reati)

Principio di liceità

⬇

Problema della base giuridica del trattamento:

⬇

L'art. 6 GDPR subordina la liceità del trattamento a due requisiti alternativi:

■ **Necessità del trattamento in uno dei seguenti casi: art. 6(1)(b-f) GDPR**

- lett. b) «il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte» → su tale base giuridica si fonda es. trattamento dei dati relativi alla gestione del rapporto di lavoro del personale docente, dirigente, tecnico-amministrativo, dei collaboratori esterni; trattamento *ex* art. 96 cod. privacy

- **lett. c)** «il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare» → su tale base giuridica si fonda es. trattamento dei dati relativi agli esiti dei concorsi pubblici mediante la pubblicazione nel portale online (diffusione)

- **lett. e)** «il trattamento è necessario per l'esecuzione di un compito di interesse pubblico…»
+ par. 3, lett. b) → la base giuridica è nel diritto interno (v. artt. 2 ter e 2 sexies cod. privacy) ↓ ..ma cosa si intende per diritto interno?
→ su tale base giuridica si fonda il trattamento dei dati nell'ambito delle attività di didattica anche a distanza
→ su tale base giuridica può fondarsi il trattamento dei dati per scopi di ricerca scientifica → v. art. 89(1)

- **lett. f)** «il trattamento è necessario per il perseguimento del **legittimo interesse del titolare o di terzi**, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato, in particolare se questi è un minore» → *balancing test* (cons. 47-49) → su tale base giuridica si fonda es. il trattamento dei dati mediante sistemi di videosorveglianza

■ **Consenso: considerando 32 e artt. 4(11), 6(1)(a) GDPR → definizione: qualsiasi manifestazione di volontà di assenso al trattamento di dati personali**

- **libera → vedi art. 7(4) e considerando 42-43 (evidente squilibrio)**
- **specifica → finalità distinte - granularità nella richiesta del consenso**
- **informata → trasparenza - possibilità di revoca ex art. 7(3)**

Prof. Francesco Giacomo Viterbo
francesco.viterbo@unisalento.it

Lecce, 27 novembre 2020

- **inequivocabile → art. 7(2)** → rischio di confusione tra consenso al contratto e consenso al trattamento dei dati personali
  Corte giust. 1 ottobre 2019, C-673/2017 (caso *Planet49*)**:** non è valido il consenso (all'installazione di cookie di profilazione) richiesto all'utente mediante casella di spunta già preselezionata che l'utente deve deselezionare per negare il suo consenso (c.d. opt-out) → la pronuncia si riferisce anche al consenso all'archiviazione delle informazioni o all'accesso a informazioni già archiviate nell'apparecchio terminale dell'utente ex artt. 5(3) della Direttiva 2002/58 e 122, comma 1, cod. privacy
  Si v. WP29 *Guidelines on consent* 2017 / EDPB *Guidelines* 5-2020

→ Esempio 1 – l'Università pianifica dei lavori di rinnovamento delle Biblioteche e offre agli studenti la possibilità di iscriversi a una mailing list per ricevere aggiornamenti sull'avanzamento dei lavori e la disponibilità delle sale.

→ Esempio 2 – l'Università chiede agli studenti presenti in un laboratorio il consenso a usare le loro fotografie nel portale online di Ateneo per illustrare le attività

- **Consenso "esplicito" richiesto in casi particolari: es. art. 9(2)(a) → trattamento di categorie particolari di dati; art. 22(2)(c) → decisione basata unicamente su trattamento automatizzato dei dati** (es. trattamento algoritmico, compresa la profilazione)
  Cosa significa "esplicito" nell'ambiente online? Es. Two-stage verification of consent

Il consenso ha un limite di tempo? Non è definito un limite temporale di efficacia
Deve essere revocato nella stessa forma in cui è stato prestato? Non necessariamente, si precisa: con la stessa facilità (es. non chiamando un call center)
Consenso del minore: art. 8 GDPR e art. 2-quinquies cod. privacy

Trasparenza ex art. 12(1) GDPR: La trasparenza mira a infondere fiducia nei processi che riguardano i cittadini, permettendo loro di comprenderli e, se necessario, di opporvisi – tale principio opera per tutto il ciclo di vita del trattamento

⬇

- **art. 12(2-3) all'interessato deve essere consentito l'esercizio dei propri diritti: accesso, rettifica, cancellazione, opposizione, revoca del consenso, diritto all'oblio, ecc.**

⬇

- diritto alla trasparenza delle informazioni (artt. 12-14) → all'interessato deve essere fornita un'informativa adeguata → obbligo di fornire all'interessato informazioni relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile – con un linguaggio semplice e chiaro → il Titolare può effettuare dei test

Prof. Francesco Giacomo Viterbo
francesco.viterbo@unisalento.it

Lecce, 27 novembre 2020

Quali informazioni? Art. 13(1-2) / art. 14(1-2) → info su: - Titolare
- trattamento
- diritti esercitabili dall'interessato
- conseguenze rischiose

Quando devono essere fornite le informazioni? Artt. 13(1-2); 14(3)

Come devono essere fornite le informazioni? Art. 12(1) → misure appropriate (es. approccio stratificato)
↓
canone di chiarezza e comprensibilità
(linguaggio semplice – lingua destinatari)
→ (5) gratuità delle informazioni
→ (7-8) icone standardizzate

canone di chiarezza e comprensibilità → **analogie con la trasparenza nei contratti con i consumatori** (v. art. 5 Dir. 93/13/Cee concernente le clausole abusive nei contratti con i consumatori cui è stata data attuazione nell'art. 35 cod. cons.)

⬇

L'eventuale violazione dei canoni di chiarezza e comprensibilità delle informazioni potrà dunque comportare l'illiceità del trattamento

Esempio: Provvedimento del Garante - **Ordinanza di ingiunzione nei confronti dell'Università Telematica San Raffaele Roma - 14 marzo 2013**

omissis

«nel form "Richiedi informazioni" presente nel sito www.unisanraffaele.gov.it il semplice richiamo al rispetto del d.lg.n. 196/2003 non risulta essere idoneo a configurare l´informativa di cui all´art. 13 del Codice; inoltre, per quanto concerne il form denominato "Modulo di domanda di immatricolazione", considerando che la procedura di immatricolazione avviene solo in via telematica e che gli studenti interessati devono necessariamente comunicare tutti i loro dati tramite il suddetto form, l´assenza di una adeguata informativa assume particolare rilevanza»

omissis

Sulle condizioni di liceità del trattamento occorre, infine, fare due precisazioni.

- Nel caso di trattamento di categorie particolari di dati personali, si deve fare riferimento non tanto all'art. 6 quanto all'art. 9 GDPR che prevede come regola generale al paragrafo 1 un divieto di trattamento, salvo poi definire nei paragrafi successivi una serie di condizioni che, in deroga al predetto divieto, legittimano il trattamento di tali dati lasciando ai singoli Stati membri un certo margine di discrezionalità nel mantenere o introdurre ulteriori condizioni o limitazioni → v. art. 9(4)

Prof. Francesco Giacomo Viterbo
francesco.viterbo@unisalento.it

Lecce, 27 novembre 2020

- Il venir meno della base giuridica del trattamento e l'assenza di altro fondamento giuridico che lo giustifichi comporta l'illiceità del trattamento e l'insorgere del diritto alla cancellazione dei dati personali senza ingiustificato ritardo (c.d. diritto all'oblio ex art. 17 GDPR) in capo all'interessato.

Principio di minimizzazione dei dati → Principi di proporzionalità e adeguatezza

⬇

Art. 5(1)(c): i dati personali devono essere **adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità** per le quali sono trattati

Esempio: Provvedimento Garante Privacy - Lavoro: comunicazione a terzi di documentazione contenente dati sensibili - 27 giugno 2013

omissis

PREMESSO

1. XY, professore associato presso la Facoltà di HH dell´Università degli Studi di QQ, ha lamentato la violazione della disciplina in materia di protezione dei dati personali in relazione all´indebita comunicazione a terzi di documentazione contenente dati personali a sé riferiti ritenuti avere natura sensibile.

In particolare, a detta della segnalante, il professore KW, docente presso diversa Facoltà dell´Ateneo, sarebbe venuto in possesso di copia di un decreto rettorale (prodotto in atti), con il quale era stata disposta a favore dell´interessata la collocazione in "interdizione dal lavoro" (e, quindi, in "congedo per maternità") ai sensi dell´art. 17, comma 2, lett. a), d.lg. 26 marzo 2001, n. 151 (Testo unico delle disposizioni in materia di tutela e sostegno della maternità e della paternità, a norma dell´articolo 15 della l. 8 marzo 2000, n. 53). Copia del menzionato decreto rettorale, infatti, sarebbe stata allegata dal professor KW alla richiesta di affidamento dell'insegnamento che si sarebbe reso vacante, dallo stesso presentata "senza aspettare che il Preside, una volta verificata l´indisponibilità di colleghi interni alla Facoltà a ricoprire la vacanza, emanasse il bando di affidamento per supplenza" (cfr. segnalazione, p. 2)

Omissis

A seguito di approfondimenti, effettuati dall´Ateneo anche mediante un´apposita "Commissione preposta a verificare il rispetto della vigente normativa" (di cui si è data notizia con nota del 20 settembre 2012), è stato successivamente precisato che (cfr. comunicazione del 18 ottobre 2012):

Omissis

c. **una comunicazione sarebbe stata "inviata dalla segreteria della Facoltà di HH […] al […] direttore del Dipartimento di YY" che, a sua volta, "ha comunicato il decreto di che trattasi al prof. KW (in servizio presso la Facoltà di ZZ ma, per affinità scientifica, afferente al Dipartimento YY) ad esclusivi fini istituzionali, per provvedere alla copertura dell'insegnamento che l'assenza della prof.ssa XY avrebbe lasciato vacante";**

d. tanto sarebbe avvenuto "in ossequio al principio statutario che richiede al dipartimento di concorrere alle attività didattiche mettendo a disposizione proprie risorse e in considerazione della circostanza che il prof. KW fosse l'unico docente del Dipartimento afferente al medesimo settore scientifico disciplinare [della segnalante]";

Lecce, 27 novembre 2020

e. il prof. KW, senza attendere l'emanazione del bando di affidamento della supplenza, "ha inviato alla Preside della Facoltà di HH (e per conoscenza alla Preside della Facoltà di ZZ, a cui il medesimo afferiva) la propria istanza di affidamento di incarico didattico, allegando il d.r. n. 779/2011";

f. la segreteria amministrativa della Facoltà di HH "ha trasmesso l'istanza del prof. KW, allegando inavvertitamente il decreto in questione, a tutti i componenti del Consiglio della Facoltà di HH in quanto la predetta istanza era stata posta dalla preside all'ordine del giorno della successiva seduta del Consiglio stesso".

3. Nel ribadire il contenuto della segnalazione e nel riportarsi alle doglianze ivi già rappresentate, l´interessata nelle proprie controdeduzioni (cfr. nota del 5 novembre 2012) ha dichiarato altresì che:

a. il c.d. polo di HHa non è "tra le strutture preposte al trattamento […] dei dati personali";

b. alla luce degli artt. 44, 48 e 52 dello Statuto dell´Università di QQ "il ruolo primario […] nell´organizzazione della didattica [spetterebbe] alle Facoltà [mentre] un ruolo complementare [competerebbe ai] Dipartimenti";

c. altri docenti nell´ambito dell´Ateneo, afferenti al medesimo settore scientifico disciplinare e nei cui confronti il decreto rettorale non sarebbe stato trasmesso, pure avrebbero avuto interesse a conoscere la vacanza dell´insegnamento (cfr. nota del 5 novembre 2012, cit.);

d. in ogni caso, di non ravvedere la "necessità di consegnare al prof. KW il decreto rettorale nella sua interezza […] diffondendo informazioni per la sottoscritta molto delicate";

e. con riguardo a quanto dichiarato dall´Università circa il fatto che "il documento è stato oggetto di comunicazione interna all´amministrazione" (cfr. nota 18 ottobre 2012 cit.), non per ciò solo ciascun dipendente dell´Università potrebbe legittimamente venire a conoscenza di vicende personali di altri dipendenti.

Omissis

Le informazioni relative all´"interdizione dal lavoro" della segnalante per le ragioni previste dal menzionato art. 17 comma 2, lett. a), d.lg. n. 151/2001 – disposizione espressamente richiamata nel decreto rettorale – fanno infatti riferimento a "gravi complicanze della gravidanza o [a] persistenti forme morbose che si presume possano essere aggravate dallo stato di gravidanza", fattispecie in relazione alla quale i competenti uffici della Direzione Provinciale del Lavoro e della Asl "dispongono […] l´interdizione dal lavoro delle lavoratrici in stato di gravidanza fino al periodo di astensione [c.d. obbligatoria]" (ex art. 17, comma 2, d.lg. n. 151/2001).

5.1. I dati sensibili in questione (desumibili dal menzionato decreto rettorale), che legittimamente possono essere trattati dalle competenti funzioni dell'Ateneo per la dichiarata finalità di "gestione del rapporto di lavoro" (cfr. artt. 11, comma 1, lett. a), 20, comma 1 e 112, comma 1, del Codice) – ed in relazione al quale il Regolamento dell´Università concernente il trattamento dei dati sensibili e giudiziari (pubblicato in http://www....), nel descrivere il "flusso informativo dei dati", individua (in particolare alla scheda A), in conformità all´art. 20, comma 2, del Codice, il tipo di dati sensibili, le operazioni eseguibili nonché i soggetti che le possono porre in essere in ragione delle mansioni svolte – non potevano invece formare legittimamente oggetto di comunicazione a vantaggio terzi. In particolare, nel caso di specie, non potevano essere comunicati ad altro docente (indipendentemente dalla Facoltà di appartenenza dello stesso), non avendo questi titolo alcuno a trattarli per la menzionata finalità di gestione del rapporto di lavoro (rientrante invece, come detto, nelle attribuzioni del personale amministrativo dell´Università a tal fine incaricato del trattamento).

A ciò va aggiunto che – al di là del profilo della lamentata presentazione della domanda di assegnazione dell'incarico di insegnamento anteriormente alla formulazione di apposito bando e prima che altri soggetti potessero venire a conoscenza di tale opportunità (aspetti che non rilevano ai fini della disciplina di protezione dei dati personali) – la comunicazione dei dati sensibili riferiti alla segnalante è altresì avvenuta in violazione del principio di necessità (cfr. art. 11, comma 1, lett. d) e 22, comma 3 del Codice), non essendo indispensabile ai fini dell´assegnazione dell´incarico resosi vacante mettere terzi a conoscenza delle motivazioni, nel caso di specie inerenti alle condizioni di salute dell´interessata, sottese alla vacanza dell'insegnamento.

Prof. Francesco Giacomo Viterbo
francesco.viterbo@unisalento.it

Lecce, 27 novembre 2020

5.2. Per le stesse ragioni deve ritenersi illecita anche la successiva comunicazione dei medesimi dati sensibili a tutti i componenti del Consiglio di Facoltà chiamati a deliberare in ordine all'assegnazione dell'insegnamento realizzatasi mettendo (nuovamente) a disposizione degli stessi il menzionato decreto rettorale, riprodotto dalla segreteria di Facoltà unitamente alla domanda del professor KW.

5.3. La necessità di particolari cautele nel trattamento di dati concernenti le condizioni di salute (desumibile anche dall´art. 22, comma 7, del Codice), peraltro, è stata da tempo evidenziata dal Garante anche nelle *Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico*, precisandosi che le amministrazioni "devono adottare maggiori cautele se le informazioni personali sono idonee a rivelare profili particolarmente delicati della vita privata dei propri dipendenti" (quali ben possono essere quelle concernenti lo stato di salute). Nella stessa sede, l´Autorità ha ribadito che, con specifico riguardo alla gestione del rapporto di lavoro, l´amministrazione deve individuare i soggetti che possono venire lecitamente a conoscenza di tali informazioni, che devono essere in ogni caso designati incaricati o responsabili del trattamento (artt. 29 e 30 del Codice) con la necessaria adozione di "particolari cautele anche nelle trasmissioni di informazioni personali che possono intervenire tra i medesimi incaricati o responsabili nelle correnti attività di organizzazione e gestione del personale. In tali flussi di dati occorre evitare, in linea di principio, di fare superflui riferimenti puntuali a particolari condizioni personali riferite a singoli dipendenti, specie se riguardanti le condizioni di salute, selezionando le informazioni di volta in volta indispensabili, pertinenti e non eccedenti (artt. 11 e 22 del Codice) […] come pure riportare tali informazioni – quale presupposto degli atti adottati – solo nei provvedimenti messi a disposizione presso gli uffici per eventuali interessati e controinteressati (limitandosi quindi a richiamarli anche nelle comunicazioni interne e indicando gli estremi o un estratto del loro contenuto)" (cfr. par 5.1 Linee guida cit.).

Omissis

Principio di limitazione della conservazione

⬇

Art. 5(1)(e) GDPR: i dati personali sono conservati per un arco di tempo non superiore al conseguimento delle finalità del trattamento – possono essere conservati per periodi più lunghi per specifiche finalità (es. di archiviazione nel pubblico interesse) o comunque se sussiste una valida base giuridica (es. se la conservazione è necessaria per difendere un diritto in sede giudiziaria)

Esattezza ex art. 5(1)(d) GDPR: i dati personali sono esatti e, se necessario, aggiornati

⬇

- **Il Titolare deve adottare tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati**

⬇

- diritti dell'interessato (artt. 15-17 GDPR):

- **diritto di accesso (art. 15) → diritto a ricevere informazioni / diritto a una copia dei dati**

- **diritto di rettifica (art. 16) → diritto di ottenere la rettifica dei dati personali senza ritardo**
  → diritto di ottenere l'integrazione dei dati personali incompleti

Prof. Francesco Giacomo Viterbo
francesco.viterbo@unisalento.it

Lecce, 27 novembre 2020

• **diritto all'oblio (art. 17)** → **diritto di ottenere la cancellazione dei dati personali se:**
- non sono più necessari rispetto alle finalità del trattamento
- viene meno la base giuridica del trattamento
- i dati personali sono trattati illecitamente
- la cancellazione è necessaria per adempiere un obbligo legale
- l'interessato **si oppone** al trattamento

↓

• **diritto di opposizione** **(art. 21)** → l'interessato può opporsi «per motivi connessi alla sua situazione particolare» al trattamento dei dati personali effettuato per l'esecuzione di un compito di interesse pubblico (art. 6, par. 1, lett. *e*) o per il perseguimento del legittimo interesse del Titolare (art. 6, par. 1, lett. *f*), compresa la profilazione → il Titolare si astiene salvo che l'interesse perseguito prevalga sui diritti dell'interessato → *balancing test*

⬇

Cfr. **diritto di opposizione (all'accesso civico) *ex* art. 5, comma 5, d.lgs. n. 33/2013**

⬇

Garante Privacy: **Parere su una istanza di accesso civico - 7 novembre 2019**

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Omissis

OSSERVA

Nel caso in esame, oggetto dell'accesso civico sono gli elaborati scritti e i curricula vitae dei candidati ad un concorso pubblico, nonché i verbali di correzione degli elaborati.

In primo luogo, per gli specifici profili inerenti all'accesso civico alla copia degli elaborati scritti di un concorso pubblico, si deve tenere presente che tali documenti, in generale, sono indicativi di molteplici aspetti di carattere personale circa le caratteristiche individuali, relativi ad esempio alla preparazione professionale, alla cultura, alle capacità di espressione, o al carattere del candidato, che costituiscono aspetti valutabili nella selezione dei partecipanti. Inoltre, in alcuni casi, e a seconda della traccia sottoposta, il contenuto degli elaborati è capace di rivelare anche informazioni e convinzioni che possono rientrare nelle «categorie particolari di dati personali» di cui all'art. 9, par. 1, del Regolamento (si pensi, in particolare, a elaborati nei quali potrebbero evincersi «opinioni politiche», «convinzioni filosofiche o di altro genere»).

Analogamente si osserva che i contenuti generalmente inseriti nel curriculum vitae sono molteplici e la relativa ostensione può consentire l'accesso, a seconda di come è redatto il cv, a numerosi dati (es.: nominativo, data e luogo di nascita, residenza, telefono, e-mail, nazionalità) e informazioni di carattere personale (es.: esperienze e competenze professionali, istruzione e formazione, competenze personali, competenze comunicative, competenze organizzative e gestionali, pubblicazioni, presentazioni, progetti, conferenze, seminari, riconoscimenti e premi, appartenenza a gruppi/associazioni, referenze, menzioni, corsi, certificazioni, ecc.), che per motivi individuali non sempre si desidera portare a conoscenza di soggetti estranei.

Tenuto quindi conto che «Tutti i documenti, le informazioni e i dati oggetto di accesso civico […] sono pubblici e chiunque ha diritto di conoscerli, di fruirne gratuitamente, e di utilizzarli e riutilizzarli ai sensi dell'articolo 7», pur nel rispetto dei limiti derivanti dalla normativa in materia di trattamento dei dati personali per ogni ulteriore trattamento (art. 3, comma 1, del d. lgs. n. 33/2013), l'ostensione dei documenti richiesti è suscettibile di determinare, a seconda delle ipotesi e del contesto in cui possono essere utilizzati da terzi,

Prof. Francesco Giacomo Viterbo
francesco.viterbo@unisalento.it

Lecce, 27 novembre 2020

proprio quel pregiudizio concreto alla tutela della protezione dei dati personali previsto dall'art. 5-bis, comma 2, lett. a), del d. lgs. n. 33/2013.

Pertanto, si ritiene che, ai sensi della normativa vigente e delle indicazioni contenute nelle Linee guida dell'ANAC in materia di accesso civico, considerando la natura dei dati personali coinvolti e il particolare regime di pubblicità dei dati e documenti oggetti di accesso civico – conformemente ai precedenti orientamenti del Garante in materia di accesso civico agli elaborati scritti dei candidati ad un concorso pubblico e/o a curricula vitae presentati dai candidati (cfr. pareri n. 162 del 30 marzo 2017, doc. web. n. **6393422**; n. 246 del 24 maggio 2017, doc. web. n. **6495600**; n. 366 del 7 settembre 2017, doc. web n. **7155171**; n. 433 del 26 ottobre 2017, doc. web n. **7156158**) – **l'amministrazione abbia correttamente respinto l'accesso civico ai documenti richiesti.**

Per completezza si rappresenta che «l'amministrazione cui è indirizzata la richiesta di accesso, se individua soggetti controinteressati, ai sensi dell'articolo 5-bis, comma 2, è tenuta a dare comunicazione agli stessi, mediante invio di copia con raccomandata con avviso di ricevimento, o per via telematica per coloro che abbiano consentito tale forma di comunicazione. Entro dieci giorni dalla ricezione della comunicazione, i controinteressati possono presentare una motivata opposizione, anche per via telematica, alla richiesta di accesso» (art. 5, comma 5, del d. lgs. n. 33/2013).

Resta, in ogni caso, salva la possibilità per l´istante di accedere alla predetta documentazione, anche per motivi diversi da quelli già oggetto di richiesta di ostensione avanzata in passato, laddove dimostri l´esistenza di «un interesse diretto, concreto e attuale, corrispondente ad una situazione giuridicamente tutelata e collegata al documento al quale è chiesto l´accesso», ai sensi degli artt. 22 ss. della l. n. 241 del 7/8/1990.

Omissis

⬇

Il GDPR non è una disciplina finalizzata a imporre adempimenti burocratici e formali, ma impone ai soggetti che effettuano trattamenti di dati personali di tenere in massima considerazione i diritti fondamentali della persona di ogni interessato

⬇

Principi di integrità e riservatezza

⬇

Art. 5(1)(f) GDPR: il Titolare deve garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e misure organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali

Principio di responsabilizzazione (*accountability*)

⬇

Artt. 5(2) e 24 GDPR → indica un approccio proattivo alla tutela dei dati personali in base al quale è il **Titolare del trattamento** di dati personali a dover valutare e mettere in atto le **misure tecniche e organizzative in concreto adeguate** per garantire che il trattamento sia conforme al GDPR e *in primis* ai principi indicati, tenuto conto della natura dei dati, del contesto e delle finalità del trattamento, nonché dei rischi per i diritti e le libertà degli interessati. Inoltre, il Titolare del trattamento **deve essere in grado di dimostrare di aver adottato misure adeguate** per rendere il trattamento conforme alla normativa e deve compiere un'attività di continuo

Prof. Francesco Giacomo Viterbo
francesco.viterbo@unisalento.it

Lecce, 27 novembre 2020

monitoraggio

⬇

Da non confondere con la responsabilità *ex* art. 82 GDPR (successiva al verificarsi del danno materiale o immateriale)

⬇

Il **principio di accountability** trova attuazione su questo triplice fronte:

i) **valutazione preventiva e predisposizione di misure adeguate** in modo che il trattamento soddisfi i requisiti previsti e garantisca la tutela dei diritti dell'interessato

ii) **assunzione e conservazione delle relative prove**: in proposito il paragrafo 3 dell'art. 24 precisa che possono costituire elemento di prova l'adesione a un codice di condotta adottato in conformità al Regolamento o a un meccanismo di certificazione avente i requisiti indicati dall'art. 42

iii) **monitoraggio dell'attività**, dal che si desume che l'accountability è un concetto dinamico, evolutivo e relazionale, da rapportarsi alle conoscenze acquisite in base al progresso tecnico e alle concrete caratteristiche del trattamento di dati da effettuarsi

⬇ ⬇

Art. 35 GDPR: *Data Protection Impact Assessment* (DPIA o Valutazione d'impatto sulla protezione dei dati) → la fase che precede lo svolgimento del trattamento di dati personali viene procedimentalizzata sulla base dei seguenti passaggi operativi, alcuni necessari ed altri solo eventuali:

- il primo è rappresentato da una **valutazione generica del rischio** che trova fondamento negli artt. 24 e 35(1) GDPR: questo primo esame serve a valutare se sussistono o meno rischi elevati per i diritti e le libertà degli interessati, correlati al trattamento che si intende eseguire

- ove emerga che il trattamento può comportare un rischio elevato per i diritti e le libertà delle persone, il titolare deve procedere col realizzare una **valutazione d'impatto sulla protezione dei dati** ↓

→ La valutazione di impatto deve contenere almeno:

- una descrizione sistematica dei trattamenti previsti e delle finalità
- la valutazione sulla necessità e la proporzionalità dei trattamenti rispetto alle finalità
- la valutazione dei rischi per i diritti e le libertà degli interessati

⬇ ⬇

Cosa deve intendersi per rischio? **Come va valutato il rischio? → Garante**

→ vi è una lista aperta di ipotesi in cui il grado elevato del rischio è presunto e la valutazione d'impatto obbligatoria (es. profilazione o trattamento su larga scala di categorie particolari di dati personali) ↓

Prof. Francesco Giacomo Viterbo
francesco.viterbo@unisalento.it

Lecce, 27 novembre 2020

Esempio 1 - l'Università è tenuta a produrre una valutazione d'impatto del proprio sistema di videosorveglianza, se applicato su larga scala e con particolari tecnologie in grado di acquisire e trattare informazioni personali (es. riconoscimento facciale).

Esempio 2 – nel caso in cui, nello svolgere un'analisi su particolari aspetti (es: l'abbandono universitario) attraverso un'interconnessione tra dati di carriera, dati anagrafici, ecc., si renda necessario prevedere degli interventi di supporto per gli interessati di carattere individuale (es: percorsi formativi o di orientamento), tale trattamento potrebbe essere considerato come un'operazione di "profilazione" per la quale è consigliabile effettuare una valutazione di impatto

- **Art. 36 GDPR:** ove dalla valutazione d'impatto risulti che il trattamento comporta un rischio elevato per i diritti degli interessati, il titolare deve consultare preventivamente l'Autorità di controllo (**consultazione preventiva** o ***prior checking***)

- in ultimo deve procedere con l'adozione delle misure di sicurezza individuate e lo svolgimento effettivo del trattamento di dati in conformità alle misure adottate e nel rispetto della disciplina in materia di protezione dei dati personali

⬇

Art. 25 GDPR: Principi della "*data protection by design and by default*"
Protezione dei dati sin dalla progettazione e per impostazione predefinita

• **data protection by design: ricorso a programmi o "modelli architettonici" del web, per impostazione predefinita, privacy-friendly volti ad attuare i principi di protezione dei dati**

Momento **font-end:** in cui l'utente si interfaccia con il servizio fornitogli (es. pseudonimizzazione)

Momento **back-end:** riguarda i modi di trattamento dei dati personali già acquisiti (es. meccanismo di cancellazione automatica dei dati quando la finalità del trattamento sia stata raggiunta)

→ implica la necessità di inserire nei prodotti e nei sistemi informatici dei meccanismi che spingano gli utenti a modificare il proprio comportamento prestando maggiore attenzione ai problemi di privacy ed ampliando la gamma delle scelte possibili in materia di protezione dei dati personali, ad esempio consentendo all'utente di scegliere se usufruire del servizio online in anonimato o permettere al gestore del servizio di acquisire e trattare i dati personali

• **data protection by default setting:** implica una decisione sul modo di impostare il funzionamento di un sistema informatico o di una piattaforma digitale con riguardo

Prof. Francesco Giacomo Viterbo
francesco.viterbo@unisalento.it

Lecce, 27 novembre 2020

all'acquisizione e al trattamento di dati personali, fatta salva la possibilità di cambiamento da parte dell'utente dell'impostazione prescelta a monte. L'utilità dei default settings si fonda sull'idea che, ove un'impostazione sia già stata preselezionata, gli utenti tendono a non modificarla e a restare sugli stessi default settings → Esempio 1 - cookie di profilazione che per impostazione vengono trasferiti nel terminale dell'utente salvo la possibilità di blocco rifiutando il consenso

→ Esempio 2 - potrebbe un Ateneo legittimamente inserire nel proprio sito Internet il plug-in «Mi piace» del social network Facebook?

Ulteriori obblighi cui è tenuto il Titolare:

- Art. 30 GDPR: di redigere e tenere i Registri delle attività di trattamento

- Artt. 37-39: di designare il Responsabile della protezione dei dati (DPO)

- Artt. 28-29: di designare uno o più Responsabili del trattamento (esterni e/o interni) e istruire il personale preposto al trattamento dei dati

⬇

Il sistema universitario è complesso → Gli Atenei non sono unici Titolari del trattamento → altri Titolari sono il MIUR e taluni Consorzi (es. Almalaurea, GARR)

→ si è creato un gruppi di coordinamento dei DPO

→ ogni Ateneo designa più Responsabili esterni (es. videosorveglianza)

→ i Responsabili interni e il DPO devono avere competenze tecniche e giuridiche ⬇

UNISALENTO: Cabina di regia in materia di privacy

Ulteriori diritti degli interessati:

- diritto a non essere profilati/a non essere sottoposti a una decisione basata unicamente sul trattamento automatizzato di dati compresa la profilazione: art. 22

↓

Divieto generale salvo eccezioni

Esempio 1 - l'Università fonda su un trattamento algoritmico di dati la valutazione dei professori e ricercatori ai fini dell'attribuzione degli scatti stipendiali (Regolamento di Ateneo D.R. n. 108/2018 e art. 6 L. n. 240/2010)

Esempio 2 – l'Università offre dei percorsi formativi o di orientamento personalizzati finalizzati a fornire degli interventi di supporto di carattere individuale, mediante il trattamento algoritmico (sistema di

Prof. Francesco Giacomo Viterbo
francesco.viterbo@unisalento.it

Lecce, 27 novembre 2020

AI) dei dati anagrafici, di carriera, ecc.

⬇

Quale sarebbe la base giuridica del trattamento?
Il trattamento sarebbe conforme ai principi previsti dall'art. 5 GDPR?

⬇

IPOTESI 1 – Processo decisionale basato sulla profilazione → Decisione adottata dall'uomo
IPOTESI 2 – Decisione basata *unicamente* sul trattamento algoritmico dei dati

- **diritto alla portabilità dei dati** (art. 20) → Il diritto alla portabilità dei dati permette agli interessati di ricevere i dati personali da loro forniti al titolare del trattamento, in un formato strutturato, di uso comune e leggibile meccanicamente, e di trasmetterli a un diverso titolare.

⬇

si applica ai dati trattati con il consenso dell'interessato o sulla base di un contratto stipulato con l'interessato e solo per i dati che siano stati "forniti" dall'interessato al titolare; fanno eccezione quindi i dati il cui trattamento si fonda sull'interesse pubblico o sull'interesse legittimo del titolare → si applica al rapporto Università-studente? → dubbi sulla base dell'art. 20(3) GDPR

⬇

a) **Diritto di ricevere un sottoinsieme di dati personali trattati da un Titolare in un formato riutilizzabile per scopi personali**
b) **Diritto di trasmettere dati personali da un Titolare ad un altro senza impedimenti**

↓

Si promuove lo sviluppo di formati interoperabili→ No a forme di "lock in" tecnologico!!

⬇

Rischio che i dati personali divengano una merce di scambio dietro remunerazione

⬇

Si può rendere l'esercizio dei diritti degli interessati come uno strumento capace di generare valore economico?

Di chi sono i dati personali? A chi appartengono? esclusione della logica proprietaria dei dati

⬇

CASO WEOPLE ("*la **prima banca per investire i dati personali***")

Più nel dettaglio, **precisa il sito**, Weople funge da "***piattaforma di marketing diretto** per offrire delle proposte e delle comunicazioni a target interessanti. In particolare Weople troverà clienti-aziende e proporrà loro di veicolare, tramite app, pacchetti, offerte personalizzate e/o comunicazione a segmenti di correntisti che Weople ha dimostrato, grazie ai dati, essere potenzialmente interessanti*".

⬇

Il GDPR adotta un approccio *user-centric* orientato al personalismo

⬇

i dati personali:

- **non sono oggetto di proprietà né sono alienabili**: difatti la disciplina in materia di

Prof. Francesco Giacomo Viterbo
francesco.viterbo@unisalento.it

Lecce, 27 novembre 2020

protezione dei dati non riconosce all'interessato la titolarità di un diritto di godimento/uso esclusivo dei dati né prevede un particolare tipo di contratto che consente all'interessato di disporre dei propri dati alla stregua delle altre situazioni soggettive di natura patrimoniale

- **si configurano come beni giuridici**, centro di riferimento di situazioni soggettive plurime e distinte, secondo che si consideri la posizione dell'interessato – titolare istituzionale dei dati –ovvero la posizione riservata a terzi qualificati in rapporto al loro interesse alla raccolta dei dati ed al relativo trattamento

- **sono elementi costitutivi dell'identità personale** e devono essere protetti in funzione di tutela della dignità e della personalità umana

- **contengono in sé l'attitudine a rilevare come risorsa oggetto**, non di appropriazione bensì di *accesso*, non di un'attività di godimento bensì **di un'attività di *trattamento*** da parte di terzi per specifiche finalità meritevoli

… in ogni caso, a presidio dei diritti e delle libertà delle persone rispetto al trattamento dei dati personali operano i principi costituzionali:

art. 2: tutela della dignità umana

art. 3: eguaglianza

art. 21: libertà di manifestazione del pensiero

art. 41: limiti all'iniziativa economica privata

⬇

Adeguarsi al GDPR significa rendere le attività, l'organizzazione e più in generale ogni espressione dell'istituzione universitaria funzionali al rispetto dei diritti della persona e alla promozione dell'università come "luogo" nella quale ogni individuo sviluppa e svolge liberamente la sua personalità

Prof. Francesco Giacomo Viterbo
francesco.viterbo@unisalento.it

Lecce, 27 novembre 2020

GRAZIE!