FAQ – PROTEZIONE DEI DATI PERSONALI

1) Principali novità introdotte dal Regolamento europeo n. 679/2016 (di seguito GDPR)

Le principali novità riguardano:

- l'introduzione del principio di responsabilizzazione ("*accountability*");
- l'istituzione del registro dei trattamenti;
- la designazione di un Responsabile della Protezione dei Dati (RPD – *Data Protection Officer* – DPO);
- la notifica di eventuali violazioni dei dati ("*data breach"*).

2) Principali fonti in materia di protezione dei dati

Le principali fonti sono:

- il Regolamento generale sulla protezione dei dati n. 679/2016 (in sigla, "RGPD" o in inglese, "GDPR" *General Data Protection Regulation*) entrato in vigore il 25 maggio 2018. Tale Regolamento, strutturato in 173 "Considerando" e 99 articoli, prevede regole immediatamente e direttamente applicabili per tutti i soggetti coinvolti nella gestione e protezione dei dati personali;
- il d.lgs. n. 196 del 30 giugno 2003 recante il "Codice in materia di protezione dei dati personali" come modificato dal d.lgs. n. 101 del 10 agosto 2018.

3) Quali sono i principi secondo cui vengono trattati i dati degli interessati?

I dati degli interessati devono essere trattati applicando i principi previsti dall'art. 5 del GDPR:

- liceità, correttezza e trasparenza (art. 5, lett. a);
- limitazione delle finalità (art. 5, lett. b);
- minimizzazione dei dati (art. 5, lett. c);
- esattezza (art. 5, lett. d);
- limitazione della conservazione (art. 5, lett. e);
- integrità e riservatezza (art. 5, lett. f).

4) Tipologie di dati personali:

4.1. Dati personali

Per "dato personale" si intende 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 (art. 4, co. 1, GDPR).

4.2. Dati personali comuni

Tutti i dati pubblici in genere.

Sono dati personali comuni, tra gli altri:

- dati anagrafici (ad. es. nome, cognome, genere, età, data di nascita);
- dati di contatto (ad. es. indirizzo, indirizzo e-mail, numero di telefono, Skype Id);
- documenti di identità e numeri identificativi (ad. es. codice fiscale, numero di targa);
- CV e relative esperienze professionali e accademiche;

- le immagini da cui è possibile identificare una persona (ad. es. fotografie, riprese video);
- i numeri identificativi utilizzati *online* (indirizzo IP, punti di geo-localizzazione).

4.3. Categorie particolari di dati personali

L'espressione "categorie particolari di dati personali" è stata introdotta dal GDPR (art. 9) ed ha sostituito la terminologia di "dato sensibile" contenuta nel Codice della *privacy*.

In particolare, con tale espressione vengono indicati i dati personali idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose, filosofiche, l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a verificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

4.4. Dati giudiziari

Si tratta dei dati personali idonei a rivelare:

- l'iscrizione nel casellario giudiziale (ad esempio: condanna penale, pene accessorie quali interdizione dai pubblici uffici, ecc.);
- l'iscrizione nell'anagrafe delle sanzioni amministrative dipendenti da reato;
- la sussistenza di carichi pendenti;
- la qualità di imputato o di indagato.

4.5. Dati relativi alla ricerca scientifica

Le attività di ricerca svolte in Sapienza presentano una significativa complessità sotto il profilo della disciplina e degli adempimenti in materia di trattamento di dati personali.

In particolare, è utile esaminare tre principali aspetti legati al trattamento dei dati personali con finalità di ricerca:

- garantire il rispetto del principio della minimizzazione dei dati (non raccogliendo informazioni che non sono necessarie per il perseguimento delle finalità di ricerca);
- informare gli interessati sull'uso dei propri dati personali nell'ambito del progetto di ricerca, fornendo tutte le informazioni previste dall'art. 13 del GDPR. Al riguardo, è necessario evidenziare che nell'ambito di attività di natura didattica e/o di ricerca proprie di Sapienza e svolte, per convenzione, presso Scuole e/o Strutture Sanitarie, è possibile che un dato raccolto da tali enti sia poi utilizzato, sia pure in forma pseudonimizzata, nell'ambito di attività proprie dell'Ateneo. L'art. 14 del GDPR esonera l'Università dal rendere un'informativa specifica agli interessati (i cui dati potrebbero essere stati raccolti, ad esempio, da una Scuola per finalità diverse da quelle di ricerca), a patto che risulti impossibile o comporti uno sforzo sproporzionato contattare l'interessato e, comunque, a condizione che esistano adeguate misure di salvaguardia.

È importante, tuttavia, che in tal caso le informazioni (di cui all'art. 13 del GDPR) siano comunque rese pubbliche, anche mediante pubblicazione sui siti istituzionali;

- predisporre adeguate misure tecniche e organizzative per garantire la protezione dei dati, a seguito di un'accurata analisi dei rischi.

5) Cosa si intende per "trattamento" dei dati personali?

Il "trattamento" dei dati personali indica qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate ai dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento, la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, la diffusione o qualsiasi altra forma di messa a

disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione (art. 4, co. 2, GDPR).

6) Modalità di trattamento dei dati personali

I dati personali possono essere trattati su supporti in formato cartaceo o elettronico. In quest'ultimo caso, possono essere utilizzati strumenti automatizzati.

7) Finalità di trattamento dei dati da parte dell'Ateneo

I dati potranno essere trattati, tra l'altro, per le seguenti finalità:

- per rendere informazioni attinenti a servizi, o per comunicazioni istituzionali;
- per fini di sicurezza e organizzazione interna;
- a fini di ricerca e statistici (elaborazione sia su base non aggregata che su base anonima ed aggregata);
- con il consenso dell'interessato, per l'invio all'indirizzo *e-mail* di pubblicazioni periodiche ossia, per le iniziative a supporto delle attività dell'Università; altre attività editoriali/digitali/ cartacee per scopi di comunicazione/promozione dell'Università ecc.;
- ai fini della gestione delle attività di biblioteca, per consentire l'accesso, tra l'altro, ai servizi e ai materiali in essa contenuti;
- per esigenze logistiche, con elaborazione di dati di geolocalizzazione.

8) Fondamenti di liceità del trattamento dei dati (basi giuridiche)

Il GDPR dispone che un trattamento di dati personali deve trovare fondamento in una base giuridica. In assenza di una base legale il trattamento è illecito.

L'articolo 6 del GDPR elenca le condizioni in base alle quali il trattamento può dirsi lecito:

- consenso dell'interessato (art. 6, lett. a);
- esecuzione di un contratto di cui l'interessato è parte o l'esecuzione di misure precontrattuali adottate su richiesta dello stesso (art. 6, lett. b);
- adempimento di un obbligo legale al quale è soggetto il titolare del trattamento (art. 6, lett. c);
- salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica (art. 6, lett. d);
- esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento (art. 6. lett. e);
- perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore (art. 6, lett. f).

Per il trattamento delle "categorie particolari di dati personali" occorre fare riferimento alle condizioni previste nell'articolo 9 del GDPR.

9) I soggetti del trattamento dei dati personali:

9.1. Il Titolare del trattamento (e i Contitolari)

Il Titolare del trattamento è la persona fisica o giuridica (società, associazione, fondazione, etc.), autorità pubblica, servizio o altro organismo che, singolarmente o insieme ad altri (**con-titolari**), determina le finalità del trattamento di dati personali, i motivi per i quali i dati personali vengono trattati, nonché le modalità (tecniche, informatiche, organizzative, etc.) con le quali si svolgono le relative attività di trattamento (art. 4, co. 7, GDPR).

Ove le decisioni relative al trattamento siano prese congiuntamente da due o più soggetti, questi ultimi vengono qualificati come **contitolari del trattamento** (art. 26 GDPR) e le relative

responsabilità (relativamente agli obblighi da osservare, all'esercizio dei diritti dell'interessato e all'informativa) vengono definite mediante un accordo interno.
Il Titolare del trattamento dei dati personali in Ateneo è l'Università Sapienza, intesa come persona giuridica, rappresentata dal suo Legale Rappresentante, la Rettrice *pro tempore*.

9.2. Il Responsabile del trattamento

Il responsabile del trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento in forza di una delega di funzioni (art. 4, co. 8, GDPR).
Il responsabile del trattamento deve essere nominato dal Titolare con apposito atto scritto contenente specifiche istruzioni a cui il responsabile si deve necessariamente attenere.

9.3. Il Responsabile della Protezione dei Dati (*Data Protection Officer* – DPO)

Il Responsabile della protezione dei dati è un consulente esperto designato dal Titolare del trattamento, per assolvere a funzioni di supporto, controllo, consultive e informative relativamente all'applicazione del Regolamento. Coopera con il Garante e costituisce il punto di contatto, anche rispetto agli interessati, per le questioni connesse al trattamento dei dati personali. I suoi compiti sono esplicati nell'art. 39 del GDPR.

9.4. I Designati

Il designato per il trattamento dei dati coadiuva il Titolare nella definizione dei mezzi atti a garantire l'osservanza della normativa comunitaria e la protezione dei dati personali e nell'individuazione delle modalità più opportune per autorizzare al trattamento dei dati personali i soggetti che operano sotto la propria autorità diretta.
Nell'organizzazione di Sapienza, la funzione di designato è assegnata al personale che ricopre funzioni di particolare rilievo organizzativo e agisce per conto del Titolare sulla base delle competenze attribuite alla funzione organizzativa o carica istituzionale che ricopre (Direttori di Dipartimento, Presidi di Facoltà, Direttori di Centri, Dirigenti delle Aree amministrative).
Il designato è nominato dalla Rettrice, in qualità di legale rappresentante del Titolare, con un atto di nomina nel quale sono contenute le istruzioni atte a garantire e a dimostrare che il trattamento sia effettuato conformemente al GDPR.

9.5. Gli Incaricati

Gli autorizzati al trattamento (docenti; personale tecnico – amministrativo e bibliotecario ecc) sono tutti quei soggetti, individuati dal Titolare o dai designati, autorizzati a compiere operazioni di trattamento sotto la loro vigilanza. Tali soggetti sono autorizzati al trattamento dei dati mediante nomina individuale da parte del Titolare o dei disegnati.

9.6 Responsabile esterno del trattamento

Il Responsabile esterno del trattamento dati è un soggetto esterno che esegue, in base ad un contratto/convenzione o altro atto giuridico, dei trattamenti di dati personali per conto del Titolare e ne risponde in solido in caso di inadempienze. Ad esso spettano tutti i compiti del Titolare all'interno del proprio organismo (valutazione d'impatto, registro dei trattamenti, eventuale nomina del proprio DPO ecc).
Il Responsabile esterno, così individuato, non può a sua volta nominare un altro Responsabile (sub-Responsabile) se non dietro autorizzazione scritta del Titolare: la catena delle responsabilità deve essere nota al Titolare. Inoltre, nei contratti con sub-responsabili devono

essere riportati gli stessi obblighi in materia di protezione dei dati personali previsti dal contratto tra Responsabile e Titolare.
Nell'ambito universitario risulta utile distinguere tra la funzione di "responsabile esterno al trattamento", così come definita all'art. 28 del GDPR, assegnata a un soggetto esterno che esegue trattamenti per conto dell'Università e la funzione di Responsabile interno (designato), assegnata al personale che ricopre funzioni di particolare rilievo organizzativo (vedi FAQ 9.4).

10) Chi è "l'interessato"?

L'interessato è la persona fisica alla quale si riferiscono i dati trattati.
L'interessato è quindi il soggetto "proprietario" dei dati personali e su questi conserva dei diritti nei confronti del Titolare del trattamento: il GDPR, al Capo III, elenca nel dettaglio tali diritti, alcuni dei quali, a seconda della finalità per la quale i dati sono stati raccolti, potrebbero non essere esercitabili dagli interessati. Ad esempio, non è possibile effettuare la cancellazione dei dati relativi alla carriera di uno studente perché tali dati devono essere conservati illimitatamente per pubblico interesse.
Nell'ambito di Sapienza è possibile individuare le seguenti principali categorie di interessati: studenti, dottorandi, specializzandi, personale tecnico-amministrativo, personale docente, collaboratori; assegnisti, privati cittadini, clienti e fornitori.

11) Quali sono i diritti dell'interessato?

Il Capo III del GDPR riconosce all'interessato una serie di diritti che gli garantiscono di esercitare un controllo sull'utilizzo dei suoi dati da parte di altri soggetti. In particolare, il GDPR disciplina:

- il diritto di accesso (art. 15);
- il diritto di rettifica (art. 16);
- il diritto alla cancellazione (il c.d. "diritto all'oblio") (art. 17);
- il diritto di limitazione del trattamento (art. 18);
- il diritto alla portabilità dei dati (art. 20);
- il diritto di opposizione (art. 21);
- il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona (art. 22).

Le modalità per l´esercizio di tutti i diritti da parte degli interessati sono stabilite, in via generale, negli artt. 11 e 12 del Regolamento.
Il termine per la risposta all´interessato è, per tutti i diritti (compreso il diritto di accesso), 1 mese, estendibile fino a 3 mesi in casi di particolare complessità; il Titolare deve comunque dare un riscontro all´interessato entro 1 mese dalla richiesta, anche in caso di diniego.

12) <u>L'informativa privacy:</u>

12.1. Che cos'è l'informativa privacy?

Il GDPR prevede che il Titolare del trattamento, al fine di assicurare la trasparenza e correttezza del trattamento medesimo, debba fornire agli interessati - salvo la legge espressamente non lo richieda o l'interessato sia già in possesso delle informazioni ovvero nei casi limite della forza maggiore e dell'impossibilità di reperire i destinatari se non a costi sproporzionati - le informazioni richieste dalle norme (art. 12 - 13 GDPR).
L'informativa è una comunicazione rivolta all'interessato che ha lo scopo di informare il cittadino, anche prima che diventi interessato (cioè prima che inizi il trattamento), sulle finalità e le modalità dei trattamenti operati dal Titolare del trattamento. Il testo deve essere conciso, trasparente, intelligibile per l'interessato e facilmente accessibile.

In particolare, l'art. 13 del GDPR elenca le informazioni che devono essere fornite qualora i dati personali siano raccolti presso l'interessato, mentre l'art. 14 del GDPR elenca le informazioni che devono essere fornite qualora i dati personali non sia stati ottenuti presso l'interessato.

12.2. Con quali modalità può essere fornita l'informativa privacy?

L'informativa viene solitamente resa per iscritto o utilizzando mezzi informatici e digitali.

Le varie informazioni possono essere anche rese oralmente, ma solo quando l'interessato ne faccia esplicita richiesta.

L'informativa è gratuita e non comporta alcun onere o esborso a carico dell'interessato.

Quanto al momento in cui l'informativa deve essere fornita, occorre distinguere:

- se i dati siano raccolti presso l'interessato, deve essere resa prima della raccolta dei dati;
- quando i dati sono ottenuti da un soggetto diverso dall'interessato, l'informativa deve essere fornita a quest'ultimo – sempre se è possibile rintracciarlo e ciò non risulta particolarmente difficile o eccessivo, come potrebbe essere, ad esempio, per una ricerca che coinvolga un numero elevatissimo di persone – entro un termine ragionevole dall'ottenimento dei dati, al più tardi entro un mese o comunque, nel caso in cui i dati personali permettano proprio di prendere contatto con l'interessato, nella prima comunicazione.

13) Che cos'è il Registro dei trattamenti?

Tra gli adempimenti principali del Titolare e del Responsabile, l'art. 30 del Regolamento europeo individua la tenuta del "registro delle attività di trattamento". Quest'ultimo è uno strumento idoneo a fornire un quadro aggiornato dei trattamenti in essere all'interno dell'organizzazione e, pertanto, costituisce uno dei principali elementi di *accountability* del Titolare.

Il Regolamento individua dettagliatamente le informazioni che devono essere contenute nel registro delle attività di trattamento del Titolare (art. 30, par. 1 del RGPD) e in quello del Responsabile (art. 30, par. 2 del RGPD).

Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.

14) La violazione dei dati personali (c.d. data breach):

14.1. Che cos'è il *data breach*?

Il "*data breach*" è una violazione di sicurezza che comporta, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati (ad esempio, la divulgazione non autorizzata dei dati personali). Una violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità di dati personali.

14.2. Cosa occorre fare in caso di *data breach*?

L'art. 33 del GDPR dispone che la notifica di violazione dei dati personali all'Autorità di controllo competente debba essere effettuata dal Titolare del trattamento senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne ha avuto conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

Inoltre, quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento, ai sensi dell'art. 34 del Regolamento, deve comunicare la violazione all'interessato senza ingiustificato ritardo.

In caso di violazione dei dati avvenuta nell'ambito dell'Ateneo, i Dirigenti/Rappresentanti di struttura, al fine di consentirne la prevista comunicazione all'Autorità di controllo, entro e non oltre 48 ore dall'acquisizione della conoscenza dell'accadimento, devono informare, con urgenza immediata, il Responsabile della protezione dei dati, utilizzando l'apposito modello Allegato 1) alla circolare n. 44407 del 25.05.2018 pubblicata sulla pagina *web* https://www.uniroma1.it/it/pagina/settore-privacy nella sezione "Atti Sapienza", da trasmettere esclusivamente all'indirizzo e-mail **responsabileprotezionedati@uniroma1.it**.

I responsabili esterni del trattamento devono, allo stesso modo, informare con urgenza immediata, il Responsabile della protezione dei dati, utilizzando l'apposito modello Allegato 1) alla circolare n. 44407 del 25.05.2018 pubblicata sulla pagina *web* https://www.uniroma1.it/it/pagina/settore-privacy nella sezione "Atti Sapienza") da trasmettere esclusivamente all'indirizzo pec **rpd@cert.uniroma1.it**.

15) Che cos'è la profilazione?

La "profilazione" è definita (art 4, n. 4, GDPR) come qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica.

Si effettua una profilazione, ad esempio, con la raccolta di dati personali tramite questionari *online* e la loro successiva elaborazione e suddivisione in gruppi omogenei in base a gusti, interessi e preferenze.

16) Sanzioni previste in caso di inosservanza delle norme del GDPR

Le conseguenze di una violazione delle norme in materia di protezione dei dati personali possono essere di diverso tipo:

- di natura penale: gli illeciti penali, di seguito indicati, sono disciplinati al Capo II del Titolo III, dagli artt. 167 al 172 del Codice *privacy* (trattamento illecito di dati; comunicazione e diffusione illecita di dati personali; acquisizione fraudolenta di dati personali; false attestazioni al Garante; interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante; inosservanza di provvedimenti del Garante; violazioni in materia di controlli a distanza dei lavoratori) e dal codice penale (interferenze illecite nella vita privata, art. 615 bis c.p.);
- di natura civile: l'omissione di idonee misure determina un obbligo risarcitorio ai sensi dell'art. 2050 c.c. (art. 15 del D.lgs n. 196/2003);
- di natura amministrativa e pecuniaria (art. 83 GDPR): il Regolamento europeo suddivide le violazioni della *privacy* in due categorie:

1) di tipo meno grave, prevede un'ammenda fino a 10 milioni di euro, o una sanzione amministrativa fino al 2 % del fatturato mondiale dell'impresa (intesa come gruppo). Rientrano in questa categoria le violazioni relative alle modalità di esecuzione del trattamento dei dati prescritte dal GDPR, ad esempio, la mancanza del registro del trattamento del Titolare o del Responsabile, l'omessa notifica di *data breach*, ecc.

2) di tipo più grave, prevede una multa fino a 20 milioni di euro, o una sanzione amministrativa fino al 4% del fatturato mondiale dell'impresa (intesa come gruppo). Rientrano in questa categoria le violazioni ai principi generali stabiliti dal GDPR, ad esempio, la mancanza del consenso al trattamento, la violazione dei diritti dell'interessato, ecc.

Il GDPR non indica un importo minimo delle sanzioni, ma stabilisce dei criteri per cui la sanzione deve essere effettiva, dissuasiva e proporzionata. Il Regolamento stabilisce poi come calcolare l'importo della sanzione, in base a:

- gravità del danno;
- dolo o colpa del titolare o del responsabile nel commettere l'infrazione;
- misure prese dal titolare o dal responsabile per attenuare il danno agli interessati;
- reiterazione dell'illecito;
- combinazione di più violazioni.

In funzione di questi criteri, l'Autorità di controllo valuta caso per caso l'importo della sanzione.

17) Domande più frequenti:

17.1 Si possono pubblicare i voti degli esami degli studenti? Con quali modalità?

Gli esiti delle prove scritte possono essere pubblicati sia mediante affissione nelle apposite bacheche, sia *online* sul sito *web* d'Ateneo a condizione che la predetta pubblicazione avvenga in osservanza dei principi di finalità e di non eccedenza nel trattamento dei dati personali. Quanto sopra in considerazione delle peculiari caratteristiche dello strumento utilizzato (*internet*) che esporrebbe i dati a un maggior rischio di abusi. Di conseguenza si dovranno adottare maggiori misure cautelative (ad esempio, limitando l'accesso alla pagina *web* ai soli studenti e docenti che operano nell'ambito della struttura).

17.2 Si possono registrare le lezioni a distanza?

L'art. 71 *sexies* della legge n. 633 del 1941 e successive modifiche in materia di diritto d'autore prevede che *"1. È consentita la riproduzione privata di fonogrammi e videogrammi su qualsiasi supporto, effettuata da una persona fisica per uso esclusivamente personale, purché senza scopo di lucro e senza fini direttamente o indirettamente commerciali […] 4. […] i titolari dei diritti sono tenuti a consentire che […] la persona fisica che abbia acquisito il possesso legittimo di esemplari dell'opera o del materiale protetto, ovvero vi abbia avuto accesso legittimo, possa effettuare una copia privata, anche solo analogica, per uso personale, a condizione che tale possibilità non sia in contrasto con lo sfruttamento normale dell'opera o degli altri materiali e non arrechi ingiustificato pregiudizio ai titolari dei diritti".* In base alla *ratio* sottesa alla norma, non appare sussistere alcun divieto circa l'effettuazione di una registrazione della lezione orale per fini di studio, ripasso o approfondimento individuale dello studente.

Le disposizioni normative, pongono, invece, diversi vincoli laddove lo studente intendesse trarre un lucro dalla propria registrazione stanti i diritti di esclusiva spettanti all'autore dell'opera in relazione alla sua comunicazione e distribuzione al pubblico.

Anche dal punto di vista della *privacy*, la sola registrazione della lezione, anche senza il consenso del docente non costituisce violazione dei suoi diritti, a meno che lo studente non comunichi a terzi o diffonda tale registrazione audio/video. Infatti, l'azione dello studente è da ricondursi nell'alveo delle ipotesi contemplate dall'articolo 2, par. 2, lett. c), del GDPR, ovverosia al trattamento di dati personali effettuato da una persona fisica "*per l'esercizio di attività a carattere esclusivamente personale o domestico*", come tale non ricadente nell'ambito di applicazione materiale del GDPR medesimo. Il consenso dovrà essere richiesto dallo studente per gli utilizzi ulteriori della registrazione. A tal proposito, anche il Garante per la protezione dei dati personali, nelle Linee guida sulla scuola, ha affermato che: "*È lecito registrare la lezione per scopi personali, ad esempio per motivi di studio individuale, compatibilmente con le specifiche disposizioni scolastiche al riguardo. Per ogni altro utilizzo o eventuale diffusione, anche su Internet, è necessario prima informare le persone coinvolte*

nella registrazione (professori, studenti) e ottenere il loro consenso" (Garante per la protezione dei dati personali, *FAQ Scuola e Privacy*).

17.3. È obbligatorio tenere attiva la webcam durante le lezioni a distanza?

Per far fronte alla diffusione del virus Covid -19, le istituzioni universitarie si sono adeguate alle misure varate dal Governo per contrastare e contenere la pandemia. Tra le varie misure, è stata introdotta, anche nell'ambito di Sapienza, la didattica a distanza che permette ai docenti e agli studenti di proseguire il percorso di formazione attraverso le video lezioni, mediante l'ausilio di *internet* e di apparecchiature informatiche.

Dal punto di vista tecnico – informatico, è possibile partecipare alla video lezione tenendo attiva la *webcam* e l'audio, oppure escludendo la *webcam* e lasciando attivo solo l'audio.

In linea generale, la *webcam* è uno strumento potenzialmente idoneo a pregiudicare il diritto alla tutela vita privata degli utenti. Tale diritto, la cui eventuale violazione dovrebbe essere accertata in relazione al contesto e alle circostanze del caso concreto, comprende situazioni di natura intima (ad es. l'abitazione), informazioni riservate e sensibili, informazioni che potrebbero pregiudicare la percezione del pubblico nei confronti di un individuo e perfino aspetti della vita professionale.

Pertanto, in linea generale, non può ritenersi sussistere l'obbligo di tenere attiva la *webcam* durante le lezioni a distanza. L'applicazione di tale principio però non deve prescindere dalla ulteriore e necessaria considerazione che soprattutto nella distanza a distanza, nella quale i docenti e gli studenti sono fisicamente lontani, il loro confronto diretto rappresenta un importante stimolo per l'apprendimento degli studenti.