Sapienza Università di Roma

Piano di Adeguamento al Regolamento Europeo 679/2016 - GDPR

Piano privacy

A cura di:

Area Affari istituzionali (ARAI)

Ha collaborato alla stesura del documento

Il Responsabile della protezione dei dati (DPO):

Dott. Andrea Putignani

Sommario

1. Premessa 5
1.1 Scopo del Piano 5
1.2 Ambiti Considerati 5

2. Il nuovo Regolamento UE 679/2016 (GDPR) 5
2.1 Iter di attuazione 5
2.2 Cosa cambia con il GDPR 6
2.3 Ambito di territorialità 6
2.4 Mutata Responsabilità del Titolare e dei Responsabili/Designati del trattamento 6
2.5 Rafforzamento delle tutele riservate all'Interessato 7
2.6 Diritti dell'Interessato 9
2.7 Sintesi delle principali novità 12

3. I soggetti del trattamento 13
3.1 I soggetti del trattamento 13
3.2 ConTitolare 14
3.3 Responsabile (Esterno) del trattamento 14
3.4 Soggetti autorizzati: Designati, Incaricati 16
3.5 DPO – Responsabile della protezione dei dati 17
3.6 Destinatario 18
3.7 Interessato 18
3.8 L'Università quale responsabile del trattamento dati 19
3.9 Autorità di controllo e Comitato Europeo 19
3.10 Finalità Istituzionali di Sapienza Università di Roma 19

4. Mappa dei trattamenti dei dati personali 20
4.1 Premesse inerenti i trattamenti di dati personali in ambito universitario 20

5. Analisi di impatto sulla protezione dei dati (DPIA) e analisi del rischio 21
5.1 Introduzione 21
5.2 Descrizione delle fasi di processo di DPIA 21

6. Trasferimento di dati personali all'estero 22

7. Ricerca scientifica e statistica 22
7.1 Premessa 22
7.2 Finalità e ambito applicativo 23
7.3 Presupposti dei trattamenti 23
7.4 Progetto di ricerca 23
7.5 Raccolta dei dati 25
7.6 Elaborazione dei dati a fini di ricerca statistica o scientifica 26
7.7 Conservazione dei dati a fini di ricerca statistica o scientifica 26
7.8 Trasferimento dei dati all'estero 27
7.9 Diffusione dei dati a fini di ricerca statistica o scientifica 27

8. Definizione delle priorità e relative azioni organizzative e tecniche..... 28
8.1 Formazione..... 28
8.2 Organizzazione funzionale e interna..... 28
8.3 Gestione e misura del rischio..... 28
8.4 Gestione ed esecuzione del trattamento..... 29
8.5 Metodo e applicazione della protezione fin falla progettazione per impostazione predefinita..... 29
8.6 Informative e misure di tutela (art. 3; artt. 12-14; artt. 24-25; art. 30; art. 32; artt.33-34)..... 29
8.7 Controllo sull'affidamento del trattamento a Responsabili Esterni. Contratto/atto giuridico e RGPD..... 31
8.8 Regolamentazione interna - Codici di Condotta di cui all'art. 40 del RGPD..... 31
8.9 Interventi di mantenimento. Azioni di revisione e miglioramento..... 31
8.10 Azioni da intraprendere 32

ALLEGATI:

Allegato 1 - Data Breach

Allegato 2 - Modelli di informativa

Allegato 3 - Informativa per il trattamento di dati sensibili in un progetto di ricerca

Allegato 4 - Informativa sul trattamento dei dati personali, particolari e genetici

Allegato 5 - Informativa sul trattamento dei dati personali e particolari

Allegato 6 - Mappa dei trattamenti

Allegato 7 - Descrizione delle fasi della DPIA

Allegato 8 - Trasferimento di dati personali all'estero

Allegato 9 - Scheda progetto di ricerca

Allegato 10 - Indicazioni per il contemperamento tra disposizioni sulla "trasparenza" e disposizioni sulla protezione dei dati personali

1. Premessa

1.1 Scopo del Piano

Finalità del presente Piano è fornire indicazioni e raccomandazioni riguardo alle operazioni di trattamento effettuate con dati personali nell'ambito di Sapienza Università di Roma. Il Piano è suscettibile di periodico aggiornamento, nel quale si tiene conto anche di precedenti decisioni del Garante per la protezione dei dati personali e delle pregresse esperienze degli Atenei italiani sulla materia.
Il documento ha un taglio pratico in modo da:

- trovare risposte concrete alle problematiche più comuni di fronte alle quali possono trovarsi gli operatori di Sapienza;
- far acquisire consapevolezza di alcune criticità non del tutto ovvie ed evidenti;
- condividere le scelte individuate per risolvere le criticità rilevate.

Si è ritenuto importante:

- ✓ partire "dall'alto", evidenziando i vincoli ed i presupposti della nuova normativa;
- ✓ prendere spunto "dal basso", individuando i casi critici per esemplificare l'applicazione delle norme (evidenziando cosa cambia).

1.2 Ambiti considerati

Il Piano, dopo aver illustrato i principi fondamentali del trattamento dei dati personali e della protezione degli stessi (base giuridica e vincoli di liceità) nel paragrafo 2, segnala le principali novità introdotte e una prima analisi sull'applicazione del GDPR in Sapienza.
Sull'argomento, al paragrafo 3 viene evidenziata la mutata configurazione dei soggetti coinvolti nel trattamento, atteso che il novellato regolatorio attiene proprio alla mutata Responsabilità del Titolare e dei Responsabili, incentrata sulla positivizzazione e sul rafforzamento del principio di accountability.
In riscontro al taglio pratico del Piano, nel paragrafo 4 vengono mappati i trattamenti di dati personali più importanti distinguendo quelli di carattere istituzionale e quelli ad essi strumentali e trasversali.
Nel paragrafo 6 è stato previsto un focus sui trattamenti di dati personali svolti nell'ambito di progetti di ricerca.

2. Il nuovo Regolamento UE 679/2016 (GDPR)

2.1 Iter di attuazione

Il nuovo Regolamento Europeo - Regolamento (UE) 2016/679 del Parlamento Europeo, di seguito GDPR, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati è stato pubblicato sulla G.U.U.E. del 4 maggio 2016.
Il GDPR è stato approvato il 27 aprile 2016, entrato in vigore il 25 maggio dello stesso anno ed ha piena attuazione dal 25 Maggio 2018.
In Italia, il previgente D. Lgs. n. 196/2003 "*Codice in materia di protezione dei dati personali*", è stato modificato dal D. Lgs. n. 101 del 10.08.2018, recante disposizioni per l'adeguamento dell'ordinamento al Regolamento UE.

2.2 Cosa cambia con il GDPR

Il GDPR consacra il diritto alla protezione dei dati personali come diritto fondamentale e costituzionale, configurandolo come diritto all'autodeterminazione informativa.
Il GDPR, inoltre, traccia il passaggio da un diritto alla protezione dei dati personali di tipo nazionale/individuale ad un diritto di tipo europeo/sociale.
In generale il GDPR:

- muta l'approccio regolatorio da "formale e re-attivo" in "sostanziale e pro-attivo": il trattamento e la protezione dei dati personali evolvono nell'acquisire una propria e autonoma rilevanza all'interno dei processi organizzativi e gestionali dell'ente;
- consolida i diritti azionabili dall'Interessato per il controllo delle proprie informazioni e l'esercizio dell'autodeterminazione (diritto ad accesso, rettifica, cancellazione, limitazione, revoca e opposizione); ne rafforza altri, in primis la disciplina del consenso del quale introduce un vera e propria definizione dell'istituto del consenso esplicito, e della trasparenza rispetto alla quale perfeziona il catalogo delle informazioni da esporre nell'informativa; introduce nuovi diritti (diritto alla portabilità, all'oblio, all'opposizione verso il trattamento di profilazione);
- positivizza il principio di accountability con la finalità di porre chi tratta i dati personali in condizione di ridurre i rischi di operazioni non conformi o non consentite;
- incoraggia meccanismi di certificazione; amplia il sistema di vigilanza; rafforza quello sanzionatorio sia nelle specifiche comuni che nelle misure applicative.

I principali fattori di novità sono riportati nei paragrafi che seguono, in corrispondenza dei quali sono indicati esempi ed implicazioni nell'ambito dell'Ateneo.

2.3 Ambito di territorialità

Il GDPR (considerando da 14 a 27, articolo 3) supera il criterio dello "stabilimento" e si applica al trattamento dei dati personali da parte di Titolari anche non stabiliti nel territorio dell'Unione, purché il trattamento riguardi l'offerta di beni, servizi o il monitoraggio del comportamento del soggetto Interessato aventi luogo nell'Unione.

Effetto pratico in ambito universitario – casi esemplificativi
Esempio 1: nell'ambito di attività di ricerca, un'università partner americana che effettua il monitoraggio del comportamento di una persona italiana, studiando come si muove all'interno di un sito di e-commerce, dovrà trattare il dato nel rispetto del GDPR.

2.4 Mutata Responsabilità del Titolare e dei Responsabili del trattamento

Al Titolare e ai Responsabili del trattamento si affianca una nuova figura obbligatoria per le pubbliche amministrazioni: il Responsabile della protezione dei dati personali (c.d. "Data Protection Officer", di seguito "DPO").
Prioritariamente rientrano tra le Responsabilità del Titolare e dei Responsabili: l'attuazione delle prassi di privacy by design/default, la valutazione d'impatto, la definizione e il mantenimento delle procedure di sicurezza e valutazione dei rischi, la tenuta dei rispettivi registri delle attività di trattamento, la valutazione prudenziale sulla violazione dei dati personali, del coefficiente di gravità e delle relative ricadute sul soggetto Interessato.
In dettaglio, ruolo e obblighi del Titolare e dei Responsabili sono descritti al successivo paragrafo 3.

2.5 Rafforzamento delle tutele riservate all'Interessato

Nel GDPR è rafforzata l'introduzione delle misure di sicurezza e delle misure di tutela e garanzia dell'Interessato nel trattamento dei suoi dati, sin dalla progettazione degli strumenti utilizzati. In particolare, sono previsti i seguenti obblighi:

"*Privacy by design" - considerando 78), articolo 25 comma 1 GDPR*
Attiene alle buone prassi di protezione dei dati personali sin dalla progettazione del trattamento. Le misure strumentali a tale scopo sono:

- la migliore applicazione del principio di minimizzazione dei dati personali oggetto del trattamento con riferimento tanto alla quantità dei dati, tanto ai tempi di conservazione e ai livelli di accessibilità, tanto alle prefissate finalità;
- la pseudonimizzazione ovvero l'oscuramento (reversibile) dei dati identificativi del soggetto Interessato;
- la definizione di dati personali e tempi strettamente necessari al trattamento, in relazione alle diverse finalità.

Effetto pratico in ambito universitario – casi esemplificativi
Esempio 1: nell'ambito di una procedura concorsuale per l'accesso a corsi di studi, l'Università è tenuta a chiedere solo i dati necessari all'espletamento del concorso, coerenti e pertinenti allo status di "non studente" del partecipante; dovrà quindi astenersi dalla richiesta di informazioni che sarebbero utili solo nel caso di successiva immatricolazione (ad esempio non possono essere richiesti la foto personale o l'Iban già in fase di iscrizione al test). *Esempio 2*: nel caso in cui debba essere comunicato agli Interessati di recarsi in una o più aule nell'ambito di una prova concorsuale o per una lezione, soprattutto nell'eventualità in cui tale comunicazione sia pubblicata su internet, l'associazione "aula-candidati" dovrebbe essere pseudonimizzata indicando solo un id-numerico (ad esempio una "pre-matricola") o anonimizzata implementando l'associazione aula-candidati per aggregazione alfabetica. *Esempio 3*: con riferimento ai procedimenti attinenti il controllo della contribuzione dello studente, prevedere il trattamento di dati personali strettamente ricadenti nei termini temporali indicati dalla norma in materia (dichiarazione ISEE per l'Università - DPCM 9 aprile 2001).

"Privacy by default" - considerando 78), articolo 25 comma 2 GDPR
Sapienza pone in atto misure organizzative adeguate per garantire che siano trattati, per impostazione predefinita (di default), solo i dati personali necessari per ogni specifica finalità del trattamento (che non risultino pertanto eccedenti rispetto al ruolo del soggetto che li tratta).

Valutazione di impatto (DPIA) - considerando da 89 a 96, articolo 35, 36 GDPR
La valutazione d'impatto precede il trattamento ed è volta a compensare particolari probabilità e gravità di rischio.
Viene richiesta per trattamenti su larga scala, con incidenza su un vasto numero di Interessati, con un elevato rischio connesso all'introduzione di nuove o particolari tecnologie, all'implementazione di trattamenti di profilazione o di sorveglianza o all'utilizzo di particolari dati (biometrici o giudiziari).
Il Garante per la protezione dei dati personali redige e pubblica l'elenco di tipologie di trattamenti obbligatoriamente soggetti a preventiva valutazione di impatto.

La valutazione di impatto deve contenere almeno:

- una descrizione sistematica dei trattamenti previsti, delle finalità e l'eventuale ricorrenza di un legittimo interesse;
- la valutazione sulla necessità e la proporzionalità dei trattamenti rispetto alle predefinite finalità;
- la valutazione dei rischi per i diritti e le libertà degli Interessati;
- le previste misure organizzative e tecniche (comprese quelle di sicurezza) e ogni meccanismo ritenuto utile per la tutela dei diritti dei soggetti Interessati.

Si rende necessaria in caso di drastica revisione tecnologica, per i trattamenti di larga scala, e per i trattamenti espressamente indicati dall'Autorità di controllo.
Si rimanda in merito al paragrafo 5.

Effetto pratico in ambito universitario e casi esemplificativi
Esempi in cui potrebbe essere opportuno condurre una DPIA: *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'abbondono 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.

Sicurezza e valutazione dei rischi - considerando 83, 84, articolo 32 GDPR
Il GDPR prevede misure di sicurezza idonee da adottare in relazione alla valutazione dei rischi.
Le misure vanno contemperate allo stato dell'arte, ai costi di attuazione, alla natura, al contesto e alla finalità di trattamento.

Violazione dei dati personali e relativa notifica - considerando da 85 a 88, articolo 4, 33, 34 GDPR
Il regolamento declina la violazione dei dati personali affiancando alla tradizionale componente dolosa quella accidentale, prevedendo pari implicazioni con riferimento all'obbligo di comunicazione all'Autorità Garante.
La violazione del dato personale viene definita come "la 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".
Sapienza comunica al Garante l'avvenuta violazione dei dati personali trattati entro e non oltre 72 ore dall'acquisizione della conoscenza dell'accadimento descrivendone la natura della violazione, le categorie e il numero approssimativo degli Interessati e del numero di registrazioni dei dati personali in questione; i dati di contatto del DPO; le probabili conseguenze della violazione; le misure adottate o che si intendono adottare per rimediare la violazione o attenuarne gli effetti negativi.
I Responsabili ai sensi dell'articolo 28 del GDPR, informano il Titolare nel caso di avvenuta violazione dei dati personali.
Oltre alla comunicazione al Garante, la violazione deve essere comunicata anche all'Interessato se è suscettibile di elevati rischi per i diritti e le libertà dell0 stesso (articolo 34 del GDPR).
Le attività prioritarie per tale adempimento sono riportate in Allegato 1 al presente Piano.

Introduzione dei registri delle attività di trattamento – considerando 82, articolo 30 GDPR
Il Titolare e i Responsabili del trattamento hanno i rispettivi registri delle attività.
Il registro del Titolare contiene i riferimenti di contatto del Titolare e del DPO; le finalità; la descrizione degli Interessati e dei destinatari; la categoria dei dati personali trattati; la presenza di trasferimenti di dati verso un Paese Terzo o un'organizzazione internazionale unitamente alla documentazione sulle appropriate garanzie; la tempistica della cancellazione dei dati; la descrizione della misure di sicurezza e organizzative adottate.
Il registro dei Responsabili contiene, oltre alle due ultime voci previste ed elencate per il registro del Titolare: i riferimenti di contatto dei Responsabili, del Titolare, del DPO; le categorie dei trattamenti effettuati per conto del Titolare.

Smaltimento di dispositivi e supporti contenenti dati personali
Permane l'obbligo di garantire la protezione dei dati anche mediante un'accurata cancellazione al momento della distruzione dei supporti che li contengono.
Sul tema, si segnala un provvedimento del Garante su "Rifiuti di apparecchiature elettriche ed elettroniche (RAAE) e misure di sicurezza dei dati personali" - 13 ottobre 2008 - G.U. n. 287 del 9 dicembre 2008.

2.6 Diritti dell'Interessato

Consenso – considerando 39 e 42, articolo 6, 7 GDPR
Secondo quanto sancito dall'art. 2-ter del D.Lgs. n. 196/2003, segnatamente al comma 1, la base giuridica prevista per il trattamento di dati personali, effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri (art. 6, paragrafo 3, lettera b) del GDPR), trova fondamento esclusivamente in una norma di legge o, nei casi previsti dalla legge, di regolamento.
Va, in proposito, tenuto conto anche della circostanza che il considerando 43 del GDPR prevede che "per assicurare la libertà di espressione del consenso, è opportuno che il consenso stesso non costituisca un valido presupposto per il trattamento dei dati personali in un caso specifico qualora esista un evidente squilibrio tra l'interessato e il Titolare del trattamento specie quando il Titolare del trattamento è un'autorità pubblica e ciò rende pertanto improbabile che il consenso sia stato espresso liberamente in tutte le circostanze di tale situazione specifica".
Ove si ritenga però di avvalersi della base giuridica consensuale ai fini del trattamento di dati personali, il consenso in generale deve essere: libero, specifico, informato e inequivocabile; non è ammesso il consenso tacito o presunto.
Deve essere reso e manifestato attraverso dichiarazione o azione positiva inequivocabile e concludente (come la selezione di un'apposita casella in un sito web, la scelta di specifiche impostazioni tecniche o qualsiasi altra dichiarazione o comportamento che indichi chiaramente la volontà dell'Interessato di accettare il trattamento proposto).

Informativa – considerando da 58 a 73, articolo 12, 13, 14 GDPR
Il Titolare del trattamento è tenuto a fornire l'informativa all'Interessato, indipendentemente dall'obbligo di acquisire il consenso, salvo il caso in cui l'Interessato sia già in possesso delle informazioni (articolo 13, comma 4 del GDPR) o in altri casi particolari descritti nel GDPR (articolo 14, comma 5).

Contenuti dell'informativa
Sapienza informa il soggetto Interessato in merito a:
- l'identità e i dati di contatto del Titolare del trattamento e del DPO;

- le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento ed i legittimi interessi perseguiti dal Titolare del trattamento o da terzi (qualora sia basato sull'articolo 6, paragrafo 1, lettera f) del GDPR);
- gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali e, nel caso in cui i dati personali non siano raccolti presso l'Interessato, anche le categorie di dati trattati e le relative fonti di provenienza;
- l'eventuale intenzione del Titolare del trattamento di trasferire dati personali a un paese terzo o ad un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso di trasferimenti di cui all'articolo 46 e 47, o all'articolo 49, comma 2, del GDPR il riferimento alle garanzie adeguate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stai resi disponibili;
- il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- i diritti azionabili dall'Interessato comprendenti: l'accesso ai dati personali, la rettifica o la cancellazione degli stessi, la limitazione del trattamento o l'opposizione; oltre al diritto alla portabilità dei dati; la revoca del consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca; il diritto di proporre reclamo a un'autorità di controllo;
- la necessità di comunicare i dati personali in base a un obbligo legale o contrattuale oppure se si tratta di un requisito necessario per la conclusione di un contratto, nonché la natura obbligatoria o facoltativa del conferimento, nonché le possibili conseguenze della mancata comunicazione di tali dati;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione e, almeno in tali casi, informazioni significative circa la logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'Interessato.

Al riguardo si segnalano alcuni punti di attenzione.
L'eventuale trasferimento di dati in un paese terzo (ad esempio nel caso di utilizzo di servizi in cloud); anche per tali servizi è responsabilità di Sapienza garantire la sicurezza dei dati e le modalità di accesso da parte dell'Interessato.
Rispetto alla normativa previgente, occorrerà garantire – in specifici casi - la limitazione del trattamento dati e la portabilità dei dati.
La necessità di indicare eventuali processi automatici di profilazione e le conseguenze per l'Interessato di tale trattamento dati.
Si precisa che nel caso in cui i dati siano raccolti presso l'Interessato, se Sapienza intende trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento, dovrà fornire all'Interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente.
Il GDPR contiene inoltre indicazioni specifiche per i casi nei quali i dati non siano stati ottenuti presso l'Interessato: in tal caso, oltre alle informazioni richieste nell'informativa all'articolo 13, sarà necessario indicare la fonte da cui hanno origine i dati personali e se si tratta di una fonte di pubblico accesso.

Caratteristiche dell'informativa
Il GDPR specifica in dettaglio le caratteristiche espositive dell'informativa, che deve avere forma concisa, trasparente, intelligibile per l'Interessato e facilmente accessibile; veicolata da un linguaggio chiaro e semplice, soprattutto nel caso in cui gli interessati siano minori.

Indicazioni pratiche per la stesura dell'informativa
Dal punto di vista pratico, tenendo conto delle indicazioni di cui sopra, si individuano le seguenti linee guida.

- Articolare l'informativa su più livelli, per garantire che:
  - le informazioni di base siano subito presentate all'Interessato e risultino di immediata lettura e comprensione;
  - maggiori dettagli siano consultabili dagli Interessati scegliendo sezioni di approfondimento.
- Per agevolare la consultazione l'informativa può essere articolata sulla base dei profili degli utenti, prevedendo ad esempio contenuti specifici per le differenti categorie (studenti, personale docente, personale tecnico - ammnistrativo), ciascuna potenzialmente caratterizzata da differenti trattamenti dei dati personali.
- Garantire che l'informativa descriva non solo i trattamenti di dati personali visualizzabili dall'utente mediante gli applicativi software (sicuramente più vicini alla percezione dell'utente) ma anche quelli trattati per attività connesse all'erogazione dei servizi informatici, effettuati dai sistemi e spesso non direttamente visibili agli utenti.
- Garantire che nel suo complesso l'informativa fornita agli Interessati soddisfi i requisiti di completezza previsti dalla normativa.
- Per i trattamenti che presentano un alto profilo di rischio per le libertà dell'Interessato, è opportuno tenere traccia esplicita dell'avvenuta consultazione dell'informativa da parte degli utenti ed eventualmente dare evidenza delle modifiche intervenute sulla stessa nel caso di cambiamenti.

Per agevolare la stesura dell'informativa, si riportano negli Allegati da 2 a 5 informazioni aggiuntive ed esempi.

Diritti "tradizionali" – considerando da 58 a 73, articoli dal 12 al 17 GDPR
In ordine ai diritti di accesso, rettifica, cancellazione e opposizione al trattamento, il nuovo GDPR prevede che:

- il riscontro deve essere fornito senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste. Nel caso di diniego, il riscontro deve essere fornito al più tardi entro un mese dal ricevimento della richiesta;
- la possibile definizione da parte del Titolare di eventuali oneri sull'Interessato nei casi particolari previsti nell'articolo 12, comma 5.

Si precisa inoltre che la risposta fornita all'Interessato non deve essere solo "intelligibile", ma anche concisa, trasparente e facilmente accessibile, oltre a utilizzare un linguaggio semplice e chiaro.

"Nuovi Diritti": diritto di limitazione; diritto di opposizione alla profilazione; diritto alla cancellazione/all'oblio; diritto alla portabilità, articolo 18, 20, 21, 22 GDPR
Il diritto alla limitazione rappresenta un diritto diverso e più esteso rispetto al "blocco" del trattamento già previsto dal codice, in particolare, è esercitabile non solo in caso di violazione dei presupposti di liceità del trattamento e quale alternativa alla cancellazione dei dati stessi, bensì anche nelle more che sia riscontrata da parte del Titolare una richiesta di rettifica dei dati o di opposizione al trattamento.

In condizioni di limitazione e con la sola eccezione della conservazione, ogni altro trattamento del dato è consentito solo in presenza del consenso dell'Interessato, o dell'accertamento di diritti in sede giudiziaria, di tutela di diritti di altra persona fisica o giuridica, o in presenza di un interesse pubblico rilevante.
Il diritto di opposizione alla profilazione riconosce all'Interessato il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare (legata ad esempio al proprio rendimento professionale o alla propria situazione economica, di salute, ecc.), al trattamento dei dati personali che lo riguardano. In tal caso Sapienza si astiene dal trattare ulteriormente i dati personali salvo che dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'Interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.
Il diritto "all'oblio" si configura come un diritto alla cancellazione dei propri dati personali in forma rafforzata nel caso questi siano stati resi pubblici on-line.
Inoltre l'Interessato ha il diritto di chiedere la cancellazione dei propri dati, per esempio, anche dopo revoca del consenso al trattamento.
Il diritto alla portabilità 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 a Sapienza; fanno eccezione quindi i dati il cui trattamento si fonda sull'interesse pubblico o sull'interesse legittimo di Sapienza.
Per tale ragione le implicazioni del Diritto di Portabilità dovrebbero solo residualmente interessare i trattamenti dei dati personali in ambito dell'Ateneo.

2.7 Sintesi delle principali novità

Le principali novità sono sintetizzate per parole chiave nelle seguenti tabelle.

Consenso	Libero, specifico, informato, inequivocabile e concludente.
Informativa	Informazioni di contatto del Titolare e del DPO; indicazione della finalità di trattamento; destinatari e categorie di dati trattati; trasferimento dati personali in paesi terzi; diritti azionabili e implicazioni; ricorrenza di altre basi giuridiche diverse dal consenso.
Valutazione di impatto (DPIA)	Ripensamento delle tecnologie a supporto dei trattamenti. Analisi e eventuale consultazione preventiva con il Garante per le implicazioni sui diritti e le libertà delle persone.
Sicurezza	Analisi dei rischi e di valutazione dell'adeguatezza delle misure tecniche e organizzative.
Violazione dei dati	Equiparazione della fattispecie accidentale con quella dolosa quanto agli obblighi di comunicazione all'Autorità garante.
Privacy by Design **Privacy by Default**	Applicazione delle tutele di trattamento sin dalla sua progettazione e avvio. Pseudonimizzazione e Minimizzazione (di dati e tempi).
DPO	Si interfaccia con le Autorità Garanti. Supporta Titolare e Responsabili del trattamento.
Registro Trattamenti	Registri di competenze in cui indicare le caratteristiche, le modalità e le finalità del trattamento. Lo redigono il Titolare e i Responsabili del trattamento.
Sanzioni	**Sanzioni amministrative pecuniarie fino a 20.000.000 EURO (fino al 4% del fatturato globale annuo dell'esercizio precedente).**
Autorità (o Autorità Garante)	Comitato di controllo europeo: assicura la uniforme applicazione del Regolamento. Autorità di Controllo: autorità pubblica indipendente di uno Stato membro (in Italia, il Garante per la protezione dei dati personali).

IN MERITO AI NUOVI DIRITTI	
Profilazione	L'Interessato ha il diritto di non subire trattamenti automatizzati (profilazione) di cui non è consapevole.
Portabilità dei dati	L'Interessato ha il diritto di ottenere la restituzione dei propri dati personali trattatati da un Titolare e di trasmetterli ad altri.
Oblio	L'Interessato ha diritto alla de-indicizzazione o alla cancellazione delle informazioni che lo riguardano.
Sportello Unico	Unicità dell'interlocutore territoriale. Semplificazione e uniformità di gestione nell'applicazione del nuovo regolamento.

3. I soggetti del trattamento

Nell'ambito di Sapienza la distribuzione dei ruoli e delle Responsabilità costituisce una misura di sicurezza essenziale per l'applicazione del GDPR.
Il GDPR individua, infatti, i soggetti coinvolti nel trattamento.

3.1 Titolare del trattamento

Il Titolare è definito all'articolo 4 del GDPR come "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali".
Pertanto il Titolare non viene designato o nominato ma diventa tale al momento che raccoglie dati personali con l'intento di trattarli per finalità lecite, come previsto all'articolo 6, e decide le modalità di trattamento.

Soggetto del trattamento	Titolare (Controller). Il soggetto che raccoglie i dati per il conseguimento di un fine dichiarato e dispone dei mezzi per il loro trattamento.
Persona giuridica/fisica	Sapienza Università di Roma
Carica/persona fisica	Rappresentante legale dell'Ente: il Rettore dell'Ateneo
Descrizione	Il Titolare applica la normativa in materia di protezione dei dati personali mettendo in atto tutte le misure tecniche ed organizzative per la distribuzione degli incarichi e delle responsabilità al suo interno; utilizza gli strumenti di governo interno previsti dalla Legge, dallo Statuto e dai Regolamenti dell'Ateneo.
Informazioni per l'Interessato	Il Titolare e il suo rappresentante legale devono essere resi noti all'Interessato.
Note	Titolare del trattamento è l'Università nel suo complesso (non può essere infatti una persona fisica ed è individuata già nel Regolamento come "l'autorità pubblica" che determina le finalità e i mezzi del trattamento), il cui rappresentante legale è il Rettore.

3.2 ConTitolare

Soggetto del trattamento	ConTitolare (Joint Controller)
Persona giuridica/fisica	Può essere sia persona giuridica che fisica
Carica/persona fisica	Rappresentante legale / persona fisica
Descrizione	Il soggetto terzo che condivide le decisioni sulle finalità per le quali trattare i dati e che contribuisce a definire le modalità di trattamento. E' il soggetto che insieme all'Ateneo collabora al raggiungimento di finalità condivise.
Informazioni per l'Interessato	Il contenuto essenziale dell'accordo stipulato fra i Contitolari deve essere reso noto all'Interessato. Questi può esercitare i propri diritti nei confronti di ogni ConTitolare.
Note	Se le finalità e i mezzi del trattamento sono individuati "insieme ad altri", i soggetti che decidono finalità e modalità di trattamento sono "Contitolari".
Esempi di Contitolarità	Può esserci Contitolarità: • nell'ambito di un trattamento svolto a fini di ricerca da due partner che decidono insieme le modalità e i mezzi del trattamento; • nell'ambito di una gestione unificata dei servizi e dei sistemi bibliotecari universitari, comunali e provinciali.

3.3 Responsabile Esterno del trattamento

Sapienza, quale Titolare, mantiene al proprio interno una distribuzione delle Responsabilità rispetto al trattamento dati, "istruendo" opportunamente le persone che dirigono strutture interne, affinché si facciano carico dell'applicazione del GDPR nel proprio ambito, collaborando con il Titolare e con il DPO.

La definizione dell'organizzazione interna finalizzata all'attuazione e al controllo efficace delle misure adottate per la protezione dei dati da parte del Titolare è infatti un elemento fondamentale per poter dimostrare che il trattamento è effettuato conformemente al GDPR.

Ai fini dell'applicazione di tale disposizione, nell'ambito universitario, risulta utile distinguere fra la funzione di "Responsabile Esterno del trattamento", così come definita all'articolo 28 del GDPR, assegnata a un soggetto esterno che esegue trattamenti per conto dell'Università e la funzione di Responsabile Interno (Designato), assegnata a personale che ricopre funzioni di particolare rilievo organizzativo (Direttori di Dipartimento, Presidi di Facoltà, Direttori di Centri, Direttori delle Aree amministrative).

Il Responsabile Esterno agisce come persona giuridica/fisica autonoma, mentre il Designato agisce per conto del Titolare all'interno dell'Università sulla base delle competenze attribuite alla funzione organizzativa o carica istituzionale che ricopre.

Il Responsabile Esterno del trattamento sarà quindi sempre un soggetto esterno all'Università, mentre il Designato sarà un soggetto interno, opportunamente "istruito" dal Titolare riguardo alle competenze anche decisionali in materia di protezione dei dati.

Soggetto del trattamento	Responsabile Esterno del trattamento dati (Processor)
Persona giuridica/fisica	Soggetto esterno
Carica/persona fisica	Rappresentante legale/persona fisica
Descrizione	Il Responsabile Esterno del trattamento dati è un soggetto esterno che esegue, in base a 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. Al Responsabile spettano tutti i compiti del Titolare all'interno del proprio organismo (valutazione impatto, registro dei trattamenti, eventuale nomina del proprio DPO, ecc.). Il Responsabile 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. 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.
Informazioni per l'Interessato	Nell'informativa devono essere indicati i destinatari o le categorie di destinatari, anche interni, ai quali sono comunicati i dati per il loro trattamento. Nel caso di trasferimento di dati in un paese terzo è obbligatorio informare di ciò l'Interessato; il Titolare deve verificare che il Responsabile (esterno) assicuri un'adeguata protezione dei dati.
Note	In ambito universitario, è Responsabile Esterno del trattamento il soggetto terzo a cui sono affidati trattamenti per finalità proprie dell'Università. Rientrano in tale categoria per esempio i soggetti che curano applicazioni in outsourcing o in hosting per conto dell'Ateneo. Devono essere predisposte clausole contrattuali che indichino gli ambiti di responsabilità e i compiti assegnati. Il Responsabile Esterno a sua volta deve garantire l'applicazione delle misure necessarie alla protezione dei dati e gli adempimenti previsti dal GDPR. Al punto 5 dell'articolo 28 GDPR è previsto che possono essere considerate garanzie sufficienti per la protezione dei dati l'adesione da parte del Responsabile esterno a codici di condotta o certificazioni approvate secondo quanto stabilito agli artt. 40 e 42 del GDPR. In caso di designazione di un sub-Responsabile, il Responsabile Esterno conserva nei confronti del Titolare del trattamento l'intera Responsabilità dell'adempimento degli obblighi del sub- Responsabile.
Esempi di Responsabili (esterni) del trattamento	Ad esempio CINECA, nel caso di erogazione di servizi applicativi in hosting, si configura come Responsabile esterno del trattamento.

3.4 Soggetti autorizzati: Responsabili Interni (Designati), Incaricati

Nelle linee guida del Garante per la protezione dei dati personali si afferma che “le disposizioni del Codice in materia di incaricati del trattamento sono pienamente compatibili con la struttura e la filosofia del regolamento”, ne consegue che quanto disposto all’articolo 29 del GDPR possa concretizzarsi con l’individuazione dei soggetti autorizzati al trattamento dati all’interno dell’Università, denominati “Designati” e “Incaricati”.
L’art. 2-quaterdecies del Codice come introdotto dal Decreto Legislativo n. 101/2018 prevede ora che “il Titolare o i Designati del trattamento possono prevedere, sotto la propria responsabilità e nell’ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità.
Il Titolare o i Designati del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta.
Nell’organizzazione della Sapienza, la funzione di “Designato” è assegnata a personale che ricopre funzioni di particolare rilievo organizzativo.
Il Designato agisce per conto del Titolare all’interno dell’Università 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).
Gli Incaricati (docenti; personale tecnico-amministrativo e bibliotecario) sono individuati dal Titolare o dal Designato ed operano sotto la loro vigilanza.
È sottolineata l’importanza di “istruire” i soggetti, sono quindi previsti percorsi formativi adeguati per coloro che sono coinvolti nel trattamento dati.

Soggetto del trattamento	Soggetti “istruiti” dal Titolare per trattare dati (person acting under the authority of the controller or of the processor) – Designato, Incaricato
Persona fisica	Soggetto interno/esterno
Carica/persona fisica	Personale dipendente o collaboratori
Descrizione	Nell’organizzazione di Sapienza, la funzione di “Designato” è assegnata a personale che ricopre funzioni di particolare rilievo organizzativo. Il Designato agisce per conto del Titolare all’interno dell’Università 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). Gli Incaricati (docenti; personale tecnico-amministrativo e bibliotecario) sono individuati dal Titolare o dal Designato ed operano sotto la loro vigilanza.
Informazioni per l’Interessato	Nell’informativa sono indicati i destinatari o le categorie di destinatari, anche interni (Designati, Incaricati), ai quali sono comunicati i dati per il loro trattamento.
Note	I soggetti sono autorizzati al trattamento dei dati mediante nomina individuale da parte del Titolare e dei Designati del trattamento dati. L’individuazione dei soggetti autorizzati al trattamento dati è una misura di sicurezza a livello organizzativo adottata da Sapienza. Gli amministratori di sistema sono Incaricati con particolari compiti, mediante nomina individuale.

3.5 DPO – Responsabile della protezione dei dati

Soggetto del trattamento	DPO (Data Protection Officer) – Responsabile della protezione dei dati (RPD), soggetto la cui nomina è obbligatoria per l'Università
Persona giuridica/fisica	Soggetto interno
Carica/persona fisica	Persona fisica con incarico specifico
Descrizione	Il DPO agisce in autonomia (non riceve alcuna istruzione per quanto riguarda l'esecuzione di tali compiti) e funge da collegamento fra il Titolare, i Responsabili, gli Interessati e l'autorità di controllo. I suoi compiti sono chiaramente definiti e gli sono garantiti supporto, risorse e tempi di lavoro adeguati allo svolgimento della sua funzione, nonché una formazione permanente per permettergli di rimanere aggiornato sugli sviluppi nel settore della protezione dei dati. Al DPO è dato ampio accesso alle informazioni e deve essere interpellato per ogni problematica inerente alla protezione dei dati e per ogni attività che implica un trattamento dati, fin dalla sua progettazione. Il DPO ha il compito di coadiuvare il Titolare e i Responsabili nella valutazione d'impatto e nella redazione del Registro dei Trattamenti, oltre che nella sorveglianza del rispetto del GDPR all'interno dell'Ateneo. Informa e fornisce consulenza al Titolare, ai Responsabili e al personale interno coinvolto nel trattamento dati sull'applicazione del GDPR. Si occupa delle comunicazioni con il Garante e con gli Interessati. Nell'assolvimento dei suoi compiti il DPO non può essere penalizzato o rimosso. La Responsabilità di eventuali mancanze è comunque a carico del Titolare e dei Responsabili. Il DPO è facilmente contattabile dal personale interno, dagli Interessati e dall'autorità di controllo; i suoi recapiti sono ampiamente pubblicizzati.
Informazioni per l'Interessato	I recapiti del DPO devono essere forniti all'Interessato nell'informativa.
Note	La figura deve avere ampia autonomia. Sul sito del Garante sono pubblicate le linee guida specifiche per tale figura (http://www.garanteprivacy.it/DPO).

3.6 Destinatario

Il GPDR, all'articolo 4, definisce destinatario "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi". Pertanto, in Sapienza sono destinatari tutti i soggetti che ricevono dati personali, che siano interni (Designato, Incaricato) o esterni, che li ricevano per eseguire trattamenti per conto del Titolare.
I destinatari o le categorie di destinatari ai quali sono comunicati i dati sono definiti in fase di raccolta dei dati e sono inseriti nell'informativa all'Interessato.
Nel caso in cui il destinatario sia un soggetto che risiede in un paese non membro dell'Unione, il Titolare verifica che le garanzie offerte da questi per la protezione dei dati siano adeguate.

Soggetto del trattamento	Destinatario (recipient)
Persona giuridica/fisica	Soggetto interno/esterno, persona fisica, persona giuridica
Carica/persona fisica	Rappresentante legale, persona fisica
Descrizione	Il destinatario è il soggetto al quale sono comunicati i dati personali da parte del Titolare. Nel GDPR il "destinatario" è definito al punto 9) dell'articolo 4 dove si precisa anche che può trattarsi di soggetto terzo o no (la definizione di "terzo" è riportata nel successivo punto 10) dello stesso articolo 4). Devono pertanto considerarsi destinatari anche coloro che trattano i dati su "istruzioni" del Titolare all'interno di Sapienza (Designati, Incaricati).
Informazioni per l'Interessato	Nell'informativa da fornire all'Interessato devono essere indicati i destinatari o le categorie di destinatari ai quali sono comunicati i dati, devono essere elencate anche le strutture interne o le categorie di personale che vengono a conoscenza dei dati personali nello svolgimento della loro attività lavorativa.
Note	Nel caso il destinatario sia un soggetto "terzo" che riceve i dati per perseguire proprie finalità, lo stesso diventerà a sua volta Titolare. Per esempio, l'Università comunica dati personali di studenti a soggetti esterni che svolgono attività di ricerca e selezione di personale per l'inserimento nel mondo del lavoro. Il destinatario che riceve i dati da altro Titolare per perseguire finalità proprie è tenuto a dare l'informativa all'Interessato nel più breve tempo possibile, sempre se l'Interessato non dispone già dell'informazione o nel caso in cui la comunicazione sia necessaria per adempiere a un obbligo di legge.

3.7 Interessato

L'Interessato (data subject) è la persona fisica alla quale si riferiscono i dati trattati.
L'Interessato è sempre una persona fisica.
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.
Per 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, mentre può essere accolta la richiesta di cancellazione dei recapiti personali.
La risposta alle richieste dell'Interessato deve comunque essere tempestiva e, ove non sia possibile soddisfarla, occorre specificare la motivazione del rifiuto.

Nell'ambito di Sapienza si possono individuare le seguenti principali categorie di Interessati, le quali possono poi essere suddivise in sottocategorie per distinguerle all'interno di alcuni trattamenti:

- studenti
- dottorandi
- specializzandi
- personale tecnico-amministrativo
- personale docente
- collaboratori
- assegnisti
- privati cittadini
- clienti e fornitori

3.8 L'Università quale Responsabile del trattamento dati

Sapienza può stipulare contratti o convenzioni con soggetti esterni, nei quali si prevede l'affidamento di compiti specifici all'Università per i quali è previsto un trattamento di dati personali per finalità proprie di un soggetto affidatario (che risulta essere Titolare degli stessi).
In questi casi l'Università sarà designata da tale Titolare esterno quale Responsabile del trattamento dati; pertanto è individuato il Designato che dovrà prevedere le misure di protezione adeguate e mantenere i rapporti con il Titolare esterno per gli adempimenti richiesti.
Un esempio di tali tipi di contratti è quello per attività conto terzi in cui sia chiesta all'Ateneo l'erogazione di un servizio specifico.

3.9 Autorità di controllo e comitato europeo

Le Autorità di controllo sono incaricate di "sorvegliare l'applicazione del GDPR al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento e di agevolare la libera circolazione dei dati personali all'interno dell'Unione" (punto 1, art. 51 del GPDR).
Ogni Stato membro istituisce una o più autorità pubbliche indipendenti.
Nel caso siano più di una deve essere designata quella che le rappresenterà nel Comitato europeo per la protezione dei dati, che ha funzioni di coordinamento delle varie autorità di controllo, per rendere coerenti e in linea con il GDPR le varie decisioni che a queste competono.
Il Comitato ha inoltre funzioni di supporto per la Commissione europea.
All'Autorità di controllo nazionale (per l'Italia, Garante per la protezione dei dati personali) sono comunicati eventuali data breach.
Le Autorità di controllo sono competenti ad accogliere e decidere su eventuali reclami presentati dagli Interessati.

3.10 Finalità istituzionali di Sapienza Università di Roma

Nell'ambito dell'ordinamento italiano Sapienza è soggetto dotato di capacità giuridica pubblica, persegue finalità di interesse generale, opera in regime di diritto amministrativo ed esercita potestà pubbliche; in sintesi è pubblica amministrazione ai sensi dell'art. 1, comma 2 del D. Lgs.165/2001 e ss.mm.ii.
L'università, quale centro istituzionale di formazione culturale e di attività di ricerca scientifica, trova il suo fondamento costituzionale nell'art. 9 Cost. e le sue attribuzioni sono meglio esplicitate nei successivi artt. 33 e 34 Cost.
In attuazione dell'art. 33 Cost. l'Università è dotata di autonomia didattica, scientifica, organizzativa, finanziaria e contabile.
L'attività di Sapienza è disciplinata dal proprio statuto, dai propri regolamenti e dalle norme legislative che vi operano espresso riferimento.
Sapienza opera per il perseguimento dei propri fini istituzionali, prioritariamente individuati nella didattica, nella ricerca e nella Terza missione.
Con riferimento a tali finalità, si riportano, a titolo esemplificativo, attività concernenti il trattamento di dati personali:

- **didattica**: attività volte a garantire il diritto allo studio, orientamento in ingresso e in itinere, attività curriculare, tutorato, programmi di mobilità internazionale ecc.;
- **ricerca**: progetti di ricerca nazionali ed internazionali, redazione di articoli scientifici;
- **terza missione**: trasferimento tecnologico (brevetti, attività per conto terzi - L. 370/1999, spin-off), educazione permanente (formazione sulla popolazione in età lavorativa, organizzazione di conferenze, convegni, ecc.), impegno sociale (Job Placement, assistenza alle startup, ecc.).

4. Mappa dei trattamenti dei dati personali

4.1 Premesse inerenti i trattamenti di dati personali in ambito universitario

Ai fini del presente Piano si è ritenuto opportuno stilare una mappatura dei principali trattamenti che trovano svolgimento in Sapienza con l'obiettivo di:

- consentire di compilare in modo più agevole il registro dei trattamenti;
- individuare le informazioni che devono essere comunicate all'Interessato, con particolare riferimento agli aspetti introdotti nel nuovo GDPR (es: indicazioni sui tempi di conservazione dei dati, finalità indicate in modo specifico), condividendo ove possibile alcune bozze di informative;
- mettere in evidenza alcune peculiarità del trattamento dei dati preso in esame ed eventuali considerazioni in merito ai principali dubbi interpretativi.

La mappatura è, altresì, contestualizzata rispetto alle singole Strutture di Sapienza, al fine di coglierne le peculiarità.

Le tabelle in Allegato 6 costituiscono pertanto una guida adattabile e da aggiornare.

Per ciascuna categoria di Interessati e nell'ambito delle differenti finalità perseguite, sono stati presi in analisi i seguenti aspetti:

Elementi considerati	
Natura dei dati	L'analisi sulla natura dei dati consente di determinare se, e in quale misura, possono essere trattati (come ad esempio: categorie particolari di dati personali di cui all'articolo 9 e/o i dati relativi a condanne penali e reati di cui all'articolo 10).
Quali sono i dati personali strettamente necessari per perseguire la finalità descritta	L'analisi sui tipi di dati che sono strettamente necessari per perseguire un obbligo legale o di quelli strettamente connessi all'esecuzione di compiti istituzionali favorisce la definizione di tempi di conservazione differenti o la previsione di differenti garanzie per l'Interessato.
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	Tenuto conto del GDPR, nonché dell'obbligo di indicare nell'informativa "la base giuridica del trattamento" e "i legittimi interessi perseguiti dal Titolare del trattamento" si ritiene opportuno fornire all'Interessato maggiori dettagli sulle finalità. Sono quindi condivise anche alcune valutazioni in merito all'opportunità di raccogliere un consenso ad hoc per le diverse finalità non connesse a obblighi legali o allo svolgimento di compiti strettamente istituzionali.
Archiviazione e conservazione (tempi, modi, quali dati)	L'informativa deve indicare il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo. Tale informazione è utile anche nell'ambito della redazione dei registri di trattamento: è infatti importante determinare i termini ultimi previsti per la cancellazione delle diverse categorie di dati. I trattamenti possono essere compiuti con o senza l'ausilio di processi automatizzati.

Categorie di Interessati	Le categorie di persone fisiche cui si riferiscono i dati personali, quali, ad esempio: studenti, personale dipendente, collaboratori, fornitori, ospiti.
Categorie di destinatari	È previsto che siano individuate nell'informativa le categorie di destinatari a cui i dati personali possono essere comunicati. Si dovrà quindi dare indicazione di tutte le persone che possono ricevere comunicazione di dati personali (es: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che possono venire a conoscenza dei dati, nonché, il Responsabile del trattamento e le persone autorizzate al trattamento dei dati personali). Nelle schede di trattamento sotto riportate, non sono stati indicati eventuali soggetti esterni che potrebbero trattare i dati in qualità, ad esempio, di amministratori di sistema o di rete o di database, considerato che tale informazione è strettamente connessa all'organizzazione dei singoli Atenei. In relazione ai destinatari, si specifica inoltre che, se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'Interessato ha l'obbligo di fornire i dati personali, occorre chiarire - nell'informativa privacy - le possibili conseguenze della mancata comunicazione dei dati.
Comunicazione e trasferimento all'estero	Occorre chiarire nell'informativa l'intenzione del Titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale. Tale dato è rilevante anche nell'ambito della redazione del registro, pertanto si è ritenuto opportuno effettuare alcune note e approfondimenti su tale aspetto.

5. Analisi di impatto sulla protezione dei dati (DPIA) e analisi del rischio

5.1 Introduzione

Prima dell'avvio di un servizio o di un'attività occorre disporre di un metodo per la valutazione degli impatti relativi alla protezione dei dati personali affinché il trattamento di dati personali venga svolto nel rispetto dei principi di privacy by design dell'art. 25 par. 1 del GDPR.
La relazione che intercorre tra la DPIA e la privacy by design risiede proprio nel fatto che la DPIA consente di individuare ed implementare le adeguate misure di sicurezza (di cui agli art. 5 par. 1 lettera f) e art 32 del GDPR).

5.2 Descrizione delle fasi di processo di DPIA

Il processo di DPIA ha inizio quando nasce l'idea di un nuovo trattamento e prima che questo sia implementato. Il processo deve essere riattivato quando ci sono variazioni significative del trattamento o delle sue modalità che possono mettere a rischio i diritti o le libertà fondamentali degli interessati.
Le fasi di processo da osservare per realizzare una DPIA sono le seguenti, più specificatamente dettagliate all'Allegato n. 7:

- ✓ Valutare la necessità di adottare e condurre un'attività di DPIA;
- ✓ Valutare la conformità al GDPR e al principio di liceità;
- ✓ Descrizione del trattamento;
- ✓ Valutazione del rischio;
- ✓ Gestione del rischio;
- ✓ Piano di azione;
- ✓ Monitoraggio del trattamento.

6. Trasferimento di dati personali all’estero

6.1 Introduzione

Il GDPR, in riferimento ai trasferimenti internazionali di dati personali, tende a chiarirne l'impiego, formalizza e amplia il numero di strumenti di trasferimento alternativi, come le clausole contrattuali tipo, affinché con il trasferimento risultino impregiudicati i livelli di protezione delle persone fisiche garantite dal GDPR (art. 44).
Scopo di questa sezione è dare indicazioni sui fattori da prendere in considerazione nell'effettuare un trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, assicurando una continuità del livello di protezione “attaccata” ai dati (sticky regulation) anche a seguito di qualsiasi ulteriore successivo trasferimento, avendo presente che gli stessi trasferimenti verso paesi esteri, in linea di principio, non sono consentiti, a meno che intervengano specifiche garanzie che il regolamento elenca in ordine gerarchico, dalle decisioni di adeguatezza alle deroghe in specifiche situazioni.
Il trasferimento verso paesi terzi è considerato un trattamento ad alto rischio per le libertà e i diritti fondamentali e pertanto può avere luogo solo nel rispetto delle condizioni di cui al Capo V del GDPR, sia che riguardino progetti di ricerca, mobilità del personale e degli studenti, richieste di dati provenienti da paesi terzi (per esempio inerenti a curriculum di laureati o dipendenti dell’Ateneo), l’utilizzo di piattaforme che non garantiscono la collocazione dei datacenter su territorio UE e altre casistiche anche frequenti in ambito universitario. Con il GDPR le decisioni di adeguatezza possono essere revocate e, in condizioni particolari, anche in tempi molto brevi per cui, nei casi di movimenti della scena politica del paese di destinazione che potrebbero inficiare i presupposti di adeguatezza, su cui si fonda una decisione esistente, e siano già osservabili al momento di avviare un trasferimento, si potrebbe preferire il ricorso a specifiche garanzie. In questo caso infatti il trasferimento troverebbe una base di legittimità che prescinde dalla presenza della decisione stessa e quindi dalla sua eventuale revoca.

Per approfondimenti sul trasferimento di dati all’estero si rinvia all’Allegato n. 8.

7. Ricerca scientifica e statistica

7.1 Premessa

Le attività di ricerca scientifica svolte in Sapienza presentano una significativa complessità sotto il profilo della disciplina e degli adempimenti in materia di trattamento di dati personali.
I motivi di tale complessità risiedono, in particolare, nelle caratteristiche delle attività di ricerca, nella natura dei dati trattati, nei peculiari ruoli e compiti riservati ai ricercatori universitari e a eventuali partner di ricerca, spesso destinatari di dati pseudonimizzati (tra cui: altre università, enti, società scientifiche, nonché altri ricercatori che operano anche all’estero).
Di seguito sono forniti alcuni elementi che possono essere uno strumento per:

- condividere le buone pratiche adottate o adottabili nell’ambito della ricerca storica, scientifica e statistica al fine di garantire una maggiore protezione dei dati personali e aderenza al GDPR;
- affrontare i temi e/o gli aspetti che presentano maggiori criticità e/o perplessità, anche con l’obiettivo di sottoporre eventuali dubbi interpretativi al Garante per la Protezione dei dati personali o, laddove possibile, allo scopo di fornire alcuni strumenti operativi a tutte le Strutture.

7.2 Finalità e ambito applicativo

“La Repubblica promuove lo sviluppo della cultura e della ricerca scientifica” (articolo 9 della Costituzione).
La cultura e la ricerca sono importanti mezzi per ampliare i confini della conoscenza, favorire la crescita delle personalità dei singoli individui, nonché consentire il progresso sociale.
È nell’ambito del perseguimento di queste finalità che può essere consentito il trattamento di dati personali; è per effetto di questo principio e del GDPR che sono previste misure di semplificazione in ambito di ricerca storica, scientifica e/o statistica.
Tali misure di semplificazione non esentano tuttavia Sapienza dall’adozione di misure idonee a prevenire possibili violazioni dei diritti degli Interessati.
La sostituzione del nominativo dell’Interessato con un codice e la conservazione dell’associazione “nominativo – codice” in un archivio separato - il cui accesso è limitato a un numero esiguo di ricercatori (operazione c.d. di “pseudonimizzazione”) -, ad esempio, è una misura necessaria per garantire il rispetto della normativa in materia di protezione dei dati personali ma non consente al Titolare di ritenere che il dato trattato sia anonimo.
È un errore comune confondere il dato pseudonimizzato (che richiede il rispetto delle norme in materia di protezione dei dati personali) con il dato anonimo (per il quale, non potendo risalire all’identità del partecipante neanche in via indiretta, non si è tenuti al rispetto del GDPR).
La forte spinta verso gli OpenData, anche in ambito di ricerca, può facilmente far riflettere sulla possibilità che lo sviluppo di sofisticate tecnologie consenta la potenziale “reidentificazione” di un Interessato i cui dati non siano stati resi del tutto anonimi.
Un altro aspetto rilevante nell’ambito della ricerca storica, scientifica e statistica è inoltre il rispetto del principio di finalità.
Spesso infatti non è possibile individuare pienamente le finalità specifiche del trattamento dei dati personali a fini di ricerca scientifica al momento della raccolta dei dati.
Una semplificazione importante su tale aspetto è prevista espressamente nel GDPR che prevede la possibilità che gli Interessati prestino il proprio consenso a determinati settori della ricerca scientifica nel rispetto delle norme deontologiche riconosciute in tale ambito (cfr. considerando n. 33 del GDPR).

7.3 Presupposti dei trattamenti

E’ 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 della ricerca);
- informare gli Interessati sull’uso di propri dati personali nell’ambito del progetto di ricerca (fornendo tutte le informazioni previste dall’articolo 13 del GDPR, salvo i casi d’esenzione che si affronteranno nei prossimi paragrafi);
- predisporre adeguate misure tecniche e organizzative per garantire la protezione dei dati, a seguito di un’accurata analisi dei rischi.

7.4 Progetto di ricerca

Avvio di un progetto di ricerca

È importante che i ricercatori che intendono avviare un progetto abbiano consapevolezza dei rischi sottesi al trattamento (al fine di evitarli) ed effettuino, laddove necessario, una “valutazione d’impatto” (così come avviene ai sensi dell'articolo 35 del GDPR per particolari categorie di dati).
I principi di protezione dei dati non si applicano a informazioni anonime, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'Interessato.

La valutazione dell'impatto deve contenere almeno:

- una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal Titolare del trattamento;
- una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
- una valutazione dei rischi per i diritti e le libertà degli Interessati;
- le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al regolamento, tenuto conto dei diritti e degli interessi legittimi degli Interessati e delle altre persone in questione.

DESCRIZIONE SISTEMATICA DEI TRATTAMENTI E DELLE FINALITÀ
Il ricercatore, prima dell'avvio di una ricerca, deve essere in grado di:
- individuare l'ambito, il contesto e le finalità della ricerca;
- effettuare una descrizione accurata del processo, con particolare riferimento alle operazioni di raccolta dei dati;
- effettuare una valutazione dei rischi per i diritti e le libertà degli Interessati, anche sulla base delle caratteristiche degli Interessati;
- prevedere, previamente alla raccolta, le eventuali modalità di comunicazione e diffusione dei dati personali, nonché rilevare le criticità che potrebbero derivare dal trasferimento dei dati all'estero;
- determinare i soggetti coinvolti nel trattamento e individuare le responsabilità a essi associate.

VALUTAZIONE DELLA LEGITTIMITÀ, NECESSITÀ E PROPORZIONALITÀ DEI TRATTAMENTI
Il ricercatore dovrà individuare le modalità per garantire la legittimità della raccolta ed elaborazione dei dati personali, nonché individuare le misure per garantire l'attuazione dei principi di necessità e proporzionalità dei trattamenti (determinando, tra gli altri aspetti, anche il periodo di conservazione/registrazione dei dati personali).

VALUTAZIONE MISURE PREVISTE PER AFFRONTARE I RISCHI
Il ricercatore dovrà identificare i beni e gli strumenti tramite i quali sono elaborati e/o archiviati i dati personali (hardware, software, reti, persone, canali di trasmissione cartacea, ecc.), effettuare l'analisi dei rischi nonché descrivere le misure previste per affrontare i rischi sottesi al trattamento.

È riportata in **Allegato 9** una scheda funzionale al ricercatore per documentare le scelte effettuate nell'ambito di un progetto di ricerca per favorire la protezione dei dati personali e la tutela dell'Interessato e/o da utilizzare per guidare il ricercatore nell'analisi di gran parte degli aspetti concernenti la materia in oggetto.

Informativa e consenso in ambito di ricerca
Il supporto ai ricercatori passa anche dalla previsione di strumenti operativi che gli consentano di informare adeguatamente eventuali partecipanti alla ricerca in merito al trattamento dei loro dati.
Tale presupposto vale anche nel caso in cui siano raccolti dati che non identificano direttamente l'Interessato (ad esempio dati che non contengono il nominativo della persona).
La raccolta di dati personali, anche quando inerenti a dati cifrati o pseudonimizzati, deve essere preceduta da un'informativa.
La messa a disposizione di informative adeguate e la raccolta dei consensi secondo le disposizioni vigenti in materia di tutela della privacy è:

- un presupposto di legittimità per lo svolgimento del progetto di ricerca in cui è prevista la raccolta;
- condizione per l'eventuale successiva conservazione dei dati al fine di procedere legittimamente a una loro ulteriore utilizzazione (ad esempio per nuove ricerche o studi nell'ambito di altri progetti o per consentire un legittimo sfruttamento dei risultati delle ricerche stesse, a meno dei casi di esenzione previsti dal GDPR).

Oltre alle informazioni di cui all'art. 13 del GDPR, è sempre opportuno nell'informativa rappresentare all'Interessato l'eventualità che i dati personali possano essere conservati e trattati (anche) per scopi statistici o scientifici.

7.5 Raccolta dei dati

Dati raccolti presso l'Interessato

La raccolta presso l'Interessato dei dati necessari per lo sviluppo di una ricerca ha l'importante vantaggio di poter rendere l'informativa (e, se previsto, acquisire il consenso) tempestivamente, fornendo al partecipante tutti i chiarimenti utili.

Dati acquisiti presso terzi

Il fatto che vi siano dati personali resi disponibili da un soggetto terzo (es: una scuola, un'agenzia interinale, ecc.) non ne implica la libera utilizzazione o diffusione da parte di un ricercatore.
Il ricercatore dovrà in ogni caso valutare se l'utilizzazione e la pubblicazione di un dato personale a fini di ricerca possa essere effettuata senza che vi sia una ragionevole aspettativa dell'Interessato in merito all'ulteriore utilizzo dei propri dati per finalità scientifiche.
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, seppur in forma pseudonimizzata, nell'ambito di attività proprie dell'Ateneo.
L'articolo 14 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.
Dall'analisi svolta da alcuni Atenei, è stato possibile evidenziare che nell'ambito di un rapporto di collaborazione tra Università e Azienda Ospedaliero-Universitaria vi siano, in relazione ai dati trattati per specifici progetti di ricerca, differenti e specifiche situazioni.
Ad esempio, esistono:

- attività di ricerca proprie dell'Ateneo svolte (anche) tramite personale e strumenti delle strutture sanitarie;
- attività di ricerca proprie delle strutture sanitarie per le quali si utilizzano (anche) personale o strumenti d'Ateneo;
- progetti di ricerca in cui le decisioni sulle modalità e gli strumenti possono essere prese congiuntamente da Ateneo e struttura sanitaria;
- casi, come le sperimentazioni di farmaci, in cui le finalità, le modalità e gli strumenti di trattamento sono decisi in modo distinto dalla società farmaceutica (sia essa committente o sponsor) e dall'Università oppure casi in cui tali decisioni sono prese congiuntamente.

7.6 Elaborazione dei dati a fini di ricerca statistica o scientifica

La valutazione dei rischi connessi al trattamento di dati personali deve tenere conto dell'impatto che potrebbe comportare.
Se l'impatto è rilevante, l'attenzione alle misure di protezione dei dati e alle garanzie da riservare all'Interessato deve essere alta.
Tali garanzie consistono:

- in una rigorosa limitazione della quantità di dati raccolti;
- nell'immediata cancellazione dei dati identificativi dopo il loro utilizzo;
- nell'adozione di misure tecniche e organizzative volte a garantire che i dati non possano essere utilizzati per adottare decisioni, intraprendere altre azioni riguardo alle persone o essere acquisite da soggetti non autorizzati ("separazione funzionale" come spesso avviene in un contesto di ricerca);
- nell'utilizzo di tecniche di anonimizzazione;
- in un'immediata aggregazione dei dati;
- nel diritto generale e incondizionato di revoca ("opt-out");
- nella pseudonimizzazione e nella cifratura di dati personali in fase di conservazione o di transito.

Tali misure devono essere adottate per ridurre la probabilità di ingerenze negli interessi o nei diritti e nelle libertà fondamentali degli Interessati.

7.7 Conservazione dei dati a fini di ricerca statistica o scientifica

Il GDPR porta con sé nuove esenzioni per la ricerca esonerandola, ad esempio, dai limiti generali imposti in merito alla conservazione.
La conservazione di dati personali raccolti per altre finalità (ad esempio didattica, cura, ecc.) è infatti consentita per esclusive finalità di ricerca, fatto salvo il rispetto dei limiti imposti dalle norme vigenti.
La legittimità della conservazione non deve tuttavia essere il pretesto per diventare "accumulatori seriali di dati personali" o per non preoccuparsi dell'integrità e dell'accuratezza nella conservazione degli stessi.
I dati personali archiviati nel tempo costituiranno infatti la base scientifica sulla quale si potranno fondare alcune ipotesi di ricerca statistica, scientifica o storica e sulla base dei quali potrebbe essere verificata l'attendibilità della ricerca stessa e l'autenticità dei risultati.
La corretta conservazione dei dati quindi non è soltanto necessaria per adempiere alla normativa in materia di protezione dei dati personali, ma costituisce un requisito fondamentale per garantire professionalità, rigore e accuratezza nell'attività di ricerca.

Dati conservati presso terzi

La corretta conservazione dei dati personali archiviati e/o trattati in formato elettronico deve avvenire tramite strumenti idonei a preservare i dati dal rischio di distruzione o perdita – anche accidentale - nonché dall'accesso abusivo da parte di terzi.
Sebbene, ad esempio, siano innegabili i vantaggi dell'uso di repository in cloud, anche in termini di sicurezza, in Sapienza devono essere tenuti in dovuta considerazione le implicazioni derivanti dalla conservazione dei dati tramite servizi in cloud di terze parti.
L'archiviazione, ad esempio su Dropbox o su Onedrive, di interviste audio-video raccolte dai ricercatori, seppur temporaneamente e con il solo obiettivo di trasferire i dati ad un partner di ricerca o di condividere uno spazio di lavoro, comporta un trattamento di dati personali da parte di terzi che offrono il servizio.

Tali soggetti dovranno pertanto essere considerati “destinatari” dei dati e segnalati opportunamente nell’informativa quali “Responsabili Esterni del trattamento”.
Questo aspetto è affrontato anche in una guida del Garante per la protezione dei dati personali intitolata "CLOUD COMPUTING - Proteggere i dati per non cadere dalle nuvole" nella quale si precisa espressamente che il “Titolare del trattamento” dei dati personali (nella fattispecie Sapienza) deve procedere a designare il fornitore dei servizi in cloud “Responsabile Esterno del trattamento” e prestare molta attenzione a come saranno utilizzati e conservati i dati personali caricati sulla “nuvola” poiché, in caso di violazioni commesse dal fornitore, anche l’Università potrebbe essere chiamata a rispondere dell’eventuale illecito trattamento.
Ulteriore attenzione deve essere poi prestata a quei fornitori di repository in cloud che dichiarano di conservare i dati in uno Stato Extraeuropeo e/o che prevedono il trattamento degli stessi all’estero, soprattutto qualora l’ordinamento del Paese di destinazione o di transito dei dati non assicuri un adeguato livello di tutela, come chiarito meglio nel seguente paragrafo.
Per garantire che i dati di ricerca siano “al sicuro”, è altresì importante curare non solo i rapporti con il fornitore e verificare le modalità con cui sono conservati i dati, ma anche curare le misure di protezione e le modalità con cui sono trasmessi (ad esempio adottando opportune tecniche di cifratura).

7.8 Trasferimento dei dati all’estero

Nel GDPR vige il principio secondo il quale il trasferimento dei dati personali oggetto di un trattamento verso un paese terzo avviene soltanto se il Titolare del trattamento e i Responsabili rispettano le condizioni dettate dal Regolamento.
A titolo esemplificativo e non esaustivo, il trasferimento dei dati può lecitamente avvenire se:

- esiste una decisione di adeguatezza da parte della Commissione europea (perché ritiene che il paese destinatario offra un livello adeguato nella protezione dei dati);
- sono adottate clausole contrattuali standard;
- si fa riferimento alle norme vincolanti di impresa cioè alle BDR (che consentono il trasferimento all’interno della società se il regime è stato pre-approvato da un Garante europeo);
- si fa riferimento a codici di condotta e certificazione;
- sono state inserite particolari disposizioni in accordi amministrativi;
- ci sono state sentenze di un’autorità giurisdizionale o amministrativa, purché basati su un accordo internazionale se c’è stato il consenso dell’Interessato.

7.9 Diffusione dei dati a fini di ricerca scientifica o statistica

Soprattutto nell’ambito di progetti europei, è richiesto al ricercatore di stimolare il dialogo e il dibattito sui risultati della ricerca scientifica, garantendo il diritto all'informazione ad un pubblico più vasto ed eterogeneo, rendendo le conoscenze acquisite più attrattive per i giovani, aumentando l’interesse della società per l’innovazione scientifica e lo sviluppo tecnologico.
Sebbene in alcuni casi, nel rispetto dell'essenzialità dell'informazione, il ricercatore possa evitare di diffondere risultati scientifici che includano riferimenti (anche indiretti) a persone fisiche, in altri casi è importante farlo poiché:

- l'informazione, anche dettagliata, può risultare indispensabile per lo sviluppo delle tesi di ricerca e dei risultati ottenuti, nonché per la qualificazione degli Interessati e di ciò che rappresentano;
- si tratta di una richiesta espressa degli stessi Interessati (magari volta a valorizzare il loro coinvolgimento in un’attività di ricerca);
- si tratta di interviste riguardanti circostanze o fatti già resi noti da altre fonti di informazione.

La divulgazione di risultati scientifici contenenti dati personali, se di rilevante interesse pubblico o sociale, non si pone in contrasto con il rispetto della sfera privata dell’Interessato a patto che lo stesso sia stato adeguatamente informato in merito alla diffusione di proprie informazioni.

Si precisa tuttavia che il ricercatore deve effettuare una valutazione di proporzionalità nella diffusione di dati personali e sull'opportunità di provvedere alla loro stessa diffusione a particolari categorie di Interessati.
Ad esempio, al fine di tutelare i diritti degli Interessati, il ricercatore non deve pubblicare nominativi di minori coinvolti in progetti di ricerca qualora il prodotto che si intenda diffondere (articolo scientifico, video, ecc.) non dia positivo risalto al minore e/o nel caso in cui la pubblicità dei suoi dati possa, in futuro, arrecagli un danno alla sua personalità. Resta fermo l'obbligo per il ricercatore di acquisire l'immagine o le informazioni, in un quadro di assoluta trasparenza, nonché di valutare, volta per volta, eventuali richieste di opposizione da parte dell'Interessato.

8. Riepilogo delle priorità e relative azioni organizzative e tecniche

Analizzato il contesto interno all'Ateneo sulle questioni attinenti alla protezione dei dati personali, e considerata la necessità di procedere in maniera sistemica alle attività di adeguamento, sono state individuate le seguenti prioritarie misure/azioni di carattere sia tecnico che organizzativo, ritenute adeguate e concorrenti per la conformità al GDPR e al Codice.

8.1 Formazione

Al fine di Istruire le risorse che partecipano alla gestione e al trattamento dei dati personali, fornendo loro le conoscenze necessarie, Sapienza attua un apposito piano di formazione, che ha previsto, tra l'altro, l'acquisizione sul Mepa di un corso on-line rivolto a tutto il personale docente e tecnico-amministrativo.
Sapienza utilizza anche il proprio portale come veicolo di in-formazione in argomento (GDPR, Codice), di misure e iniziative per la protezione dei dati personali.

8.2 Organizzazione funzionale interna

Sapienza ha provveduto alla nomina del Responsabile della Protezione dei Dati (RPD) per il quale designazione, ruolo e compiti sono specificati agli artt. 37-39 del GDPR e richiamati nella delibera di nomina.
Sulla base del vigente organigramma delle proprie strutture amministrative/didattiche, Sapienza, ai sensi dell'art. 2 – quaterdecies del Codice (Attribuzione di funzioni e compiti a soggetti designati), ha designato, per ciascuna struttura, le figure di Responsabili Interni del Trattamento (Designati) e ha disposto la nomina, da parte degli stessi Designati, degli Amministratori di Sistema e degli Incaricati Istruiti del Trattamento.

8.3 Gestione e misura del rischio

Quando un tipo di trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, Sapienza, tenuto conto della natura, dell'oggetto, del contesto, delle finalità del trattamento e dell'utilizzo di nuove tecnologie, effettua, ai sensi dell'art. 35 del GDPR, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali.

8.4 Gestione ed esecuzione del trattamento

Sapienza gestisce il trattamento dei dati personali in pieno adempimento dei principi prescritti dall'art. 5 del Regolamento:

- liceità, correttezza e trasparenza
- limitazione della finalità
- minimizzazione dei dati
- esattezza
- limitazione della conservazione
- integrità
- riservatezza
- responsabilizzazione

8.5 Metodo e applicazione della protezione fin falla progettazione per impostazione predefinita

Sapienza progetta ed esegue il trattamento mettendo in atto misure tecniche e organizzative adeguate quali la pseudonimizzazione, minimizzazione e misure tecniche organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento.

8.6 Informative e misure di tutela (art. 3; artt. 12-14; artt. 24-25; art. 30; art. 32; artt.33-34)

Artt. 12, 13 e 14: con specifiche Direttive Sapienza ha adottato misure appropriate per fornire all'interessato adeguate informative. Per ciascun trattamento di dati, deve essere resa specifica informativa, che deve avere forma concisa, trasparente, intelligibile per l'interessato e facilmente accessibile; veicolata da un linguaggio chiaro e semplice.

In particolare, il soggetto interessato del trattamento deve essere informato in merito a:

- identità e dati di contatto del titolare del trattamento, del suo rappresentante e del responsabile della protezione dei dati personali;
- e finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento ed i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
- gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali e, nel caso in cui i dati personali non siano raccolti presso l'interessato, anche le categorie di dati trattati e le relative fonti di provenienza;
- l'eventuale intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili;
- il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- i diritti azionabili dall'interessato comprendenti: l'accesso ai dati personali, la rettifica o la cancellazione degli stessi, la limitazione del trattamento o l'opposizione; oltre al diritto alla portabilità dei dati; la revoca del consenso esercitabile in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca; il diritto di proporre reclamo a un'autorità di controllo;
- la necessità di comunicare i dati personali in base a un obbligo legale o contrattuale oppure se si tratta di un requisito necessario per la conclusione di un contratto, nonché la natura obbligatoria o facoltativa del conferimento, nonché le possibili conseguenze della mancata comunicazione di tali dati;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione e, almeno in tali casi, informazioni significative circa la logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Al fine della redazione delle specifiche informative da fornire agli interessati, si allegano le tabelle tipo redatte sulla base della mappatura delle principali tipologie di trattamenti che trovano svolgimento in ambito universitario.

Artt. 24 e 25: Sapienza progetta ed esegue il trattamento utilizzando il metodo illustrato nel precedente paragrafo 8.5.

Art. 30: Con specifica Direttiva Sapienza ha invitato ciascun Dirigente/Rappresentante di struttura, a compilare, e costantemente aggiornare, il Registro dei trattamenti accessibile al link
https://docs.google.com/forms/d/e/1FAIpQLSf5KrzQpoKouUWt8IW6F7sP9ts1qFb-5DlwsCHh85ixRamPOg/viewform?usp=sf_link
mediante l'inserimento, per ciascun trattamento svolto, dei seguenti dati:

- i riferimenti di contatto del Dirigente/Rappresentante di struttura;
- le finalità;
- la descrizione degli interessati;
- la descrizione dei destinatari;
- le categorie dei dati personali trattati;
- la presenza di trasferimenti di dati verso un paese terzo o un'organizzazione internazionale unitamente alla documentazione sulle appropriate garanzie;
- la descrizione della misure di sicurezza e organizzative adottate.

Sulla base della mappatura dei trattamenti così ottenuta, Sapienza ha redatto un nuovo Registro, ampliato e perfezionato, che costituisce l'Allegato 1) al presente Piano.

Art. 32: Sapienza, attraverso la propria capillare organizzazione interna, che vede la nomina dei Designati corrispondenti ai direttori delle singole strutture universitarie, ha altresì messo in atto un livello di sicurezza adeguato, comprensivo della capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento, nonché della capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico. In particolare, Sapienza ha disposto una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento. Tale procedura, attuata dai Responsabili interni, prevede che chiunque agisca sotto la loro autorità e abbia accesso a dati personali, tratti tali dati sulla base di istruzioni impartite in tal senso dal titolare del trattamento.

Artt. 33 e 34 - PROCEDURA PER LA NOTIFICA DI VIOLAZIONE DEI DATI PERSONALI (DATA BREACH): Sapienza, con specifiche Direttive ha dato indicazioni della procedura da attuare in caso di violazione dei dati personali.
In particolare, Sapienza ha disposto che in caso di violazione dei dati personali, avvenuta accidentalmente o in modo illecito, che si concretizzi con la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati, i Designati presso le singole strutture universitarie (Facoltà, Scuole, Dipartimenti, Centri di ricerca, Centri di ricerca e servizi, Centri di servizi, Aree amministrative e Uffici equiparati, Polo Museale e Sistema Bibliotecario), al fine di consentirne la prevista comunicazione all'Autorità di controllo, devono informare con urgenza immediata, comunque entro e non oltre 48 ore dall'acquisizione della conoscenza dell'accadimento, il Responsabile della protezione dei dati, utilizzando l'apposito modello Allegato 1, da trasmettere esclusivamente al seguente indirizzo e-mail responsabileprotezionedati@uniroma1.it.

Art. 3: Sapienza applica il Regolamento al trattamento dei dati personali indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione.

8.7 Controllo sull'affidamento del trattamento a Responsabili Esterni. Contratto/atto giuridico e RGPD

Sapienza, in caso di presenza di strutture esterne all'amministrazione universitaria che concorrano al trattamento dei dati dell'ateneo, formalizza, con atto negoziale o contratto o clausola contrattuale specifica, la nomina della struttura esterna come responsabile esterno del trattamento; oggetto del contratto o della clausola contrattuale deve essere l'assolvimento di tutti gli obblighi prescritti dal Regolamento e dal Codice, prevedendo garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, in modo tale che il trattamento soddisfi i requisiti del Regolamento e del Codice.

8.8 Regolamentazione interna - Codici di Condotta di cui all'art. 40 del RGPD

Sapienza, con Atti interni rivolti alle strutture universitarie (Facoltà, Scuole, Dipartimenti, Centri di ricerca, Centri di ricerca e servizi, Centri di servizi, Aree amministrative e Uffici equiparati, Polo Museale e Sistema Bibliotecario), ha elaborati rispettivi codici per l'applicazione del Regolamento UE relativamente, tra l'altro, a:

a) il trattamento corretto e trasparente dei dati;
b) i legittimi interessi perseguiti dal responsabile del trattamento in contesti specifici;
c) la raccolta dei dati personali;
d) la pseudonimizzazione dei dati personali;
e) l'informazione fornita al pubblico e agli interessati;
f) l'esercizio dei diritti degli interessati;
g) l'informazione fornita e la protezione del minore e le modalità con cui è ottenuto il consenso dei titolari della responsabilità genitoriale sul minore;
h) le misure e le procedure di cui agli articoli 24 e 25 del Regolamento e le misure volte a garantire la sicurezza del trattamento di cui all'articolo 32 del Regolamento;
i) la notifica di una violazione dei dati personali alle autorità di controllo e la comunicazione di tali violazioni dei dati personali all'interessato.

8.9 Interventi di mantenimento. Azioni di revisione e miglioramento

Il piano è stato articolato per configurare le azioni e le priorità di intervento affinché queste non solo rispondano a esigenze puntuali e immediate di adeguamento, ma possano anche concretizzarsi in una serie di attività specifiche e dimostrabili, riesaminate e aggiornate nell'ottica di un miglioramento continuo.

La durata del presente Piano è di 18 mesi, con verifiche interne semestrali. Trascorsi i 18 mesi e in continuità, il Piano sarà aggiornato e/o riformulato in coerenza all'attività di riesame e allo stato di attuazione.

Gli interventi di mantenimento, riesame e miglioramento dipendono dai progressivi risultati e, comunque, saranno contestualizzati agli aggiornamenti e alle linee guida prodotte dal Garante e dal Comitato Europeo.

La diffusione e l'informazione sullo svolgimento del presente piano avvengono anche tramite l'aggiornamento periodico della sezione *privacy* di Ateneo.

8.10 Azioni da intraprendere

Attivazione di attività di audit interna
Al fine di monitorare il sistema di protezione dei dati adottato da Sapienza, è opportuno, nelle more della definizione organizzativa più adeguata, avviare un'attività di audit interna - con personale qualificato delle Aree dell'Amministrazione Centrale -, per la verifica della conformità delle strutture universitarie ai requisiti del sistema stesso.

Analisi del rischio per i trattamenti fondamentali
Una delle attività principali per un corretto processo di adeguamento al Regolamento è l'analisi dei rischi dei trattamenti dei dati, per l'adozione di corrispondenti, idonee misure di sicurezza.
A tal fine, l'Ateneo mette in atto una serie di azioni finalizzate ad una dettagliata individuazione e valutazione dei rischi connessi al trattamento dei dati personali.
La valutazione del rischio viene aggiornata in occasione di modifiche ai processi (utilizzo di nuovi prodotti e nuove tecnologie, cambiamenti nell'organizzazione), nuove prescrizioni legislative, risultati delle verifiche di soggetti istituzionali, segnalazioni degli interessati.

Ciò premesso, al fine di una maggiore sicurezza dei dati trattati in Sapienza, si rende opportuno prevedere una valutazione dei rischi dei trattamenti, almeno una volta all'anno, mediante apposite schede di analisi da somministrare alle strutture universitarie, al fine di accertare l'eventuale necessità di aggiornamento del tasso di gravità.

Adozione di un Regolamento in materia di protezione dei dati personali di Ateneo in attuazione del GDPR
Al fine di disciplinare la protezione delle persone fisiche in relazione al trattamento dei dati personali, si rende opportuno valutare la possibile adozione di un Regolamento in materia di protezione dei dati personali di Ateneo, in attuazione di quanto previsto dal GDPR e dal D.Lgs. n. 196/2003, come modificato dal D.Lgs. n. 101/2018, anche sulla base della bozza di regolamento predisposta al riguardo dalla CRUI.