

Linee guida in materia di privacy e protezione dei dati personali in ambito universitario

Versione 1.1 – novembre 2017

Redazione a cura di:

Nicla Diomede (Università degli Studi di Milano – Statale)

Pasquale Ficara (Università degli Studi di Milano-Bicocca)

Alessandra Magri (Università degli Studi di Milano-Bicocca)

Marisa Morbidi (Università degli Studi di Firenze)

Fabrizio Pedranzini (Politecnico di Milano)

Daniela Prestipino (Università degli Studi di Messina)

Paolo Sanna (Università degli Studi di Milano – Statale)

Manuela Zecca (Alma Mater Studiorum – Università Bologna)

Revisione a cura del Gruppo di lavoro “Linee Guida Privacy e GDPR” del CODAU

Sommario

1.	Premessa	5
1.1	Scopo delle linee guida	5
1.2	Ambiti considerati	5
2.	Il nuovo Regolamento UE 679/2016	6
2.1	Iter di attuazione	6
2.2	Cosa cambia con il nuovo regolamento	6
2.2.1	Ambito di territorialità.....	7
2.2.2	Accresciuta responsabilità dei titolari e dei responsabili del trattamento.	8
2.2.3	Rafforzamento delle tutele riservate all'interessato	8
2.2.4	Diritti dell'interessato.....	12
2.2.5	Sintesi delle principali novità	15
3.	I soggetti del trattamento	17
3.1	Titolare del trattamento	17
3.2	Contitolare	18
3.3	Responsabile del trattamento dati	18
3.4	Soggetti autorizzati	20
3.5	Responsabile della protezione dati	21
3.6	Destinatario.....	22
3.7	Interessato.....	23
3.8	L'Università quale Responsabile del trattamento dati	23
3.9	Autorità di controllo e comitato europeo	23
4.	Finalità istituzionali dell'Università	24
5.	Mappa dei trattamenti dei dati personali.....	25
5.1	Premesse inerenti i trattamenti di dati personali in ambito universitario	25
5.2	Trattamenti principali inerenti gli studenti	27
5.2.1	Trattamento finalizzato all'orientamento	27
5.2.2	Trattamento finalizzato all'erogazione dei test di ingresso o alla verifica dei requisiti di accesso	28
5.2.3	Trattamento finalizzato per l'erogazione del percorso formativo e gestione della carriera (dall'immatricolazione alla laurea)	30
5.2.4	Trattamento finalizzato all'attività di tirocinio.....	32
5.2.5	Trattamento finalizzato ad attività di job placement.....	33
5.2.6	Trattamento finalizzato ad attività di fundraising, di comunicazione e informazione istituzionale e sviluppo di community	34
5.2.7	Trattamento finalizzato a rilevazioni statistiche e valutazione della didattica	35
5.2.8	Trattamento finalizzato al caso di diffusione dell'elaborato finale o di elementi ad esso connessi	36
5.2.9	Trattamento finalizzato a servizi di tutorato, assistenza, inclusione sociale	37

5.2.10	Trattamento finalizzato all'erogazione di servizi e attività per il diritto allo studio.	38
5.2.11	Procedimenti di natura disciplinare a carico di studenti.....	39
5.3	Trattamenti principali inerenti a dipendenti e/o collaboratori	40
5.3.1	Trattamento finalizzato allo svolgimento di prove concorsuali/selezioni	40
5.3.2	Trattamento finalizzato alla gestione del rapporto di lavoro	41
5.3.3	Trattamento di dati personali ai fini di formazione e aggiornamento professionale	43
5.3.4	Trattamento di dati personali necessario alla gestione di progetti di ricerca	44
5.3.5	Trattamento di dati personali al fine di garantire il monitoraggio e la valutazione della ricerca	45
5.3.6	Trattamento di dati personali nell'ambito di attività di trasferimento tecnologico	46
5.3.7	Trattamento necessario per politiche Welfare e per la fruizione di agevolazioni .	46
5.3.8	Trattamenti per la salute e la sicurezza delle persone nei luoghi di lavoro.....	47
5.3.9	Trattamento dei dati personali nell'ambito dell'erogazione del servizio di telefonia fissa e mobile	49
5.4	Trattamenti trasversali o connessi ad attività trasversali	50
5.4.1	Trattamento dei dati nell'ambito della gestione degli spazi	50
5.4.2	Trattamento dei dati personali per la gestione delle postazioni.....	51
5.4.3	Trattamento per attività di gestione degli organi e delle cariche istituzionali	52
5.4.4	Trattamento per la gestione degli infortuni	55
5.4.5	Trattamento in ambito bibliotecario	56
5.4.6	Trattamento di dati nell'ambito dei servizi di protocollo e conservazione documentale	57
5.4.7	Trattamento finalizzato all'acquisto di beni e servizi, stipula di contratti, recupero crediti, gestione del contenzioso	60
5.4.8	Trattamento di dati nell'ambito dei servizi di posta elettronica e strumenti di collaboration	63
5.5	Trattamento di dati personali nell'ambito dell'erogazione federata di servizi.....	65
5.5.1	Trattamento finalizzato all'erogazione del servizio Eduroam	66
5.5.2	Trattamento finalizzato all'accesso a servizi federati (es IDEM)	66
5.5.3	Trattamento nell'ambito dell'accesso ai servizi con autenticazione SPID	69
5.6	Tracciamento di informazioni non primarie	71
5.6.1	Raccomandazioni	71
5.6.2	Finalità del tracciamento	72
5.6.3	Tracciamento sistemistico e di rete.....	72
5.6.4	Tracciamento applicativo.....	74
6.	Ricerca scientifica e statistica.....	76
6.1	Premessa	76
6.2	Finalità e ambito applicativo	76
6.3	Presupposti dei trattamenti.....	77
6.4	Progetto di ricerca	77
6.4.1	Avvio di un progetto di ricerca	77

6.4.2	Raccolta dei dati	80
6.4.3	Elaborazione dei dati a fini di ricerca statistica o scientifica.....	83
6.4.4	Conservazione dei dati a fini di ricerca statistica o scientifica	83
6.4.5	Trasferimento dei dati all'estero	84
6.4.6	Diffusione dei dati a fini di ricerca scientifica o statistica.....	85
7.	Link utili.....	85
Allegato 1 - Riepilogo degli adempimenti e delle priorità di intervento		86
Allegato 2 - Scheda di approfondimento per la redazione delle informative		90
Allegato 3 - Scheda di analisi per progetti di ricerca.....		96
Allegato 4 – Informativa per il trattamento di dati sensibili in un progetto di ricerca.....		108

1. Premessa

1.1 Scopo delle linee guida

Per fornire indicazioni e raccomandazioni riguardo alle operazioni di trattamento effettuate con dati personali in ambito universitario e alla protezione degli stessi, il CODAU ravvisa l'esigenza di adottare le presenti linee guida, suscettibili di periodico aggiornamento, nelle quali si tiene conto anche di precedenti decisioni dell'Autorità Garante per la protezione dei dati personali e delle pregresse esperienze degli Atenei 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 Atenei
- 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

Le linee guida, dopo aver illustrato i principi fondamentali del trattamento e della protezione dei dati personali (base giuridica e vincoli di liceità) – paragrafo 2, illustra le principali novità introdotte e una prima analisi sull'applicazione nel sistema universitario italiano.

Sull'argomento viene evidenziato la mutata configurazione dei soggetti gestori del trattamento (paragrafo 3), atteso che il novellato regolatorio attiene proprio l'accresciuta e mutata responsabilità del titolare e del responsabile incentrata sulla positivizzazione e sul rafforzamento del principio di accountability.

In riscontro al taglio pratico delle linee guida nel capitolo 5 vengono mappati i trattamenti più importanti distinguendo quelli di carattere istituzionale e quelli ad essi strumentali e trasversali. Infine nel capitolo 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

2.1 Iter di attuazione

Il nuovo Regolamento Europeo - Regolamento (UE) 2016/679 del Parlamento Europeo (L. 119) *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati* è stato pubblicato sulla GUUE del 04 maggio 2016.

Il testo è disponibile alla risorsa:

http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC

Il Regolamento Europeo (di seguito indicato come "Regolamento UE" o come "GDPR") è direttamente applicabile e vincolante in tutti gli Stati membri e non richiede una legge di recepimento nazionale, fatta eccezione per alcuni ambiti sui quali rimanda, deroga o richiede l'integrazione regolatoria dei singoli Stati.

La diversa forma dell'atto – da Direttiva a Regolamento, risponde alla primaria volontà del legislatore europeo di porre sullo stesso piano tutti gli Stati membri, garantendo medesimi diritti e doveri, assicurando uniformità alla protezione dei dati personali e certezza al diritto.

Il Regolamento UE è stato approvato il 27 aprile 2016, entrato in vigore il 25 Maggio dello stesso anno ma destinato ad avere piena attuazione dal 25 Maggio 2018, data a partire dalla quale abrogherà la Direttiva 95/46/CE del Parlamento europeo e del Consiglio, 24 ottobre 1995, *relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati* (c.d. Direttiva Madre).

Nonostante il differimento temporale della piena efficacia del GDPR alcune sue parti ne richiedono immediata applicazione, pertanto fino al 24 maggio 2018, è necessario considerare tre atti normativi regolatori: la Direttiva Madre, quindi per l'Italia, il Decreto Legislativo n. 196/2003 (Codice in materia di dati personali) e il Regolamento UE.

2.2 Cosa cambia con il nuovo regolamento

Il Regolamento UE cambia profondamente la prospettiva in cui si colloca la protezione dei dati personali sebbene a una prima lettura possa rispecchiare una impostazione simile a quella della Direttiva Madre rispetto al costrutto portante (informativa, finalità, consenso), ai ruoli, ai diritti degli interessati e ai doveri dei titolari e dei responsabili.

Il GDPR consacra il diritto alla protezione dei dati personali come diritto fondamentale e costituzionale configurandolo come diritto alla autodeterminazione informativa. Questo è un principio portante fondato dalla Direttiva, che il Regolamento UE eredita, ma di cui ne ridisegna radicalmente l'implementazione passando dalla logica dell'adempimento prevalentemente formale ad un approccio regolatorio fortemente sostanziale e centrato sulla responsabilità di assicurare/mantenere la conformità al regolamento nonché di tutelare i diritti e la dignità degli interessati.

Il Regolamento UE, inoltre, traccia il passaggio da un diritto alla protezione dei dati personali di tipo *nazionale/individuale* ad un diritto di tipo *europeo/sociale*¹.

In generale il GDPR – collocandolo in questa premessa e provando a dimensionarlo su diritti-doveri-controllo:

- a) 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

¹ Questo aspetto trova il suo fondamento nel considerando 4) secondo cui *"Il trattamento dei dati personali dovrebbe essere al servizio dell'uomo. Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va temperato con altri diritti fondamentali, in ossequio al principio di proporzionalità."*

autonoma rilevanza all'interno dei processi organizzativi e gestionali di un ente o di un'azienda;

- b) consolida le garanzie e i diritti azionabili dall'interessato per il controllo delle proprie informazioni e l'esercizio dell'autodeterminazione ereditati dalla Direttiva, riaffermandone molti (diritto all'accesso, rettifica, cancellazione, limitazione, revoca e opposizione); rafforzandone altri - in primis la disciplina del consenso del quale introduce un vera e propria definizione dell'istituto del consenso esplicito², e della trasparenza rispetto alla quale perfeziona il catalogo delle informazioni da esporre nell'informativa; introducendone di nuovi (diritto alla portabilità, all'oblio, all'opposizione verso il trattamento di profilazione);
- c) accresce le responsabilità del titolare e del responsabile con la positivizzazione del principio di accountability con la finalità di porre chi tratta i dati personali in una posizione di ridurre i rischi di operazioni non conformi o non consentite motivando, in tal senso, il titolare e il responsabile a comportamenti e prassi virtuose;
- d) centralizza la governance e il controllo sul rispetto e la conformità dei trattamenti alla normativa, tramite la cooperazione e la valorizzazione delle Autorità di Controllo nazionali verso il Comitato; incoraggiando meccanismi di certificazione; ampliando il sistema vigilanza; rafforzando 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 in ambito universitario.

2.2.1 Ambito di territorialità

Il regolamento (considerando da 14 a 27, art. 3³) 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 – ad esempio – effettua il monitoraggio del comportamento di una persona italiana (studiando ad esempio come si muove all'interno di un sito di e-commerce) dovrà trattare il dato nel rispetto del Regolamento UE.

² art. 4 comma 11) «consenso dell'interessato»: *qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;*

³ **Art- 3 Ambito di applicazione territoriale**

1. Il presente regolamento si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione.
2. Il presente regolamento si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano: a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione.
3. Il presente regolamento si applica al trattamento dei dati personali effettuato da un titolare del trattamento che non è stabilito nell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico.

2.2.2 Accresciuta responsabilità dei titolari e dei responsabili del trattamento.

La responsabilità dei titolari (art. 24 e 25)^{4,5} e del responsabile (art. 28) **si configura come una sostanziale assunzione di rischio**, atteso che il titolare deve mettere in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, la conformità del trattamento al regolamento tenendo conto, inoltre, della natura, dell'obbligo, del contesto e delle finalità di trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.

A titolari e responsabili di trattamento si affianca una nuova figura obbligatoria per le pubbliche amministrazioni: il responsabile della protezione dei dati personali (c.d. "data protection officer").

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 dei titolari e dei responsabili sono descritti al successivo paragrafo 3.

2.2.3 Rafforzamento delle tutele riservate all'interessato

Nel nuovo Regolamento 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:

a. *Privacy by design - considerando 78) art. 25 comma 1*

Attiene le buone prassi di protezione dei dati personali sin dalla progettazione del trattamento. Le misure strumentali a tale scopo sono:

- i) 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;

⁴ Articolo 24 Responsabilità del titolare del trattamento

1. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.
2. Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento.
3. L'adesione ai codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento.

⁵ Articolo 25 Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.
2. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.
3. Un meccanismo di certificazione approvato ai sensi dell'articolo 42 può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2 del presente articolo.

- ii) la pseudonimizzazione ovvero l'oscuramento (reversibile) dei dati identificativi del soggetto interessato;
- iii) 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 (ad esempio 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 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 09 Aprile 2001).

b. Privacy by default - considerando 78) art. 25 comma 2

Il titolare del trattamento deve mettere in atto misure tecniche e 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). Sarà quindi di fondamentale rilevanza curare, ad esempio, le diverse autorizzazioni di lettura e di modifica dei dati (in relazione ai diversi profili dei soggetti autorizzati al trattamento), curando adeguatamente anche eventuali procedure organizzative interne.

c. Valutazione di impatto (DPIA) - considerando da 89 a 96, art. 35, 36

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).

L'Autorità di controllo redige e pubblica l'elenco di tipologie di trattamenti 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.

La responsabilità della valutazione d'impatto attiene prioritariamente il Titolare supportato dal Responsabile protezione dei dati. 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.

Effetto pratico in ambito universitario e casi esemplificativi

Per quanto concerne la valutazione di impatto sulla protezione dei dati, l'Ateneo, consultandosi con il Responsabile della protezione dei dati personali, dovrebbe stabilire alcune linee guida su:

- i casi in cui condurre o meno una DPIA;
- le metodologie da adottare nel condurre una DPIA;
- le salvaguardie da applicare (comprese misure tecniche e organizzative, per attenuare i rischi per i diritti e gli interessi delle persone interessate).

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'abbondanza universitaria) attraverso un'interconnessione tra dati di carriera, dati anagrafici, ecc., si renda necessario prevedere degli interventi di supporto per gli interessati da 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.

d. Sicurezza e valutazione dei rischi - considerando 83, 84, art. 32

Il regolamento prevede misure di sicurezza idonee da adottare in relazione alla valutazione dei rischi.

Titolare e responsabile sono tenuti tanto alla valutazione dei rischi quanto all'adozione delle misure che comprendono: la pseudonimizzazione, la cifratura; misure implementative della riservatezza, dell'integrità, della disponibilità delle informazioni; la resilienza dei sistemi e delle applicazioni di trattamento nonché il loro tempestivo ripristino in caso di incidente fisico o tecnico.

Le misure vanno temperate allo stato dell'arte, ai costi di attuazione, alla natura, al contesto e alla finalità di trattamento. Alcuni indicatori di rischio (soprattutto connessi ai trattamenti informatizzati) sono declinati nella definizione di violazione di dato personale.

e. Violazione dei dati personali e relativa notifica - considerando da 85 a 88, art. 4, 33, 34

Il regolamento declina la violazione dei dati personali affiancando alla tradizionale componente dolosa quella accidentale prevedendo pari implicazioni.

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*.

Il titolare deve comunicare all'Autorità di Controllo 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 responsabile della protezione dei dati; le probabili conseguenze della violazione; le misure adottate o che si intendono adottare per rimediare la violazione o attenuarne gli effetti negativi.

Nel caso in cui sia determinato un Responsabile, tale soggetto deve informare il Titolare nel caso di avvenuta violazione di dati personali da lui trattati.

Oltre alla comunicazione all'Autorità di Controllo, la violazione deve essere comunicata anche all'interessato se la violazione è suscettibile di elevati rischi per i diritti e le libertà dell'interessato (art. 34 del GDPR).

Le attività prioritarie per tale adempimento sono riportate in *Allegato 1 – Resoconto adempimenti e priorità di intervento*.

Effetto pratico in ambito universitario

Nel caso vi sia una violazione del sistema informativo di gestione dei dati di login (di studenti o personale) tale da creare un pericolo concreto per le credenziali gestite dal sistema, il Titolare (eventualmente supportato dal Responsabile, se individuato) esegue una valutazione prudentiale della violazione.

Per il caso di specie, si potrebbero delineare tre scenari:

Scenario A - il sistema di gestione delle credenziali usato dall'Ateneo archivia in chiaro le credenziali: il titolare deve notificare, entro 72 ore dal momento in cui ne è venuto a conoscenza, la violazione all'Autorità di Controllo e agli interessati.

Scenario B - il sistema di gestione delle credenziali usato dall'Ateneo cifra le credenziali mediante hash irreversibile: il titolare deve notificare, entro 72 ore dal momento in cui ne è venuto a conoscenza, la violazione all'Autorità di Controllo e facoltativamente agli interessati.

Scenario C - il sistema di gestione delle credenziali usato dall'Ateneo cifra le credenziali mediante hash irreversibile e ha una gestione separata dei sistemi di login rispetto alle risorse che le identificano: il titolare valuta se notificare la violazione all'Autorità di Controllo.

f. Introduzione dei registri delle attività di trattamento – considerando 82, art. 30.

Il titolare e il responsabile⁶ di trattamento devono tenere i rispettivi registri delle attività.

Il registro del titolare deve contenere: riferimenti di contatto del titolare/i, del rappresentante del titolare del trattamento nell'Unione (in caso di non stabilimento nell'Unione) e del responsabile della protezione dei dati; le finalità; descrizione degli interessati e dei destinatari; la categoria dei dati personali trattati; la presenza di trasferimenti di dati verso un Paese Terzo un'organizzazione internazionale unitamente alla documentazione sulle appropriate garanzie; la tempistica della cancellazione dei dati; la descrizione delle misure di sicurezza e organizzative adottate.

Il registro del responsabile deve contenere oltre alle due ultime voci previste ed elencate per il registro del titolare: i riferimenti di contatto dei responsabili, dei titolari per conto dei quali operano, dei rappresentanti e del responsabile della protezione dei dati; le categorie dei trattamenti effettuati per conto del titolare.

Le attività prioritarie per tale adempimento sono riportate in *Allegato 1 – Resoconto adempimenti e priorità di intervento*.

g. 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 dell'Autorità Garante su "Rifiuti di apparecchiature elettriche ed elettroniche (Raee) e misure di sicurezza dei dati personali" - 13 ottobre 2008 - G.U. n. 287 del 9 dicembre 2008 (<http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1571514>).

⁶ I registri sono due, quello del responsabile attiene le attività svolte da questi per conto del titolare.

2.2.4 Diritti dell'interessato

Consenso – considerando 39 e 42, art. 6, 7

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). Non è richiesta necessariamente la forma scritta anche se questa risulta essere la modalità più idonea ad accertare che il consenso sia stato inequivocabilmente fornito e che sia esplicito.

Si precisa che nel caso il trattamento richieda il consenso, il titolare dovrà essere in grado di dimostrare inequivocabilmente di averlo ottenuto.

Per il trattamento di dati sensibili (il GDPR parla di categorie particolari di dati) è necessario il consenso (art.9 comma 2 lettera a)) a meno che il trattamento non sia necessario per la tutela di diritti di grado superiore dell'interessato stesso o pubblici o di terzi, oppure per obbligo di legge, qualora l'interessato non sia in grado di fornire il consenso (art. 9 comma 2 lettere c, f, g, i, j).

Informativa – considerando da 58 a 73, art. 12, 13, 14

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 (art. 13 co. 4) o in altri casi particolari descritti nel regolamento (art. 14 co. 5).

Contenuti dell'informativa

Il titolare del trattamento è tenuto a informare il soggetto interessato in merito a:

- identità e dati di contatto del titolare del trattamento, del suo rappresentante e del responsabile della protezione dei dati personali;
- 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'art. 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 a 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, il riferimento alle garanzie adeguate o opportune 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 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.

A riguardo si segnalano alcuni punti di attenzione:

- Deve essere chiarito l'eventuale trasferimento di dati in un paese terzo (ad esempio nel caso di utilizzo di servizi cloud). Si ricorda che anche per tali servizi è responsabilità del titolare 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, il titolare del trattamento che intenda 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
- nel caso in cui i dati non siano stati ottenuti presso l'interessato, il titolare del trattamento che intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento, potrà non fornire l'informativa all'interessato qualora risulti impossibile o farlo implicherebbe uno sforzo sproporzionato (in particolare per il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici e fatte salve le condizioni e le garanzie di cui all'articolo 89, paragrafo 1, o nella misura in cui l'obbligo di rendere l'informativa rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità di tale trattamento. In questo caso, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, anche rendendo pubbliche le informazioni.

Il GDPR contiene inoltre indicazioni specifiche per i casi nei quali i dati non siano stati ottenuti presso l'interessato: oltre alle informazioni richieste nell'informativa all'art. 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 regolamento 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.

Per agevolare la comprensione, il regolamento incoraggia l'utilizzo di icone in combinazione con la forma estesa per presentare i contenuti dell'informativa in forma sintetica, icone che dovranno essere identiche in tutta l'Ue e dovranno essere definite dalla Commissione.

Una maggiore comprensione e chiarezza dell'informativa si potrebbe altresì ottenere mediante la redazione di più informative che si differenzino, ad esempio, in relazione alle diverse categorie di interessati e/o servizi resi loro disponibili.

Indicazioni pratiche per la stesura dell'informativa

Dal punto di vista pratico, tenendo conto delle indicazioni di cui sopra, si possono individuare le seguenti linee guida:

- a. Articolare l'informativa su più livelli, per garantire che:
 - o le informazioni di base siano subito presentate all'interessato e risultino di immediata lettura e comprensione
 - o maggiori dettagli siano consultabili dagli interessati scegliendo sezioni di approfondimento
- b. 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 - amministrativo), ciascuna potenzialmente caratterizzata da differenti trattamenti dei dati personali

- c. 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
- d. Garantire che nel suo complesso l'informativa fornita agli interessati soddisfi i requisiti di completezza previsti dalla normativa
- e. Per i trattamenti che presentano un alto profilo di rischio per le libertà dell'interessato, potrebbe essere opportuno tenere traccia esplicita dell'avvenuta consultazione dell'informativa da parte degli utenti ed eventualmente dare evidenza dei cambiamenti intervenuti sulla stessa nel caso di cambiamenti.

Per agevolare la stesura dell'informativa, si riportano nell'Allegato 2 informazioni aggiuntive ed esempi.

Diritti "tradizionali" – considerando da 58 a 73, art. 12 a 17

I diritti azionabili dall'interessato già previsti dalla Direttiva e dal Codice, oltre a quello di ricevere idonea informativa riguardano: il diritto di accesso, la rettifica, la cancellazione, l'opposizione al trattamento.

Tra le novità previste nel nuovo GDPR rispetto alla Direttiva 95/46/CE e al Codice Italiano si citano:

- 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 definizione da parte del titolare di eventuali oneri sull'interessato nei casi particolari previsti nell'art. 12 comma 5.

A differenza della normativa previgente, è posto meno l'accento sul riscontro da fornire all'interessato per quanto attiene le modalità del trattamento: viceversa è posto l'accento su altri elementi come, ad esempio, il periodo di conservazione e le garanzie applicate in caso di trasferimento dei dati verso Paesi terzi.

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; – art. 18, 20, 21, 22

Questi nuovi diritti estendono o rafforzano analoghi diritti presenti nella Direttiva e attuati dal Codice Italiano.

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 diritti in sede giudiziaria, di tutela diritti di altra persona fisica o giuridica, o in presenza di un interesse pubblico rilevante.

Il diritto di opposizione alla profilazione che 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 compresa la profilazione. Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli 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. I titolari hanno l'obbligo di informare della richiesta di cancellazione ogni altro titolare che tratta i dati personali cancellati, compresi "qualsiasi link, copia o riproduzione". 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 al titolare; fanno eccezione quindi i dati il cui trattamento si fonda sull'interesse pubblico o sull'interesse legittimo del titolare. Per tale ragione le *implicazioni del Diritto di Portabilità dovrebbero solo residualmente interessare i trattamenti dei dati personali in ambito universitario*.

2.2.5 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 titolare, rappresentante e responsabile protezione dei dati; 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. Usabilità dell'esposizione.
Valutazione impatto	Ripensamento delle tecnologie a supporto dei trattamenti. Analisi e eventuale consultazione preventiva con l'Autorità Garante per le implicazioni sui diritti e le libertà delle persone. Obbligo del titolare, supportato dal responsabile protezione dati.
Sicurezza	Analisi dei rischi e di valutazione dell'adeguatezza delle misure tecniche e organizzative. Obbligo congiunto del titolare e del responsabile del trattamento dati.
Violazione dei dati	Equiparazione della fattispecie accidentale con quella dolosa.
Privacy by Design Privacy by Default	Applicazione delle tutele di trattamento sin dalla sua progettazione e avvio. Pseudonimizzazione e Minimizzazione (di dati e tempi) come garanzia e misura di PbD. Obbligo del titolare.
Responsabile PDP (detto anche DPO)	Si interfaccia con le Autorità Garanti. Supporta titolare e responsabile del trattamento. Obbligatorio nelle PA.
Registro Trattamenti	Registri di competenze in cui indicare le caratteristiche, le modalità e le finalità del trattamento. Lo redigono titolare e responsabile del trattamento.
Sanzioni	Sanzioni amministrative pecuniarie fino a 20 000 000 EUR

	(per le imprese, fino al 4% del fatturato globale annuo dell'esercizio precedente)
Autorità	Comitato di controllo europeo: assicura la uniforme applicazione del Regolamento. Autorità di Controllo: autorità pubblica indipendente di uno Stato membro.

IN MERITO AI NUOVI DIRITTI	
Profilazione	L'interessato ha il diritto di non subire trattamenti automatizzati (profilazione) inconsapevoli.
Portabilità dei Dati	L'interessato ha il diritto ottenere la restituzione dei propri dati personali trasmessi e trattati da un titolare e 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

Il GDPR individua i soggetti coinvolti nel trattamento sulla base:

1) delle finalità per le quali sono raccolti:

- il Titolare è la persona giuridica o la persona fisica che raccoglie i dati personali per proprie finalità e decide i mezzi per il trattamento;
- il Contitolare è la persona giuridica o la persona fisica che condivide le finalità con altro Contitolare e stabilisce insieme a questi le modalità di trattamento,
- il Responsabile del trattamento è la persona giuridica o la persona fisica che esegue dei trattamenti di dati per conto del Titolare, sulla base di un contratto o altro atto giuridico,
- il Destinatario è la persona giuridica o la persona fisica che riceve i dati dal Titolare per eseguire i trattamenti secondo le istruzioni ricevute o che esegue trattamenti per proprie finalità, nel qual caso diventa a sua volta Titolare per i trattamenti dei dati ricevuti,
- il soggetto autorizzato è la persona fisica che ha ricevuto dal titolare precise istruzioni per l'esecuzione dei trattamenti dati di sua competenza;
- l'interessato è la persona fisica che fornisce i propri dati personali a un Titolare per le finalità specificate nell'informativa;

2) delle caratteristiche del Titolare/Responsabile e delle tipologie e quantità di dati trattati:

- il Responsabile della Protezione dei Dati è la persona giuridica o la persona fisica che segue tutti i vari aspetti relativi all'applicazione del GDPR per conto del Titolare/Responsabile, deve obbligatoriamente essere presente nelle pubbliche amministrazioni;

3) dell'ambito territoriale:

- il Rappresentante nell'Unione del Titolare/Responsabile che ha la propria sede in uno stato terzo è la persona giuridica o la persona fisica che su mandato del Titolare/Responsabile funge da interlocutore per gli interessati e per le Autorità di controllo dell'Unione (ferma restando la responsabilità generale del titolare del trattamento o del responsabile del trattamento);
- l'Autorità di Controllo è la persona giuridica pubblica istituita da ogni Stato membro per sovrintendere all'applicazione e al rispetto del GDPR nell'ambito del proprio territorio;
- il Comitato Europeo per la Protezione dei Dati è la persona giuridica che a livello europeo ha il compito di coordinare il lavoro delle varie Autorità di Controllo e di supportare la Commissione.

Nell'ambito universitario la distribuzione dei ruoli e delle responsabilità costituisce una misura di sicurezza essenziale per l'applicazione del GDPR.

3.1 Titolare del trattamento

Il titolare è definito all'art. 4 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'art. 6, e decide le modalità di trattamento.

Soggetto del trattamento	Titolare (definito anche "Controller")
Persona giuridica / fisica	Università
Carica / persona fisica	Rappresentante legale dell'Ente => il Rettore dell'Ateneo
Descrizione	Il soggetto che raccoglie i dati per il conseguimento di un fine dichiarato e dispone dei mezzi per il loro trattamento.

	Il Titolare è responsabile del rispetto del GDPR all'interno del proprio ente e deve mettere in atto tutte le misure tecniche ed organizzative necessarie a garantire la protezione dei dati personali. Per dimostrare di aver rispettato tali obblighi il Titolare può aderire a codici di condotta o conseguire certificazioni come previsto dagli artt. 40 e 42 del GDPR.
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. Il Titolare risponde della corretta applicazione della normativa in materia di protezione dei dati personali. La distribuzione degli incarichi e delle responsabilità al suo interno sarà effettuata utilizzando gli strumenti di governo interno previsti dalla Legge o dallo Statuto e Regolamenti dell'Ateneo.

3.2 Contitolare

Soggetto del trattamento	Contitolare (Joint Controllers)
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. Potrebbe essere 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 potrebbero essere "contitolari" per alcune tipologie di trattamenti.
Esempi di contitolarità	Potrebbero 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 del trattamento dati

Il GDPR definisce all'art. 4 il Responsabile del trattamento quale "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento" e ne descrive le funzioni all'art.28. Differisce dalla figura di responsabile prevista dall'attuale Codice, soprattutto per quanto concerne il rispondere in solido con il Titolare di

eventuali inadempienze. Attualmente l'incarico di Responsabile del trattamento dei dati è stato assegnato internamente all'Ateneo a coloro che ricoprono funzioni di particolare rilievo organizzativo o cariche istituzionali, oltre che a soggetti esterni che eseguono trattamenti di dati per conto dell'Ateneo. Certamente è necessario che l'Università, quale Titolare, mantenga 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 Responsabile della Protezione Dati. La definizione di un'organizzazione interna finalizzata all'attuazione e al controllo efficace delle misure adottate per la protezione dei dati da parte del Titolare è un elemento fondamentale per poter dimostrare che il trattamento è effettuato conformemente al GDPR. Pertanto, per l'applicazione di tale disposizione, nell'ambito universitario, risulta utile distinguere fra la funzione di "Responsabile del trattamento", così come definita all'art.28 del GDPR, assegnata a un soggetto esterno che esegue trattamenti per conto dell'Università e la funzione che possiamo definire di "Responsabile interno" che è assegnata a personale che ricopre funzioni di particolare rilievo organizzativo. Il responsabile esterno agisce come persona giuridica/fisica autonoma e quindi risponde in solido con il titolare di eventuali inadempienze, mentre il responsabile interno agisce per conto del titolare all'interno dell'Università sulla base delle competenze attribuite alla funzione organizzativa o carica istituzionale che ricopre. Possono quindi delinearsi vari scenari di distribuzione delle responsabilità interne, secondo la dimensione e la complessità della struttura universitaria. Il Responsabile del trattamento sarà quindi sempre un soggetto esterno all'Università, mentre il responsabile interno sarà un soggetto interno, opportunamente "istruito" dal Titolare riguardo alle competenze anche decisionali in materia di protezione dei dati.

Soggetto del trattamento	Responsabile (Processor) del trattamento dati
Persona giuridica/fisica	Soggetto esterno
Carica / persona fisica	Rappresentante legale/persona fisica
Descrizione	Il responsabile 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 Responsabile della Protezione Dati, ecc.) Il Responsabile così individuato non può a sua volta nominare un altro 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 e il Titolare deve verificare che il responsabile assicuri un'adeguata protezione dei dati.
Note	In ambito universitario, è considerato "Responsabile 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 a sua volta deve garantire l'applicazione delle misure necessarie alla protezione dei dati e gli adempimenti previsti dal Regolamento. Al punto 5 dell'art. 28 è previsto che possono essere considerate garanzie sufficienti per la protezione dei dati l'adesione da parte del responsabile 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 conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi del sub-responsabile.
Esempi di responsabili del trattamento	Ad esempio CINECA, nel caso di erogazione di servizi applicativi in hosting, si configura come Responsabile del trattamento.

3.4 Soggetti autorizzati

Nelle linee guida del Garante (<http://www.garanteprivacy.it/guida-all-applicazione-del-regolamento-europeo-in-materia-di-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'art. 29 del GDPR possa concretizzarsi con l'individuazione dei soggetti autorizzati al trattamento dati all'interno dell'Università, prima denominati "incaricati". È sottolineata l'importanza di "istruire" i soggetti, sarà quindi opportuno prevedere percorsi formativi adeguati per coloro che saranno 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)
Persona fisica	Soggetto interno/esterno
Carica / persona fisica	Personale dipendente o collaboratori
Descrizione	Il GDPR non prevede espressamente la figura dell'incaricato del trattamento, ma all'art. 29 prescrive che l'accesso ai dati personali e i loro trattamenti devono essere effettuati da soggetti "istruiti" (in inglese è "on instructions") dal Titolare. Tale affermazione non esclude tuttavia che all'interno dell'Ateneo possano essere individuati coloro che sono autorizzati a effettuare i trattamenti, così come suggerito dal Garante Privacy nella guida http://www.garanteprivacy.it/guida-all-applicazione-del-regolamento-europeo-in-materia-di-protezione-dei-dati-personali. A tale scopo può essere individuata una organizzazione funzionale alla protezione dei dati, nella quale si delineano i vari ambiti di trattamento che competono ad ogni struttura e l'individuazione dei soggetti "incaricati" dei trattamenti secondo le afferenze, le mansioni e le responsabilità.
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.
Note	Analogamente a quanto è stato fatto fino ad oggi, è possibile individuare i soggetti che sono autorizzati al trattamento dei dati, mediante una nomina individuale da parte del Titolare o Responsabile del trattamento dati, oppure individuando i trattamenti che competono all'unità organizzativa di afferenza del soggetto, che risulta pertanto incaricato per "documentata preposizione ad unità organizzativa". La necessità di prevedere la designazione per iscritto del singolo incaricato o la documentata preposizione così come concepita dall'attuale normativa, non emerge in maniera esplicita dall'art. 29 del GDPR. Il termine "istruzione" del soggetto da parte del titolare indica che è necessaria una formazione/informazione specifica alla persona per ritenerla "autorizzata" ai

	trattamenti di dati personali di sua competenza. Del resto, già nella disposizione "data protection by default and by design" è previsto che in fase di progettazione di un'attività, che comporti trattamenti di dati personali, debbano essere individuate le misure di sicurezza idonee alla protezione dei dati e di conseguenza anche le opportune istruzioni per gli incaricati. L'individuazione dei soggetti autorizzati al trattamento dati è una misura di sicurezza a livello organizzativo che comunque il Titolare è tenuto ad adottare. Salvo ulteriori precisazioni da parte del Garante, gli amministratori di sistema risultano essere incaricati con particolari compiti, pertanto per questa tipologia è opportuno mantenere la nomina individuale.
--	---

3.5 Responsabile della protezione dati

Soggetto del trattamento	Responsabile della protezione dati (Data Protection Officer)
Persona giuridica / fisica	Soggetto interno/esterno
Carica / persona fisica	Persona fisica/giuridica o Gruppo di Lavoro con incarico specifico
Descrizione	Per le Università è obbligatoria la nomina di un Responsabile della Protezione Dati. L'incarico può essere affidato a personale interno o a soggetto esterno, verificando che non vi siano conflitti d'interesse. A seconda della complessità e della quantità di dati trattati, può essere individuato un team di persone che svolgono tale funzione, purché siano ben definite le mansioni e le responsabilità al suo interno. Così anche nel caso di affidamento dell'incarico a persona giuridica esterna, la quale può assolvere tale compito incaricando più persone. In questo caso, è opportuno che sia individuata una persona specifica quale punto di riferimento per l'ente. Diversamente la funzione di RPD può essere svolta per più organismi dalla stessa persona, nel caso che non sia previsto un impegno a tempo pieno. Il RPD agisce in autonomia (non riceve alcuna istruzione per quanto riguarda l'esecuzione di tali compiti) e funge da collegamento fra Titolare/Responsabile, gli interessati e l'autorità di controllo. I suoi compiti devono essere chiaramente definiti e devono essergli garantiti supporto, risorse e tempi di lavoro adeguati allo svolgimento della sua funzione. Nel caso di personale interno deve inoltre essergli garantita una formazione permanente per permettergli di rimanere aggiornato sugli sviluppi nel settore della protezione dei dati. Al RPD deve essere dato ampio accesso alle informazioni e deve essere interpellato per ogni problematica inerente la protezione dei dati e per ogni attività che implica un trattamento dati, fin dalla sua progettazione. Il RPD ha il compito di coadiuvare il Titolare/responsabile 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/Responsabile e al personale interno coinvolto nel trattamento dati sull'applicazione del GDPR. Si occupa delle comunicazioni con l'autorità di controllo e con gli interessati. Nell'assolvimento dei suoi compiti il RPD non può essere penalizzato o rimosso. Le eventuali osservazioni del RPD sull'applicazione del GDPR possono essere non accolte dal Titolare/Responsabile, specificandone i motivi. La responsabilità di eventuali mancanze è comunque a carico del solo Titolare/Responsabile. Il RPD deve essere facilmente contattabile dal personale interno, dagli interessati e dall'autorità di controllo. Pertanto i suoi recapiti (è consigliato indicare anche il nominativo, ma non è obbligatorio) devono essere ampiamente pubblicizzati.

Informazioni per l'interessato	I recapiti del RPD devono essere forniti all'interessato nell'informativa.
Note	La figura deve avere ampia autonomia. Ogni Università valuterà in base alle proprie disponibilità e caratteristiche se affidare l'incarico a personale interno o esterno. È importante verificare che non vi siano conflitti d'interesse, ossia che il RPD nominato non debba controllare attività nelle quali è direttamente coinvolto. Sul sito del Garante sono pubblicate delle linee guida specifiche per tale figura (http://www.garanteprivacy.it/rpd).

3.6 Destinatario

Il GDPR all'art. 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 debbono essere considerati destinatari tutti i soggetti che ricevono dati personali da un titolare, sia che siano interni o esterni, sia che li ricevono per eseguire trattamenti per conto del titolare sia che li ricevono per conseguire proprie finalità. I destinatari o le categorie di destinatari ai quali verranno comunicati i dati devono essere definiti in fase di raccolta dei dati per inserirli nell'informativa all'interessato. Nel caso che il destinatario sia un soggetto che risiede in un paese non membro dell'Unione, è richiesto che il Titolare verifichi 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 (recipient) è il soggetto al quale sono comunicati i dati personali da parte di un titolare. Nel GDPR il "destinatario" è definito al punto 9) dell'art. 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 art. 4). Devono pertanto considerarsi destinatari anche coloro che trattano i dati su "istruzioni" del titolare all'interno dell'Università.
Informazioni per l'interessato	Nell'informativa da fornire all'interessato devono essere indicati i destinatari o le categorie di destinatari ai quali saranno comunicati i dati, dovranno essere elencati anche le strutture interne o le categorie di personale che verranno 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, 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 che ciò non sia impossibile o richieda uno sforzo sproporzionato o

	se l'interessato 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. 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 di questi, 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 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, anche nel caso non sia possibile soddisfarla, occorre specificare la motivazione del rifiuto. Il titolare ha il compito di facilitare l'accesso all'interessato ai suoi dati, predisponendo dei canali di comunicazione dedicati, quali ad esempio i recapiti del Responsabile della Protezione dei Dati.

Per la descrizione dei trattamenti si usa raggruppare gli interessati in categorie omogenee a seconda del tipo di rapporto che questi hanno con il titolare. In ambito universitario si possono individuare le seguenti principali categorie d'interessati, le quali possono poi essere suddivise in sottocategorie per distinguerle all'interno di alcuni trattamenti:

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

3.8 L'Università quale Responsabile del trattamento dati

L'Università 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 tali casi l'Università sarà designata da tale Titolare quale Responsabile del trattamento dati. In questi casi sarà necessario prevedere l'individuazione del responsabile interno che dovrà prevedere le misure di protezione adeguate e mantenere i rapporti con il Titolare per gli adempimenti richiesti.

Un esempio di tali tipi di contratti potrebbero essere quelli per attività conto terzi in cui, ad esempio, è chiesto 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 presente regolamento (GRPD) 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 GDPR).

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 devono essere comunicati eventuali data breach.

Le Autorità di controllo sono competenti ad accogliere e decidere su eventuali reclami presentati dagli interessati.

4. Finalità istituzionali dell'Università

Nell'ambito dell'ordinamento italiano l'università 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 c. 2 del D.lgs. 165/2001 e ss.mm.

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 dell'università è disciplinata dal proprio statuto, dai propri regolamenti e dalle norme legislative che vi operano espresso riferimento.

L'università opera per il perseguimento dei propri fini istituzionali, prioritariamente individuati nella didattica e nella ricerca.

Con riferimento alle due principali finalità, si riportano, a titolo esemplificativo, i rispettivi elenchi di attività:

- 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.

Nel corso degli ultimi anni si è affiancata la c.d. Terza missione, assunta al rango di finalità istituzionale con i riconoscimenti operati, tra i primi, dal D.lgs. 19/2012, di definizione dei principi del sistema di autovalutazione, valutazione periodica e accreditamento, e dal successivo D.M. 47/2013, di identificazione degli indicatori e dei parametri di valutazione periodica della ricerca e della terza missione, con particolare riferimento all'allegato E al D.M.

Per Terza missione dell'università si intende il complesso delle attività volte alla diffusione della conoscenza e delle tecnologie, ovvero l'offerta dell'istituzione accademica a beneficio diretto della società, ovvero di soggetti terzi rispetto all'istituzione universitaria (esterni pubblici o privati).

Alla Terza missione sono riconducibili i seguenti settori:

- il trasferimento tecnologico (brevetti, attività per conto terzi - L. 370/1999, spin-off);
- l'educazione permanente (formazione sulla popolazione in età lavorativa, organizzazione di conferenze, convegni, ecc.);
- l'impegno sociale (Job Placement, assistenza alle startup, ecc.).

All'interno della Terza missione possono essere individuate attività di natura prettamente economica, ovvero attività svolta nel prevalente interesse del committente (pubblico o privato) a fronte di un corrispettivo. Detta attività è resa dall'università in ragione della sua capacità negoziale attraverso l'utilizzo del proprio personale e apparato strutturale, compatibilmente con le prioritarie ed imprescindibili finalità istituzionali di didattica e di ricerca (a titolo esemplificativo e non esaustivo si possono citare le seguenti attività: prestazioni conto terzi, prestazione a tariffario, ...).

Rileva precisare che le attività riconducibili alla Terza missione, che costituiscono appositi criteri di valutazione utilizzati dall'Agenzia Nazionale di Valutazione del Sistema Universitario e della Ricerca (ANVUR), come puntualizzato dalla stessa Agenzia, costituiscono responsabilità istituzionale a cui ogni ateneo risponde in relazione alle proprie peculiarità ed aree disciplinari, a differenza degli originari doveri istituzionali di didattica e ricerca cui non è possibile prescindere.

5. Mappa dei trattamenti dei dati personali

5.1 Premesse inerenti i trattamenti di dati personali in ambito universitario

Nel presente capitolo si è ritenuto opportuno stilare una mappatura dei principali trattamenti che trovano svolgimento in ambito universitario con l'obiettivo di:

- 1) Consentire di completare in modo più agevole il registro dei trattamenti, tenuto conto del fatto che gran parte dei dati personali e delle finalità del trattamento sono comuni a molti Atenei
- 2) Individuare le informazioni che dovranno 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
- 3) Mettere in evidenza alcune peculiarità del trattamento dei dati preso in esame ed eventuali considerazioni fatte in merito ai principali dubbi interpretativi.

La mappatura, che non è esaustiva, deve altresì essere contestualizzata rispetto al singolo Ateneo, al fine di coglierne le peculiarità. Le tabelle che seguono costituiscono pertanto una guida adattabile ai diversi contesti universitari.

Si è proceduto, innanzitutto, prendendo in considerazione la categoria di interessati cui il trattamento è rivolto (studenti – dipendenti – trattamenti trasversali a più categorie di interessati), per poi dettagliare i singoli trattamenti in relazione alle finalità da perseguire.

Infine, per ciascuna categoria di interessati e nell'ambito delle differenti finalità perseguite, sono 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'art. 9 e/o i dati relativi a condanne penali e reati di cui all'art. 10), evidenziando eventuali accorgimenti adottati da alcuni Atenei nel trattamento di tali dati.
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 nuovo 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 sulla privacy dovrà 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: sarà 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.
Note sui diritti dell'interessato	Si è ritenuto opportuno esplicitare in questa sezione alcune note inerenti i diritti dell'interessato.
Categorie di interessati	Le categorie di persone fisiche cui si riferiscono i dati personali. Ad esempio: studenti, personale dipendente, collaboratori, fornitori, ospiti.
Categorie di destinatari	È previsto individuare nell'informativa le categorie di <u>destinatari</u> 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.

5.2 Trattamenti principali inerenti gli studenti⁷

Sono indicati in questo paragrafo i principali trattamento di dati personali che riguardano le seguenti categorie di interessati:

- Coloro che intendono usufruire di attività di orientamento da parte dell'Ateneo e/o che effettuano delle prove concorsuali o selezioni allo scopo di immatricolarsi;
- Gli studenti, cioè coloro che si sono iscritti ad uno specifico corso e non hanno concluso il percorso universitario;
- Gli ex-studenti per i quali sono svolte attività di formazione, job placement o con i quali vi potrebbe essere l'interesse di mantenere e consolidare una relazione (creazione di community per attività con parti sociali o per attività di fundraising);

5.2.1 Trattamento finalizzato all'orientamento

	Elementi considerati
Descrizione del trattamento	Il dato è trattato per favorire azioni di accompagnamento e monitoraggio atte a prevenire la dispersione scolastica. I dati sono trattati, ad esempio, nell'ambito di attività di: ▪ Iscrizione ad eventi di orientamento ▪ Partecipazione a simulazioni di test o a colloqui individuali di orientamento ▪ Invio di notifiche agli interessati per iniziative di orientamento o nuovi corsi ▪ Miglioramento di attività di orientamento e di riduzione dell'abbandono, anche tramite percorsi personalizzati
Natura dei dati	Personalì, categorie particolari di dati personali (disabilità), giudiziari Dati comuni di interessati che possono essere: ▪ Persone che decidono volontariamente di aderire ad attività di orientamento e che in casi particolari possono essere anche minorenni ▪ Referenti presenti nelle Scuole.
Quali sono i dati personali strettamente necessari per	I dati personali strettamente necessari per perseguire la finalità descritta sono: dati anagrafici, dati di contatto, scuola frequentata/ente di riferimento, aree di interesse.

⁷ Si riportano di seguito le principali norme di riferimento per il trattamento di dati personali degli studenti:

R.D. 1592/1933 e successive modificazioni e integrazioni. (Testo unico delle leggi sull'istruzione superiore); R.D. 1269/1938 e successive modificazioni e integrazioni. (Approvazione del regolamento sugli studenti); D.P.R. 382/1980 (Riordinamento della docenza universitaria, relativa fascia di formazione nonché sperimentazione organizzativa e didattica); L. 168/1989 (Istituzione del Ministero dell'Università e della Ricerca scientifica e Tecnologica); L. 398/1989 (Norme in materia di borse di studio universitarie); L. 341/1990 (Riforma degli ordinamenti didattici universitari); L. 104/1992 (Legge-quadro per l'assistenza, l'integrazione sociale ed i diritti delle persone handicappate); D.M. 224/1999 (Norme in materia di dottorato di ricerca); D.lgs. 445/2000 (Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa); L. 148/2002 (Ratifica ed esecuzione della Convenzione di Lisbona dell'11 aprile 1997); D.M. 270/2004 (Modifiche al Regolamento recante norme concernenti l'autonomia didattica degli Atenei, approvato con decreto MURST 3 novembre 1999, n. 509); D.P.R. 334/2004 (Regolamento recante norme di attuazione del testo unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulle condizioni dello straniero); D.M. 25/3/1998, n. 142 e L. 24 giugno 1997, n. 196 (Normativa relativa agli stage); L. 14 febbraio 2003, n. 30 (c.d. Legge Biagi, di riforma del mercato del lavoro); Contratto Istituzionale Socrates Erasmus vigente; Statuto di Ateneo, Regolamento Didattico di Ateneo, Regolamento per la Finanza e la Contabilità, Regolamento didattico d'Ateneo ed altri Regolamenti di Ateneo vigenti; Leggi Regionali vigenti in materia di diritto allo studio universitario.

perseguire la finalità descritta	
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	Il conferimento pur essendo facoltativo è necessario perché strettamente connesso allo svolgimento di attività di interesse pubblico. È consigliato tuttavia chiarire in modo specifico le differenti finalità nell'informativa per le quali si intende trattare il dato. Nel caso di minorenni si consiglia la pubblicazione dell'informativa sui siti universitari affinché i genitori possano venire a conoscenza della stessa.
Archiviazione e conservazione (tempi, modi, quali dati)	Considerato che il dato potrebbe essere utilizzato per favorire l'analisi della qualità delle attività di orientamento (confrontando i dati raccolti, effettuando delle elaborazioni e raffronto di dati e/o verificare il successo di azioni correttive) i dati potrebbero essere archiviati e mantenuti in coerenza con il consenso acquisito per un periodo massimo di 10 anni. Tale periodo è valutato sulla base del termine massimo di durata di un percorso universitario riferito a un singolo interessato.
Note sui diritti dell'interessato	Non è consentita la rettifica dei risultati previsti nelle prove di orientamento.
Categorie di interessati	Studenti delle Scuole Superiori Studenti
Categorie di destinatari	Tutor; Uffici competenti in materia di orientamento ad es. Servizio Assistenza Disabili, Enti quali Almalaurea, Strutture addette a Counseling Psicologico
Comunicazione e trasferimento all'estero	I dati non sono comunicati all'estero.

5.2.2 Trattamento finalizzato all'erogazione dei test di ingresso o alla verifica dei requisiti di accesso

	Elementi considerati
Descrizione del trattamento	Il dato è trattato per permettere lo svolgimento delle prove di ammissione ai Corsi di Laurea a numero programmato e le prove per la valutazione della preparazione iniziale, ove previsto. I dati personali dell'interessato e i risultati ottenuti nelle prove potranno essere oggetto di trattamento anche per finalità di ricerca statistica o scientifica o per individuare delle azioni volte al miglioramento dei servizi didattici.
Natura dei dati	Personalì, categorie particolari di dati personali (dati inerenti lo stato di salute), dati personali relativi a condanne penali e reati (nel caso di studenti detenuti)
Quali sono i dati personali strettamente necessari per	Dati anagrafici, di contatto, estremi documenti identificativi, dati per la verifica dei requisiti (es. titoli) sono dati necessari per l'erogazione del servizio e per il perseguimento di attività di ricerca scientifica e/o statistica.

perseguire la finalità descritta	Nel caso in cui la pubblicazione della graduatoria sia a carico dell'Ateneo, si ritiene possano essere diffusi soltanto: nome e cognome dell'interessato (qualora non sia dotato di numero di matricola provvisoria) e, nel caso di omonimie, la data di nascita. Nel caso di disabilità o in presenza di disturbi specifici dell'apprendimento l'utente dovrà fornire anche eventuali certificazioni della diagnosi. Tali dati non dovranno essere necessariamente forniti alla Commissione se l'individuazione gli strumenti forniti per favorire lo svolgimento della prova di selezione non è effettuata dalla Commissione ma da una specifica unità organizzativa d'Ateneo a ciò deputata.
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	Si precisa che il trattamento dei dati svolto nell'ambito dei diversi corsi di laurea potrebbe essere differente e richiedere specifiche informative nelle quali dare evidenza delle responsabilità che sono in capo ad altri soggetti (es: società esterne che danno supporto per la lettura ottica dei test, CINECA, MIUR per bandi a numero programmato nazionale, ecc).
Archiviazione e conservazione (tempi, modi, quali dati)	Rispetto ai tempi di archiviazione/conservazione si specifica quanto segue: - L'anagrafica di soggetti che abbiano sostenuto la prova può essere conservata dall'Ateneo anche per interesse storico - I documenti in cui sono stampati i quesiti relativi alla prova o le risposte sono conservati secondo i tempi stabiliti nel proprio massimario. In mancanza dello stesso, si potrebbe prevedere un tempo di conservazione pari a cinque anni. - I dati inerenti graduatorie o verbali sono conservati illimitatamente nel tempo.
Note sui diritti dell'interessato	- Per quanto attiene la cancellazione, potrebbe essere concessa la cancellazione dei dati di contatto (es: indirizzo e-mail o numero di telefono), a meno che il dato non sia conservato per altre finalità (es: l'interessato è anche un dipendente dell'Ateneo). - Nel caso in cui l'interessato si opponga al trattamento della diffusione del suo nominativo tramite la graduatoria, potrebbe essere consentita la sostituzione del nominativo con le iniziali, ferma restando la necessaria valutazione che ciascun Ateneo dovrà fare in merito ai tempi di pubblicazione delle graduatorie. - Si precisa che sarebbe comunque preferibile pubblicare le graduatorie in modo da consentire la conoscenza dei risultati tramite aree riservate (il cui accesso sarà consentito a tutti i partecipanti interessati). - Coloro che risultano iscritti a una prova o selezione e non si siano presentati possono chiedere la cancellazione anche dei dati anagrafici.
Categorie di interessati	Soggetti che intendono iscriversi a un corso di laurea. In particolare nella maggior parte dei casi si tratta di studenti delle superiori (superiori ai 16 anni).
Categorie di destinatari	Uffici di Ateneo preposti alla gestione dell'iscrizione e delle carriere degli studenti, Scuole, ricercatori, servizi che si occupano di definire azioni volte al miglioramento della qualità della didattica

		Cineca (per corsi a numero programmato nazionale), società esterne alle quali è affidata la gestione di test (soprattutto nei casi di corsi a numero programmato locale), CISIA (quale Titolare autonomo), Ambasciate (in relazione all'eventuale visto rilasciato).
Comunicazione e trasferimento all'estero	e	NO

5.2.3 Trattamento finalizzato per l'erogazione del percorso formativo e gestione della carriera (dall'immatricolazione alla laurea)

	Elementi considerati
Descrizione del trattamento	Il dato è trattato per permettere la gestione degli eventi inerenti la carriera dello studente, quali la gestione del piano di studio, la registrazione degli esami e la domanda di laurea.
Natura dei dati	Personalì, categorie particolari di dati personali (stato di salute), dati personali relativi a condanne penali e reati
Quali sono i dati personali strettamente necessari per perseguire la finalità descritta	Dati anagrafici, di contatto, dati per la verifica dei requisiti e inerenti la carriera (es: titoli, valutazione di prove intermedie, prova finale). In funzione della provenienza dello studente potrebbero rendersi necessari ulteriori dati (esempio: informazioni sul permesso di soggiorno). Vengono gestite anche altre informazioni non obbligatorie in termini generali ma richieste in situazioni specifiche: dati bancari, ISEE, fotografia, contatti telefonici, contatti email personale/i). Sono di seguito descritte le principali finalità di trattamento di dati sensibili e/o dati personali relativi a condanne penali e reati: - dati relativi agli studenti e/o a familiari diversamente abili o ad elementi reddituali ai fini di un eventuale controllo sulle autocertificazioni relative alle tasse universitarie e di eventuali esoneri dal versamento delle tasse universitarie e/o fruizione di eventuali agevolazioni previste dalla legge, nonché dati relativi alla gestione dei contributi straordinari per iniziative degli studenti; - dati relativi allo status di rifugiato per la fruizione di esoneri e borse di studio; - dati relativi allo stato di gravidanza al fine di attuare tutte le cautele necessarie per la tutela della donna in stato di gravidanza, sia per motivi didattici, quali la frequenza di laboratori, sia al fine della fruizione di eventuali agevolazioni e benefici di legge; - dati idonei a rivelare le opinioni politiche o l'adesione a partiti, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale per esigenze connesse allo svolgimento delle procedure elettorali interne all'Ateneo; - dati sensibili e dati personali relativi a condanne penali e reati che si rilevano nell'ambito di procedimenti disciplinari a carico degli studenti;

	f. dati relativi alla propria condizione di salute per attività di mediazione del rapporto con i docenti, attività di interpretariato, tutorato, trasporto e servizi analoghi per tutti gli studenti con disabilità o disturbi specifici dell'apprendimento.
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	È redatta un'unica informativa e non è necessario acquisire il consenso.
Archiviazione e conservazione (tempi, modi, quali dati)	Rispetto ai tempi di archiviazione/conservazione si specifica quanto segue: ▪ L'anagrafica degli studenti e i dati di carriera sono conservati dall'Ateneo illimitatamente nel tempo ▪ I dati inerenti graduatorie o verbali sono conservati illimitatamente nel tempo ▪ La conservazione dei restanti dati è sotteso ai tempi di conservazione degli atti amministrativi che li contengono.
Note sui diritti dell'interessato	In merito alla cancellazione dei dati – non può essere concessa la cancellazione di dati personali che, per la normativa vigente o in ragione di regole d'Ateneo previste nei massimari o nei regolamenti interni: ▪ possono essere cancellati solo successivamente alla data di richiesta dell'interessato ▪ devono essere conservati illimitatamente nel tempo. In merito alla rettifica dei dati, deve essere concessa la rettifica del sesso, soprattutto a fronte di una sentenza che stabilisca l'avvenuto cambio di genere.
Categorie di interessati	Studenti Familiari (solo a fini dell'esercizio al diritto allo studio)

Categorie destinatari	di	Strutture interne dell'Ateneo preposte quali, ad esempio, Segreterie Studenti, Uffici di Segreteria Didattica, Scuole, Dipartimenti, strutture preposte alla Comunicazione. Responsabili di trattamento: eventuali fornitori di servizi per uso di canali social (es. gruppo ex-alumni); società che stampano le pergamene di laurea; ecc.. ▪ Amministrazioni certificanti in sede di controllo delle dichiarazioni sostitutive rese ai fini del DPR 445/2000; ▪ Enti locali ai fini di eventuali sussidi a favore di particolari categorie di studenti ▪ Avvocatura dello Stato, Ministero degli Affari esteri, Questure, Ambasciate, Procura della Repubblica relativamente a permessi di soggiorno, al riconoscimento di particolari status ▪ Enti di assicurazione per pratiche infortuni ▪ Organismi Regionali di Gestione (Enti dotati di autonomia amministrativo-gestionale istituiti ai sensi delle norme vigenti in materia di diritto agli studi universitari) ed altri istituti per favorire la mobilità internazionale degli studenti, ai fini della valutazione dei benefici economici e dell'assegnazione degli alloggi ▪ Agenzia Entrate per 730 nel caso di dottorandi o specializzandi ▪ MIUR ▪ Soggetti pubblici e privati per consentire agli studenti di fruire di agevolazioni, sussidi e servizi. Al fine di favorirne l'integrazione nel territorio e nell'ambiente universitario, possono altresì essere comunicati i dati inerenti agli studenti di scambio a enti, istituti o associazioni ▪ Finanziatori di premi, borse di dottorato e assegni, anche stranieri, nel caso di studenti e/o dottorandi che abbiano usufruito di finanziamenti ▪ Atenei stranieri, impegnati in percorsi formativi con rilascio di titoli congiunti ▪ Servizi penitenziari
Comunicazione trasferimento all'estero	e	I dati inerenti agli studenti di scambio possono essere traferiti, su richiesta a: ▪ Autorità all'estero (nel caso in cui sia necessario verificare il titolo di studi per ragioni professionali o per prosecuzione degli studi) ▪ Ambasciate all'estero (anche per esoneri dal servizio militare) ▪ Università extra UE (nell'ambito di scambi internazionali per studenti in-going e out-going)

5.2.4 Trattamento finalizzato all'attività di tirocinio

	Elementi considerati
Descrizione del trattamento	Il dato è trattato per la gestione dei tirocini curriculari, ovvero avviati per studenti ancora iscritti ad un CdS, che extracurriculari, dedicati a soggetti che hanno già concluso il percorso di studi. I dati sono trattati, ad esempio, nell'ambito della stipula della

	convenzione tra l'Università e l'ente/azienda o nell'ambito delle attività svolte con il supporto del tutor.
Natura dei dati	Personalì, categorie particolari di dati personali (in caso di disabilità o nel caso di disturbi specifici dell'apprendimento, dati del transgender nel caso in cui non sia intervenuta una sentenza di cambio di genere).
Quali sono i dati personali strettamente necessari per perseguire la finalità descritta	Dati anagrafici, di contatto e di carriera degli studenti. Dati dei referenti aziendali o rappresentanti legali delle aziende, informazioni necessarie per la stipula della convenzione.
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	Le informazioni inerenti questo trattamento dovrebbero essere incluse dell'informativa redatta per il trattamento di cui al paragrafo 5.2.3.
Archiviazione e conservazione (tempi, modi, quali dati)	Rispetto ai tempi di archiviazione/conservazione, si ritiene che trattandosi di dati che confluiscono nella carriera si tratti di informazioni da conservare secondo le indicazioni di cui al paragrafo 5.2.3.
Note sui diritti dell'interessato	
Categorie di interessati	Studenti, specializzandi, referenti e rappresentanti legali dell'azienda.
Categorie di destinatari	▪ Medico del lavoro o strutture sanitarie convenzionate per verifiche o cure (nei casi in cui si renda necessario verificare di aver contratto malattie infettive o nel caso di infortuni) ▪ Regione e Direzione territoriale del lavoro. ▪ Operatori pubblici e privati accreditati o autorizzati e potenziali datori di lavoro ai fini dell'orientamento e inserimento nel mondo del lavoro (ai sensi della legge 30/2003, sulla riforma del mercato del lavoro, e successive attuazioni) ▪ Enti di assicurazione per pratiche infortuni.
Comunicazione e trasferimento all'estero	Solo per tirocini attivati con Enti/aziende con sede all'estero.

5.2.5 Trattamento finalizzato ad attività di job placement

	Elementi considerati
Descrizione del trattamento	Il dato è trattato per fornire a studenti/laureati ed aziende/enti l'assistenza necessaria per l'inserimento nel mondo del lavoro, attraverso canali dedicati. Inoltre, al fine del miglior orientamento in uscita, i dati sono trattati per l'organizzazione di seminari, career day, ecc.
Natura dei dati	Personalì, categorie particolari di dati personali (disabilità, transgender).

Quali sono i dati personali strettamente necessari per perseguire la finalità descritta	Dati anagrafici, di contatto e di carriera degli studenti, CV. Dati dei referenti aziendali e/o rappresentanti legali, informazioni necessarie per la stipula della convenzione.
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	Atteso che l'attività riguarda la terza missione affidata all'Ateneo, il trattamento è di natura istituzionale.
Archiviazione e conservazione (tempi, modi, quali dati)	Nessun vincolo di conservazione.
Note sui diritti dell'interessato	-
Categorie di interessati	Laureati, studenti, referenti aziendali e rappresentanti legali
Categorie di destinatari	▪ Strutture di Ateneo preposte al Passaggio dati a Enti/aziende coinvolti nel placement. ▪ Potenziali datori di lavoro: Enti/Aziende Privati quali ad es. Banche, Comunità, Case di Cura, Fondazioni, Consorzi, congregazioni, Diocesi e Associazioni ▪ gli Enti e le Aziende diventano titolari autonomi nel trattamento effettuato, comunque connesso ai fini di selezione del personale ▪ Categorie particolari di dati personali o dati personali relativi a condanne penali e reati potranno essere comunicati ove previsto per legge o regolamento ▪ Almalaurea, nel caso in cui l'attività sia gestita in convenzione con tale soggetto.
Comunicazione e trasferimento all'estero	Solo nei casi di placement presso Enti/aziende con sede all'estero.

5.2.6 Trattamento finalizzato ad attività di fundraising, di comunicazione e informazione istituzionale e sviluppo di community

	Elementi considerati
Descrizione del trattamento	Il dato potrebbe essere trattato: ▪ per finalità di reperimento fondi ▪ sviluppo di community (anche relativi a ex studenti o ex dipendenti dell'Ateneo) ▪ promozione dell'immagine dell'Ateneo e delle sue attività, conferendo conoscenza e visibilità ad eventi organizzati dallo stesso e nei quali è coinvolto.
Natura dei dati	Personalì
Quali sono i dati personali	Dati anagrafici, di contatto, eventuali video e immagini di studenti e dipendenti, soggetti terzi (ex studenti, sostenitori, ecc.).

strettamente necessari per perseguire la finalità descritta	
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	Si precisa che il trattamento dei dati svolto nell'ambito delle diverse finalità potrebbe essere differente e richiedere specifiche informative.
Archiviazione e conservazione (tempi, modi, quali dati)	Nessun vincolo di conservazione, archiviazione di lungo periodo a fronte del consenso dell'interessato.
Note sui diritti dell'interessato	
Categorie di interessati	Studenti, Laureati, Terzi donanti, Personale, collaboratori ricerca, docenti esterni.
Categorie di destinatari	Strutture di Ateneo preposte al servizio, servizi esterni di gestione community e/o fundraising, società di spedizione, società organizzatrici di eventi.
Comunicazione e trasferimento all'estero	Sono nel caso in cui i destinatari sopra riportati (es: società americana che organizza un evento di ricerca presso l'Ateneo italiano) operino/trattino i dati in aree extra UE

5.2.7 Trattamento finalizzato a rilevazioni statistiche e valutazione della didattica

	Elementi considerati
Descrizione del trattamento	Il dato è trattato a fini di rilevazioni statistiche volte a perseguire fini istituzionali dell'Ateneo (es: attività di ricerca o attività di quality assurance o attività volte a migliorare l'immagine complessiva dell'Ateneo).
Natura dei dati	Personalì
Quali sono i dati personali strettamente necessari per perseguire la finalità descritta	Dipende dalla rilevazione richiesta e dall'ambito. Esempio: potrebbero essere trattati dati anagrafici (e/o di contatto) e dati di carriera per verificare l'adeguatezza della formazione acquisita in università, la coerenza delle competenze apprese rispetto alla futura attività lavorativa dello studente, l'utilità del titolo ottenuto rispetto all'attività lavorativa svolta o da svolgere.
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	L'informativa dovrà dettagliare le specifiche finalità della rilevazione tenuto comunque conto di quanto riferito nella legge n. 300/1970 art. 8.

Archiviazione e conservazione (tempi, modi, quali dati)	Nessun vincolo di conservazione. Conservazione dei dati dipende dal tempo definito per la finalità della raccolta posta in origine.
Note sui diritti dell'interessato	Cancellazione non possibile per questionari anonimizzati
Categorie interessati di	Studenti, Docenti
Categorie destinatari di	Strutture di Ateneo preposte al servizio (ad es. segreteria didattica, Dipartimenti, Consigli di Facoltà, Commissioni, Nucleo di Valutazione), ANVUR, MIUR,
Comunicazione trasferimento all'estero e	-

5.2.8 Trattamento finalizzato al caso di diffusione dell'elaborato finale o di elementi ad esso connessi

	Elementi considerati
Descrizione del trattamento	Il dato è trattato al fine di garantire la divulgazione dell'elaborato finale (tesi di laurea, tesi di dottorato, ecc.) e/o di elementi ad esso connessi (autore, titolo e, in genere, metadati associati), nel rispetto delle leggi sul diritto di autore
Natura dei dati	Personalì
Quali sono i dati personali strettamente necessari per perseguire la finalità descritta	Dati anagrafici, di carriera, dati di contatto e dati inerenti l'elaborato finale
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	Sarebbe preferibile consentire allo studente di individuare i dati che possono essere oggetto di diffusione, salvo il caso in cui la diffusione dei dati sia prevista da norma di legge o da un regolamento d'Ateneo. L'informativa dovrà quindi dare evidenza delle opzioni di diffusione consentite.
Archiviazione e conservazione (tempi, modi, quali dati)	Basato su obblighi di legge e regolamenti.
Note sui diritti dell'interessato	L'interessato può opporsi in qualsiasi momento alla diffusione del dato
Categorie interessati di	Studenti di corsi di Laurea e post Laurea (specializzazione, dottorato, master)

Categorie destinatari	di	Le segreterie studenti, i relatori/correlatori/contro-relatori della tesi trattano i dati personali nell'ambito della finalità descritta nella presente scheda. Trattandosi di diffusione, i destinatari sono indeterminabili. Nel caso di tesi di dottorato i dati (metadati e Full Text - dopo periodo embargo se presente) sono inviati alla Biblioteca Nazionale
Comunicazione trasferimento all'estero	e	-

5.2.9 Trattamento finalizzato a servizi di tutorato, assistenza, inclusione sociale

	Elementi considerati
Descrizione del trattamento	Trattamento finalizzato a servizi di tutorato, assistenza, inclusione sociale, supporto a persone con disabilità o disturbi specifici dell'apprendimento (DSA). È escluso il trattamento di dati personali per fini strettamente connessi alla gestione della carriera universitaria. Il trattamento di questi dati attiene ad esempio: ▪ Servizi che possono essere messi a disposizione per supportare gli studenti con disabilità negli spostamenti da e verso le strutture universitarie ▪ La diffusione di informazioni o iniziative utili a favorire l'inclusione sociale ▪ L'erogazione di servizi di supporto durante tutto il percorso di studi, con l'obiettivo di individuare e progettare i tipi di sostegno necessari ad ogni studente per svolgere con profitto il proprio corso di studi.
Natura dei dati	Personalì, categorie particolari di dati personali (inerenti lo stato di salute)
Quali sono i dati personali strettamente necessari per perseguire la finalità descritta	Dati anagrafici, di carriera, sensibili (legati, ad esempio, alla specifica disabilità o DSA)
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	Si rende opportuno redigere un'unica informativa che dia contezza delle specifiche finalità perseguite dall'Ateneo nell'ambito dell'erogazione di attività di supporto per studenti disabili o con DSA
Archiviazione e conservazione (tempi, modi, quali dati)	Basato su obblighi di legge e regolamenti. ▪ Legge 104/92 - Legge-quadro per l'assistenza, l'integrazione sociale e i diritti delle persone handicappate. ▪ Legge 170/10 - Nuove norme in materia di disturbi specifici di apprendimento in ambito scolastico. ▪ Legge 68/99 - Norme per il diritto al lavoro dei disabili ▪ Legge 4/04 - Disposizioni per favorire l'accesso dei soggetti disabili agli strumenti informatici

		Legge 17/99 - Integrazione e modifica della legge-quadro 5 febbraio 1992, n. 104, per l'assistenza, l'integrazione sociale e i diritti delle persone handicappate
Note sui diritti dell'interessato		-
Categorie interessati	di	Studenti di corsi di laurea e post laurea, specializzandi, dottorandi, familiari/accompagnatori/curatori
Categorie destinatari	di	Strutture di Ateneo preposte, società di trasporti, helping services, meeting services, tutor, associazioni o organizzazioni con le quali sono avviate attività di collaborazione per la realizzazione delle finalità suddette (esempio: fondazioni che si occupano di DSA, associazioni specifiche).
Comunicazione trasferimento all'estero	e	-

5.2.10 Trattamento finalizzato all'erogazione di servizi e attività per il diritto allo studio.

	Elementi considerati
Descrizione del trattamento	Il trattamento è finalizzato a garantire il diritto allo studio attraverso il quale lo studente ha la possibilità di fruire di agevolazioni, sussidi, borse di studio e servizi: - per il miglioramento delle condizioni di studio e di vita degli studenti; - per la realizzazione di attività culturali, sportive e ricreative a favore della popolazione studentesca
Natura dei dati	Personalì, categorie particolari di dati personali (disabilità, DSA o, nel caso di organizzazioni studentesche che hanno una connotazione politica o religiosa, potrebbero essere trattati dati idonei a rivelare convinzioni politiche, religiose, filosofiche, ecc..).
Quali sono i dati personali strettamente necessari per perseguire la finalità descritta	Dati anagrafici, di carriera, sensibili, economici per procedure di esonero o di rimborso, borse di studio
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	Le informazioni inerenti il trattamento di dati personali per questa finalità dovrebbero essere inseriti nell'informativa generale resa al momento dell'iscrizione.
Archiviazione e conservazione (tempi, modi, quali dati)	Basato prevalentemente su obblighi di legge e regolamenti.

Note sui diritti dell'interessato	-
Categorie interessati	di Studenti, specializzandi, dottorandi, familiari
Categorie destinatari	di Strutture di Ateneo preposte (es segreterie studenti), enti esterni per realizzare servizi integrati a favore degli studenti universitari e preposti per favorire l'esercizio del diritto allo studio.
Comunicazione trasferimento all'estero	e -

5.2.11 Procedimenti di natura disciplinare a carico di studenti

	Elementi considerati	
Descrizione del trattamento	Il trattamento è finalizzato allo svolgimento di procedimenti disciplinari a carico di studenti	
Natura dei dati	Personalì, categorie particolari di dati personali e dati personali relativi a condanne penali e reati	
Quali sono i dati personali strettamente necessari per perseguire la finalità descritta	Dati anagrafici, di carriera e dati inerenti lo specifico procedimento	
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	Le informazioni inerenti il trattamento di dati personali per questa finalità dovrebbero essere inseriti nell'informativa generale resa al momento dell'iscrizione.	
Archiviazione e conservazione (tempi, modi, quali dati)	Basato su obblighi di legge e regolamenti. Il periodo di conservazione indicato in alcuni massimari di scarto per la conservazione degli atti connessi a questa attività è: - illimitato, per il provvedimento finale - 5 anni per i provvedimenti revocati o annullati.	
Note sui diritti dell'interessato	-	
Categorie interessati	di	Studenti, specializzandi, dottorandi, eventuali ulteriori soggetti coinvolti nel procedimento
Categorie destinatari	di	Strutture di Ateneo preposte, Autorità Giudiziaria, Docenti
Comunicazione trasferimento all'estero	e	Per studenti internazionali, Università di provenienza

5.3 Trattamenti principali inerenti a dipendenti e/o collaboratori

Sono indicati in questo paragrafo i principali trattamento di dati personali che riguardano:

- il personale dipendente e/o i collaboratori
- soggetti terzi (esempio: fornitori, partner di ricerca, ecc.).

5.3.1 Trattamento finalizzato allo svolgimento di prove concorsuali/selezioni

	Elementi considerati
Descrizione del trattamento	Il dato è trattato al fine di consentire agli interessati di accedere ai ruoli previsti dai bandi di Ateneo, accertandone la sussistenza dei requisiti richiesti per l'espletamento delle attività di selezione.
Natura dei dati	Personalì, categorie particolari di dati personali, dati personali relativi a condanne penali e reati.
Quali sono i dati personali strettamente necessari per perseguire la finalità descritta	Anagrafica (nome, cognome, la data ed il luogo di nascita, CF residenza, cittadinanza italiana), documento identità, contatti, curriculum vitae, eventuali disabilità, eventuali condanne penali, cariche politiche (solo ai commissari di concorso), titoli, ecc., esiti concorso.
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	L'informativa deve essere resa specificatamente per la selezione.
Archiviazione e conservazione (tempi, modi, quali dati)	Basato su obblighi di legge e regolamenti.
Note sui diritti dell'interessato	-
Categorie di interessati	Partecipanti alla selezione/concorso.
Categorie di destinatari	▪ Area del personale e strutture di Ateneo per finalità istituzionali o per osservanza obblighi legislativi (nome, cognome ed esito pubblico) ▪ Membri delle Commissioni esaminatrici ▪ MIUR, nell'ambito delle comunicazioni obbligatorie previste per il personale docente e ricercatore che risulti vincitore ▪ Amministrazioni certificanti in sede di controllo delle dichiarazioni sostitutive rese ai fini del DPR 445/2000
Comunicazione e trasferimento all'estero	I dati non sono trasferiti all'estero.

5.3.2 Trattamento finalizzato alla gestione del rapporto di lavoro

	Elementi considerati
Descrizione del trattamento	Trattamento necessario per la gestione del rapporto di lavoro o di collaborazione, anche per personale in convenzione. In questo trattamento rientrano anche la: ▪ gestione dell'offerta formativa e dell'assegnazione degli incarichi (quadro didattico) ▪ gestione della struttura organizzativa, dell'anagrafica del personale e registrazione degli eventi di carriera (giuridico) ▪ gestione delle pratiche assicurative e previdenziali; trattamenti assistenziali; denunce e pratiche di infortunio, trattamenti assistenziali ▪ trattamento dei dati inerenti i procedimenti disciplinari a carico del personale e nei giudizi pendenti di fronte a tutte le giurisdizioni che coinvolgono docenti, dipendenti, collaboratori ▪ gestione delle risorse umane (posizioni organizzative, profili di competenza, repertorio aziendale delle conoscenze, processo di selezione, politiche retributive) ▪ gestione della formazione ▪ rilevazione e gestione delle presenze ▪ gestione retributiva ▪ gestione dei provvedimenti per il personale (es. mobilità, trasferimenti, ecc.) ▪ programmazione annuale degli obiettivi e dei progetti, finalizzata alla valutazione del personale, alla pianificazione finanziaria e alla predisposizione del budget di Area/Amministrazione Centrale.
Natura dei dati	Personalì, categorie particolari di dati personali, dati personali relativi a condanne penali e reati.
Quali sono i dati personali strettamente necessari per perseguire la finalità descritta	Il principio di minimizzazione impone una selezione dei dati da trattare in relazione allo specifico servizio o finalità perseguita, ad esempio: ▪ per la gestione dei dati anagrafici e amministrativo contabili dei collaboratori esterni possono essere trattati dati inerenti l'anagrafica, dati bancari, fiscali e previdenziali; ▪ per la gestione del personale docente possono essere trattati dati relativi alla costituzione/cessazione del rapporto di lavoro, alle procedure di valutazione comparativa, al reclutamento, agli affidamenti, agli incarichi esterni; ▪ per la gestione personale T.A. possono essere trattati dati relativi alla costituzione/cessazione del rapporto di lavoro, a concorsi e selezioni, a incarichi esterni, alla mobilità. ▪ per la gestione degli istituti contrattuali possono essere trattati dati relativi a congedi, permessi, aspettative, malattie, infortuni, partecipazioni a scioperi e assemblee, ecc.
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	Le informazioni inerenti il trattamento di dati personali per questa finalità dovrebbero essere inseriti nell'informativa generale resa al momento dell'assunzione e dell'avvio del rapporto di collaborazione.
Archiviazione e conservazione	Rispetto ai tempi di archiviazione/conservazione si specifica quanto segue: ▪ L'anagrafica e i dati di carriera sono conservati dall'Ateneo illimitatamente nel tempo

(tempi, modi, quali dati)		▪ I dati inerenti graduatorie o verbali sono conservati illimitatamente nel tempo ▪ La conservazione dei restanti dati è sotteso ai tempi di conservazione degli atti amministrativi che li contengono (per maggiori info si veda il "Massimario di selezione dei documenti inerenti al fascicolo di personale universitario")
Note sui diritti dell'interessato		In merito alla cancellazione dei dati – non può essere concessa la cancellazione di dati personali che, per la normativa vigente o in ragione di regole d'Ateneo previste nei massimari o nei regolamenti interni devono essere conservati illimitatamente nel tempo.
Categorie interessati	di	Tutti i dipendenti dell'organizzazione e collaboratori.
Categorie destinatari	di	Strutture di Ateneo (ad es. Strutture del Personale e Stipendi) Altri soggetti pubblici o privati, tra cui: ▪ Amministrazioni certificanti in sede di controllo delle dichiarazioni sostitutive rese ai fini del DPR 445/2000; ▪ INPDAP – INPS (per erogazione e liquidazione trattamento di pensione, L. 335/1995; L. 152/1968); ▪ Comitato di verifica per le cause di servizio e Commissione medica territorialmente competente (nell'ambito della procedura per il riconoscimento della causa di servizio/equo indennizzo, ai sensi del DPR 461/2001); ▪ INAIL, Autorità di P.S., Sportello unico per l'immigrazione (DPR n. 334/2004) e/o altre Autorità previste dalla legge (per denuncia infortunio, DPR 1124/1965); ▪ Strutture sanitarie competenti (per visite fiscali, art. 21 CCNL del 06/07/1995, CCNL di comparto); ▪ Soggetti pubblici e privati ai quali, ai sensi delle leggi regionali/provinciali, viene affidato il servizio di formazione del personale; ▪ Direzione Territoriale del lavoro (per le aspettative e per i casi di contenzioso) ▪ Centro per l'impiego o organismo territorialmente competente per le assunzioni ai sensi della legge 68/1999; ▪ Amministrazioni provinciali e Centro regionale per l'impiego in ordine al prospetto informativo delle assunzioni, cessazioni e modifiche al rapporto di lavoro, redatto ai sensi della L. 68/1999; ▪ Autorità giudiziaria (C.P. e C.P.P.); ▪ Organizzazioni sindacali per gli adempimenti connessi al versamento delle quote di iscrizione e per la gestione dei permessi sindacali; ▪ Ministero delle Finanze, nell'ambito dello svolgimento da parte delle Università del ruolo di Centro di assistenza fiscale (CAF), relativamente alla dichiarazione dei redditi dei dipendenti (art.17 D.M. 164/1999 e art. 2-bis D.P.R. 600/1973); ▪ Pubbliche Amministrazioni presso le quali vengono comandati i dipendenti, nell'ambito della mobilità dei lavoratori.
Comunicazione trasferimento all'estero	e	I dati personali potrebbero essere trasferiti all'estero nel caso di periodi di formazione del personale all'estero.

5.3.3 Trattamento di dati personali ai fini di formazione e aggiornamento professionale

	Elementi considerati
Descrizione del trattamento	Il trattamento di dati personali è svolto per l'erogazione di attività didattiche e di formazione/aggiornamento (frontale, multimediale e a distanza). Rientrano in questo tipo di trattamento anche i trattamenti per: ▪ Iscrizione a corsi di formazione ▪ Gestione dei registri delle attività didattiche: consuntivazione attività didattiche e non, a preventivo e consuntivo ▪ Valutazioni qualità, nell'ipotesi in cui i questionari possano essere indirettamente riconducibili a un interessato. ▪ Eventuali attestati di frequenza ai corsi
Natura dei dati	Personalì, categorie particolari di dati personali (solo per i casi in cui debbano essere predisposte misure particolari per l'organizzazione dei corsi)
Quali sono i dati personali strettamente necessari per perseguire la finalità descritta	In relazione allo specifico corso/servizio erogato, potrebbero essere trattati: dati presenti in anagrafica, dati di carriera, curriculum vitae, ore di rendicontazione della docenza, iscrizioni e partecipazioni a corsi di formazione.
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	L'informativa potrebbe essere inclusa tra le informazioni rese al momento della gestione del rapporto di dipendenza o collaborazione. Nel caso in cui, durante la sessione di formazione, siano registrate le immagini e/o le voci di docenti e/o partecipanti, si rende opportuno informare gli interessati di tale trattamento mediante, ad esempio, affissione dei cartelli informativi
Archiviazione e conservazione (tempi, modi, quali dati)	Gli atti connessi alle attività di formazione svolte dai partecipanti potrebbero avere un tempo di conservazione simile a quello previsto per gli atti di carriera. La conservazione delle registrazioni audio/video dovrà essere stabilita nell'informativa in relazione alle specifiche finalità perseguite dall'ente.
Note sui diritti dell'interessato	Potrebbe essere garantita l'opposizione a specifiche operazioni di trattamento delle riprese audio-video (es: nel caso di diffusione del video su internet).
Categorie di interessati	Personalì (personale docente, T.A., assegnisti, collaboratori, studenti 150 ore, laureati frequentatori).

Categorie di destinatari	Strutture di Ateneo deputate alla formazione e all'aggiornamento professionale di dipendenti e collaboratori altre Università (ad esempio nell'ambito di corsi di formazione erogati tra più università partner) Enti/Aziende esterne eroganti il servizio di formazione e aggiornamento professionale Enti pubblici convenzionati, con lo scopo di migliorarne la fruibilità e di garantire la qualità e l'efficacia della formazione sul territorio nazionale.
Comunicazione e trasferimento all'estero	Eventuali Università/Enti esteri, ad esempio per favorire la formazione all'estero dei dipendenti dell'Ateneo.

5.3.4 Trattamento di dati personali necessario alla gestione di progetti di ricerca

	Elementi considerati
Descrizione del trattamento	Il trattamento dei dati è finalizzato, in particolare, a: ▪ curare le attività legate ai finanziamenti per la ricerca e la formazione scientifica; ▪ garantire il coordinamento delle attività di ricerca, in particolare a livello comunitario ed internazionale; ▪ favorire lo sviluppo dell'attività di ricerca e valorizzarne i risultati.
Natura dei dati	Personali
Quali sono i dati personali strettamente necessari per perseguire la finalità descritta	Dati di anagrafica e di carriera, dati di contatto, codici identificativi univoci internazionali (es.: ORCID) riferiti a uno specifico ricercatore. Per quanto riguarda l'anagrafica della gestione dei progetti: dati descrittivi ricerca, finanziamenti e cofinanziamenti erogati, gruppo ricerca (anagrafica interni), enti partner e ente finanziatore. Per quanto attiene gli strumenti di rendicontazione e di consuntivazione (ad es. tramite TimeSheet UGOV) sono trattati: Anagrafica, Carriera, Attribuzione Ore a ricerca e didattica
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	Le informazioni inerenti questo trattamento potrebbero essere integrate nell'informativa generale inerente la gestione del rapporto di lavoro.
Archiviazione e conservazione (tempi, modi, quali dati)	I tempi di conservazione dei dati sono strettamente dipendenti dagli ambiti di gestione (es: carriera, rendicontazione, ecc..) e dalle norme vigenti in tali ambiti.
Note sui diritti dell'interessato	-
Categorie di interessati	Personale Docente/Ricercatori/Assegnisti/Dottorandi e Tecnico Amministrativo

Categorie destinatari	di	▪ Strutture di Ateneo deputate (Contabilità, Servizi per Ricerca) ▪ CINECA (Responsabili Esterni) ▪ ANVUR ▪ Soggetti finanziatori (MIUR, Regioni, UE, ecc)
Comunicazione trasferimento all'estero	e	Enti/Aziende estere quali partecipanti alla ricerca o finanziatori

5.3.5 Trattamento di dati personali al fine di garantire il monitoraggio e la valutazione della ricerca

	Elementi considerati
Descrizione del trattamento	Il trattamento è finalizzato al monitoraggio e valutazione della ricerca: classificazione e catalogazione dei prodotti della ricerca (IRIS Sistema di Gestione dei dati della Ricerca) e valutazione della ricerca
Natura dei dati	Personalì
Quali sono i dati personali strettamente necessari per perseguire la finalità descritta	Dati di anagrafica e di carriera, dati di contatto, codici identificativi univoci internazionali (es.: ORCID) riferiti a uno specifico ricercatore. Per quanto riguarda l'anagrafica della gestione dei progetti: dati descrittivi ricerca, finanziamenti e cofinanziamenti erogati, gruppo ricerca (anagrafica interni), enti partner e ente finanziatore. Per quanto attiene gli strumenti di rendicontazione e di consuntivazione (ad es. tramite TimeSheet UGOV) sono trattati: Anagrafica, Carriera, Attribuzione Ore a ricerca e didattica
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	Le informazioni inerenti questo trattamento potrebbero essere integrate nell'informativa generale inerente la gestione del rapporto di lavoro.
Archiviazione e conservazione (tempi, modi, quali dati)	I tempi di conservazione dei dati sono strettamente dipendenti dagli ambiti di gestione (es: carriera, rendicontazione, ecc.) e dalle norme vigenti in tali ambiti.
Note sui diritti dell'interessato	-
Categorie interessati	Personale Docente/Ricercatori/Assegnisti/Dottorandi e Tecnico Amministrativo
Categorie destinatari	▪ Strutture di Ateneo deputate (Contabilità, Servizi per Ricerca) ▪ CINECA (Responsabili Esterni) ▪ ANVUR ▪ Soggetti finanziatori (MIUR, Regioni, UE, ecc.)

Comunicazione trasferimento all'estero	e	Enti/Aziende estere quali partecipanti alla ricerca o finanziatori
---	----------	--

5.3.6 Trattamento di dati personali nell'ambito di attività di trasferimento tecnologico

		Elementi considerati
Descrizione del trattamento		Il trattamento è finalizzato alla valorizzazione commerciale dei risultati della ricerca scientifica e tecnologica conseguiti nell'ambito dell'organizzazione universitaria, nonché alla tutela dell'opera dell'ingegno. In particolare i dati sono trattati per la valorizzazione delle invenzioni, per il deposito delle domande di brevetto e per la ricerca di partner interessati alla commercializzazione dei brevetti. Il trattamento è altresì funzionale alla creazione di iniziative imprenditoriali innovative (spin-off).
Natura dei dati		Personalì
Quali sono i dati personali strettamente necessari per perseguire la finalità descritta		Dati di anagrafica e di carriera e dati di contatto.
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso		L'informativa è da rendersi al primo contatto.
Archiviazione e conservazione (tempi, modi, quali dati)	e	I tempi di conservazione dei dati sono strettamente dipendenti dagli ambiti di gestione (es: carriera, rendicontazione, ecc.) e dalle norme vigenti in tali ambiti.
Note sui diritti dell'interessato		-
Categorie interessati	di	Personale Docente/Ricercatori/Assegnisti/Dottorandi/Studenti e Tecnico Amministrativo, soggetti partner e finanziatori.
Categorie destinatari	di	Strutture di Ateneo deputate (Area della Ricerca), Istituzioni, Consulenti, altri Atenei, Uffici brevetti, Partners.
Comunicazione trasferimento all'estero	e	In occasione del deposito di domande di brevetto internazionali e della stipula di accordi con soggetti extra UE.

5.3.7 Trattamento necessario per politiche Welfare e per la fruizione di agevolazioni

		Elementi considerati
Descrizione del trattamento	del	Il dato è trattato al fine di consentire la promozione di politiche volte a consentire al personale dell'Ateneo di fruire di agevolazioni, servizi e/o sussidi.

Natura dei dati	Personalì, categorie particolari di dati personali (disabilità, DSA).
Quali sono i dati personali strettamente necessari per perseguire la finalità descritta	Anagrafica (eventualmente anche dati familiari), carriera e dati, ISEE. Potrebbero rendersi necessari altri dati connessi al tipo di servizio.
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	Le informazioni inerenti il trattamento di dati personali per questa finalità dovrebbero essere inseriti nell'informativa generale resa al momento dell'assunzione.
Archiviazione e conservazione (tempi, modi, quali dati)	Basato prevalentemente su obblighi di legge e regolamenti.
Note sui diritti dell'interessato	-
Categorie di interessati	Dipendenti e familiari.
Categorie di destinatari	▪ Strutture di Ateneo preposte ▪ Fornitori/Enti/Cooperative ad es. per attività dopo Lavoro, Aziende per erogazione polizze assicurative per il personale ▪ Enti esterni per realizzare servizi integrati a favore dei dipendenti e/o preposti a favorire l'attuazione di politiche Welfare
Comunicazione trasferimento all'estero	I dati non sono comunicati all'estero.

5.3.8 Trattamenti per la salute e la sicurezza delle persone nei luoghi di lavoro

5.3.8.1 Trattamenti effettuati dal Medico Competente

	Elementi considerati
Descrizione del trattamento	Il dato è trattato dal Medico Competente al fine di svolgere l'attività di sorveglianza sanitaria obbligatoria del personale, ottemperando agli obblighi di legge come definiti dal D. Lgs. 81/08 - Testo Unico in materia di salute e sicurezza del lavoro e dal D.Lgs. 230/95
Natura dei dati	Personalì, categorie particolari di dati personali (dati inerenti lo stato di salute, referti medici)
Quali sono i dati personali strettamente necessari per perseguire la finalità descritta	Dati anagrafici, dati di contatto, dati inerenti lo stato di salute, dati inerenti l'attività lavorativa svolta e di carriera

Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	Informativa specifica per il servizio da rendere all'interessato all'atto della visita medica
Archiviazione e conservazione (tempi, modi, quali dati)	I tempi di conservazione dei dati sono strettamente dipendenti dagli ambiti di gestione (es: fascicolo sanitario/referti/gestione amministrativa) e dalle norme vigenti in tali ambiti
Note sui diritti dell'interessato	-
Categorie interessati di	Tutti i dipendenti dell'organizzazione ed eventualmente studenti (es. CdL di area medica) e collaboratori sulla base dei protocolli di rischio in rapporto alle attività svolte
Categorie destinatari di	Ufficio Prevenzione, Protezione e Sicurezza; Ufficio Personale; ASST
Comunicazione trasferimento all'estero e	I dati non vengono comunicati all'estero, salvo casi specifici che lo richiedano (es. emergenze sanitarie)

5.3.8.2 Trattamenti effettuati dall'Ufficio Prevenzione, Protezione e Sicurezza

	Elementi considerati
Descrizione del trattamento	Il dato è trattato dall'Ufficio Prevenzione, Protezione e Sicurezza al fine di supportare il Medico Competente nell'attività di sorveglianza sanitaria obbligatoria del personale, ottemperando agli obblighi di legge come definiti dal D. Lgs. 81/08 - Testo Unico in materia di salute e sicurezza del lavoro.
Natura dei dati	Personalì, categorie particolari di dati personali (dati inerenti lo stato di salute).
Quali sono i dati personali strettamente necessari per perseguire la finalità descritta	Dati anagrafici, dati di contatto, dati inerenti lo stato di salute, dati inerenti l'attività lavorativa svolta e di carriera.
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	Le informazioni inerenti il trattamento di dati personali per questa finalità dovrebbero essere inseriti nell'informativa generale resa al momento dell'assunzione.
Archiviazione e conservazione (tempi, modi, quali dati)	I tempi di conservazione dei dati sono strettamente dipendenti dagli ambiti di gestione e dalle norme vigenti in tali ambiti.
Note sui diritti dell'interessato	-

Categorie interessati	di	Tutti i dipendenti dell'organizzazione ed eventualmente studenti (es. CdL di area medica) e collaboratori sulla base dei protocolli di rischio in rapporto alle attività svolte.
Categorie destinatari	di	Ufficio Personale; Medico Competente; ASST; Responsabili di struttura.
Comunicazione trasferimento all'estero	e	I dati potrebbero essere comunicati all'estero in rapporto alle attività svolte (es. ricerche svolte all'estero o svolte sul territorio italiano con necessità di trasmissione all'estero).

5.3.9 Trattamento dei dati personali nell'ambito dell'erogazione del servizio di telefonia fissa e mobile

	Elementi considerati
Descrizione del trattamento	Il dato è trattato al fine di gestire tutte le attività inerenti la gestione delle linee telefoniche fisse e/o mobili e dei dispositivi, la relativa rendicontazione, nonché il servizio di assistenza all'utenza.
Natura dei dati	Personalì.
Quali sono i dati personali strettamente necessari per perseguire la finalità descritta	Anagrafica del personale, carriera, struttura di appartenenza, prefissi (livelli di autorizzazione per l'effettuazione di chiamate), chiamate da/all'esterno, spese, abilitazioni alla doppia fatturazione, altre informazioni sul traffico dati, quali: a. il numero o l'identificazione dell'utente e del soggetto cui la chiamata è trasmessa; b. il numero totale degli scatti o il tempo di durata del traffico da considerare per il periodo di rendicontazione; c. il tipo, l'ora di inizio e la durata delle chiamate effettuate e il volume dei dati trasmessi; d. la data della chiamata o dell'utilizzazione del servizio; e. informazioni concernenti i pagamenti. Con riguardo alla telefonia mobile, verranno trattati anche ulteriori dati personali con finalità di rendicontazione ed addebito.
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	Con riferimento alla telefonia fissa, le informazioni inerenti il trattamento di dati personali per questa finalità dovrebbero essere inseriti nell'informativa generale resa al momento dell'assunzione. In relazione alla telefonia mobile, è opportuno rilasciare apposita informativa all'atto della consegna del telefono di servizio.
Archiviazione e conservazione (tempi, modi, quali dati)	6 mesi per i dati di traffico telefonico (nel caso di dati non tracciati dall'operatore telefonico). I tempi di conservazione dei dati di traffico telefonico tracciati dall'operatore sono quelli stabiliti dalla normativa vigente.
Note sui diritti dell'interessato	-

Categorie interessati	di	Tutti gli intestatari di un'utenza fissa e/o mobile; soggetti che ricevono o effettuano delle chiamate su utenze d'Ateneo.
Categorie destinatari	di	I responsabili delle strutture per le utenze di competenza; i soggetti che gestiscono la fatturazione nelle singole strutture; la struttura che si occupa della gestione dei servizi di telefonia.
Comunicazione trasferimento all'estero	e	I dati non vengono comunicati all'estero.

5.4 Trattamenti trasversali o connessi ad attività trasversali

5.4.1 Trattamento dei dati nell'ambito della gestione degli spazi

	Elementi considerati
Descrizione trattamento	del Il dato è trattato al fine di permettere l'utilizzo degli spazi dell'Ateneo, per attività quali: ▪ assegnazione degli spazi alle strutture, allocazione delle persone negli spazi; ▪ controllo accessi ai varchi da parte di: dipendenti, collaboratori e studenti; ▪ la gestione centralizzata e coordinata delle aule e degli spazi per la didattica; ▪ la gestione delle procedure amministrative per richieste di spazi per eventi istituzionali; ▪ la gestione delle procedure amministrative per richieste di spazi da parte di soggetti terzi.
Natura dei dati	Personalì, categorie particolari di dati personali (dati inerenti lo stato di salute).
Quali sono i dati personali strettamente necessari per perseguire la finalità descritta	Con riferimento al richiedente lo spazio, verranno trattati dati di anagrafica personale e di carriera. In relazione all'utilizzo degli spazi da parte di soggetti terzi, verranno trattati anche ulteriori dati personali, riconducibili ad esigenze di carattere amministrativo (es. per verificare la validità delle autorizzazioni ad accedere a spazi d'Ateneo). Per l'accesso agli spazi da parte di soggetti disabili, potranno esser trattati dati inerenti lo stato di salute. L'eventuale decisione di effettuare il controllo degli accessi potrebbe comportare la raccolta di dati di ingresso/uscita/identificativo utente (ad es. il badge).
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	Con riferimento a soggetti interni all'ente, le informazioni inerenti il trattamento di dati personali per questa finalità dovrebbero essere inseriti nell'informativa generale resa al momento dell'attivazione del rapporto con l'Ateneo (assunzione, immatricolazione, attivazione del contratto di collaborazione). Nel caso di soggetti terzi, dovrà essere rilasciata apposita informativa all'atto del conferimento dei dati.

Archiviazione e conservazione (tempi, modi, quali dati)	I tempi di conservazione dei dati personali sono legati alle procedure interne di gestione degli spazi. Nel caso in cui siano affidati spazi a soggetti esterni (a fronte di un compenso) la conservazione dei dati sarà strettamente connessa ai tempi di conservazioni previsti dalle norme vigenti in materia contabile.
Note sui diritti dell'interessato	-
Categorie interessati di	Tutti i dipendenti, collaboratori, studenti e soggetti terzi.
Categorie destinatari di	Strutture di Ateneo preposte alla gestione logistica, responsabili di struttura ed eventuali soggetti delegati alla gestione della logistica. Alcune informazioni potrebbero essere disponibili con accesso pubblico (es: consultazione da rubrica della collocazione delle persone negli spazi).
Comunicazione trasferimento all'estero e	-

5.4.2 Trattamento dei dati personali per la gestione delle postazioni

	Elementi considerati
Descrizione del trattamento	Il dato è trattato per garantire il corretto funzionamento di postazioni di lavoro fisse / mobili assegnate agli utenti, la sicurezza delle stesse e per fornire il necessario supporto nell'utilizzo. Per questo tipo di trattamento è necessario effettuare la DPIA.
Natura dei dati	Qualsiasi tipologia di dato utilizzato dall'utente (in alcuni casi perfino di natura genetica se l'utente dovesse svolgere ricerca nel campo della genetica medica).
Quali sono i dati personali strettamente necessari per perseguire la finalità descritta	Dati relativi all'utente, struttura di appartenenza, dati di contatto. Associazione utenti/postazioni assegnate. Nella gestione delle postazioni, in dipendenza del tipo di intervento, potrebbero verificarsi da parte degli amministratori di sistema accessi, anche fortuiti, a categorie particolari di dati personali memorizzati sulle postazioni, in ragione dell'effettiva capacità di azione sulle informazioni e della rilevanza e specificità del ruolo.
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	Le informazioni inerenti il trattamento di dati personali per questa finalità dovrebbero essere inseriti nell'informativa generale resa al momento dell'attivazione del rapporto con l'Ateneo (assunzione, attivazione del contratto di collaborazione) o al momento dell'iscrizione a un corso (per gli studenti).
Archiviazione e conservazione (tempi, modi, quali dati)	I tempi di conservazione dei dati personali relativi alle assegnazioni ed ai ticket di segnalazioni sono legati alle procedure interne di gestione. I tempi di conservazione di altre informazioni personali variano in funzione del tipo di intervento effettuato (es. dati per troubleshooting).

Note sui diritti dell'interessato		Anche in relazione alla tipologia di monitoraggio effettuato e ai software utilizzati, nell'eventualità in cui possa derivarne un controllo a distanza del lavoratore, occorrerà verificare la necessità di stipulare un accordo con le rappresentanze sindacali o con la sede territoriale competente dell'Ispettorato nazionale del lavoro. Al contrario, l'installazione e utilizzo di software per garantire il monitoraggio, la sicurezza e la gestione delle postazioni saranno possibili se strettamente connessi al rapporto di lavoro.
Categorie interessati	di	Tutti gli utilizzatori di postazioni soggette ad autenticazione.
Categorie destinatari	di	Gestore delle postazioni e dell'assistenza.
Comunicazione trasferimento all'estero	e	Eventuale produttore di soluzioni SW installate (S.O., applicativi, endpoint security)

5.4.3 Trattamento per attività di gestione degli organi e delle cariche istituzionali

5.4.3.1 Trattamento finalizzato alla gestione degli elenchi per l'elettorato attivo e passivo

	Elementi considerati
Descrizione del trattamento	Il dato è trattato, nell'ambito del rinnovo degli organi istituzionali, per la gestione degli elenchi dell'elettorato attivo e passivo, per le sostituzioni dei componenti e per verificare i requisiti di eleggibilità. In dato considerato è inerente alle elezioni in senso stretto e a eventuali valutazioni di incompatibilità.
Natura dei dati	Personalì, categorie particolari di dati personali (es: per l'appartenenza a organizzazioni sindacali, associazioni politiche, religiose, ecc), dati personali relativi a condanne penali e reati. I verbali potrebbero riportare dati relativi allo stato di salute nel caso in cui un elettore abbia fatto ricorso al voto assistito.
Quali sono i dati personali strettamente necessari per perseguire la finalità descritta	Oltre ai nominativi, al ruolo e a eventuali informazioni connesse alla presentazione delle liste elettorali, in alcuni Atenei e/o per alcune elezioni specifiche, potrebbero rendersi necessaria la: ▪ Consultazione del Casellario Giudiziale (dato acquisito e conservato tipicamente in forma cartacea dall'ufficio preposto). ▪ Consultazione carriera studente per verifica dello stato di attività e di regolarità dei pagamenti.
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	Le informazioni inerenti il trattamento di dati personali per questa finalità dovrebbero essere inseriti nell'informativa generale resa: ▪ al momento dell'assunzione, per il personale Docente/Ricercatore e Tecnico Amministrativo; ▪ al momento dell'immatricolazione, per la popolazione studentesca.

Archiviazione e conservazione (tempi, modi, quali dati)	Il tempo di conservazione dei dati dipende dallo specifico procedimento e si basa su quanto previsto da obblighi di legge o regolamenti interni.
Note sui diritti dell'interessato	Eventuale cancellazione solo dopo espletamento degli obblighi di legge o regolamento interno.
Categorie interessati di	Tutti i potenziali eletti ed elettori.
Categorie destinatari di	Strutture dell'Ateneo preposte (ad es. Ufficio affari istituzionali), MIUR per specifici organi, associazioni studentesche.
Comunicazione trasferimento all'estero e	-

5.4.3.2 Trattamento finalizzato alla nomina degli eletti e delle cariche accademiche

	Elementi considerati
Descrizione del trattamento	Il dato è trattato ai fini della gestione della nomina degli eletti e delle cariche accademiche, nonché per la verifica della presenza di eventuali cause di incompatibilità con la carica da assumere.
Natura dei dati	Personalì, categorie particolari di dati personali, dati personali relativi a condanne penali e reati.
Quali sono i dati personali strettamente necessari per perseguire la finalità descritta	Dati di anagrafica e di carriera, dati di contatto e dati personali relativi a condanne penali e reati per l'eventuale consultazione del casellario giudiziale.
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	Le informazioni inerenti il trattamento di dati personali per questa finalità dovrebbero essere inseriti nell'informativa generale resa: ▪ al momento dell'assunzione, per il personale Docente/Ricercatore e Tecnico Amministrativo; ▪ al momento dell'immatricolazione, per la popolazione studentesca.
Archiviazione e conservazione (tempi, modi, quali dati)	Il tempo di conservazione dei dati dipende dallo specifico procedimento e si basa su quanto previsto da obblighi di legge o regolamenti interni.
Note sui diritti dell'interessato	Eventuale cancellazione solo dopo decadenza carica, espletamento degli obblighi di legge o regolamento interno.
Categorie interessati di	Tutto il personale dell'organizzazione, studenti, eventuali terzi

Categorie destinatari	di	Ufficio di Ateneo preposto, tutta la popolazione dell'organizzazione.
Comunicazione trasferimento all'estero	e	-

5.4.3.3 Trattamento finalizzato alla pubblicizzazione di atti ai fini di trasparenza

	Elementi considerati
Descrizione del trattamento	Il dato è trattato per finalità di trasparenza come da normativa vigente sul sito istituzionale per la parte di "Amministrazione Trasparente". Si precisa che i dati potrebbero essere originariamente raccolti per finalità differente (ad es. espletamento di un incarico istituzionale), ma che, per vincoli normativi, vengono trattati anche a tal fine.
Natura dei dati	Personalì.
Quali sono i dati personali strettamente necessari per perseguire la finalità descritta	Dati di carriera, dati di reddito, curriculum vitae, cariche, sovvenzioni, contributi, sussidi, vantaggi economici, spese sostenute. Tale trattamento riguarda, ad es., la pubblicazione del C.V. e della situazione reddituale delle cariche del Consiglio di Amministrazione e del Senato Accademico, nonché del C.V. e dei dati retributivi del Direttore Generale e dei Dirigenti.
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	Le informazioni inerenti il trattamento di dati personali per questa finalità dovrebbero essere inseriti nell'informativa generale resa: ▪ al momento dell'assunzione, per il personale Docente/Ricercatore e Tecnico Amministrativo; ▪ al momento dell'immatricolazione, per la popolazione studentesca; ▪ all'atto dell'inizio del rapporto di collaborazione per soggetti esterni.
Archiviazione e conservazione (tempi, modi, quali dati)	Sulle pagine web del sito di Ateneo vengono, ai fini della trasparenza, pubblicate informazioni già presenti nelle basi di dati del sistema informativo gestionale. Tempi e contenuti di pubblicazione su web di tali informazioni sono normati dagli obblighi di legge in materia di trasparenza, cui deve conformarsi il processo di generazione e pubblicazione delle pagine, nel rispetto dei vincoli imposti dal GDPR. Ciò impone l'individuazione di un corretto bilanciamento tra gli obblighi di pubblicazione e la necessità di minimizzare, in termini di articolazione e tempo di esposizione, il set di dati personali presentati sulle pagine web utilizzando ove necessario pseudonimizzazione o anonimizzazione. I tempi di archiviazione e conservazione sono quelli specifici delle singole informazioni e dei relativi trattamenti primari e non dipendono dal processo di pubblicazione sul web ai fini della trasparenza.
Note sui diritti dell'interessato	L'eventuale cessazione di carica, incarico o rapporto di lavoro o collaborazione dell'interessato non implicano la corrispondente rimozione delle relative informazioni dalle pagine web di

		pubblicazione ai fini della trasparenza, comunque subordinata a suddetti obblighi di legge. Non possono pertanto essere accolte eventuali richieste di rimozione di informazioni da tali pagine che risultino in contrasto con gli obblighi di pubblicazione.
Categorie interessati	di	Personale dell'organizzazione, studenti, soggetti terzi.
Categorie destinatari	di	Ufficio di Ateneo preposto, tutta la popolazione dell'organizzazione. Si precisa che tali dati sono soggetti a diffusione.
Comunicazione trasferimento all'estero	e	-

5.4.4 Trattamento per la gestione degli infortuni

		Elementi considerati
Descrizione del trattamento	del	Il trattamento viene effettuato in relazione agli infortuni occorsi al personale docente, tecnico amministrativo, agli studenti ed ai soggetti terzi in visita. In particolare nell'ambito della gestione di tali eventi da parte degli uffici dell'Ateneo preposti, dalla presa in carico della segnalazione di infortunio fino alla chiusura della relativa pratica, includendo: - l'interazione con enti esterni - la gestione di eventuali prescrizioni da parte dell'INAIL - l'apertura e gestione della segnalazione di sinistro nell'ambito di copertura delle polizze assicurative dell'Ateneo - la valutazione delle proposte di liquidazione del danno - gli eventuali prolungamenti del periodo di infortunio
Natura dei dati		Personalì, categorie particolari di dati personali (dati inerenti lo stato di salute).
Quali sono i dati personali strettamente necessari per perseguire la finalità descritta		Dati anagrafici, di carriera e dati inerenti lo stato di salute. Dati specifici relativi all'infortunio occorso (es referti, certificati).
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso		Le informazioni inerenti il trattamento di dati personali per questa finalità dovrebbero essere inseriti all'atto dell'apertura del sinistro.
Archiviazione e conservazione (tempi, modi, quali dati)	e	Il tempo di conservazione dei dati dipende dallo specifico procedimento e si basa su quanto previsto da obblighi di legge o regolamenti interni.
Note sui diritti dell'interessato		-
Categorie interessati	di	Tutto il personale dell'organizzazione e soggetti terzi.

Categorie destinatari	di	Uffici dell'Ateneo coinvolti nella gestione degli infortuni, broker, compagnia assicuratrice, Inail, eventuali ulteriori enti coinvolti (Aziende ospedaliere).
Comunicazione trasferimento all'estero	e	I dati saranno comunicati e/o trasferiti all'estero in presenza di una compagnia assicuratrice estera o nel caso di soggetti coinvolti in infortuni all'estero.

5.4.5 Trattamento in ambito bibliotecario

	Elementi considerati
Descrizione del trattamento	Il dato è trattato al fine di consentire al personale docente, tecnico amministrativo, popolazione studentesca e ai cittadini, di accedere ai servizi centralizzati offerti dal sistema bibliotecario e ai locali e servizi offerti dalle singole Biblioteche di Ateneo (consultazione e prestito patrimonio bibliografico e documentale su supporto cartaceo e elettronico, prestito interbibliotecario e document delivery, reference, ecc.) e per informazione sulle attività e servizi offerti. I dati possono essere oggetto di trattamento in forma anonima per lo svolgimento di attività statistiche e rilevazioni del grado di soddisfazione finalizzate al miglioramento dei servizi offerti. Differente è il caso che la biblioteca tratti dati relativi alle condizioni di salute nel caso eroghi servizi specificamente o esclusivamente rivolti a utenti con disabilità (es. postazioni o dispositivi con tecnologie assistive, ecc.)
Natura dei dati	Personalì (Dati anagrafici, di contatto, estremi documenti identificativi nel caso di utenti esterni), categorie particolari di dati personali (esempio nel caso di utenti in stato di transizione) È altresì possibile che la biblioteca tratti dati relativi alle condizioni di salute nel caso eroghi servizi specificamente o esclusivamente rivolti a utenti con disabilità (es. postazioni o dispositivi con tecnologie assistive, ecc.)
Quali sono i dati personali strettamente necessari per perseguire la finalità descritta	Dati anagrafici, di contatto e di carriera (personale o studenti), materiali bibliografici e documentali in prestito o consultati.
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	Le informazioni inerenti il trattamento di dati personali per questa finalità dovrebbero essere rese nel momento in cui l'utente accede ad un servizio bibliotecario.
Archiviazione e conservazione (tempi, modi, quali dati)	I tempi di conservazione sono strettamente dipendenti dall'esistenza di vincoli di archiviazione di tali informazioni.
Note sui diritti dell'interessato	Cancellazione solo dopo espletamento degli obblighi di legge o regolamento interno (es. completata restituzione di materiale)

		bibliografici e documentali in prestito, ecc.) e in assenza di vincoli archivistici.
Categorie interessati	di	Tutto il personale dell'organizzazione e soggetti terzi.
Categorie destinatari	di	Strutture Bibliotecarie dell'ente, altre strutture dell'Ateneo (es. Segreterie Studenti per nulla osta per iter conseguimento titolo). Eventuali aziende/cooperative che prestano servizio per le biblioteche dell'ente. Nel caso in cui i servizi bibliotecari siano integrati con quelli di altri enti sottoscrittori di una convenzione ad hoc. Biblioteche di altre istituzioni e università (prestito interbibliotecario/document delivery).
Comunicazione trasferimento all'estero	e	Nel caso di utilizzo in cloud di soluzioni Integrated Library Systems (ILS) ed altri applicativi per servizi di biblioteca quali Discovery tool, link resolver, Ask a librarian, ecc.

5.4.6 Trattamento di dati nell'ambito dei servizi di protocollo e conservazione documentale

5.4.6.1 Trattamento finalizzato alla gestione del protocollo in entrata/uscita

		Elementi considerati
Descrizione trattamento	del	Gestione del protocollo informatico nelle fasi di entrata/uscita al fine di fornire data e ora certa agli atti acquisiti o trasmessi da una Pubblica Amministrazione. Le registrazioni di protocollo ed i file a esso associati, prodotti e raccolti nell'ambito delle funzioni dell'Ente ed entro le Aree Organizzative Omogenee dello stesso per l'espletamento di procedimenti, affari ed attività, sono: - accessibili ai responsabili ed agli operatori preposti, con diritti di registrazione e consultazione definiti da specifiche policy indicate nel manuale di gestione del protocollo; - ottemperano quando previsto dal DPCM 3.13.2013 – regole tecniche per il protocollo informatico e in particolare dagli articoli 6, 7, 8, 18, 20, 21; - sottoposte alla gestione dei pacchetti di distribuzione e di versamento sulla base degli accordi presi con il conservatore accreditato prescelto.
Natura dei dati		In funzione del procedimento/affare/attività i documenti possono contenere dati personali, anche appartenenti a particolari categorie (es sensibili o giudiziari). Ogni dato e documento inserito nel sistema di protocollo potrebbe contenere tali dati nella: - descrizione del documento e sua rappresentazione, oggetto, allegati, classificazione, file associati (nativi digitali o loro conversione in formato digitale)

	indicazione dei corrispondenti/contraenti e dei responsabili e assegnatari del documento.
Quali sono i dati personali strettamente necessari per perseguire la finalità descritta	Dati anagrafici dei mittenti e destinatari. Il campo oggetto, incluso nel nucleo minimo delle informazioni necessarie per la registrazione a protocollo, potrebbe per sua natura riportare dati personali, anche appartenenti a particolari categorie (es sensibili o giudiziari). I dati trattati dipendono dallo specifico procedimento/affare/attività e sempre nell'osservanza del DPCM 3.12.2013, tanto in materia di protocollo informatico (ai sensi degli articoli 40bis, 41, 47, 57bis e 71 del CAD) tanto in materia di conservazione (ai sensi degli articoli 20, commi 3 e 5bis, 23ter, comma 3, 43, commi 1 e 3, 44, 44bis e 71 comma 1 del CAD) Potrebbe rendersi necessaria anche la registrazione di ulteriori dati personali per supportare e motivare (a titolo di esempio): - la creazione del pacchetto di distribuzione per motivi legali o accessi agli atti concorsuali - l'accesso al sistema di conservazione per la verifica dell'operato del conservatore o per verifiche di carattere tecnico.
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	Le informazioni inerenti il trattamento di dati personali per questa finalità dovrebbero essere inseriti nell'informativa generale resa: - al momento dell'assunzione, per il personale Docente/Ricercatore e Tecnico Amministrativo; - al momento dell'immatricolazione, per la popolazione studentesca - all'inizio di un rapporto di collaborazione con un soggetto esterno.
Archiviazione e conservazione (tempi, modi, quali dati)	Il tempo di conservazione dei dati dipende dallo specifico procedimento/affare/attività e si basa su quanto previsto da obblighi di legge e regolamenti interni.
Note sui diritti dell'interessato	-
Categorie di interessati	Studenti, personale, terzi.
Categorie di destinatari	Strutture di Ateneo – e loro operatori e delegati - preposte al processo di gestione documentale attraverso l'utilizzo dei sistemi di protocollo informatico o applicativi verticali che concorrono al popolamento del registro di protocollo informatico. Mittenti o destinatari delle registrazioni a protocollo.
Comunicazione e trasferimento all'estero	-

5.4.6.2 Trattamento finalizzato alla Conservazione Documentale

	Elementi considerati
--	-----------------------------

Descrizione del trattamento	Gestione delle attività di conservazione documentale ai sensi della normativa vigente.
Natura dei dati	Ogni dato e documento inserito nel sistema di protocollo informatico e potenziale oggetto di invio in conservazione, ovvero: - descrizione del documento e sua rappresentazione, ovvero numero di protocollo ed eventuale repertorio, data, oggetto, allegati, classificazione, file associati (nativi digitali o loro conversione in formato digitale) - indicazione dei corrispondenti/contraenti e dei responsabili e assegnatari del documento In funzione del procedimento/affare/attività i documenti possono contenere dati personali, anche appartenenti a particolari categorie (es. sensibili o giudiziari).
Quali sono i dati personali strettamente necessari per perseguire la finalità descritta	Dati anagrafici dei mittenti e destinatari. Il campo oggetto, incluso nel nucleo minimo delle informazioni necessarie per la registrazione a protocollo, potrebbe per sua natura riportare dati personali, anche appartenenti a particolari categorie (es sensibili o giudiziari). I dati trattati dipendono dallo specifico procedimento/affare/attività e sempre nell'osservanza del DPCM 3.12.2013, tanto in materia di protocollo informatico (ai sensi degli articoli 40bis, 41, 47, 57bis e 71 del CAD) tanto in materia di conservazione (ai sensi degli articoli 20, commi 3 e 5bis, 23ter, comma 3, 43, commi 1 e 3, 44, 44bis e 71 comma 1 del CAD) Potrebbe rendersi necessaria anche la registrazione di ulteriori dati personali per supportare e motivare (a titolo di esempio): - la creazione del pacchetto di distribuzione per motivi legali o accessi agli atti concorsuali - l'accesso al sistema di conservazione per la verifica dell'operato del conservatore o per verifiche di carattere tecnico.
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	Le informazioni inerenti il trattamento di dati personali per questa finalità dovrebbero essere inseriti nell'informativa generale resa: - al momento dell'assunzione, per il personale Docente/Ricercatore e Tecnico Amministrativo; - al momento dell'immatricolazione, per la popolazione studentesca
Archiviazione e conservazione (tempi, modi, quali dati)	Il tempo di conservazione dei dati dipende dallo specifico procedimento/affare/attività e si basa su quanto previsto da obblighi di legge e da regolamenti interni. Per quanto attiene la conservazione illimitata, si ricordano le principali tipologie di documentazione: Registro di protocollo informatico e RIP, Decreti (rettorali, direttoriali, dirigenziali), Verbali e Delibere degli Organi di Governo (CDA, Senato, Nucleo di valutazione), Verbali e Delibere di Scuole, Scuole Specializzazione, Consigli di Dipartimento, Contratti (compresi i contratti di lavoro),

		gare e convenzioni, Circolari di Ateneo. Per quanto riguarda le fatture e i documenti contabili la conservazione è 10 anni. In materia di conservazione accreditata, ogni accordo di versamento prevede specifico riferimento al tempo di conservazione (illimitato, limitato).
Note sui diritti dell'interessato		-
Categorie di interessati	di	Studenti, personale, terzi.
Categorie destinatari	di	- Strutture di Ateneo – e loro operatori e delegati - preposte al processo di gestione documentale e alla conservazione. - Conservatore digitale accreditato AgID - Destinatari del pacchetto di distribuzione per motivi legali o accesso agli atti (interni Ateneo o esterni) previa autorizzazione della struttura organizzativa coinvolta.
Comunicazione e trasferimento all'estero	e	-

5.4.7 Trattamento finalizzato all'acquisto di beni e servizi, stipula di contratti, recupero crediti, gestione del contenzioso

5.4.7.1 Trattamento finalizzato all'acquisizione di beni e servizi

	Elementi considerati
Descrizione del trattamento	Il dato è trattato per consentire la verifica di posizioni giudiziarie, fiscali e di condotta di fornitori ed operatori economici che sono in rapporto con l'Ateneo al fine di: ▪ svolgere le attività preliminari connesse alle procedure di acquisizione di beni e servizi; ▪ coordinare e analizzare la redazione della documentazione tecnica, amministrativa e contrattuale; ▪ gestire il procedimento e le attività connesse (stipula del contratto, monitoraggio dei tempi del procedimento in affidamento).
Natura dei dati	Personalità, dati personali relativi a condanne penali e reati
Quali sono i dati personali strettamente necessari per perseguire la finalità descritta	Potrebbe rendersi necessaria la registrazione di dati personali presenti nella documentazione inerente: ▪ DURC (acquisendo parte dei dati da Inps e altri da Inail) ▪ Visure camerali (acquisiti da Infocamere) ▪ Certificato di Casellario Giudiziale (Tribunale) ▪ accertamenti sulla situazione societaria e personale delle controparti (Anac) ▪ verifica regolarità fiscale (Agenzia delle entrate ed Equitalia per il pregresso) Nel caso di acquisti sopra soglia è necessario altresì acquisire i dati inerenti:

	▪ Offerta economica, in sede di apertura del fascicolo di gara (svolto dalla Commissione per la valutazione dell'offerta); ▪ certificazioni antimafia (acquisita presso la Prefettura/Questura). Tali verifiche potrebbero essere svolte anche per i casi di avvalimento.
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	L'informativa può essere resa al momento della pubblicazione del bando per la fornitura di beni o servizi. Al momento della stipula del contratto si può consegnare un'ulteriore informativa più specifica in funzione del servizio reso o del bene acquisito.
Archiviazione e conservazione (tempi, modi, quali dati)	I tempi possono essere molto diversi a seconda del tipo di contratto e dell'oggetto della fornitura. Il criterio per stabilirli si basa su principi di buon senso e sulle precisazioni dell'Autorità Garante secondo cui i dati possono essere conservati in generale "finché sussista un interesse giustificabile" e cioè finché la loro conservazione risulti necessaria agli scopi per i quali sono stati raccolti e trattati. Ad esempio nel caso in cui si acquisti un bene con garanzia a vita o un software con licenza d'uso illimitata in senso temporale i dati possono essere conservati a tempo indeterminato, comunque fino a che il bene o il software non viene dismesso. Più in generale, i dati dovrebbero essere conservati in linea con quanto previsto dal Codice Civile (art. 2220).
Note sui diritti dell'interessato	-
Categorie di interessati	Fornitori di beni e servizi, operatori economici.
Categorie di destinatari	Strutture preposte all'acquisto di beni e servizi, alla liquidazione o alla gestione del contenzioso; struttura preposta al rispetto delle norme su trasparenza e anticorruzione.
Comunicazione e trasferimento all'estero	-

5.4.7.2 Trattamento finalizzato alle verifiche sull'espletamento di lavori, in cantiere o presso installazioni in Ateneo

	Elementi considerati
Descrizione del trattamento	Il dato è trattato per la valutazione amministrativa ed economica di terzi, fornitori dell'Ateneo per l'espletamento di lavori in appalto, verifiche sui cantieri o presso installazioni in Ateneo.
Natura dei dati	Personalì, categorie particolari di dati personali, dati personali relativi a condanne penali e reati.
Quali sono i dati personali strettamente necessari per	Potrebbe rendersi necessaria la registrazione di dati personali per consentire, ad esempio: - La consultazione del contratto dei lavoratori delle ditte appaltatrici e di quelle sub-appaltate;

perseguire la finalità descritta	- La verifica di atti relativi ai dipendenti delle società.
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	L'informativa è predisposta al momento della gara e allegata al bando.
Archiviazione e conservazione (tempi, modi, quali dati)	I tempi di conservazione dei dati dipendono dallo specifico procedimento e dalla normativa vigente in materia di appalti, sicurezza sul lavoro e conduzione di cantieri.
Note sui diritti dell'interessato	-
Categorie di interessati	Fornitori.
Categorie di destinatari	Strutture di Ateneo preposte al processo (area edilizia e sicurezza sul lavoro).
Comunicazione e trasferimento all'estero	Normalmente non ci sono comunicazioni all'esterno.

5.4.7.3 Trattamento finalizzato alla gestione del contenzioso e del recupero crediti

	Elementi considerati
Descrizione del trattamento	Il dato è trattato per: - la gestione dei contenziosi instaurati avanti le diverse autorità giudiziarie in cui sia coinvolta l'Università; - l'attività di recupero dei crediti dell'Università nei confronti di personale docente/ricercatore e tecnico-amministrativo, degli studenti e di soggetti terzi inadempienti.
Natura dei dati	Personalì, categorie particolari di dati personali, dati personali relativi a condanne penali e reati.
Quali sono i dati personali strettamente necessari per perseguire la finalità descritta	I dati trattati possono essere differenti a seconda del tipo di contenzioso; includerà in ogni caso i dati anagrafici e il tipo di rapporto con l'Ateneo; potrebbe includere dati sanitari. Per il recupero crediti, la tipologia di dati trattati sarà in correlazione alla categoria di interessati coinvolta.
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	Le informazioni inerenti il trattamento di dati personali per questa finalità potrebbero essere inserite in un'apposita informativa o nell'informativa generale resa: - al personale docente/ricercatore e tecnico-amministrativo; - agli studenti; - a soggetti terzi e aziende fornitrici di beni e servizi.

Archiviazione e conservazione (tempi, modi, quali dati)		I tempi di conservazione sono definiti per legge.
Note sui diritti dell'interessato		-
Categorie di interessati	di	Sono interessati potenzialmente tutti i soggetti che abbiano un rapporto con l'Ateneo: personale docente-ricercatore, personale tecnico-amministrativo, studenti dell'Ateneo o di altri Atenei, candidati, soggetti terzi (fornitori). Può interessare anche persone che non hanno rapporti di alcun tipo con l'Ateneo (es. studente di scuola superiore che accede ai locali per informazioni). Con riguardo ad alcuni contenziosi e procedimenti di recupero crediti potrebbero essere interessati anche i familiari dei soggetti direttamente coinvolti (ad es. richiesta di restituzione borse di studio a seguito di verifica autocertificazione situazione reddituale/patrimoniale).
Categorie destinatari	di	Ufficio d'Ateneo preposto, Avvocatura dello Stato (quando rappresenta l'Ateneo in giudizio), Autorità Giudiziarie, MIUR (nei casi di coinvolgimento anche del Ministero nel contenzioso), Presidenza del Consiglio dei Ministri (ad es. per i casi di contenzioso riguardanti l'adeguamento retributivo dei medici specializzandi) e Agenzia delle Entrate (nel caso di iscrizione a ruolo dei crediti).
Comunicazione trasferimento all'estero	e	Potrebbe esser necessaria la comunicazione e/o il trasferimento di dati all'estero nei casi di contenzioso con soggetti esteri e nel caso di recupero crediti da debitori esteri, con affidamento della pratica a professionisti stabiliti nei paesi dei soggetti con i quali si sia instaurata la lite.

5.4.8 Trattamento di dati nell'ambito dei servizi di posta elettronica e strumenti di collaboration

5.4.8.1 Trattamento finalizzato all'accesso agli strumenti di collaboration

	Elementi considerati
Descrizione del trattamento	Al fine di favorire la collaborazione, l'Ateneo potrebbe fornire strumenti informatici (es: web conference, spazi virtuali di collaborazione, ecc) tramite i quali possono essere trattati dati personali funzionali: ▪ all'erogazione del servizio stesso ▪ a connesse attività di risoluzione dei guasti (troubleshooting) ▪ alla valutazione dell'uso del servizio e della qualità (es: mediante rilevazioni statistiche basate sull'uso di tali strumenti) ▪ a garantire la sicurezza informativa dei dati trattati mediante tali strumenti di collaboration.
Natura dei dati	Personalì, categorie particolari di dati personali.
Quali sono i dati personali	A seconda del tipo di attività o strumento di collaborazione potrebbero essere utilizzati dati quali, l'indirizzo di posta

strettamente necessari per perseguire la finalità descritta	elettronica, l'indirizzo IP del sistema utilizzato, dati relativi alla carriera, dati anagrafici, ecc.
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	L'informativa dovrebbe essere resa prima dell'accesso al sistema, qualora non specificato in informative specifiche.
Archiviazione e conservazione (tempi, modi, quali dati)	I tempi possono essere molto diversi a seconda del tipo di strumento utilizzato e della finalità perseguita. Il criterio per stabilirli si basa su principi di buon senso e sulle precisazioni dell'Autorità Garante secondo cui i dati possono essere conservati in generale "finché sussista un interesse giustificabile" e cioè finché la loro conservazione risulti necessaria agli scopi per i quali sono stati raccolti e trattati. Normalmente tale periodo di conservazione non supera i 6 mesi.
Note sui diritti dell'interessato	-
Categorie di interessati	Personale dipendente, collaboratori esterni, studenti interni, studenti di altro ateneo, altri soggetti utilizzatori del servizio
Categorie di destinatari	Ufficio di Ateneo preposto alla gestione e/o utilizzo dello strumento di collaboration
Comunicazione e trasferimento all'estero	Solo in caso di servizio erogato outsourcer estero e nel caso in cui sia lecita la comunicazione di tali dati personali

5.4.8.2 Trattamento finalizzato all'erogazione di servizi di posta elettronica

	Elementi considerati
Descrizione del trattamento	Al fine di favorire la comunicazione istituzionale tramite i servizi di posta elettronica, l'Ateneo potrebbe trattare dati personali funzionali a: ▪ l'erogazione del servizio stesso ▪ lo svolgimento attività connesse alla risoluzione dei guasti (troubleshooting) ▪ la valutazione dell'uso del servizio e della qualità del servizio (es: mediante rilevazioni statistiche basate sull'uso di tali strumenti) ▪ garantire la sicurezza informativa dei dati trattati (tramite ad esempio la gestione di incidenti di sicurezza e tramite azioni preventive sulla diffusione di messaggi contenenti malware).
Natura dei dati	Personalì.
Quali sono i dati personali strettamente necessari per perseguire la finalità descritta	Indirizzi e-mail. All'atto della creazione dell'account o in caso di cambio di status dell'utente all'interno dell'Ateneo (se sono previste differenze di gestione delle caselle a seconda del ruolo), anche anagrafica dell'utente (codice fiscale, matricola, ruolo ricoperto).

	Nella gestione legata al troubleshooting, incidenti di sicurezza e azioni preventive sulla diffusione di messaggi malevoli, potrebbe rendersi necessario il trattamento dei seguenti dati connessi ai messaggi di posta: casella di posta sorgente, casella destinataria, server in entrata e uscita, server di transito, oggetto mail, timestamp.
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	Le informazioni inerenti il trattamento di dati personali per questa finalità dovrebbero essere inseriti nell'informativa generale resa: ▪ all'assunzione, per il personale docente/ricercatore e tecnico-amministrativo; ▪ all'immatricolazione, per gli studenti; ▪ alla richiesta di creazione dell'account per soggetti terzi.
Archiviazione e conservazione (tempi, modi, quali dati)	In generale dipende dai regolamenti interni, che spesso prevedono differenze di trattamento a seconda del tipo di utente (es. tempi di cancellazione della casella di posta diversi a seconda del ruolo).
Note sui diritti dell'interessato	Cancellazione solo dopo un determinato periodo dalla cessazione del rapporto.
Categorie di interessati	Personale dipendente e non (inclusi docenti a contratto), studenti, associazioni ufficiali, ospiti frequentatori.
Categorie di destinatari	Struttura di Ateneo preposta al servizio di posta elettronica (in genere area IT) e aziende fornitrici.
Comunicazione e trasferimento all'estero	Solo nel caso di servizio di posta esternalizzato su outsourcer estero.

5.5 Trattamento di dati personali nell'ambito dell'erogazione federata di servizi

Al fine di garantire un maggior livello di sicurezza della gestione delle identità digitali e dell'autorizzazione nell'accesso ai servizi, è ormai assunto come riferimento un modello basato su nodi che possono implementare i seguenti ruoli:

- **Identity Provider (IdP)**: gestore delle identità digitali degli utenti:
 - o supporta la registrazione e gestione delle informazioni ad esse associate nonché delle credenziali di accesso
 - o rende disponibile servizi di autenticazione.
- **Service Provider (SP)**: erogatore di servizi ad utenti autenticati ed opportunamente profilati.

In ambito universitario i principali esempi di fruizione federata di servizi fanno riferimento a:

- **Eduroam** <https://www.servizi.garr.it/eduroam>: servizio che permette agli utenti in mobilità presso organizzazioni federate di accedere in modo semplice e sicuro alla rete wireless usando le credenziali fornite dalla propria organizzazione
- **IDEM** <https://www.idem.garr.it/>: federazione italiana di Identity e Service Provider (in gran parte Università ed Enti di Ricerca) gestita e coordinata da GARR, che federa infrastrutture di autenticazione ed autorizzazione basate su SAML2 e tipicamente implementate tramite Shibboleth.

- **SPID** (Sistema Pubblico di Identità Digitale) <https://www.spid.gov.it/>: permette di accedere a tutti i servizi online della Pubblica Amministrazione:
 - o utilizzando Identità Digitali gestite da un ristretto set di IdP certificati
 - o mediante credenziali (es. username, password, OTP) caratterizzate da un Level of Assurance adeguato al livello di sicurezza richiesto dal SP.

5.5.1 Trattamento finalizzato all'erogazione del servizio Eduroam

	Elementi considerati
Descrizione del trattamento	Il trattamento è volto a garantire l'accesso in mobilità degli utenti alla rete Eduroam. Nel caso l'ente sia IdP e nel caso accetti di avere informazioni relative ai propri utenti, l'ente potrà ricevere i log di connessione degli utenti appartenenti alla propria organizzazione anche quando tali utenti sono in altre università. Se l'ente è un SP, allora tratterà dati personali di utenti appartenenti ad altra organizzazione solo nel caso in cui l'IdP di appartenenza dell'utente non supporti il passaggio anonimo delle identità degli utenti
Natura dei dati	Personalì.
Quali sono i dati personali strettamente necessari per perseguire la finalità descritta	Username, MAC, IP, timestamp.
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	Le informazioni registrate vengono mantenute per un periodo di 6 (sei) mesi, o maggiore se prescritto dalla legislazione in vigore. https://www.servizi.garr.it/eduroam/aderire/documenti-template/1-regolamento-della-federazione-italiana-eduroam
Archiviazione e conservazione (tempi, modi, quali dati)	Non è possibile la cancellazione dei log di autenticazione se non dopo 6 mesi o per il periodo prescritto dalla legislazione.
Note sui diritti dell'interessato	Cancellazione log di autenticazione.
Categorie di interessati	Personale docente e tecnico amministrativo, studenti, ospiti di università federate.
Categorie destinatari	Università federate, Polizia in caso di incidente.
Comunicazione e trasferimento all'estero	Università federate se estere.

5.5.2 Trattamento finalizzato all'accesso a servizi federati (es IDEM)

Nell'ambito di federazioni di Identity e Service Provider, l'accesso ai servizi da parte degli utenti prevede tipicamente che, nell'ambito di una sessione autenticata da uno degli IdP, il SP di competenza riceva alcuni attributi aggiuntivi necessari per l'autorizzazione e la profilazione dell'utente.

Il set di informazioni personali passato dall'IdP è variabile in funzione del servizio e può andare dalla semplice attestazione di appartenenza ad una categoria (es studenti o personale docente) ad attributi più specifici utilizzati per modulare opportunamente la disponibilità di funzioni e risorse in base all'accordo di servizio stipulato con la federazione (ed eventualmente con l'Ente).

L'utente deve essere consapevole del passaggio di tali informazioni e, in funzione del tipo di servizio, potrebbe rendersi necessaria un'informativa o un consenso.

Esistono soluzioni standard per implementare l'acquisizione di tale consenso nell'ambito della fruizione federata di servizi, ad esempio può essere utilizzata la funzionalità uApprove, disponibile come addin per Shibboleth Identity Provider v2.x ed integrata dalla v3.x, che può essere configurata per:

- acquisire dall'utente, al primo accesso all'IdP, il consenso alle condizioni d'uso dello stesso
- informare l'utente del passaggio di alcune sue informazioni personali all'atto dell'accesso ai Service Provider ed acquisire un consenso globale una tantum o un consenso specifico per ciascun SP (espresso al primo accesso o a fronte di variazioni ai valori degli attributi passati).

SWITCHaai

Stai accedendo al seguente servizio:

aai-demo.switch.ch di [AAI Demo Home Organisation](#)

Descrizione del servizio:

Dati utente richiesti dal servizio	
uid	demouser
surname	SWITCHaai
givenName	Demouser
Principal Name	234567@aai-demo-idp.switch.ch
eduPersonAffiliation	member staff
eduPersonEntitlement	http://example.org/res/99999 http://publisher-xy.com/e-journals urn:mace:dir:entitlement:common-lib-terms
swissEduPersonStudyLevel	7915-15
Tipo di membro	staff@aai-demo-idp.switch.ch member@aai-demo-idp.switch.ch
homePhone	+41 44 234 5678
preferredLanguage	de-ch
Home organization	aai-demo-idp.switch.ch
swissEduPersonHomeOrganization	aai-demo-idp.switch.ch
swissEduPersonUniqueID	234567@aai-demo-idp.switch.ch
swissEduPersonHomeOrganizationType	others
swissEduPersonStudyBranch3	7915
commonName	Demouser SWITCHaai Demouser
swissEduPersonDateOfBirth	19800401
swissEduPersonGender	2
Tipo di Home organization	urn:schac:homeOrganizationType:ch:others
swissEduPersonMatriculationNumber	01911506
email	demouser@example.org
telephoneNumber	+41 44 234 5678
postalAddress	ETH Zentrum CH-8092 Zürich
swissEduPersonStaffCategory	201
displayName	Demouser SWITCHaai
mobile	+41 79 234 5678

Il servizio chiede di accedere ai miei dati utente sopralencati. Accetto di trasmettere sempre i miei dati utente ogni volta che utilizzo questo servizio?

► [Non mostrare più questa pagina.](#)

Rifiutare

Accettare

uApprove tiene traccia del consenso espresso da ciascun utente in relazione ai singoli servizi e registra data/ora di tale acquisizione.

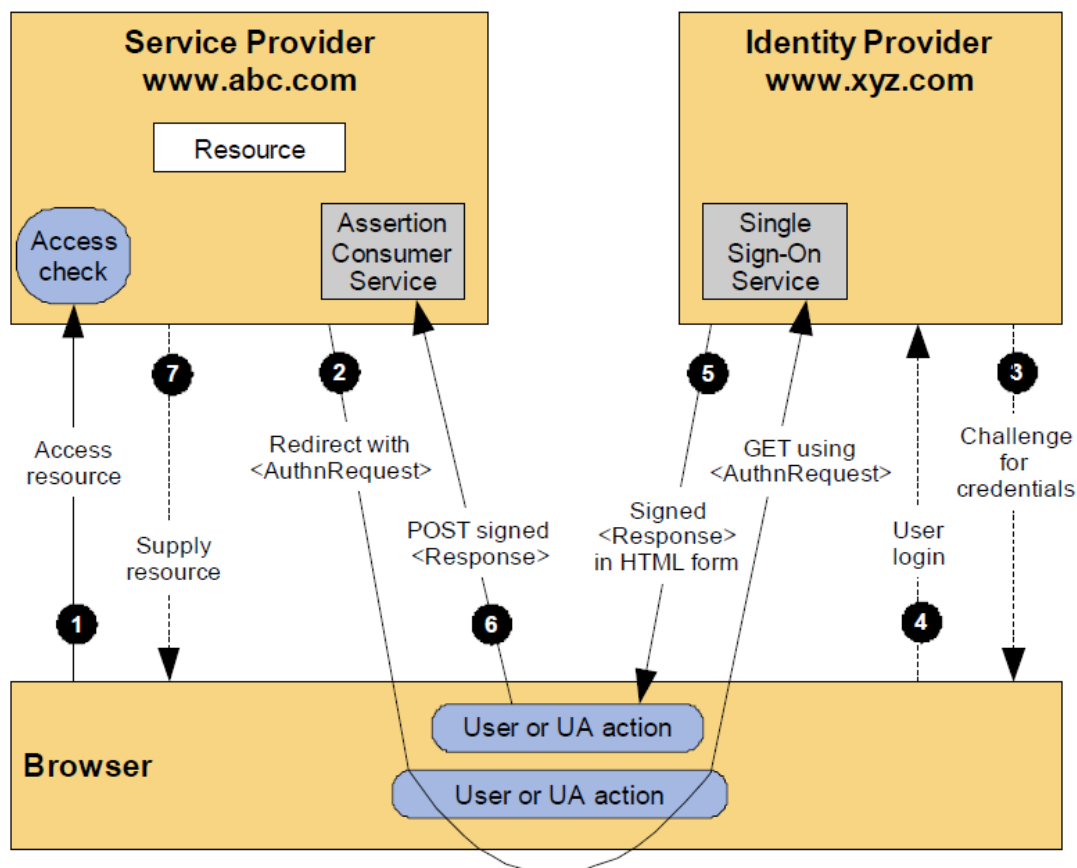
Notare che la form uApprove (o equivalente) di acquisizione del consenso nel passaggio al SP, potrebbe non esaurire di per sé gli obblighi di informativa in relazione ai trattamenti di dati personali effettuati dal SP, che dovrebbero essere consultabili dall'utente prima dell'espressione del consenso.

In termini più generali è opportuno segnalare che, sulla tematica relativa al passaggio di attributi da IdP e SP nell'ambito di federazioni, è stato attivato da [GEANT](#), infrastruttura di collegamento tra le reti nazionali europee a supporto della ricerca e della formazione, uno specifico [progetto](#) per la stesura di un "Data Protection Code of Conduct". Tale codice di condotta, attualmente in [revisione](#) per gli adeguamenti implicati dal GDPR, definisce:

- regole comuni alle quale dovrebbero conformarsi i "Service Provider" nel trattamento dei dati ricevuti dalle "Home Organisation" degli utenti per l'accesso ai servizi
- linee guida e template relativi alle modalità con le quali le "Home Organisation" dovrebbero informare gli utenti del passaggio di attributi ai "Service Provider".

5.5.3 Trattamento nell'ambito dell'accesso ai servizi con autenticazione SPID

L'accesso ad un SP tramite autenticazione effettuata da un IdP SPID prevede le seguenti interazioni:



In accordo con quanto previsto dal DPCM. 24 ottobre 2014 http://www.agid.gov.it/sites/default/files/leggi_decreti_direttive/dpcm_24_ottobre_2014a.pdf e dal REGOLAMENTO RECANTE LE REGOLE TECNICHE art. 4.2, DPCM 24/10/14 http://www.agid.gov.it/sites/default/files/circolari/spid-regole_tecniche_v1.pdf :

- l'assertion prodotta dall'IdP deve essere conforme allo standard SAML v2.0 e può includere l'elemento <AttributeStatement> riportante gli attributi identificativi certificati dall'IdP (Codice identificativo, Nome, Cognome, Luogo di nascita, Provincia di nascita, Data di nascita, Sesso, Ragione o denominazione sociale, Sede legale, Codice fiscale, Partita IVA, Documento d'identità
- http://www.agid.gov.it/sites/default/files/regole_tecniche/tabella_attributi_idp_v1_0.pdf) che l'IdP rilascia in base alla richiesta del SP espressa attraverso l'attributo AttributeConsumingServiceIndex della AuthnRequest.
- il SP deve provvedere alla conservazione per **24 mesi** delle informazioni necessarie a imputare alle singole identità digitali le operazioni effettuate sui propri sistemi a fronte di autenticazione SPID. A tal fine dovrà mantenere un Registro delle transazioni contenente i tracciati delle richieste di autenticazione, è opportuno che vengano memorizzate direttamente informazioni estratte dai messaggi SAML.

Potrebbero essere adottati meccanismi di cifratura dei dati o impiegati sistemi di basi di dati (DBMS) che realizzano la persistenza cifrata delle informazioni.

L'accesso deve essere riservato a personale incaricato.

La conservazione deve essere implementata garantendo l'integrità ed il non ripudio delle registrazioni.

5.6 Tracciamento di informazioni non primarie

5.6.1 Raccomandazioni

Le comunicazioni elettroniche fatte nei luoghi di lavoro possono essere coperte dalle nozioni di "vita privata" e "corrispondenza" ai sensi dell'articolo 8, paragrafo 1 della Convenzione europea.

Pertanto, nell'esecuzione delle attività di log e tracciamento è necessario considerare quanto stabilito sui principi fondamentali della protezione dei dati dalla direttiva UE Directive 95/46/EC (UE) e dagli ulteriori obblighi introdotti dal GDPR. A tale scopo il WP art. 29 ha recentemente espresso il suo parere (opinion 02/2017 http://ec.europa.eu/newsroom/document.cfm?doc_id=45631) sul trattamento dei dati sul posto di lavoro e sulla sorveglianza delle comunicazioni elettroniche, che integra quanto già precedentemente espresso con il 08/2001 al fine di fornire orientamenti per bilanciare le aspettative della privacy dei lavoratori (e/o collaboratori) sul posto di lavoro con il legittimo interesse del datore di lavoro.

Dunque, i datori di lavoro possono raccogliere i dati ad es. di monitoraggio solo per scopi specifici e legittimi, con l'elaborazione che si svolge in condizioni adeguate (ad esempio, proporzionate e necessarie, per un interesse reale e attuale, in modo legittimo, articolato e trasparente) sulla base di un fondamento giuridico per il trattamento dei dati personali raccolti o generati tramite comunicazioni elettroniche.

Poiché il consenso espresso dal lavoratore può solo raramente essere considerato libero, visto lo squilibrio di potere del datore di lavoro, allora il fondamento giuridico al monitoraggio può essere costituito dal legittimo interesse ma questo solo se l'elaborazione è strettamente necessaria per uno scopo legittimo e l'elaborazione è conforme ai principi di proporzionalità e di sussidiarietà.

Perciò prima di introdurre uno strumento che può dar luogo al monitoraggio e tracciamento dei lavoratori (ad es. connesso ad adozione di tecnologie quali Next Generation Firewall, Data Loss Prevention, Bring Your Own Device, Mobile Device Management) è necessario condurre un test di proporzionalità per valutare se tutti i dati siano necessari, se questa elaborazione non contrasta con i diritti generali sulla privacy che i dipendenti hanno sul posto di lavoro e quali misure devono essere adottate per garantire che siano minimizzati al minimo le possibilità di sconfinamento nella vita privata e nel diritto alla segretezza delle comunicazioni.

E' altrettanto importante adottare il principio di minimizzazione dei dati così raccolti, inoltre le informazioni (ad es. i log) devono essere memorizzate per il periodo di tempo minimo necessario e devono essere cancellate appena non risultano più necessarie,.

Come esempio di buone pratiche, prima di introdurre nuovi strumenti potenzialmente intrusivi, o qualsiasi tecnologia di monitoraggio va effettuata un Data Protection Impact Assessment (DPIA). In secondo luogo, i datori di lavoro devono attuare e comunicare le Acceptable Use Policy (AUP) che descrivono l'utilizzo consentito della rete e delle attrezzature dell'organizzazione. In terzo luogo è opportuno fornire una comunicazione efficace ai dipendenti in merito a qualsiasi monitoraggio che si svolge, alle finalità di questo monitoraggio e alle circostanze, nonché alle possibilità per i dipendenti di impedire che i propri dati siano acquisiti mediante tecnologie di monitoraggio. Le politiche e le norme relative al legittimo monitoraggio devono essere chiare e facilmente accessibili.

Sarà necessario valutare a seconda dei casi, se l'adozione di una certa tecnologia di monitoraggio, non richieda legalmente l'approvazione dei Sindacati o di una rappresentanza dei lavoratori.

In generale alla prevenzione dovrebbe essere dato molto più peso rispetto alla rilevazione: gli interessi del datore di lavoro sono meglio serviti prevenendo l'uso abusivo degli strumenti piuttosto che l'adozione di tecnologie atte ad individuare i casi di abuso.

5.6.2 Finalità del tracciamento

La registrazione di eventi, caratterizzati anche dal trattamento di dati personali, effettuata su file di log o tabelle da parte di componenti sistemiche o applicative trasversali, fa tipicamente riferimento alle seguenti finalità:

- Registrazione per adempimento di un obbligo normativo (es. leggi o regolamenti)
- Registrazione di eventi per vincoli di natura sistemistica (es. dati che per motivi di carattere tecnico sono strettamente necessari per l'erogazione di un servizio)
- Registrazione di eventi per garantire la protezione dei dati e/o dei sistemi informatici (es. per supportare attività proattive o reattive di cyber security o di protezione dei dati)
- Registrazione di eventi a supporto del troubleshooting per garantire il regolare funzionamento dei servizi informatici
- Registrazione della sequenza di eventi generati dagli utenti nell'ambito di un processo amministrativo al fine di supportare attività di ricostruzione e verifica
- Verifica del reale utilizzo di un servizio o di un suo utilizzo coerente con le finalità d'uso previste ed autorizzate.
- Rendicontazione interna per fini amministrativi (es. imputazione dei costi telefonici, di servizi di copisteria, di servizi in cloud)

Nei tempi e nei modi previsti dalla normativa, le informazioni registrate per le finalità sopra descritte possono essere oggetto di acquisizione da parte della Polizia giudiziaria per eventuali attività di indagine.

5.6.3 Tracciamento sistemistico e di rete

Ricadono in questo ambito i dati di tracciamento generati da apparati di rete e componenti infrastrutturali.

a. Obbligo normativo	b. Vincoli tecnologici	c. Protezione dati e sistemi	d. Troubleshooting	e. Analisi workflow	f. Verifica utilizzo risorsa	g. Rendicontazione	Ambito di servizio del trattamento	Informazioni tracciate
X	X	X	X				Connessione a reti autenticate (sia wifi che wired) in contesto 802.1x tramite credenziali o certificato	MAC address, username, IP assegnato, versione SO, nome AP, timestamp (start e stop), numero byte, causa chiusura sessione.
X	X	X	X			X	Strumenti di analisi e gestione della sicurezza di rete e dei sistemi client/server	A seconda del tipo di strumento si raccolgono dati di tipo diverso: Ad es. Firewall di rete e gestione Sicurezza: Timestamp /Log connessioni Layer 4 (IP SRC/ IP DEST/ porta SRC – PORT DST/) e di APPLICAZIONE / in aggiunta se disponibile: username, MAC ADDRESS/ URL malevole, THREAT LOG: (nome vulnerabilità, nome spyware, nome virus e file malevolo). Per traffico

								autenticato (MAC address, tipo di dispositivo, username, IP assegnato, log connessioni di layer 4, tipo dispositivo, Applicazione, URL *).
								Per Console Antivirus: Hostname/IP/ultimo utente loggato/URL malevole/path e filename dei virus su disco locale * I dati di tracciamento di livello superiore al 4, vanno conservati seguendo le disposizioni normative e considerando la cifratura, l'anonimizzazione e minimizzando la retention, dandone adeguata informativa agli interessati in osservanza delle disposizioni di diritto e sindacale.
X	X	X	X				Accesso a file server	Timestamp / Username / Hostname
X	X	X	X				Accesso remoto alle applicazioni	Timestamp / Username / Hostname
X	X	X	X		X	X	Utilizzo di pacchetti sw	Timestamp / Username / Hostname / Software richiesto
X	X	X	X		X	X	Utilizzo e gestione delle postazioni gestite	Timestamp logon-off / Username / Hostname/ IP/ INVENTARIO DI HW E SW INSTALLATO/USATO;
	X		X		X	X	Applicazioni di gestione Ticket	Anagrafica (Nome utente, sede, telefono, struttura di appartenenza) motivo ticket
	X	X	X		X	X	Utilizzo di servizi di stampa	Timestamp / Username / Hostname / Nome documento
X	X	X	X		X	X	Accesso VPN	ID utente ed entitlement nell'anagrafica di Ateneo, indirizzo IP (sia esterno e interno), data e ora, (LOG del traffico)
	X	X	X	X	X	X	Gestione traffico telefonico e contabilizzazione	Dati telefonate in/out
	X	X	X		X	X	Gestione traffico rete per videoconferenza, streaming e videosorveglianza	Timestamp / Username / Hostname
		X	X	X	X	X	Gestione e movimentazione linea telefonica	Timestamp / Username / Hostname
X	X	X	X		X	X	Accesso remoto alle postazioni utente	Timestamp / Username / Hostname/IP/altro sono potenzialmente accessibili tutti i dati contenuti nel sistema.
	X	X	X		X		Accesso a risorse (file) in Cloud	Timestamp / Username / Hostname/IP
X	X	X	X		X		Accesso a risorse su directory (LDAP/AD) locali/remote	Timestamp logon-off / Username / Hostname
X	X	X	X		X		Accesso a sistema di autenticazione centrale	Timestamp logon-off/Username/IP/audit operazioni
X	X	X	X		X		Gestione utenze per Identity ed Access Management	Timestamp logon-off / Username / Hostname
X	X	X	X		X		Accesso a macchine virtuali/servizi OnPremise/Cloud	Timestamp logon-off / Username / Hostname/Task operazione (azioni in vmware)

X	X	X	X		X		Gestione di servizi di proxy	Timestamp logon-off / Username / Hostname Nel caso di proxy web (ad es. biblioteche e aule) potrebbe essere tracciata anche la URL visitata e in alcuni casi i contenuti visualizzati.
X	X	X	X		X		Gestione di servizi per il load-balancing	Timestamp logon-off / Username / Hostname/IP
X	X	X	X		X		Accesso amministrativo esterno su nostre risorse sistemiche	Timestamp logon-off / Username / Hostname/IP
X	X	X	X		X		Accesso a postazioni dei laboratori informatici	Timestamp logon-off / Username / Hostname
X	X	X	X		X		Accesso su dispositivi mobili aziendali	Timestamp logon-off / Username / Hostname
X	X	X	X		X		Gestione Sistema di Posta OnPremise/Cloud	TimeStamp, IP utente, account posta, flussi di mail in transito (dominio mittente/ricevente)

5.6.4 Tracciamento applicativo

Dati di sessione e di tracciamento applicativo delle attività dell'utente.

a. Obbligo normativo	b. Vincoli tecnologici	c. Protezione dati e sistemi	d. Troubleshooting	e. Analisi workflow	f. Verifica utilizzo risorsa	g. Rendicontazione	Ambito di servizio del trattamento	Informazioni tracciate
X	X	X	X	X	X	X	Autenticazione e Single Sign On per tutti i servizi web federati con il sistema di autenticazione dell'Ateneo	Timestamp / Username / Servizio / IP.
X	X	X	X	X	X	X	Navigazione dell'utente nelle applicazioni sviluppate dall'Ateneo Web	Subset degli attributi previsti dal formato W3C standard, potrebbe dipendere dal livello di trace attivato. https://www.w3.org/TR/WD-logfile.html https://msdn.microsoft.com/it-it/library/windows/desktop/aa814385(v=vs.85).aspx (si veda tabella sotto riportata)
X	X	X	X	X	X	X	Navigazione dell'utente nelle applicazioni Web sviluppate da terzi	Da verificare con il fornitore, potrebbe dipendere dal livello di trace attivato.
			X		X	X	Monitoraggio ai fini statistici dell'accesso ai siti web (es tramite Google Analytics)	Cookie anonimi con registrazione di: lingua di visualizzazione; paese e città di provenienza; browser utilizzato; sistema operativo; provider del servizio internet; risoluzione schermo. Non vengono registrati né l'IP né dati sensibili.

		X	X	X	X	X	Autenticazione per l'accesso alle applicazioni da client	Timestamp / Username / Servizio
		X	X	X	X	X	Utilizzo di applicazioni sviluppate dall'Ateneo	Traccia delle attività svolte dall'utente con dettagli dipendenti dal contesto applicativo e dal livello di trace attivato..
		X	X	X	X	X	Utilizzo di applicazioni client sviluppate da terzi	Da verificare con il fornitore, potrebbe dipendere dal livello di trace attivato.
		X	X	X	X		Accesso a basi di dati esterne (Miur, Agenzia Entrate, Inps/Inail, Bandi Concorsi, Progetti di Ricerca, Statistiche)	Da verificare con il fornitore, potrebbe dipendere dal livello di trace attivato.
		X	X	X	X	X	Utilizzo di App "mobile" esterne o proprie.	Da verificare con il fornitore, potrebbe dipendere dal livello di trace attivato. Verificare uso interno.
X	X	X	X	X	X	X	Utilizzo di piattaforme per l'invio e la consultazione di dati in conservazione digitale	Da verificare con il fornitore, potrebbe dipendere dal livello di trace attivato.

Attributi di tracciamento previsti dal formato W3C standard:

Field	Appears As	Description
Date	date	The date on which the activity occurred.
Time	time	The time, in coordinated universal time (UTC), at which the activity occurred.
Service Name and Instance Number	s-sitename	The Internet service name and instance number that was running on the client.
Server Name	s-computername	The name of the server on which the log file entry was generated.
Server IP Address	s-ip	The IP address of the server on which the log file entry was generated.
Method	cs-method	The requested verb, for example, a GET method.
URI Stem	cs-uri-stem	The target of the verb, for example, Default.htm.
URI Query	cs-uri-query	The query, if any, that the client was trying to perform.
Server Port	s-port	The server port number that is configured for the service.
User Name	cs-username	The name of the authenticated user that accessed the server.
Client IP Address	c-ip	The IP address of the client that made the request.
Protocol Version	cs-version	The HTTP protocol version that the client used.
User Agent	cs(User-Agent)	The browser type that the client used.
Cookie	cs(Cookie)	The content of the cookie sent or received, if any.
Referrer	cs(Referrer)	The site that the user last visited. This site provided a link to the current site.
Host	cs-host	The host header name, if any.

HTTP Status	sc-status	The HTTP status code.
Protocol Substatus	sc-substatus	The substatus error code.
Win32 Status	sc-win32-status	The Windows status code.
Bytes Sent	sc-bytes	The number of bytes sent by the server.
Bytes Received	cs-bytes	The number of bytes received and processed by the server.
Time Taken	time-taken	The length of time that the action took, in milliseconds.

6. Ricerca scientifica e statistica

6.1 Premessa

Le attività di ricerca scientifica svolte negli Atenei 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 nuovo Regolamento (UE) 2016/679.
- 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 tutti gli Atenei.

6.2 Finalità e ambito applicativo

"La Repubblica promuove lo sviluppo della cultura e della ricerca scientifica" (art. 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 Regolamento (UE) 2016/679 che sono previste misure di semplificazione in ambito di ricerca storica, scientifica e/o statistica.

Tali misure di semplificazione non esentano tuttavia il Titolare dall'adozione di accorgimenti idonei 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)⁸.

⁸ I dati personali sottoposti a pseudonimizzazione sono quelli attribuiti a una persona fisica mediante l'utilizzo di ulteriori informazioni (es: un codice numerico) e devono essere considerati "informazioni su una persona fisica identificabile"

La forte spinta verso gli OpenData, anche in ambito di ricerca, può facilmente farci 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. Per approfondimenti si rimanda alla lettura del Parere 05/2014 sulle tecniche di anonimizzazione http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_it.pdf del Gruppo di Lavoro ex art. 29.

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 Regolamento (UE) 2016/679 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).

È tuttavia importante attendere l'emanazione di norme o prescrizioni più specifiche sul tema, da parte del legislatore italiano, per poter delineare un quadro più certo e completo in materia di protezione di dati personali trattati a fini di ricerca storica, scientifica e/o statistica.

6.3 Presupposti dei trattamenti

Sembra 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 Regolamento (UE) 2016/679), 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.

6.4 Progetto di ricerca

6.4.1 Avvio di un progetto di ricerca

6.4.1.1 Analisi dei rischi e DPIA (Data Protection Impact Assessment)

È consigliabile che i ricercatori che intendono avviare un progetto abbiano consapevolezza dei rischi sottesi al trattamento (al fine di ridurli) ed effettuarlo, laddove necessario, una "valutazione d'impatto" (così come avviene ai sensi dell'articolo 35 del GDPR per particolari categorie di dati). Il DPIA è un esercizio di analisi dei rischi che somiglia alle procedure che vengono eseguite nell'ambito di progetti europei, nei quali - come parte integrante del progetto - si richiede agli enti di effettuare una valutazione degli aspetti etici (ad esempio tramite la descrizione dei dati personali utilizzati e un'accurata analisi delle responsabilità connesse ai dati gestiti nell'ambito di progetti H2020 o ERC).

(cfr. il considerando n. 26 del GDPR). Per stabilire l'identificabilità di una persona è opportuno considerare tutti i mezzi, come l'individuazione, di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica direttamente o indirettamente. Per accertare la ragionevole probabilità di utilizzo dei mezzi per identificare la persona fisica, si dovrebbe prendere in considerazione l'insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici. I principi di protezione dei dati non devono applicarsi 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 dovrebbe contenere almeno:

- a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
- b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
- c) una valutazione dei rischi per i diritti e le libertà degli interessati;
- d) 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, dovrebbe 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 3 una scheda che potrebbe essere 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. Si precisa che la scheda dovrà essere aggiornata, anche in relazione alla possibilità che nell'ambito della ricerca scientifica e statistica intervengano delle disposizioni differenti da quelle oggi previste nell'all. a.4 del d.lgs. 196/03.

6.4.1.2 Comitati etici, di bioetica, unità di supporto per la ricerca e DMB

L'attività di analisi di cui al paragrafo precedente, in alcuni Atenei è già condotta – a seconda delle specifiche realtà - tramite il supporto e/o la verifica di uffici competenti in materia di privacy, Comitati etici e/o organi di supporto (come il "Data Monitoring Board").

Sebbene la previsione di un passaggio formale da un'unità organizzativa/organo per l'avvio di un progetto di ricerca sia spesso vista come un impedimento alla realizzazione della ricerca

stessa, l'esperienza perpetrata in alcuni Atenei ha dimostrato alcuni cambiamenti positivi, tra i quali:

- la creazione di maggiore consapevolezza nei ricercatori in merito alla delicatezza delle operazioni di trattamento svolte;
- la possibilità di conoscere più dettagliatamente le esigenze dei ricercatori in merito alla gestione e archiviazione dei dati e la possibilità di individuare più agevolmente servizi informatici a supporto della ricerca;
- un maggiore controllo dei trattamenti svolti e delle misure di sicurezza da prevedere per rispettare la normativa in materia di protezione dei dati personali.

Dalla condivisione delle esperienze sul tema e da un confronto tra diversi Atenei, è possibile individuare cinque suggerimenti per la realizzazione dei cambiamenti sopra richiamati:

1. Chiarire le competenze sui temi etici

Ogni Ateneo dovrebbe fare chiarezza sugli organi preposti a esaminare i profili etici dei protocolli sottoposti dai ricercatori, chiarendo quali siano gli ambiti di operatività dei Comitati Etici⁹ di cui all'art. 12, commi 10 e 11, del decreto-legge 13 settembre 2012, n. 158, convertito, con modificazioni, dalla legge 8 novembre 2012, n. 189 e quali siano gli ambiti di operatività dei Comitati etici previsti dallo Statuto dell'Ateneo e/o da eventuali regolamenti universitari (d'ora in poi definiti "Comitati etici interni").

2. Definire la natura dei pareri da sottoporre al Comitato interno

Nel caso in cui sia previsto il ricorso a Comitati etici "interni", sarebbe auspicabile prevedere la natura obbligatoria o facoltativa del ricorso a tali Comitati nel caso di avvio di un progetto di ricerca.

3. Coinvolgere il Data Protection Officer

In considerazione del ruolo attribuito dal Regolamento (UE) 2016/679 al Data Protection Officer, sarebbe preferibile inserire la figura del DPO nel Comitato etico interno, anche al fine di favorire interventi formativi o azioni volte all'attuazione del nuovo Regolamento.

4. Coinvolgimento di un gruppo IT

In considerazione dell'esperienza maturata in alcuni Atenei, appare auspicabile il coinvolgimento di un gruppo di esperti IT (tra cui il dirigente dell'Area IT o un suo rappresentante) per quei progetti di ricerca che richiedono la conservazione di dati personali (pseudonimizzati e non) in formato elettronico, con modalità differenti da quelle regolamentate o prescritte in Ateneo. Il gruppo potrebbe avere l'onere di verificare l'adeguatezza agli standard di sicurezza previsti dall'Ateneo, delle policy di sicurezza adottate e delle infrastrutture impiegate nella ricerca.

5. Supporto concreto ai ricercatori

Instaurare un rapporto di fiducia e collaborazione con il ricercatore è necessario per favorire il rispetto della norma. Sarà importante fornire al ricercatore strumenti e soluzioni concrete e attuabili invece che complesse interpretazioni che non lo aiutano ad individuare le modalità più idonee a favorire il rispetto della norma.

⁹ I Comitati Etici hanno competenza ad esprimere parere per gli studi clinici condotti nelle strutture sanitarie. I Comitati Etici valutano le domande di approvazione di sperimentazioni o gli studi clinici in tutti i loro aspetti, compresi quelli economici rilevanti ai fini del giudizio etico (sostenibilità dei costi previsti dalla sperimentazione e congruità del compenso economico), nonché quelli relativi alla congruità della struttura ove si svolge lo studio o la sperimentazione. I Comitati Etici effettuano la valutazione di tutta la documentazione tecnica (esempio: protocollo sperimentale, modulistica privacy, consenso informato). Per esprimere le proprie valutazioni nelle materie di competenza (rischi/benefici, copertura assicurativa, modalità di pubblicazione dei risultati, congruità dei costi), il Comitato Etico verifica le proposte dell'eventuale promotore/sponsor e la conformità della modulistica presentata rispetto alla normativa vigente e ai modelli proposti (schema di convenzione, modulo dei costi, modulistica privacy). È infatti nel ruolo del Comitato Etico quello di garantire la tutela dei diritti delle persone in sperimentazione e di fornire pubblica garanzia di tale tutela, tra cui il diritto alla protezione dei dati personali.

6.4.1.3 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 Regolamento (UE) 2016/679, 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. In molti casi, tuttavia, non è possibile individuare pienamente la finalità del trattamento al momento della raccolta dei dati; pertanto, nel caso in cui un ricercatore dovesse raccogliere dati personali nell'ambito di uno specifico progetto di ricerca e dovesse avere interesse a conservare i dati identificativi per futuri progetti potrebbe essere chiesto all'interessato di prestare il proprio consenso alla conservazione ed eventuale trattamento dei suoi dati nell'ambito di future attività di ricerca **purché limitatamente a uno specifico settore di ricerca.**

Il settore da richiamare nell'informativa potrebbe essere uno di quelli indicati nelle classificazioni ufficiali dell'European Research Council (organismo europeo istituito per sostenere la ricerca di frontiera) che ha recentemente proposto una nuova classificazione dei settori di ricerca <https://erc.europa.eu/sites/default/files/document/file/erc%20peer%20review%20evaluation%20panels.pdf>

Dovrebbe pertanto essere consentito agli interessati di dare il proprio consenso ad alcune aree della ricerca scientifica, in linea - naturalmente - con gli standard etici riconosciuti nei diversi settori di ricerca.

Si riporta in allegato 4 un esempio di informativa che potrebbe essere fornita nel caso si intenda avviare un progetto di ricerca che utilizzi dati sensibili raccolti presso l'interessato. Si precisa che tale informativa non si presta tuttavia ad essere usata nel caso di sperimentazioni cliniche su pazienti.

6.4.2 Raccolta dei dati

6.4.2.1 Dati raccolti presso l'interessato

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

Tuttavia, questo tipo di raccolta non deve indurre a ritenere automaticamente riconducibile il titolare del trattamento all'ente o al soggetto terzo presso il quale avviene la raccolta dei dati.

Come più volte si è detto, il Titolare è "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".

La raccolta di un dato personale presso una sede diversa da quella del Titolare può quindi essere una mera operazione di trattamento preceduta da una scelta organizzativa (l'individuazione di una specifica sede come luogo di raccolta) da parte di un soggetto diverso che ha determinato finalità e mezzi del trattamento.

Questo è estremamente rilevante soprattutto se si pensa a contesti, come le scuole o le strutture sanitarie, in cui il dato è raccolto da ricercatori che (indipendentemente dal ruolo ricoperto nella sede presso la quale avviene la raccolta) operano una raccolta di informazioni autonomamente, dato che la scuola o la struttura sanitaria potrebbe non avere interesse alla raccolta di quei dati.

Per fare un esempio, nel caso in cui un ricercatore universitario chieda di compilare un sondaggio a un certo numero di pazienti ricoverati presso una struttura sanitaria sulla percezione del dolore e nel caso in cui detto studio non comporti l'uso o la correlazione dei dati raccolti con altri dati raccolti a fini di cura, non è possibile affermare che il luogo di raccolta sia di per sé idoneo a determinare una responsabilità in capo alla struttura sanitaria per ciò che attiene la tutela dei dati personali conferiti tramite il sondaggio. È ovvio che il ricercatore dovrà chiarire bene e in assoluta trasparenza che i dati conferiti saranno trattati per fini di ricerca propri dell'Ateneo, se l'Ateneo è il soggetto che ha determinato le finalità e i mezzi della raccolta.

6.4.2.2 Dati acquisiti presso terzi (es: altre strutture sanitarie)

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. A tal fine sarebbe importante valutare, ad esempio, la natura della relazione tra Ateneo e soggetto terzo, il servizio fornito o gli obblighi giuridici o contrattuali applicabili, poiché l'interessato potrebbe avere ragionevoli aspettative riguardo a una riservatezza più rigorosa e a limitazioni più severe in merito all'ulteriore utilizzo.

Nell'ambito di attività di natura didattica e/o di ricerca proprie dell'Ateneo e svolte, per convenzione, presso Scuole e/o Strutture Sanitarie, è frequente 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.

Si precisa che, come precisato anche nel considerando 53 del GDPR, sebbene il regolamento intenda creare "condizioni armonizzate per il trattamento di categorie particolari di dati personali", la legislazione dell'Unione o del nostro Stato potrebbe prevedere misure più specifiche e appropriate per proteggere i dati inerenti lo stato di salute, i dati genetici e/o biometrici. Pertanto, la raccolta e l'utilizzo di tali dati per fini di ricerca potrebbero essere soggetti ad aggiornamenti e a restrizioni.

Con particolare riferimento a queste tipologie di dati, si riportano alcune considerazioni che, per quanto strettamente connesse al quadro normativo vigente nel settembre 2017, possono comunque essere d'aiuto a inquadrare le modalità di raccolta dei dati da parte di soggetti terzi e le criticità connesse a questo tema.

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.

Il delicato ambito delle attività di ricerca nel settore medico-sanitario, che solitamente comporta il trattamento di dati sensibili, di dati genetici e/o campioni biologici, richiede un attento monitoraggio da parte dell'Ateneo delle attività di trattamento svolte in tali contesti, a motivo della natura e dell'importanza dei diritti in gioco e delle responsabilità in capo all'Ateneo e ai suoi ricercatori.

Nel caso i dati personali necessari allo svolgimento della ricerca debbano essere acquisiti da un soggetto terzo diverso dall'interessato, occorre garantire che tale comunicazione dei dati avvenga legittimamente.

Per fare un esempio, nel caso in cui un ricercatore universitario, dopo aver reso opportuna informativa, chieda a un paziente di compilare un sondaggio sulla percezione del dolore e nel caso in cui tale ricercatore intenda correlare i dati raccolti con altri dati raccolti dalla struttura sanitaria a fini di cura, sarà necessario rendere evidente nell'informativa resa al paziente che, con il suo consenso, la struttura sanitaria potrà comunicare all'Ateneo i suoi dati di interesse per la ricerca, elencandone opportunamente le caratteristiche e il Titolare o i titolari cui è in capo la responsabilità dei dati trattati a fini di ricerca.

In una prospettiva più ampia e che tenga conto delle reali dinamiche di collaborazione fra Ateneo e strutture sanitarie, occorre coordinarsi con queste affinché, nei limiti e nel rispetto dei requisiti imposti dalla normativa vigente, i dati raccolti dalle strutture sanitarie che collaborano con l'Ateneo possano essere legittimamente trasferiti all'Ateneo per consentirgli lo svolgimento di proprie attività di ricerca, prevedendo – ad esempio – un consenso esplicito alla comunicazione del dato da parte dell'interessato.

Si suggerisce quindi che, nel caso in cui vi siano soggetti terzi che raccolgono dati potenzialmente utilizzabili in progetti di ricerca, sia comunicato all'interessato da tali soggetti terzi che i dati potrebbero essere forniti all'Ateneo per una specifica finalità.

È necessario inoltre uno stretto coordinamento con le strutture sanitarie con le quali l'Ateneo collabora per lo svolgimento di attività di ricerca, con le quali costruire un dialogo volto a definire protocolli e procedure che, nel semplificare la gestione degli adempimenti privacy e quindi lo svolgimento delle rispettive attività, contemporaneamente garantiscano la piena legittimità del trattamento dei dati.

Non risulterebbero corretti "accordi quadro" che prevedano una rigida e generalista intesa sulla titolarità dei dati trattati per tutti i progetti di ricerca, atteso che ciascun progetto di ricerca potrebbe comportare un diverso assetto delle responsabilità.

6.4.2.3 Dati acquisiti da internet

Il dato diffuso su internet dallo stesso interessato può essere usato per fini di ricerca? È una delle domande che alcuni ricercatori, sempre più spesso, si pongono nel caso in cui si presenti la necessità di svolgere una ricerca di "sociologia visuale" o una ricerca che intende analizzare l'interazione di un gruppo di utenti, magari in un social network. Si pensi al valore che, per ricerche di natura sociologica, possa avere, ad esempio, l'utilizzo di fotografie pubblicate su internet, raccolte come "materiale di analisi" da contestualizzare e mettere in relazione con altre fotografie per approfondire e studiare alcuni fenomeni sociali. Si pensi inoltre a come possa poi rivelarsi utile per il ricercatore poter eventualmente anche diffondere le foto in un articolo di ricerca a sostegno della propria tesi o pubblicare parti di dialoghi tra utenti su un social network

allo scopo di fare analisi qualitativa del dato (con il rischio che, pur omettendo i dati personali dell'interessato o oscurando i tratti somatici di una foto, tali dati possano consentire la re-identificazione dell'interessato mediante l'uso di un semplice motore di ricerca).

Di seguito alcune considerazioni:

- il trattamento di dati personali diffusi dall'interessato (ad esempio attraverso piattaforme social) potrebbero essere usate a fini di ricerca scientifica o storica o a fini statistici a patto che l'Ateneo utilizzi tecniche di anonimizzazione dei dati che non consentirebbero più di identificare l'interessato (come ad esempio la pseudonimizzazione dei dati personali).
- l'informativa agli utenti potrebbe non essere resa qualora l'Ateneo riuscisse a dimostrare l'impossibilità di fornire l'informativa all'interessato o il fatto che tale adempimento comporti uno sforzo sproporzionato.
- pur operando le valutazioni di cui ai punti precedenti, rimane una dose di incertezza legata alla mancanza di criteri oggettivi o linee guida per effettuare queste valutazioni.

Auspichiamo che questi temi siano affrontati dalle Autorità competenti, affinché sia possibile per il ricercatore avere tutti gli elementi per svolgere i propri compiti in modo conforme alla normativa vigente in materia di protezione di dati personali¹⁰.

6.4.3 Elaborazione dei dati a fini di ricerca statistica o scientifica

La valutazione dei rischi connessi al trattamento di dati personali dovrà tenere conto dell'impatto che potrebbe comportare, ad esempio, la diffusione di informazioni raccolte per fini scientifici. Se l'impatto è rilevante, l'attenzione alle misure di protezione dei dati e alle garanzie da riservare all'interessato dovrà essere alta. Tali garanzie potrebbero consistere:

- 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 accedute da soggetti non autorizzati ("separazione funzionale" come spesso avviene in un contesto di ricerca)
- utilizzo di tecniche di anonimizzazione
- immediata aggregazione dei dati
- diritto generale e incondizionato di revoca ("opt-out")
- la pseudonimizzazione e la 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.

6.4.4 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 (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

¹⁰ Occorrerà, naturalmente, approfondire i profili che concernono il diritto d'autore che, per quanto non di competenza di questa trattazione, possono ricoprire un aspetto molto determinante nell'utilizzo dei dati.

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.

6.4.4.1 Dati conservati presso terzi (es: cloud)

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 - dei dati, nonché dall'accesso abusivo da parte di terzi.

Sebbene siano innegabili i vantaggi dell'uso di repository in cloud, anche in termini di sicurezza, l'Ateneo e i suoi ricercatori devono tenere in dovuta considerazione le implicazioni derivanti dalla conservazione dei dati tramite servizi 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 delle terze parti che offrono il servizio. Tali soggetti dovranno pertanto essere considerati "destinatari" dei dati e segnalati opportunamente nell'informativa quali "responsabili 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 l'Ateneo) dovrebbe procedere a designare il fornitore dei servizi cloud "responsabile 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 il titolare potrebbe essere chiamato 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", sarà 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).

6.4.5 Trasferimento dei dati all'estero

Non muta il quadro generale rispetto alla direttiva 95/46/CE (art. 44). Nel Regolamento vige, in linea di massima, 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 il responsabile 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)
- se sono adottate clausole contrattuali standard;
- se 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)
- se si fa riferimento a codici di condotta e certificazione
- se sono state inserite particolari disposizioni in accordi amministrativi

- se ci sono state sentenze di un'autorità giurisdizionale o amministrativa, purché basati su un accordo internazionale
- se c'è stato il consenso dell'interessato.

6.4.6 Diffusione dei dati a fini di ricerca scientifica o statistica

6.4.6.1 Diffusione risultati di ricerca scientifica

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 a 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 l'interessato sia stato adeguatamente informato in merito alla diffusione di proprie informazioni.

Si precisa tuttavia che il ricercatore dovrebbe effettuare una valutazione di proporzionalità nella diffusione di dati personali e sull'opportunità di provvedere alla diffusione di dati riferiti a particolari categorie di interessati. Ad esempio, al fine di tutelarne i diritti degli interessati, il ricercatore non dovrebbe 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, arrecargli 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.

Potrebbe invece essere consentito l'uso e la diffusione a fini di ricerca di immagini che ritraggono persone in luoghi pubblici (ad esempio per ricerche di sociologia visuale), anche senza il consenso dell'interessato, purché non siano lesive della dignità e del decoro della persona, anche in relazione alla pertinenza dei contenuti dell'articolo scientifico e/o del video realizzato.

In relazione alle attività di dissemination, occorrerà tuttavia verificare la legittimità della diffusione di dati personali, tenuto conto delle modifiche che interverranno al d.lgs. 196/03. Al momento, non è infatti possibile diffondere dati personali a fini di ricerca scientifica, a meno dell'esistenza di una legge o di un regolamento che preveda la diffusione degli stessi. In mancanza di una previsione giuridica, anche il consenso dell'interessato non potrebbe ritenersi condizione sufficiente per pubblicare un'intervista ad alcuni stakeholder a fini scientifici o non sarebbe altrettanto lecita la pubblicazione di un video realizzato da alcuni alunni a fini di dissemination.

7. Link utili

- Codice in materia di protezione dei dati personali Decreto legislativo 30 giugno 2003, n. 196
<http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1311248>

- Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali dell'Autorità Garante per la protezione dei dati personali
<http://www.garanteprivacy.it/guida-all-applicazione-del-regolamento-europeo-in-materia-di-protezione-dei-dati-personali>
- Regolamento Europeo Regolamento (UE) 2016/679 del Parlamento Europeo (L 119/34) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati:
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC
- Misure minime per la sicurezza ICT delle pubbliche amministrazioni Agenzia per l'Italia Digitale (AgID)
<http://www.agid.gov.it/notizie/2017/04/07/pubblicate-gazzetta-ufficiale-misure-minime-sicurezza-informatica-pa>

Allegato 1 - Riepilogo degli adempimenti e delle priorità di intervento

La principale novità introdotta dal regolamento è il principio di "responsabilizzazione" (cd. accountability), che attribuisce direttamente ai titolari del trattamento il compito di assicurare, ed essere in grado di dimostrare, il rispetto dei principi applicabili al trattamento dei dati personali (art. 5).

In quest'ottica, la nuova disciplina impone alle amministrazioni un diverso approccio nel trattamento dei dati personali, prevede nuovi adempimenti e richiede un'intensa attività di adeguamento, preliminarmente alla sua definitiva applicazione a partire dal 25 maggio 2018.

Al fine di fornire un primo orientamento, il Garante per la protezione dei dati personali ha suggerito, anche nell'incontro con il gruppo di redazione delle linee guida e nella pagina <http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6498465>, di avviare con assoluta priorità:

- la designazione del Responsabile della protezione dei dati – RPD (artt. 37-39)
- l'istituzione del Registro delle attività di trattamento (art. 30 e cons. 171)
- la notifica delle violazioni dei dati personali (cd. data breach, art. 33 e 34)

DESIGNAZIONE DEL RESPONSABILE DELLA PROTEZIONE DEI DATI – RPD

In merito alla designazione del Responsabile della protezione dei dati si evidenziano di seguito gli adempimenti richiesti.

	Adempimenti sulla nomina del RPD
Entro il 30 settembre 2017	▪ Nomina del Responsabile della protezione dei dati
Entro il 25 maggio 2018	▪ Pubblicazione dei riferimenti del Responsabile della protezione dei dati sui siti istituzionali ▪ Comunicazione all'Autorità Garante dei riferimenti del Responsabile della protezione dei dati sui siti istituzionali

Il Responsabile della protezione dei dati, entro il 25 maggio 2018, tenuto conto dei compiti che gli sono attribuiti dall'art. 39, potrebbe individuare le seguenti priorità di intervento:

Ambito	Attività che potrebbero essere messe in campo dal RPD
---------------	--

Formazione	▪ Predisporre un piano formativo con l'obiettivo di favorire la conoscenza del nuovo regolamento a tutto il personale (tecnico-amministrativo, docenti e collaboratori)
Attribuzione Responsabilità	▪ Individuare l'assetto organizzativo e di responsabilità più idoneo a favorire il rispetto del GDPR, eventualmente avviando un gruppo di lavoro tra le aree dell'Ateneo che abbiano specifiche competenze sull'organizzazione e sullo stato giuridico del personale e dei collaboratori. ▪ Verificare che il personale che partecipa ai trattamenti sia dotato di strumenti volti a favorire il rispetto delle norme per ciò che attiene la nomina di eventuali responsabili esterni di trattamento (linee guida su come effettuare la nomina di un Responsabile del trattamento, template di nomina, ecc.) ▪ Redazione di un regolamento d'Ateneo che favorisca un corretto ed efficace recepimento delle prescrizioni del GDPR
Valutazione d'impatto	▪ Predisposizione di regole o linee guida idonee a favorire l'analisi dei rischi inerenti al trattamento anche in relazione ai diversi ambiti di applicazione, ai diversi contesti e finalità del trattamento.

ISTITUZIONE DEL REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

È assolutamente essenziale avviare quanto prima le attività idonee ad adottare un registro delle attività di trattamento. In particolare, queste potrebbero consistere nelle attività di seguito descritte:

Attività previste entro il 25 maggio 2018	Descrizione delle attività
Selezione del software usato per il Registro	Sarà necessario individuare una soluzione informatizzata per la gestione del registro delle attività di trattamento. Il registro, infatti, non può essere cartaceo.
Individuazione di eventuali "referenti privacy" per ciascuna struttura d'Ateneo	Per favorire la ricognizione dei trattamenti svolti dalle diverse strutture e delle principali caratteristiche di tali trattamenti, è consigliabile chiedere l'individuazione di almeno un "referente privacy" per ciascuna struttura (cioè un dipendente che possa interfacciarsi con il Responsabile della protezione dei dati per tutti gli aspetti concernenti la protezione dei dati trattati dalla struttura di appartenenza).
Ricognizione dei trattamenti svolti e delle loro principali caratteristiche	Per ciascun trattamento dovranno essere individuati seguenti elementi: finalità del trattamento, descrizione delle categorie di dati e interessati, categorie di destinatari cui è prevista la comunicazione, misure di sicurezza, tempi di conservazione, e ogni altra informazione che il titolare ritenga opportuna al fine di documentare le attività di trattamento svolte
Redazione piano di conformità al GDPR	La ricognizione dei trattamenti dovrebbe essere l'occasione per verificare anche il rispetto dei principi fondamentali del GDPR (art. 5), la liceità del trattamento (verifica dell'idoneità della base giuridica, artt. 6, 9 e 10) nonché l'opportunità

	dell'introduzione di misure a protezione dei dati fin dalla progettazione e per impostazione (privacy by design e by default, art. 25), in modo da assicurare, entro il 25 maggio 2018, la piena conformità dei trattamenti in corso (cons. 171).
--	---

Una prima ricognizione dei trattamenti solitamente svolti negli Atenei è presente nel capitolo 5 e riguarda i seguenti trattamenti inerenti gli studenti:

Trattamenti principali inerenti gli studenti
Trattamento finalizzato all'orientamento
Trattamento finalizzato all'erogazione dei test di ingresso o alla verifica dei requisiti di accesso
Trattamento finalizzato per l'erogazione del percorso formativo e gestione della carriera (dall'immatricolazione alla laurea)
Trattamento finalizzato all'attività di tirocinio
Trattamento finalizzato ad attività di job placement
Trattamento finalizzato ad attività di fundraising, di comunicazione e informazione istituzionale e sviluppo di community
Trattamento finalizzato a rilevazioni statistiche e valutazione della didattica
Trattamento finalizzato al caso di diffusione dell'elaborato finale o di elementi ad esso connessi
Trattamento finalizzato a servizi di tutorato, assistenza, inclusione sociale
Trattamento finalizzato all'erogazione di servizi e attività per il diritto allo studio
Procedimenti di natura disciplinare a carico di studenti

Trattamenti principali inerenti a dipendenti e/o collaboratori:

Trattamenti principali inerenti a dipendenti e/o collaboratori
Trattamento finalizzato allo svolgimento di prove concorsuali/selezioni
Trattamento finalizzato alla gestione del rapporto di lavoro
Trattamento di dati personali ai fini di formazione e aggiornamento professionale
Trattamento di dati personali necessario alla gestione di progetti di ricerca
Trattamento di dati personali al fine di garantire il monitoraggio e la valutazione della ricerca
Trattamento di dati personali nell'ambito di attività di trasferimento tecnologico
Trattamento necessario per politiche Welfare e per la fruizione di agevolazioni
Trattamenti per la salute e la sicurezza delle persone nei luoghi di lavoro
Trattamento dei dati personali nell'ambito dell'erogazione del servizio di telefonia fissa e mobile

Trattamenti trasversali o connessi ad attività trasversali:

Trattamenti trasversali o connessi ad attività trasversali
Trattamento dei dati nell'ambito della gestione degli spazi
Trattamento dei dati personali per la gestione delle postazioni

Trattamento per attività di gestione degli organi e delle cariche istituzionali
Trattamento per la gestione degli infortuni
Trattamento in ambito bibliotecario
Trattamento di dati nell'ambito dei servizi di protocollo e conservazione documentale
Trattamento finalizzato all'acquisto di beni e servizi, stipula di contratti, recupero crediti, gestione del contenzioso
Trattamento di dati nell'ambito dei servizi di posta elettronica e strumenti di collaboration
Trattamento di dati personali nell'ambito dell'erogazione federata di servizi
Trattamento finalizzato all'erogazione del servizio Eduroam
Trattamento finalizzato all'accesso a servizi federati (es: IDEM)
Trattamento nell'ambito dell'accesso ai servizi con autenticazione SPID
Tracciamento di informazioni non primarie

NOTIFICA DELLE VIOLAZIONI DEI DATI PERSONALI

Attività previste entro il 25 maggio 2018 in merito alla notifica	Descrizione delle attività
Redazione procedure per la notifica delle violazioni	È necessario individuare idonee procedure organizzative per dare attuazione alle nuove disposizioni sulla notifica delle violazioni dei dati personali (cd. data breach, art. 33 e 34) in cui siano chiariti i seguenti elementi: - Modalità per contattare il Responsabile della Protezione dei dati nel caso di violazioni e tempi di intervento - Casi esemplificativi in cui si rende necessaria la violazione - Casi in cui risulti improbabile che la violazione dei dati presenti un rischio per i diritti e le libertà dell'interessato - Casi e elementi utili a valutare se esiste un "rischio elevato" per i diritti e le libertà dell'interessato - Misure considerate sufficienti per scongiurare il sopraggiungere di un rischio elevato nel caso di violazioni - Individuazione di modalità per effettuare una comunicazione pubblica nell'eventualità indicati all'art. 34 comma 3 lettera c) del GDPR.
Diffusione istruzioni	Data la complessità dei nostri Atenei, è di fondamentale importanza individuare gli strumenti più idonei a favorire la conoscenza delle procedure per la notifica delle violazioni da parte di tutte le persone che trattano dati di titolarità dell'Ateneo.

Allegato 2 - Scheda di approfondimento per la redazione delle informative

Articolazione multilivello dell'informativa

I principi di trattamento corretto e trasparente implicano che l'interessato sia informato dell'esistenza del trattamento e delle sue finalità. Potrebbe a tal fine essere utile pubblicare sui siti istituzionali un'informativa che dia evidenza all'interessato delle diverse finalità del trattamento e delle modalità con le quali i dati sono trattati (magari fornendo un'informativa per ciascun trattamento inserito nel registro delle attività di trattamento di cui all'art. 30 del GDPR).

Per la redazione di un'informativa articolata su più livelli e con schede di dettaglio riferite a ciascun trattamento, si rimanda, a puro titolo esemplificativo, a quanto fatto dall'Alma Mater Studiorum – Università di Bologna che rende pubbliche sul suo Portale le informative concernenti i diversi interessati (<http://www.unibo.it/it/ateneo/privacy-e-note-legali/privacy/informative-sul-trattamento-dei-dati-personali>) e che sono raggiungibili da tutte le pagine del dominio.

Informativa per categorie di utenti

In merito alla redazione di un'informativa specifica per categorie di utenti, si riporta a titolo di esempio un modello relativo agli studenti che si immatricolano per la prima volta (si veda in particolare quanto riportato nella sezione "2 - Finalità e trattamenti" in cui si fa riferimento a una specifica categoria; le restanti sezioni hanno invece valenza generale).

1. Titolare e RPD	Titolare del Trattamento dati: Università <i>[indicare riferimenti specifici]</i> - Legale rappresentante: Rettore - Indirizzo - Telefono - e-mail - PEC Responsabile della protezione dei dati: <i>[indicare riferimenti specifici]</i> - Indirizzo - Telefono - e-mail - PEC
2. Finalità trattamenti giuridica e base dei	I trattamenti dei dati personali richiesti all'interessato sono effettuati ai sensi dell'art. 6 lettera e) del regolamento UE 2016/679, per le seguenti finalità: 1. iscrizione e frequenza di corsi di studi universitari in presenza e in modalità e-learning 2. gestione della carriera universitaria 3. utilizzo di servizi di orientamento 4. conseguimento del titolo di studio 5. calcolo degli importi delle tasse dovute 6. utilizzo dei servizi telematici e di posta elettronica 7. utilizzo dei servizi bibliotecari 8. accesso ai laboratori e ad altre strutture protette 9. fruizione di contributi, agevolazioni e servizi relativi al diritto allo studio universitario

	10. applicazione delle misure di sicurezza degli ambienti di lavoro secondo le disposizioni previste dal D.Lgs. 81/2008 11. invio di comunicazioni inerenti la propria carriera universitaria 12. rilevazioni per la valutazione della didattica e per la customer satisfaction 13. archiviazione e conservazione degli atti inerenti la carriera universitaria, sia riguardo agli studi svolti, sia riguardo agli eventuali incarichi ricoperti, e dei titoli di studio conseguiti 14. elezioni dei rappresentanti degli studenti e per eventuale svolgimento dei compiti inerenti la carica elettiva ricoperta dall'interessato negli organi di governo dell'Ateneo 15. statistiche e ricerca storica e scientifica, in forma anonima 16. eventuale utilizzo di agevolazioni inerenti la disabilità cronica o temporanea dell'interessato. È inoltre previsto il trattamento (non obbligatorio e soggetto a consenso) di dati personali identificativi e di carriera universitaria per le seguenti finalità: - comunicazione a soggetti esterni pubblici o privati per fini occupazionali o culturali - [indicare altre finalità] Il titolare non utilizza processi automatici finalizzati alla profilazione dell'interessato.
3. Destinatari dei dati personali ed eventuali trasferimenti di dati all'estero	I dati personali saranno trattati all'interno dell'Ateneo dai docenti del percorso di studio prescelto e dal personale tecnico-amministrativo afferente alle strutture competenti per le varie tipologie di trattamento. I dati personali potrebbero essere comunicati anche ad altre amministrazioni pubbliche, qualora queste debbano trattare i medesimi per eventuali procedimenti di propria competenza istituzionale. In particolare per usufruire dei contributi e servizi per il diritto allo studio universitario i dati saranno comunicati a <i>[indicare riferimenti specifici e recapiti]</i>, per i percorsi di studio che prevedono l'accesso alle strutture sanitarie e ospedaliere all'Azienda Sanitaria <i>[indicare riferimenti specifici e recapiti]</i> I dati personali potranno essere comunicati anche ad aziende pubbliche o private presso le quali potrebbero svolgersi attività didattiche o di ricerca o di tirocinio inerenti il percorso di studio prescelto. L'Ateneo si avvale del supporto di fornitori esterni per l'erogazione di alcuni servizi necessari alla gestione tecnico-amministrativa, i quali potrebbero venire a conoscenza dei dati personali degli studenti, ai soli fini della prestazione richiesta. L'elenco dei fornitori è consultabile alla pagina <i>[indicare riferimenti specifici]</i>.

4. Tempo di conservazione dei dati personali	Il titolare informa che i dati personali inerenti la carriera universitaria saranno conservati illimitatamente, tenuto conto degli obblighi di archiviazione imposti dalla normativa vigente. Gli altri dati raccolti per l'utilizzo dei servizi e per le comunicazioni saranno conservati per i tempi stabiliti dalla normativa vigente o dai regolamenti d'Ateneo.
5. Diritti dell'interessato	L'interessato ha diritto a: - Chiedere al titolare, ai sensi degli artt. 16, 17, 18, 19 e 21 del Regolamento (UE) 2016/679, l'accesso ai propri dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati. La cancellazione non è consentita per i dati contenuti negli atti che devono obbligatoriamente essere conservati dall'Università; - revocare il consenso in qualsiasi momento, senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca; - proporre reclamo a un'autorità di controllo.
6. Obbligo di conferimento dei dati	L'interessato è obbligato a conferire i dati personali richiesti, in caso di rifiuto l'Università <i>[indicare riferimenti specifici]</i> non potrà accettare l'iscrizione. La revoca del consenso può essere esercitata solo per i trattamenti opzionali.

Informativa per i trattamenti trasversali di natura sistemistica

Si riporta di seguito un esempio di informativa di primo livello riferita ai trattamenti trasversali di natura sistemistica effettuati dai servizi e dai sistemi informatici di Ateneo; ove ritenuto opportuno, tale informativa potrebbe essere integrata con approfondimenti tecnici in corrispondenza di specifici trattamenti effettuati.

1. Titolare e RPD	Titolare del Trattamento dati: Università <i>[indicare riferimenti specifici]</i> - Legale rappresentante: Rettore - Indirizzo - Telefono - e-mail - PEC Responsabile della protezione dei dati: <i>[indicare riferimenti specifici]</i> - Indirizzo - Telefono - e-mail - PEC
2. Finalità dei trattamenti	I dati personali raccolti dall'Ateneo, in qualità di Titolare del trattamento (di seguito "Ateneo" o "Titolare"), saranno trattati per la corretta e completa esecuzione dei servizi (di seguito "Servizi") offerti agli Utenti attraverso i sistemi informatici dell'Ateneo, compresi <i>[elenco da integrare/rivedere in base alle specifiche esigenze]</i>: - i sistemi di identificazione degli Utenti (es. credenziali, badge) - i servizi online messi a disposizione degli utenti, eventualmente forniti da terze parti

	- le reti cablate o Wi-Fi alle quali gli utenti accedono, eventualmente attraverso dispositivi personali (es. computer portatili, tablet, smartphone) - le postazioni informatiche fisse e mobili in dotazione al personale amministrativo/docente, o fruibili da studenti e da eventuali visitatori - i sistemi di controllo accessi ad aule, laboratori e spazi dell'Ateneo - i sistemi di videosorveglianza - i sistemi di telefonia fissa e mobile La presente informativa riguarda i trattamenti dei dati degli Utenti che usufruiscono delle risorse IT del Titolare. I dati dell'Utente, forniti volontariamente o comunque raccolti nella fruizione dei Servizi previa richiesta di consenso ove necessario, saranno trattati dal Titolare per le seguenti finalità: a) per finalità istituzionali e amministrative; b) per adempiere ad ogni obbligo di legge connesso con il suo rapporto con l'Ateneo; c) finalità inerenti l'erogazione dei Servizi richiesti (es: registrazione al portale dell'Ateneo, accesso all'area riservata, utilizzo delle reti Wi-Fi dell'Ateneo, ecc.) d) finalità di ricerche/analisi statistiche su dati aggregati o anonimi, senza dunque possibilità di identificare l'utente, volti a misurare il funzionamento dei Servizi; e) per adempiere a specifici obblighi derivanti dalla legge o da regolamenti; f) per garantire la protezione dei dati e/o dei sistemi informatici o per supportare attività di setup e troubleshooting dei servizi o per vincoli di natura tecnico/sistemistica g) per far valere o difendere diritti in giudizio o in fasi ad esso propedeutiche in caso di abusi e/o attività illecite operate dagli interessati o da terzi nell'ambito delle attività di cui alle finalità a), b), c), d), e), f). Il conferimento dei dati è necessario per le finalità a), b), e) ed f). Il loro eventuale mancato conferimento non permetterebbe al titolare di soddisfare gli obblighi previsti dalla legge, da un regolamento o dalla normativa comunitaria. Il conferimento dei dati per le finalità di cui alla lettera c) è facoltativo, ma il loro eventuale mancato conferimento non consentirebbe l'erogazione dei servizi richiesti. I trattamenti su dati aggregati o anonimi, di cui alla lettera d), non prevedono l'applicazione del Codice Privacy e del GDPR. Per ulteriori dettagli si faccia riferimento alla scheda "Modalità di trattamento e tipologie di dati trattati" sotto riportata.
3. Destinatari dei dati personali ed eventuali trasferimenti di dati all'estero	I dati personali potranno essere portati a conoscenza di dipendenti o collaboratori del Titolare, appartenenti alle categorie degli addetti amministrativi, commerciali, legali, contabili o degli amministratori di sistemi informatici, a seconda del trattamento, i quali, operando sotto la diretta

	autorità di quest'ultimo, sono nominati responsabili o incaricati del trattamento ai sensi degli artt. 29 e 30 del Codice Privacy o referenti ai sensi degli artt. 28 e 29 del RGPD, e ricevono al riguardo adeguate istruzioni operative. I dati personali non saranno oggetto di comunicazione verso terzi, se non nei confronti di: - soggetti, enti o Autorità, verso i quali la comunicazione sia obbligatoria in forza di disposizioni di legge o di regolamento. - fornitori, limitatamente alle necessità strettamente connesse all'erogazione dei servizi di cui sopra
4. Tempo di conservazione dei dati personali	I dati raccolti saranno conservati per i tempi stabiliti dalla normativa vigente.
5. Diritti degli interessati	L'interessato ha diritto a: - chiedere al titolare, ai sensi degli artt. 16, 17, 18, 19 e 21 del Regolamento (UE) 2016/679, l'accesso ai propri dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati. La cancellazione non è consentita per i dati contenuti negli atti che devono obbligatoriamente essere conservati dall'Università; - revocare il consenso in qualsiasi momento, senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca; - proporre reclamo a un'autorità di controllo.
7. Obbligo di conferimento dei dati	L'interessato è obbligato a conferire i dati personali richiesti, in caso di rifiuto l'Università <i>[indicare riferimenti specifici]</i> non potrà consentire l'accesso ai servizi. La revoca del consenso può essere esercitata solo per i trattamenti opzionali.
Per ulteriori dettagli si faccia riferimento alla scheda "Modalità di trattamento e tipologie di dati trattati" sotto riportata.	

Modalità di trattamento e tipologie di dati trattati

Modalità di trattamento	Il trattamento dei dati personali avverrà mediante strumenti manuali, informatici e telematici comunque idonei a garantire la sicurezza e la riservatezza dei dati stessi. Specifiche misure di sicurezza sono osservate per prevenire la perdita dei dati, usi illeciti o non corretti ed accessi non autorizzati nel pieno rispetto di quanto previsto dagli artt. 31 e seguenti del Codice Privacy e dal Disciplinare Tecnico – Allegato B al Codice Privacy – in materia di misure minime di sicurezza e dall'art. 32 RGPD. Con riferimento ai lavoratori e collaboratori, i file di log delle attività eseguite attraverso gli strumenti informatici messi a disposizione dall'Ateneo sono trattati e conservati in tutte le evidenze e per tutti i fini connessi al rapporto di lavoro, come previsto dal Regolamento per il trattamento dei dati personali, sensibili e giudiziari dell'Ateneo.
--------------------------------	---

	Con riferimento a tutti gli utenti, si potranno operare estrazioni dei file di log (relativi alle attività compiute attraverso i Servizi), anche mediante incroci ed elaborazioni di tali dati per identificare i responsabili di abusi e/o attività illecite operate dagli interessati o da terzi.
Dati di navigazione ed utilizzo delle applicazioni e dei servizi	I sistemi informatici dell'Ateneo, le procedure software e gli applicativi che ne supportano il funzionamento e l'erogazione dei servizi acquisiscono, nel corso del loro normale esercizio, alcuni dati personali sull'utilizzo degli applicativi messi a disposizione dall'Ateneo. Suddetti dati non vengono raccolti per essere posti in relazione con le attività di soggetti identificati, tuttavia per loro stessa natura, attraverso successive elaborazioni ed eventuali integrazioni con dati detenuti da terzi, potrebbero venire correlati agli utenti. In questa categoria di dati rientrano ad esempio: la data e l'ora della richiesta, gli indirizzi IP del server e del richiedente, il nome del server, il protocollo, la porta ed il metodo (POST/GET) utilizzati per sottoporre la richiesta al server, il browser impiegato, lo username, il servizio acceduto, le risorse richieste e gli eventuali cookie associati, il numero di byte inviati e ricevuti, il codice di errore restituito, il tempo richiesto per l'esecuzione della richiesta. Nell'ambito dell'interazione di un utente con servizi web resi disponibili dall'Ateneo in un contesto autenticato, vengono tracciate su log informazioni di base relative all'accesso al singolo servizio (timestamp, username, servizio) ed informazioni di sessione strutturate in conformità al formato W3C standard https://www.w3.org/TR/WD-logfile.html. Per la gestione del single sign on ai servizi vengono utilizzati cookie di sessione. Al fine di supportare elaborazioni aggregate di carattere statistico sull'uso dei servizi, vengono utilizzati cookie anonimi con registrazione limitata alle seguenti informazioni: lingua di visualizzazione, paese e città di provenienza, browser utilizzato, sistema operativo, provider del servizio internet, risoluzione schermo.
Dati di connessione alla rete di Ateneo	A fronte dell'accesso da parte di un utente ai servizi di rete (ad esempio: connessione alla rete dati wired/wireless autenticata, utilizzo di una postazione gestita, assegnazione dinamica di un IP address, accesso da remoto tramite VPN, utilizzo di proxy, ecc.), vengono registrati nei log generati dai sistemi e dagli apparati alcuni dati tecnici specifici relativi al servizio acceduto. Ad esempio: indirizzo IP dell'utente, data e ora di connessione, MAC address e nome del dispositivo dal quale viene effettuato l'accesso, ID utente, tipo di rete utilizzata, ecc. Si tratta di informazioni che non vengono raccolte per essere poste in relazione con l'attività di soggetti identificati, tuttavia per loro stessa natura, attraverso successive elaborazioni ed eventuali integrazioni con dati detenuti da terzi, potrebbero essere correlate agli utenti a fronte di specifiche richieste o segnalazioni ad esempio da parte dell'autorità giudiziaria.

Allegato 3 - Scheda di analisi per progetti di ricerca

DESCRIZIONE DEI TRATTAMENTI E DELLE FINALITÀ

Il ricercatore, prima dell'avvio di una ricerca, dovrebbe individuare l'ambito, il contesto e le finalità della ricerca.

Descrizione del Progetto	
1. Data di inizio prevista	
2. Data di fine prevista	
3. Ipotesi/Breve stato dell'arte / giustificazione teorica	
4. Obiettivi / Risultati attesi	
5. Metodologia	
6. Descrizione della procedura	

Dovrebbe altresì essere in grado di effettuare una descrizione accurata del processo - con particolare riferimento alle operazioni di raccolta dei dati.

Modalità e procedure	
7. Modalità di raccolta dei dati	☐ utilizzo di questionari ☐ interviste strutturate o semi-strutturate ☐ interviste in profondità ☐ focus group ☐ raccolta di diari (diary keeping) ☐ osservazione del comportamento dei soggetti a loro insaputa ☐ osservazione del comportamento dei soggetti ☐ registrazioni audio o video dei soggetti ☐ somministrazione di stimoli, compiti o procedure e registrazione di risposte comportamentali, opinioni o giudizi ☐ somministrazione di stimoli, compiti o procedure che il soggetto potrebbe trovare fastidiosi, stressanti, fisicamente o psicologicamente dolorosi, sia durante sia successivamente la conduzione dello studio ☐ registrazione di movimenti ☐ immersione in ambienti di realtà virtuale ☐ registrazione di potenziali evocati ☐ somministrazione di test, questionari o protocolli sperimentali attraverso internet (web, posta elettronica)

	☐ utilizzo di test neuropsicologici e di tecniche di neuroimmagine ☐ somministrazione di sostanze o agenti (ad es., farmaci, alcol) ☐ partecipazione ad un trial clinico ☐ altro (<i>specificare</i>) <i>Allegare copia delle domande che verranno poste (se previsto dalla procedura utilizzata); ove questo non sia possibile, indicare gli argomenti che verranno trattati</i>
8. Descrizione del flusso dei dati	

Il ricercatore dovrebbe altresì effettuare una valutazione dei rischi per i diritti e le libertà degli interessati, anche sulla base delle caratteristiche degli interessati

Partecipanti al progetto	
9. Tipologia	☐ Maggiori d'età ☐ Minori d'età ☐ Studenti ☐ Lavoratori ☐ Soggetti con disabilità fisica e psichica o con limitata capacità d'intendere o volere ☐ Soci, associati, aderenti o iscritti a organizzazioni a carattere religioso, politico, filosofico o sindacale ☐ Condannati, detenuti, imputati, indagati o sottoposti a misure di sicurezza o prevenzione ☐ Volontari sani ☐ Pazienti ☐ altro

10. Numero indicativo di partecipanti	
11. Caratteristiche del gruppo partecipanti ricerca	☐ Gruppi omogenei per abitudini sessuali ☐ Gruppi omogenei per appartenenza razziale o etnica ☐ Gruppi omogenei per area geografica ☐ Gruppi omogenei per caratteristiche fisiche ☐ Gruppi omogenei per consanguineità ☐ Gruppi omogenei per fattori di rischio ☐ Gruppi omogenei per convinzioni religiose, filosofiche, politiche o sindacali <i>Specificare eventuali e ulteriori criteri di inclusione/esclusione</i>
12. È possibile che alcuni dei soggetti si trovino in una posizione di dipendenza nei confronti del ricercatore o dei suoi collaboratori, tale per cui si possa supporre che l'espressione del consenso a partecipare allo studio non sia del tutto libera e priva da ogni tipo di pressione?	☐ Sì ☐ No <i>Se sì, indicare come si intende provvedere per minimizzare la possibilità che il soggetto si senta obbligato a prendere parte alla ricerca (ad es. nel rapporto studente/professore, paziente/medico, dipendente/datore di lavoro)</i> <i>Esempio: Il soggetto valuta senza alcuna fretta o pressione psicologica le informazioni ricevute tramite i moduli e decide di aderire alla ricerca, fornendo il consenso al trattamento dei dati, solo in un momento successivo alla cura/incontro informativo</i>
13. Come verranno diffuse le informazioni/l'invito a partecipare alla ricerca?	
14. È prevista qualche forma di incentivo per i partecipanti allo studio?	☐ Sì ☐ No <i>Se sì, indicare quali</i>

Modalità e procedure									
15. Rischi per i partecipanti	☐ Nessuno ☐ Rischi sociali, legali o economici ☐ Disagi o rischi per il benessere fisico e psicologico ☐ altro (<i>specificare</i>) 								
16. Benefici per i partecipanti	☐ Nessuno ☐ Benefici di natura sociale ottenuti attraverso un miglioramento delle conoscenze scientifiche ☐ Compenso o altri vantaggi materiali ☐ altro (<i>specificare</i>) 								
17. È prevista una specifica polizza di assicurazione per responsabilità civile aggiuntiva a quella di Ateneo? <i>[Da compilare soprattutto nel caso di sperimentazioni mediche]</i>	☐ Sì, è stata stipulata una polizza assicurativa che copre tutti i danni strettamente connessi alla partecipazione allo studio. La copertura assicurativa è stata stipulata con la seguente compagnia assicurativa: <table border="1"> <thead> <tr> <th>Nome</th><th>telefono</th><th>fax</th><th>Numero polizza assicurativa</th></tr> </thead> <tbody> <tr> <td> </td><td> </td><td> </td><td> </td></tr> </tbody> </table> ☐ Lo studio è no-profit e osservazionale e viene utilizzata l'assicurazione d'Ateneo ☐ Lo studio è no-profit, interventistico e viene aggiunto un premio assicurativo ☐ Non è prevista alcuna forma di assicurazione	Nome	telefono	fax	Numero polizza assicurativa				
Nome	telefono	fax	Numero polizza assicurativa						
18. Come si prevede di affrontare il caso in cui l'interessato intenda non aderire alla ricerca (anche in un momento successivo)?	☐ L'interessato potrà ritirare il consenso in qualsiasi momento e senza fornire spiegazioni alcuna, con la conseguente distruzione dei dati ☐ L'interessato potrà richiedere che tutti i dati precedentemente raccolti siano distrutti o resi anonimi in modo definitivo solo nelle fasi antecedenti alla irreversibile anonimizzazione o aggregazione ☐ altro (<i>specificare</i>) 								

Sarà opportuno inoltre che il ricercatore sia in grado di prevedere, previamente alla raccolta, le modalità di comunicazione e diffusione dei dati personali, nonché l'eventuale trasferimento dei dati all'estero.

Comunicazione e diffusione dei dati	
19. I dati <u>personali</u> (non anonimi o aggregati) vengono diffusi?	☐ No ☐ Sì Se sì, selezionare una o più modalità: ☐ Stampa quotidiana e periodica anche elettronica ☐ Stampati in genere ☐ TV ☐ Posta ☐ Fax ☐ Posta elettronica ☐ Internet ☐ A mezzo confezione del prodotto ☐ Affissione dei dati in luoghi pubblici ☐ Radio ☐ Telefono ☐ Televideo ☐ Agenzie di stampa ☐ Strumenti multimediali (cd, dvd...) ☐ Altro, specificare in dettaglio
20. I dati <u>personali</u> (pseudonimizzati e che non siano pertanto anonimi o aggregati) vengono comunicati?	☐ No ☐ Sì Se sì, selezionare uno o più ambiti di comunicazione: ☐ Soggetti privati ☐ Soggetti pubblici ☐ Persone giuridiche, società di persone o di capitali, imprese individuali ☐ Organi costituzionali o di rilevanza costituzionale ☐ Amministrazioni dello Stato ☐ Amministrazioni regionali ☐ Enti locali (comuni e province) ☐ Associazioni di enti locali ☐ Altre amministrazioni ed enti pubblici

	☐ Organismi del servizio sanitario nazionale ☐ Enti pubblici non economici ☐ Enti pubblici economici ☐ Autorità giudiziaria ☐ Uffici giudiziari ☐ Società di vigilanza private ☐ Società controllanti, controllate e/o collegate ☐ Associazioni di imprenditori o di imprese ☐ Organismi sindacali o patronali ☐ Organismi paritetici in materia di lavoro ☐ Consulenti e liberi professionisti anche in forma associata ☐ Banche ☐ Intermediari finanziari ☐ Gestori di sistemi informatici centralizzati (centrali rischi, antifrode, ecc.) ☐ Assicurazioni ☐ Soci associati e iscritti ☐ Clienti e/o utenti ☐ Altro, specificare in dettaglio
--	--

Trasferimento di dati all'estero (extra UE)	
21. I dati <u>personali</u> (pseudonimizzati e che non siano pertanto anonimi o aggregati) vengono trasferiti all'estero?	☐ No ☐ Sì Se sì, in che area geografica sono trasferiti i dati? ☐ Paesi dell'America del centro-nord ☐ Paesi dell'America del sud ☐ Paesi dell'area asiatica ☐ Paesi dell'area africana ☐ Paesi dell'Oceania ☐ Paesi dell'Europa extra UE In quale/i Paese/i all'interno dell'area

TITOLARE E INTERESSI LEGITTIMI PERSEGUITI

È importante che il ricercatore sia guidato nella determinazione dei soggetti coinvolti nel trattamento e nell'individuazione delle responsabilità a essi associate.

Soggetti coinvolti nel Progetto									
22. Titolare									
23. Responsabile scientifico									
24. Personale coinvolto									
25. È necessaria l'autorizzazione di altri Enti/soggetti terzi per l'accesso ai dati o per il coinvolgimento di partecipanti?	☐ Sì ☐ No <i>Se sì, allegare copia della lettera di autorizzazione e/o la lettera di richiesta di eventuali dati provenienti da soggetti terzi)</i>								
26. Sono previsti, ai sensi della normativa vigente, interventi che richiedono specifiche professionalità (ad es. medico, psicologo, infermiere, ecc.)?	☐ No ☐ Sì <i>Se sì, specificare quali istruzioni sono fornite in merito al trattamento dei dati personali</i> 								
27. Ci sono eventuali partner, enti, sponsor o finanziatori che potrebbero venire a conoscenza dei dati personali?	☐ No ☐ Sì <i>Se sì, indicare tali soggetti e il ruolo che hanno del progetto</i> <table border="1"> <thead> <tr> <th>Nominativo</th> <th>Ruolo</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> </tr> <tr> <td></td> <td></td> </tr> <tr> <td></td> <td></td> </tr> </tbody> </table>	Nominativo	Ruolo						
Nominativo	Ruolo								

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).

Informativa e consenso

28. È stata prevista adeguata informativa per i partecipanti?	☐ No ☐ Sì <i>Se sì, allegare una copia dell'Informativa e dell'eventuale dichiarazione di consenso</i>
29. È possibile fornire l'informativa ai partecipanti alla ricerca (soggetti interessati)?	☐ Sì ☐ No <i>Se no, nel caso di ricerca medica, biomedica ed epidemiologica, indicare le ragioni, considerate del tutto particolari o eccezionali, documentate nel progetto di ricerca:</i> ☐ No, per motivi etici riconducibili alla circostanza che l'interessato ignora la propria condizione¹¹ ☐ Sebbene sia stato svolto ogni ragionevole sforzo organizzativo¹², non è possibile contattare gli interessati in ragione: ☐ del numero molto alto di interessati che è stato stimato ☐ perché ci sarebbero conseguenze significative per lo studio in termini di alterazione dei risultati ☐ del fatto che i soggetti sono deceduti o persi al follow up
<i>[Da completare nel caso in cui non sia possibile fornire l'informativa ai <u>soggetti interessati non in grado di esprimere il consenso</u>]</i> 30. Indicare a chi si chiederà di acconsentire alla partecipazione precisandone il ruolo e i motivi	☐ I dati di minori o di soggetti incapaci di esprimere il consenso saranno utilizzati soltanto, se sarà ottenuto il consenso dei genitori o dell'altro genitore in mancanza di uno di essi o del rappresentante legale ☐ Nei casi di incapacità temporanea, all'atto della riacquisizione delle proprie capacità decisionali, al soggetto sarà richiesto il consenso ☐ altro (specificare)
<i>[Da completare nel caso in cui, per la realizzazione dello studio, non dovesse essere possibile <u>informare i partecipanti prima dell'inizio della ricerca</u>]</i>	<i>Nel caso di trattamenti di dati di natura non sensibile, né <u>giudiziaria</u>, indicare le ragioni per le quali si è reso necessario differire o non fornire l'informativa:</i>

¹¹ Rientrano in questa categoria le ricerche per le quali l'informativa sul trattamento dei dati da rendere agli interessati comporterebbe la rivelazione di notizie concernenti la conduzione dello studio la cui conoscenza potrebbe arrecare un danno materiale o psicologico agli interessati stessi (possono rientrare in questa ipotesi, ad esempio, gli studi epidemiologici sulla distribuzione di un fattore che predica o possa predire lo sviluppo di uno stato morboso).

¹² Motivi di impossibilità organizzativa riconducibili alla circostanza che la mancata considerazione dei dati riferiti al numero stimato di interessati che non è possibile contattare per informarli, rispetto al numero complessivo dei soggetti che si intende coinvolgere nella ricerca, produrrebbe conseguenze significative per lo studio in termini di alterazione dei relativi risultati; ciò avuto riguardo, in particolare, ai criteri di inclusione previsti dallo studio, alle modalità di arruolamento, alla numerosità statistica del campione prescelto, nonché al periodo di tempo trascorso dal momento in cui i dati riferiti agli interessati sono stati originariamente raccolti (ad esempio, nei casi in cui lo studio riguarda interessati con patologie ad elevata incidenza di mortalità o in fase terminale della malattia o in età avanzata e in gravi condizioni di salute).

31. Specificare quali saranno le modalità con le quali sarà resa successivamente l'informativa	☐ L'informativa è differita perché ci sarebbero conseguenze significative per lo studio in termini di alterazione dei risultati ☐ Rendere l'informativa comporta un impiego di mezzi manifestamente sproporzionato perché <i>[Indicare le motivazioni per le quali si è ritenuto di differire l'informativa e quali saranno le modalità adottate per informare gli interessati quando saranno venuti meno i motivi che giustificano il differimento, ovvero le ragioni portate per il mancato completamento dell'informativa]</i> <u>Nel caso di trattamenti di dati raccolti presso terzi (es: altri enti o aziende) per altri scopi, indicare le forme di pubblicità adottate nel caso in cui fornire l'informativa agli interessati comporti uno sforzo sproporzionato rispetto al diritto tutelato.</u> È prevista, previa informazione al Garante: ☐ l'inserzione su almeno un quotidiano di larga diffusione nazionale o annuncio presso un'emittente radiotelevisiva a diffusione nazionale, per trattamenti riguardanti insiemi numerosi di soggetti distribuiti sull'intero territorio nazionale ☐ l'inserzione su un quotidiano di larga diffusione regionale (o provinciale) o annuncio presso un'emittente radiotelevisiva a diffusione regionale (o provinciale), per trattamenti riguardanti insiemi numerosi di soggetti distribuiti su un'area regionale (o provinciale) ☐ l'inserzione in strumenti informativi (es. sito web) di cui gli interessati sono normalmente destinatari, per trattamenti riguardanti insiemi di specifiche categorie di soggetti, identificate da particolari caratteristiche demografiche e/o da particolari condizioni formative o occupazionali o analoghe
32. Quali modalità saranno adottate per ricevere espressioni di dubbi e rispondere a richieste di precisazioni da parte dei soggetti nel corso dello studio?	☐ Verrà fornita indicazione dei soggetti a cui poter inviare le richieste. Per qualsiasi informazione e chiarimento sullo studio o per qualsiasi necessità nel corso dello studio, i soggetti partecipanti potranno rivolgersi al dottor/professor _____ che è a disposizione per ogni domanda o dubbio ☐ Tramite moduli che sono stati predisposti per raccogliere i reclami/segnalazioni e suggerimenti ☐ altro (specificare) _____ _____

33. *[Da compilare nel caso in cui siano acquisiti dati inerenti lo stato di salute]*

In che modo i partecipanti saranno informati della possibilità di ricevere, direttamente o indirettamente, ogni altro dato relativo alle loro condizioni psico-fisiche che dovesse diventare disponibile durante la ricerca?

I partecipanti saranno edotti di tale possibilità nell'informativa. Nel caso in cui dovesse acconsentire alla conoscenza di risultati o notizie inattese, l'interessato potrà ricevere le comunicazioni a mezzo:

- ☐ Posta
- ☐ Fax
- ☐ Telefono
- ☐ Posta elettronica
- ☐ Medico curante
- ☐ altro (*specificare*)

Misure di Sicurezza	
34. Verranno conservati i dati identificativi dei partecipanti?	☐ No ☐ Sì Se sì, specificare le ragioni sottese a tale esigenza
35. Descrivere le procedure utilizzate per non identificare direttamente o rendere anonimi i dati dei partecipanti nelle diverse fasi della ricerca	<u>Per non identificare direttamente l'interessato</u> sono adottate le seguenti misure: ☐ Adozione di tecniche crittografiche ☐ Utilizzo di codici univoci per ciascun partecipante. Solo il responsabile della ricerca o altri soggetti autorizzati, possono (con l'uso di mezzi ragionevoli¹³) collegare i codici all'identità dei partecipanti ☐ Il trattamento dei dati avverrà tramite l'uso di un codice che sarà consegnato ai partecipanti in modo casuale all'inizio dell'esperimento ☐ Il trattamento dei dati avverrà tramite l'uso di un codice che sarà scelto dai partecipanti ☐ Altro, specificare in dettaglio <u>Per anonimizzare o aggregare i dati</u>, anche in un momento successivo alla raccolta, sono adottate le seguenti misure: ☐ I dati personali, a seguito della raccolta sono eliminati definitivamente senza la possibilità di risalire ai dati originali

¹³ Ad esempio, tramite:

- l'uso di risorse *hardware* e *software* per effettuare le elaborazioni necessarie per collegare informazioni non nominative ad un soggetto identificato, tenendo anche conto delle effettive possibilità di pervenire in modo illecito alla sua identificazione in rapporto ai sistemi di sicurezza ed al *software* di controllo adottati;
- la conoscenza delle procedure di estrazione campionaria, imputazione, correzione e protezione statistica adottate per la produzione dei dati.

	☐ I dati personali sono sostituiti da uno o più identificatori, che possono essere utilizzati per un set di dati o per ogni singolo dato ☐ Sono distrutti i dati che possono essere idonei a identificare gli interessati e sono conservati i soli dati aggregati ¹⁴ ☐ Altro (<i>specificare</i>)
36. Individuazione di misure che contribuiscono alla proporzionalità e alla necessità dell'elaborazione dei dati	

Conservazione	
37. Per quanto tempo i dati raccolti verranno conservati dalla conclusione della ricerca?	I dati saranno conservati per: _____ Al termine di questo periodo i dati saranno: ☐ distrutti ☐ conservati in forma anonima
38. Indicare le modalità di conservazione dei dati	☐ In formato cartaceo ☐ In formato digitale ☐ altro (<i>specificare</i>)

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...) nonché descrivere le misure di protezione adottate.

¹⁴ Si considerano dati aggregati le combinazioni di modalità alle quali è associata una frequenza non inferiore a una soglia prestabilita, ovvero un'intensità data dalla sintesi dei valori assunti da un numero di unità statistiche pari alla suddetta soglia. Il valore minimo attribuibile alla soglia è pari a tre.

Allegato 4 – Informativa per il trattamento di dati sensibili in un progetto di ricerca

TITOLO STUDIO:	
PROTOCOLLO N.:	
SPERIMENTATORE:	
COLLABORATORI:	

Lei è invitato a prendere parte ad uno studio che si propone di verificare *[indicare obiettivo della ricerca]* condotto nel *[indicare Unità Organizzativa]*, in collaborazione con *[indicare, se presenti, eventuali enti o soggetti terzi che collaborano alla ricerca]*. Le caratteristiche dello studio e le sue modalità di svolgimento sono descritte nel dettaglio nel documento "Informazioni in merito alla partecipazione allo studio".

L'Università, *quale centro di sperimentazione* e in qualità di Titolare del trattamento, tratterà i Suoi dati personali soltanto nella misura in cui siano indispensabili in relazione all'obiettivo dello studio, nel rispetto di quanto previsto dalla normativa vigente in materia di protezione dei dati personali e conformemente alle disposizioni di cui alle autorizzazioni generali dell'Autorità Garante per la protezione dei dati personali *[indicare eventuali specifici riferimenti]*.

FINALITÀ E MODALITÀ DEL TRATTAMENTO

I dati personali dell'interessato, in particolare quelli sensibili inerenti *[specificare la tipologia dei dati trattati a seconda delle caratteristiche dello studio]*, saranno trattati con un livello di sicurezza assai elevato. Sono implementate tutte le misure di tutela indicate dalla normativa sulla protezione dei dati personali e dalla normativa applicabile nonché quelle determinate dall'Ateneo. In particolare, i Suoi dati saranno trattati

- con modalità che permetteranno di identificarla solo in caso di necessità;
- esclusivamente all'interno di locali e sistemi (hardware e software) protetti e secondo le misure di sicurezza previste.

I dati saranno trattati dal/i Responsabile/i del trattamento sotto indicati e dagli incaricati, con strumenti automatizzati e non, esclusivamente ai seguenti fini:

(i) per consentire lo svolgimento della ricerca in parola e di tutte le relative operazioni ed attività connesse, comprese quelle amministrative.

[indicare come saranno trattati i dati personali]

Esempio: I dati saranno trattati mediante strumenti cartacei ed elettronici *[specificare analiticamente le modalità di trattamento dei dati: CRF cartacea, CRF elettronica ecc.]*. Il medico (Sperimentatore)/i medici (sperimentatori)/i ricercatori che seguirà/seguiranno lo studio identificherà/identificheranno l'interessato con un codice. I dati raccolti nel corso dello studio saranno registrati, elaborati e conservati per x anni unitamente a tale codice *[indicare il tempo di conservazione che deve comunque essere commisurato alle finalità della raccolta. Per le sperimentazioni cliniche è di almeno 7 anni]*. Soltanto il medico/ricercatore ed i soggetti autorizzati potranno collegare questo codice al Suo nominativo.

I dati verranno conservati dal Titolare sotto la responsabilità del/della *[indicare il "Responsabile del trattamento" con particolare riferimento alla conservazione]*.

[indicare i soggetti ai quali i dati saranno comunicati]

Esempio: I dati sensibili saranno raccolti dall'[indicare unità organizzativa] e potranno essere comunicati per [indicare le attività/finalità perseguite dagli altri centri nell'ambito dello studio in epigrafe] a [...] e alle persone o società esterne che agiscono per loro conto, tra le quali [inserire gli estremi identificativi di almeno uno dei terzi cui i dati saranno trasmessi]. [Se per raggiungere le finalità dello studio è indispensabile trasferire i dati al di fuori dell'Ue aggiungere "I dati, contraddistinti esclusivamente da un codice numerico, saranno altresì trasmessi anche in Paesi non appartenenti all'Unione europea che non garantiscono un adeguato livello di protezione dei dati personali" [inserire gli estremi identificativi dei destinatari]].

Se l'Interessato accetta di prendere parte al presente studio, si informa che - oltre ai ricercatori indicati in epigrafe (Sperimentatore e Collaboratori) e agli altri soggetti sopra indicati partecipanti alla ricerca - le Autorità Regolatorie competenti, il Comitato etico del [indicare CE di riferimento] e le autorità sanitarie italiane e straniere potranno esaminare tutta la documentazione sanitaria raccolta nel corso dello studio: lo scopo di queste verifiche è controllare che la ricerca sia condotta correttamente e in conformità alle disposizioni vigenti e l'Interessato non avrà la facoltà di impedire tali attività.

[indicare se i dati personali saranno oggetto di diffusione e in quali modalità]

Esempio: I dati saranno diffusi solo in forma rigorosamente anonima, ad esempio attraverso pubblicazioni scientifiche, statistiche e convegni scientifici.

[da inserire nel caso di utilizzo di immagini riferite all'Interessato]

Se strettamente necessario alle finalità di ricerca, il trattamento può avere, inoltre, ad oggetto le immagini dell'Interessato (fotografie, riprese-video, riprese audio-video, radiografie).

Il trattamento di tali immagini avverrà nel rispetto delle disposizioni di legge, garantendo *in tutti i casi in cui ciò sia possibile* l'anonimato dell'Interessato tramite l'oscuramento dei tratti somatici.

Per il trattamento delle immagini, è richiesto all'Interessato uno specifico consenso, anche ai sensi delle disposizioni di legge sul diritto d'autore, considerato che, sia pure in casi particolari, anche immagini relative a persone il cui viso è stato oscurato possono consentirne l'identificazione.

(ii) considerato che nuove scoperte potrebbero indicare inedite opportunità di indagine ai ricercatori o consentire di effettuare ulteriori studi e ricerche sui dati sensibili per lo studio di cui trattasi, per eventualmente ricontattare l'Interessato affinché possa esprimere, se lo riterrà, un nuovo specifico consenso e autorizzare così una nuova ricerca sui propri dati. Sempre e soltanto nell'ambito delle finalità descritte, i dati personali che la riguardano potranno altresì essere comunicati/trasmessi a ... [indicare partner di ricerca o altro soggetto che potrebbe ricevere i dati], quale [autonomo titolare del trattamento/responsabile del trattamento] e o [nell'ambito di ricerche congiunte/di ricerche che tale struttura intenda svolgere autonomamente].

NATURA DEL CONFERIMENTO DEI DATI E CONSEGUENZE DI UN EVENTUALE RIFIUTO DI RISPONDERE

Il conferimento dei dati per le finalità di cui al punto (i) è indispensabile allo svolgimento dello studio e non discende da un obbligo normativo. Il rifiuto di conferirli non consentirà

all'Interessato di partecipare allo studio in parola. Si precisa che tale rifiuto non pregiudicherà in alcun modo le cure o le prestazioni sanitarie cui ha diritto.

Il conferimento dei dati ai fini di cui al punto (ii) è facoltativo, cioè non discende da un obbligo normativo, ma è necessario per consentire la conservazione dei dati per un periodo più lungo di quello previsto per la conclusione del presente studio ed eventualmente permettere al Titolare di ricontattare l'Interessato affinché possa esprimere, se lo riterrà, un nuovo specifico consenso per una nuova ricerca. Il mancato conferimento dei dati per tali finalità avrà come unica conseguenza l'impossibilità di realizzare quanto da ultimo descritto.

SOGGETTI DEL TRATTAMENTO

Il Titolare dei dati è l'Università [...], con sede [...], Italia. Responsabile del trattamento è il *[indicare i riferimenti al Responsabile]*, domiciliato per la sua carica presso la sede *[indicare la sede]* (di seguito "Responsabile"). *[Indicare eventuali ulteriori Responsabili del trattamento o specificare le modalità attraverso le quali è conoscibile l'elenco completo e aggiornato. Quando non è possibile conoscere al momento della redazione dell'informativa l'elenco completo dei soggetti terzi a cui i dati saranno trasmessi, anche in paesi extra-UE, occorre specificare come e quando l'elenco completo verrà reso disponibile].*

DIRITTI DELL'INTERESSATO

Nella sua qualità di Interessato, il soggetto partecipante allo studio in parola gode dei diritti di cui alla sezione 2, 3 e 4 del capo III del Regolamento (UE) 2016/679 (es. chiedere al titolare del trattamento: l'accesso ai dati personali e la rettifica o la cancellazione degli stessi; la limitazione del trattamento che lo riguardano; di opporsi al loro trattamento).

L'Interessato ha altresì il diritto di:

- revocare il consenso in qualsiasi momento senza tuttavia pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca. In tal caso, non saranno raccolti ulteriori dati che lo riguardano, ferma restando l'utilizzazione di quelli eventualmente già raccolti per determinare, senza alterarli, *i risultati della ricerca* o di quelli che, in origine o a seguito di trattamento, non siano riconducibili a una persona identificata o identificabile.
- proporre reclamo a un'autorità di controllo.

In merito all'esercizio di tali diritti, l'Interessato può rivolgersi a [...], con sede [...], Tel. [...], Fax. [...], e-mail [...]