ALLEGATO 2:

Università degli Studi dell'Aquila

Responsabile della Protezione Dati personali

Piano di adeguamento dell'Università degli Studi dell'Aquila al Regolamento UE 2016/679

Regolamento Generale sulla Protezione dei dati del Parlamento europeo e del Consiglio del 27 aprile 2016

Redatto da Gianfranco Cardinale	Rev. 02	Data ultima revisione 30/06/2020

Il documento è destinato esclusivamente ad uso interno ed è soggetto a revisione.

Pillole di GDPR

Cos'è il regolamento generale sulla protezione dei dati

Il Regolamento Generale sulla Protezione dei Dati, altresì noto come GDPR, è la nuova normativa in materia di protezione dei dati personali, che si applica sull'intero territorio europeo. Emanato in data 27 aprile 2016, è entrato in vigore in data 25 maggio 2018 ed integra e sostituisce, per le parti non compatibili, ogni disposizione previgente in materia di *privacy*. A titolo di precisazione, trattandosi di regolamento europeo esso non necessita di alcuna norma di recepimento ed è quindi pienamente efficace in tutte le sue parti. Si applica nei confronti di tutte le organizzazioni pubbliche e private, indipendentemente dal settore di attività.

Cosa accade al Codice Privacy?

E' entrato in vigore il Decreto legislativo 10 agosto 2018, n. 101 che adegua il Codice in materia di protezione dei dati personali (Decreto legislativo 30 giugno 2003, n.106) alle disposizioni del Regolamento (UE) 2016/679. Viene dunque rivista la vecchia versione del D. Lgs. 196/2003 – Codice Privacy sostituito dal testo ampiamente novellato con funzione di armonizzazione al GDPR per quanto attiene la regolamentazione in materia di protezione dei dati personali.

Quali sono le novità sostanziali?

I principi di protezione dei dati personali sono stati rafforzati ed è stato in particolare introdotto, in capo ad enti pubblici e privati, quello di *accountability* ovvero di responsabilità e di capacità di dimostrare di aver agito responsabilmente.

Sono state identificate tassativamente sei ipotesi di base giuridica che garantiscono la liceità del trattamento dei dati personali e sono state rafforzate le protezioni relativamente ai dati particolari, categoria entro la quale sono annoverati i dati sensibili, i dati giudiziari, i dati biometrici. Modifiche di rilievo sono state apportate anche alle modalità di rilascio del consenso.

Il titolare del trattamento è obbligato a fornire informazioni molto più dettagliate agli interessati circa le modalità con cui avviene il trattamento dei dati personali. Tali informazioni sono normalmente inserite all'interno delle informative sulla privacy comunque denominate.

Il regolamento amplia la portata dei diritti esistenti e ne introduce di nuovi. A tal proposito, l'esercizio di tali diritti da parte degli interessati non può prevedere oneri a loro carico e deve pertanto avvenire in maniera totalmente gratuita.

Sono state abolite le cosiddette misure minime di protezione: sta al titolare stabilire quale sia il giusto livello di misure tecniche ed organizzative da porre in essere per garantire la protezione dei dati personali. Si tratta di una diretta conseguenza del principio di *accountability*.

La protezione dei dati personali non va più intesa come adempimento formale utile ad evitare sanzioni, ma come cultura da promuovere e diffondere all'interno degli enti, delle organizzazioni, delle imprese e tra i cittadini. Tra gli obblighi posti in capo al titolare figurano: la stesura di registro dei trattamenti completo ed esaustivo; la valutazione di impatto dei trattamenti sulla protezione dei dati personali; la nomina formale dei responsabili dei trattamenti, ossia soggetti esterni

all'organizzazione, che trattano i dati in nome e per conto del titolare; l'adozione di misure di *privacy by design* e *privacy by default* nella scelta e nella progettazione dei sistemi per il trattamento dati; la notifica delle violazioni dei dati personali entro 72 ore dalla scoperta.

Le modifiche avranno un impatto significativo sulle modalità con cui enti pubblici e privati, Università comprese, trattano i dati personali loro conferiti.

Cosa si rischia?

La sanzione massima che il Garante potrebbe infliggere all'Ateneo ammonta a € 20.000.000,00 o il 4% delle entrate annuali. Anche per questo è strettamente necessario uno sforzo collettivo nella comprensione dei principi del regolamento e nell'applicazione di corrette metodologie di trattamento dei dati personali. È essenziale passare dalla logica dell'adempimento a quella della cultura responsabile.

Una sintesi su cosa c'è da fare nell'immediato (dal sito del Garante per la protezione dei dati personali)

Rispettare i diritti delle persone	Ogni trattamento deve fondarsi sul rispetto dei principi fissati nel regolamento (artt. 5-6) e garantire agli interessati tutti i diritti previsti (artt. 13-22).
Individuare il rischio e svolgere una valutazione di impatto	Ai titolari spetta il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali, anche attraverso un apposito processo di valutazione che tenga conto dei rischi noti o evidenziabili e delle misure tecniche, organizzative e di sicurezza necessarie per mitigare tali rischi, eventualmente consultando il Garante alla luce di questa valutazione
Redigere un registro dei trattamenti	Si tratta di uno strumento fondamentale per disporre di un quadro aggiornato dei trattamenti in essere. I contenuti minimi sono indicati all'art. 30 del Regolamento. Deve avere una forma scritta, anche elettronica, e va esibito su richiesta del Garante.
Garantire la sicurezza dei dati	Il titolare e il responsabile del trattamento sono obbligati ad adottare misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio del trattamento (con l'obiettivo di evitare distruzione accidentale o illecita, perdita, modifica, rivelazione, accesso non autorizzato)
Nominare un Responsabile della protezione dei dati	La designazione di un Responsabile della Protezione Dati personali (RPD) riflette l'approccio responsabilizzante del Regolamento. Fra i suoi compiti rientrano la sensibilizzazione e formazione del personale, la sorveglianza sullo svolgimento della valutazione di impatto, la funzione di punto di contatto per gli interessati e per il Garante per ogni questione attinente l'applicazione del Regolamento.

Come impatta il GDPR sull'attività dell'Ateneo?

Obiettivamente la maggior parte delle modifiche richieste dal regolamento possono e devono trovare risposta nella modifica dei processi gestiti dall'amministrazione dell'Ateneo. Alcuni tra questi riguardano infatti delle azioni e delle attività la cui responsabilità ultima è posta proprio in capo all'Ateneo nel suo complesso, quali ad esempio le modifiche regolamentarie, la progettazione e l'attuazione di politiche in materia di protezione dati, la formazione del personale, la tenuta del registro dei trattamenti, l'adozione di misure sanzionatorie e correttive di comportamenti non conformi alle previsioni del GDPR. Altre riguardano l'adozione di misure tecniche ed informatiche, che pure sono generalmente supervisionate a livello centrale. Al tempo stesso, alcuni cambiamenti devono essere implementati anche a livello di dipartimenti e di strutture periferiche: ciò al fine di garantire che tutti i processi posti in essere siano in linea con la nuova normativa.

Quali sono i tempi di adeguamento dell'Ateneo alle previsioni del GDPR?

Come segnalato in precedenza, il regolamento europeo è stato approvato il 27 aprile 2016 ed è entrato in vigore il 25 maggio 2018, quindi l'Ateneo ha avuto due anni di tempo per provvedere all'adeguamento. Come per la maggior parte delle amministrazioni pubbliche e delle imprese italiane, ciò non è accaduto anche perché, ed è opportuno precisare questo passaggio, il Garante italiano non ha fornito tempestivamente indicazioni in materia. Basti pensare che il primo ed unico incontro con le Università è avvenuto in data 6 aprile 2018, a poco più di un mese dall'entrata in vigore del regolamento e che l'unico incontro dedicato alla nuova figura del Responsabile della Protezione Dati personali si è tenuto in data 25 maggio 2018.

Il piano di adeguamento

Il presente documento è stato realizzato dal Responsabile della Protezione Dati personali con lo scopo di indicare un percorso funzionale al progressivo adeguamento dell'Ateneo alle previsioni della normativa entrata in vigore in data 25 maggio 2018. Sono stati individuati una serie di interventi volti in parte ad innovare, in parte a verificare il funzionamento del sistema di protezione dei dati personali. Il piano coinvolge tutti i dipendenti dell'Ateneo e prevede, in particolare, l'assegnazione di un ruolo attivo in capo ai responsabili di dipartimento, di area e di ufficio. Un compito centrale sarà assegnato ad un gruppo di lavoro a composizione mista con la collaborazione dei Referenti privacy, ossia quello relativo alla stesura, analisi e armonizzazione di tutta la documentazione necessaria ai fini della conformità con le previsioni del regolamento. Inoltre lo stesso gruppo dovrà curare il monitoraggio delle attività sia in relazione all'effettivo svolgimento delle stesse, sia ai tempi di esecuzione.

Tempi di adeguamento

Ragionevolmente, sembra opportuno ipotizzare che il processo di adeguamento dell'Ateneo possa avere luogo nell'arco di 12/14 mesi. L'indicazione temporale in questione non è casuale, ma basata su precedenti relativi ad altre Università europee. Nel corso degli eventuali controlli, il Garante terrà conto dell'adeguamento in corso, a patto naturalmente che si possa dimostrare l'impegno in questa direzione.

Chi curerà l'attuazione del piano

Tanto l'azione propulsiva, quanto quella di riferimento, sono poste in capo al vertice amministrativo, al gruppo di lavoro e al Responsabile per la Protezione dei Dati personali. Tutto il personale docente, ricercatore e tecnico-amministrativo è tenuto allo svolgimento delle attività assegnate in base al presente piano di adeguamento.

Chi vigilerà sull'adeguamento dell'Ateneo alle previsioni del GDPR?

Il titolare del trattamento è tenuto ad adeguarsi al regolamento europeo, quindi tanto il vertice politico, quanto quello amministrativo sono tenuti al controllo in prima persona. L'azione di monitoraggio è inoltre affidata al gruppo di lavoro, il quale potrà, in forma collegiale o nella persona dei singoli componenti, effettuare verifiche in merito allo svolgimento delle attività. In posizione diversa, il Responsabile della Protezione Dati personali, in quanto punto di contatto tra Garante e Ateneo, sarà anch'egli tenuto a vigilare e a segnalare non solo ai vertici dell'Ateneo, ma anche al Garante per la privacy, eventuali criticità.

Organigramma e Struttura privacy in Ateneo

La normativa privacy prevede l'individuazione e la definizione dei soggetti protagonisti del trattamento dei dati personali, appare opportuno chiarire quali sono i ruoli e le responsabilità delle persone fisiche che operano nell'organizzazione di enti privati o pubblici. Oltre le figure individuate nell'organigramma privacy

approvato dall'Ateneo, vi sono altri due elementi da considerare per la verifica della compliance al Regolamento e, vista la struttura organizzativa di Ateneo costituita da Dipartimenti e Amministrazione centrale, saranno:

1) Gruppo di lavoro privacy
   Il gruppo è costituito dai Direttori dei dipartimenti, dal Direttore generale, dai dirigenti, dai coordinatori di area o loro delegati.
   Il compito centrale sarà quello relativo alla stesura, analisi ed armonizzazione di tutta la documentazione necessaria ai fini della conformità con le previsioni del Regolamento, dovrà curare il monitoraggio delle attività sia in relazione all'effettivo svolgimento delle stesse, sia ai tempi di esecuzione
   Il gruppo di lavoro privacy concorre all'individuazione dei trattamenti svolti nella struttura di appartenenza, all'analisi del rischio e alla relativa misurazione, all'attuazione delle adeguate misure di sicurezza, alla valutazione d'impatto se necessaria, alla progettazione del trattamento, al riesame del trattamento e delle misure di tutela.
2) Referenti privacy
   I referenti privacy, designati dai Direttori dei dipartimenti e dal Direttore generale, saranno chiamati al controllo e verifica del rispetto degli adempimenti privacy nel proprio Dipartimento, saranno supporto e punto di unione tra i dipendenti ed il DPO per tutte azioni richieste dalla normativa.

Azioni di adeguamento

Di seguito il piano di adeguamento, articolato in fasi, con l'indicazione dei soggetti deputati a porre in essere le singole azioni e i termini di completamento. Ciascuno dei soggetti sarà coinvolto a riesaminare il lavoro nella seguente tabella indicando se l'attività è ancora in corso o se è conclusa. Le azioni previste dovranno essere riesaminate almeno con cadenza annuale.

Legenda "Tempi di completamento": DI= Data inizio; CON= Data conclusione;

Legenda "Soggetti": TDT = Titolare; DPO= Responsabile protezione dati; GLP= Gruppo di lavoro privacy; RP= Referenti privacy

Fase	Intervento da effettuare	Soggetto/i deputato/i	Tempi di completamento	Completato
0.1	Nomina del Responsabile della Protezione dei Dati personali	TDT	DI: 21/12/2018 CON:	
0.2	Redazione del registro dei trattamenti per macrotrattamenti	TDT; DPO; RP	DI: 20/07/2018 CON:	
0.3	Redazione del documento per la segnalazione delle violazioni dei dati personali (data breach)	DPO	DI: 30/07/2019 CON:	

0.4	Ricognizione sui trattamenti svolti da soggetti esterni (ex Art. 28)	GLP; RP	DI: CON:	
0.5	Predisposizione piano di adeguamento alle previsioni del Regolamento UE 2016/679 – Regolamento Generale sulla Protezione dei dati del Parlamento europeo e del Consiglio del 27 aprile 2016	DPO	DI: 30/06/2020 CON:	
1.1	Nomina del gruppo di lavoro	TDT	DI: 10/02/2020 CON:	
1.2	Predisposizione elenco dei trattamenti posti in essere da ciascuna struttura di Ateneo	GLP; RP	DI: CON:	
1.3	Predisposizione scheda del trattamento	GLP; RP; DPO	DI: CON:	
1.4	Predisposizione elenco delle informative in uso presso ciascuna struttura di Ateneo	GLP; RP	DI: CON:	
2.1	Analisi e valutazione della documentazione prodotta da ciascuna struttura di Ateneo	GLP; DPO	DI: CON:	
2.2	Valutazione di impatto protezione dati (DPIA) per ciascun trattamento	GLP; RP	DI: CON:	
2.3	Aggiornamento del registro dei trattamenti	RP; DPO	DI: CON:	
2.4	Redazione delle nuove informative e/o modifica di quelle in uso presso ciascuna struttura di Ateneo in base a modello predefinito	GLP; RP	DI: CON:	
2.5	Stesura informative generali di Ateneo	GLP; RP	DI: CON:	
2.6	Predisposizione delle linee di condotta per il trattamento dei dati personali	GLP	DI: CON:	
3.1	Controllo delle informative	GLP; RP; DPO	DI: CON:	
3.2	Cancellazione di tutte le informative basate sulla precedente normativa	GLP; RP	DI: CON:	
3.3	Cancellazione delle informative non necessarie	GLP; RP	DI: CON:	
4.1	Verifica e modifica dei moduli di immatricolazione ed iscrizione ad anni successivi	GLP; RP	DI: CON:	
4.2	Verifica e modifica dei moduli relativi ad attività connesse al percorso formativo di studenti, dottorandi, specializzandi	GLP; RP	DI: CON:	

4.3	Verifica e modifica dei meccanismi di acquisizione del consenso al trattamento dei dati personali	GLP; RP	DI: CON:	
4.4	Verifica della base giuridica dell'invio di comunicazioni a potenziali futuri studenti, futuri studenti, studenti, dottorandi, specializzandi	GLP; RP	DI: CON:	
5.1	Verifica della base giuridica dell'invio di comunicazioni a laureati, ex studenti, partecipanti ad iniziative di Ateneo	GLP; RP	DI: CON:	
5.2	Verifica della concessione del consenso per le azioni di job-placement rivolte ai laureati	GLP; RP	DI: CON:	
5.3	Verifica e modifica dei moduli di partecipazione ad iniziative promosse dall'Ateneo	GLP; RP	DI: CON:	
6.1	Verifica e modifica dei moduli per la partecipazione a concorsi e selezioni finalizzati all'assunzione	GLP; RP	DI: CON:	
6.2	Verifica e modifica dei moduli relativi ad attività connesse al rapporto di lavoro o di collaborazione	GLP; RP	DI: CON:	
7.1	Predisposizione e adozione di linee guida per le attività di ricerca che prevedono il trattamento di dati personali	GLP	DI: CON:	
7.2	Predisposizione e adozione della scheda di progetto finalizzata all'analisi di impatto sulla protezione dati personali	GLP; RP	DI: CON:	
8.1	Individuazione dei ruoli e delle responsabilità ai sensi del GDPR	GLP; RP; DPO	DI: CON:	
8.1.a	Predisposizione moduli dell'obbligo di riservatezza	GLP; DPO	DI: CONC:	
8.1.aa	Verifica della sottoscrizione dell'obbligo di riservatezza	GLP; RF; DPO	DI: CONC:	
8.2.b	Predisposizione del piano di formazione per il personale di Ateneo	GLP; RP; DPO	DI: CON:	
8.2.c	Attuazione del piano di formazione per il personale di Ateneo	GLP; RP; DPO	DI: CON:	
8.3	Revisione del regolamento sulla protezione dati di Ateneo alla luce delle previsioni del GDPR	DPO	DI: CON:	
8.4	Verifica e modifica delle procedure di gestione e conservazione documentale	GLP; Responsabile della Gestione Documentale, Responsabile della Conservazione; DPO	DI: CON:	

8.5	Verifica e modifica delle procedure di trasmissione / trasferimento dei dati personali	GLP; RP	DI: CON:	
8.6	Verifica e modifica dei contratti in essere con fornitori che trattano dati in nome e per conto dell'Ateneo, ai fini della loro nomina quali responsabili del trattamento ai sensi del GDPR (ex. Art. 28)	GLP; RP	DI: CON:	
8.7	Introduzione, in sede di emanazione di bando di gara e/o di stipula di contratto, delle clausole di coerenza con le previsioni del GDPR per tutti i sistemi da acquisire in futuro	GLP; RP	DI: CON:	
9.1	Verifica e modifica dell'informativa sulla protezione dei dati personali presente sul sito internet di Ateneo	Responsabile del sito internet di Ateneo, responsabili siti internet singole strutture	DI: CON:	
9.2	Verifica e modifica il sito internet per renderlo conforme alle previsioni del GDPR	Responsabile del sito internet di Ateneo, responsabili siti internet singole strutture	DI: CON:	
9.3	Notifica agli interessati in merito alla pubblicazione di profili contenenti dati personali sul sito internet di Ateneo	Responsabile del sito internet di Ateneo, responsabili siti internet singole strutture	DI: CON:	
9.4	Verifica e modifica degli applicativi prodotti e utilizzati dall'Ateneo per renderli conformi alle previsioni del GDPR o dismetterli	Responsabile dell'area informatica di riferimento	DI: CON:	
9.5	Verifica e richiesta di modifica degli applicativi prodotti da terzi e utilizzati dall'Ateneo per renderli conformi alle previsioni del GDPR o dismetterli	Responsabile dell'area informatica di riferimento	DI: CON:	
9.6	Verifica delle capacità di risposta rispetto alle richieste di accesso ai dati presenti all'interno dei server e dei database di Ateneo	Responsabile dell'area informatica di riferimento	DI: CON:	
9.7	Verifica delle capacità di dare seguito alle richieste di esercizio dei propri diritti (rettifica, limitazione, cancellazione, portabilità, opposizione) da parte degli interessati	Responsabile dell'area informatica di riferimento	DI: CON:	
9.8	Verifica delle misure tecnologiche e informatiche di sicurezza di Ateneo	Responsabile dell'area informatica di riferimento	DI: CON:	
9.9	Verifica delle misure di sicurezza della strumentazione informatica messa a disposizione dei dipendenti e degli utenti	Responsabile dell'area informatica di riferimento	DI: CON:	
10.1	Monitoraggio sull'applicazione del piano di adeguamento	GLP; DPO	DI: CON:	
10.2	Monitoraggio del sistema di protezione dati personali	DPO	DI: CON:	

1 Predisposizione della documentazione e nomina gruppo di lavoro		
1.1	Nomina gruppo di lavoro **Chi: Direttore generale, Direttori dei Dipartimenti** Procede alla nomina di un gruppo di lavoro deputato al monitoraggio sull'applicazione del piano di adeguamento, alla valutazione della documentazione prodotta dalle singole strutture e alla stesura di quella di carattere generale. La composizione dove rispecchiare le diverse aree dell'Ateneo (personale docente e ricercatore, personale tecnico-amministrativo). È essenziale che vi faccia parte il Responsabile della Protezione Dati personali.	Per quanto il Responsabile della Protezione Dati personali sia una delle figure cardine nel sistema di protezione dei dati personali definito dal GDPR, questi è chiamato a svolgere mansioni di supporto e non può sostituirsi al titolare nell'esercizio delle sue funzioni. Tenuto conto della complessità organizzativa di un Ateneo è quindi opportuna la costituzione di un gruppo di lavoro cui siano demandate le attività di monitoraggio sull'effettiva applicazione del piano di adeguamento. Il gruppo deve svolgere quindi una funzione propulsiva e di controllo ed essere quindi dotato di poteri ispettivi. Deve altresì occuparsi delle attività di stesura, analisi e revisione della documentazione per la protezione dei dati personali (principalmente le schede di trattamento, le informative sulla privacy, le linee di condotta in materia di trattamento dati personali, le linee guida per le attività di ricerca che necessitano di azioni quali raccolta e analisi di dati personali). Il gruppo di lavoro potrebbe essere infine la sede migliore per la modifica e l'integrazione del presente piano di lavoro. La composizione del gruppo deve tenere conto delle diverse aree di competenze presenti nell'Ateneo e dovrebbe vedere coinvolto anche il personale docente relativamente ai trattamenti effettuati per la didattica e la ricerca.

1.2	Predisposizione elenco dei trattamenti posti in essere da ciascuna struttura di Ateneo **Chi: Responsabile di Dipartimento, Area, Ufficio** Redige un elenco dei trattamenti effettuati nella struttura, ponendo particolare attenzione al fatto che ciascun trattamento deve essere identificato in base alla finalità perseguita.	Un buon sistema di protezione dei dati personali presuppone innanzi tutto la conoscenza dei trattamenti effettuati. È essenziale quindi procedere alla redazione di un loro elenco il più possibile esaustivo che superi l'approccio per macrocategorie, precedentemente individuato per far fronte a tempistiche stringenti. Un errore piuttosto comune è quello di identificare il trattamento con lo strumento informatico utilizzato per la gestione dei dati o con il singolo procedimento svolto dalla struttura. Un simile approccio non è corretto perché un singolo software può essere utilizzato per più trattamenti, mentre una singola attività può costituire solo una parte di un trattamento. L'elemento qualificante è costituito dalla determinazione della finalità, ossia dalla risposta alla domanda "perché raccolgo i tuoi dati personali?". Per lo svolgimento di questo intervento si può certamente prendere spunto dalle linee guida elaborate dal CODAU, sebbene si tratti di un documento che risente di un certo grado di genericità e che risulta incompleto rispetto ai contenuti minimi pervisti dal GDPR per ciascuna scheda. Il suggerimento è quindi quello di considerarlo come un quadro di riferimento, all'interno del quale però vanno individuati con maggior precisione i singoli trattamenti svolti.
1.3	Predisposizione scheda del trattamento **Chi: Responsabile di Dipartimento, Area, Ufficio** Redige, per ciascun trattamento individuato, la relativa scheda in base al modello ad uopo predisposto. Adotta scrupolosamente la terminologia indicata all'interno dello stesso. È possibile che uno o più trattamenti effettuati dalla struttura sia in comune con altre strutture. In questo caso è opportuno redigere la scheda in maniera congiunta. Nel caso di dubbi di natura interpretativa, consultare il Responsabile della Protezione Dati personali.	Definito l'elenco dei trattamenti, sarà possibile procedere alla compilazione della scheda in base al modello che sarà fornito dal Responsabile della Protezione Dati personali. L'Ateneo è dotato di un gestionale per la tenuta del registro dei trattamenti, la singola scheda sarà compilabile direttamente attraverso apposito portale. Diversamente, il modello potrebbe tranquillamente essere predisposto attraverso documento di testo oppure foglio di calcolo. Nella compilazione è opportuno attenersi ad una terminologia comune, in particolare laddove si vadano a descrivere categorie di interessati, modalità di trattamento, tipologie di trattamenti. In ogni caso, tutti i testi dovranno essere facilmente comprensibili evitando, ove possibile, l'uso di tecnicismi, la ridondanza delle parole, le abbreviazioni non autorizzate dall'Ateneo. Nota a margine: la descrizione dovrà essere veritiera e potrà costituire il primo elemento di riflessione per interventi di messa in sicurezza o di miglioramento nel trattamento dati personali.

1.4	Predisposizione elenco delle informative in uso presso ciascuna struttura di Ateneo **Chi: Responsabile di Dipartimento, Area, Ufficio** Redige un elenco delle informative sul trattamento dei dati personali che la struttura fornisce ai soggetti interessati. Si tenga conto che è del tutto normale che una singola informativa possa fare riferimento a più trattamenti, specie se questi ultimi risultano connessi tra loro. Associa ciascuna informativa esistente al relativo trattamento.	Aspetto essenziale del GDPR è costituito dall'informativa da sottoporre agli interessati prima di iniziare le attività di trattamento (artt. 13-21). Benché, in astratto, sarebbe necessario produrre un'informativa per ogni singolo trattamento, non si può negare come, molto spesso, più trattamenti si basino sui medesimi dati raccolti e siano funzionali al perseguimento di finalità simili, analoghe o comunque connesse tra loro ed ascrivibili a finalità più generiche (es. il trattamento per l'iscrizione ad anno successivo è parte del trattamento per la gestione delle carriere studenti). A tal proposito il regolamento europeo autorizza alla redazione di un'informativa generale che riguardi più trattamenti, a patto che le informazioni trasmesse siano chiare e il più possibile complete. In un siffatto contesto, è possibile che la medesima informativa possa riguardare trattamenti effettuati strutture diverse. Nella redazione dell'elenco, sarebbe opportuno inserire un richiamo in tal senso sotto forma di "nota bene".

2 Revisione della documentazione, adozione di politiche di sicurezza e analisi dei rischi		
2.1	Analisi e valutazione della documentazione prodotta da ciascuna struttura di Ateneo **Chi: Gruppo di lavoro** Procede alla valutazione della documentazione prodotta da ciascuna struttura, con particolare riferimento alla coerenza delle schede di trattamento e delle informative con le previsioni del GDPR. Verifica altresì per quali trattamenti sussistano le condizioni per una valutazione di impatto protezione dati (DPIA).	Analisi e valutazione della documentazione prodotta devono tener conto: - della completezza delle descrizioni effettuate; - ove possibile, della rispondenza tra le attività di ufficio e i trattamenti effettuati - del grado di dettaglio con il quale le strutture hanno identificato i trattamenti di propria competenza. È opportuno che terminologia e livello di dettaglio nella descrizione siano armonizzati, onde evitare differenze eccessive tra un trattamento e l'altro. Con riferimento alla valutazione di impatto sulla protezione dati, essa si rende obbligatoria quando un tipo di trattamento prevede l'uso di nuove tecnologie e può, considerati la natura, l'oggetto, i contesto e le finalità del trattamento, presentare un rischio elevato per i diritti degli interessati.
2.2	Valutazione di impatto protezione dati (DPIA) per ciascun trattamento **Chi: Gruppo di lavoro** Laddove dall'analisi delle schede di trattamento sia emersa la necessità di una di una valutazione di impatto sulla protezione dati, procede in questa direzione.	La valutazione di impatto sulla protezione dati deve contenere almeno: - una descrizione sistematica del trattamento previsto e delle finalità che, tramite esso, si intendono perseguire - una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità - una valutazione dei rischi per i diritti e le libertà degli interessati - le misure previste per affrontare i rischi così individuati, con particolare riferimento alle misure di sicurezza atte a garantire la protezione dei dati personali In presenza di trattamenti che presentano caratteristiche simili e rischi analoghi, è possibile effettuare una singola valutazione, evitando così la proliferazione di documenti.
2.3	Aggiornamento del registro dei trattamenti **Chi: Responsabile della Protezione Dati personali** In qualità di Responsabile della Protezione Dati personali, può essere affidato anche il compito di provvedere alla tenuta del registro dei trattamenti. Una volta che le schede dei trattamenti risultano validate dal gruppo di lavoro procede al loro inserimento all'interno del registro dei trattamenti sostituendo le eventuali schede precedenti.	È opportuno che la tenuta del registro dei trattamenti sia affidata al Responsabile della Protezione Dati personali. Infatti, nelle sue attività di audit, egli sarà chiamato a verificare, tra le altre cose, anche la rispondenza tra quanto indicato nelle schede di trattamento e i trattamenti effettivamente posti in essere. Inoltre egli avrà necessità di accedervi in presenza di richieste degli interessati o del Garante.

2.4	Redazione delle nuove informative e/o modifica di quelle in uso presso ciascuna struttura di Ateneo in base a modello predefinito **Chi: Responsabile di Dipartimento, Area, Ufficio** Laddove dall'analisi del gruppo di lavoro dovessero emergere omissioni, lacune o criticità, lo stesso ne darà tempestivamente notizia alle strutture interessate. Qualora si riceve una comunicazione in tal senso, deve provvedere quanto prima ad apportare le modifiche richieste. Nel caso di dubbi o di richieste inapplicabili, consulta il Responsabile per la Protezione Dati personali.	A seguito della valutazione effettuata dal gruppo di lavoro, è possibile che si rendano necessarie delle modifiche di rilievo nella documentazione per la protezione dei dati personali. In questo caso è opportuno che tali modifiche siano effettuate direttamente dagli uffici interessati, in quanto è assai probabile che esse andranno ad impattare sulle modalità di svolgimento dei trattamenti. Oltretutto è altresì possibile che suggerimenti e richieste di modifica non siano in realtà adottabili in quanto incompatibili con l'attività di ufficio, fatto questo che rende ancor più necessario che ad effettuare materialmente gli interventi siano le strutture direttamente coinvolte.
2.5	Stesura informative generali di Ateneo **Chi: Gruppo di lavoro** Il gruppo, partendo dalle informative prodotte dalle singole strutture, provvederà alla stesura di informative generali che saranno pubblicate sul sito internet di Ateneo e che fungeranno da riferimento per tutte le attività di trattamento poste in essere.	Normalmente le informative devono essere rese prima della raccolta dei dati personali presso gli interessati. Accade però che, una volta rese, il singolo interessato perda contezza di tutte o di parte delle informazioni ricevute. Onde evitare di dover evadere richieste continue e anche in ragione degli obblighi di trasparenza, è necessario procedere alla pubblicazione delle informative sul sito internet di Ateneo. Tenendo conto che è consentito redigere informative relative a più trattamenti, è opportuno provvedere alla stesura di informative generali riferite alle categorie di interessati con cui l'Ateneo interagisce: futuri studenti, studenti, laureati, personale, fornitori.
2.6	Predisposizione delle linee di condotta per il trattamento dei dati personali **Chi: Gruppo di lavoro** Procede alla stesura delle linee di condotta cui tutti i dipendenti dovranno attenersi nelle attività di trattamento dei dati personali.	L'adozione di linee di condotta per il trattamento dei dati personali può rivelarsi particolarmente utile ai fini dell'adeguamento dell'Ateneo alle previsioni del GDPR. Al di là della conoscenza della normativa, che pure costituisce un aspetto qualificante, ciò che rileva ai fini della tutela dei dati personali è il modo in cui essi vengono trattati. Diventa fattore essenziale comprendere quali siano le condizioni di liceità, le tipologie e le modalità di trattamento consentite. Bisogna inoltre considerare che, nella maggior parte dei casi, gli accessi non autorizzati derivano da errori umani che rendono inefficaci le misure di sicurezza adottate. Di conseguenza, una particolare attenzione va posta all'introduzione di comportamenti che non espongano queste ultime al rischio di violazione. Una volta prodotto, il documento in questione deve essere inviato a tutti i dipendenti, i quali dovranno conformare ad esso i propri comportamenti. È opportuno, anche nell'ottica di dimostrare l'impegno dell'Ateneo nella tutela della privacy, che il medesimo sia pubblicato sul sito internet in apposita sezione.

3 Informative sulla protezione dati personali (informative privacy)		
3.1	Controllo delle informative **Chi: Responsabile di Dipartimento, Area, Ufficio** Verifica che le informative generali sul trattamento dei dati personali, fornite dall'Università ai diversi interessati, siano coerenti con l'attività che la struttura svolge con tali dati. Qualora si dovesse appurare che la struttura utilizzi i suddetti dati con altre modalità e/o per altre finalità, consulta il Responsabile della Protezione Dati personali. Rammenta infine che la mancata messa a disposizione di una corretta informativa costituisce violazione sanzionabile ai sensi del GDPR.	Ai sensi del GDPR, dobbiamo fornire alle persone informazioni dettagliate circa le modalità con cui tratteremo i loro dati personali. Le informative generali sul trattamento dei dati personali dell'Ateneo saranno complete e assicureranno la copertura di tutte le attività poste in essere dalle singole strutture. Queste ultime non potranno utilizzare i dati in modi diversi da quelli previsti da tali informative. Qualora vi fossero altri utilizzi o si perseguissero altre finalità, sarà necessario concordare con il Responsabile della Protezione Dati personali la stesura di un'informativa ad hoc oppure di un avviso integrativo.
3.2	Cancellazione di tutte le informative basate sulla precedente normativa **Chi: Responsabile di Dipartimento, Area, Ufficio** Se ancora si utilizzano informative basate sulla precedente normativa sulla protezione dei dati personali, si procede alla loro cancellazione o sostituzione con l'eventuale collegamento esistente con uno che indirizzi alle informative generali che saranno pubblicate sul sito internet di Ateneo. La mancata messa a disposizione di una corretta informativa costituisce violazione sanzionabile ai sensi del GDPR.	Benché buona parte delle previsioni del GDPR fossero già presenti nella precedente versione del Codice Privacy, l'aggiornamento delle informative passa dalla cancellazione di tutta la documentazione pregressa. Ciò al fine di evitare che, anche solo per mero errore materiale, siano fornite informative non conformi al Regolamento europeo.
3.3	Cancellazione delle informative non necessarie **Chi: Responsabile di Dipartimento, Area, Ufficio** Se ancora si utilizzano informative relative a trattamenti per i quali sono già disponibili informative generali di Ateneo, si procede alla loro cancellazione o sostituisci l'eventuale collegamento esistente con uno che indirizzi a queste ultime. La mancata messa a disposizione di una corretta informativa costituisce violazione sanzionabile ai sensi del GDPR.	Laddove già esistano informative generali di Ateneo, non è opportuno che i dipartimenti, le aree o gli uffici ne forniscano di proprie. In linea di massima queste ultime informative devono essere cancellate. Qualora lo si ritenga necessario, è possibile integrare le informative generali di Ateneo con avvisi speciali. Tale istruzione non si applica nell'ipotesi in cui i dipartimenti, le aree o gli uffici siano responsabili in via esclusiva di specifici trattamenti (qualora cioè l'Ateneo non abbia alcun ruolo nelle attività di trattamento). In tal caso è necessario concordare con il Responsabile della Protezione Dati personali la stesura di un'informativa ad hoc.

4 Futuri studenti, studenti, dottorandi e specializzandi		
4.1	Verifica e modifica dei moduli di immatricolazione ed iscrizione ad anni successivi **Chi: Responsabile di Dipartimento, Area, Ufficio** Assicurarsi che i moduli di immatricolazione ed iscrizione ad anno successivo contemplino o contengano un collegamento all'informativa per l'immatricolazione, l'iscrizione ad anno successivo, la gestione delle carriere. Se così non è, si interviene direttamente modificando gli eventuali moduli cartacei, nel caso di moduli on-line contatta l'ufficio informatico competente e, ove necessario, chiedi il supporto del Responsabile della Protezione Dati personali.	L'informativa generale di Ateneo contempla tutte le ipotesi di trattamento finalizzate alla gestione delle carriere degli studenti dall'immatricolazione alla conclusione del percorso formativo scelto. Base giuridica della liceità dei trattamenti è costituita dall'interesse pubblico perseguito dall'Ateneo. Base giuridica del trattamento dei dati particolari (c.d. sensibili) è invece costituita dal rilevante interesse pubblico perseguito dall'Ateneo nel trattare tali informazioni (ad esempio per la conessione di esoneri o benefici per particolari condizioni di salute). È indispensabile che gli studenti prendano visione dell'informativa, pertanto tutti i moduli di immatricolazione e iscrizione ad anni successivi devono contemplarne il testo o rinviare al collegamento presente sul sito internet di Ateneo. A tal proposito, potrebbe essere opportuno inviare una comunicazione a tutti gli indirizzi di posta elettronica istituzionale assegnati agli studenti.
4.2	Verifica e modifica dei moduli relativi ad attività connesse al percorso formativo di studenti, dottorandi, specializzandi **Chi: Responsabile di Dipartimento, Area, Ufficio** Qualora un trattamento riguardi attività connesse, ma che non sono espressamente parte, del percorso formativo di studenti, dottorandi, specializzandi, assicurati che i moduli utilizzati contemplino o contengano un collegamento alla specifica informativa. Se così non è, intervieni direttamente modificando gli eventuali moduli cartacei, nel caso di moduli on-line contatta l'ufficio informatico competente e, ove necessario, chiedi il supporto del Responsabile della Protezione Dati personali.	Qualora un trattamento dati non sia previsto nell'ambito dell'informativa generale, sono prodotte delle informative specifiche che presentano le medesime caratteristiche di quelle principali. È indispensabile che gli studenti ne prendano visione, pertanto tutti i relativi moduli devono contemplarne il testo o rinviare al collegamento presente sul sito Internet di Ateneo.

4.3	Verifica e modifica dei meccanismi di acquisizione del consenso al trattamento dei dati personali **Chi: Responsabile di Dipartimento, Area, Ufficio** Se sino ad oggi hai ritenuto che la base giuridica di un trattamento dati posto in essere dalla tua struttura sia il consenso, verifica innanzi tutto che effettivamente tu abbia bisogno di acquisirlo. Se è davvero così, assicurati che si tratti di una scelta libera da parte dello studente, che questi non debba rimuovere spunte preinserite e che la sua decisione sia registrata. Considera inoltre che, il mancato rilascio del consenso, non deve arrecare pregiudizio alcuno allo studente. Se anche solo una delle predette condizioni non si verifica, ciò significa che non puoi adoperare il consenso quale base giuridica del trattamento e devi individuarne una diversa tra quelle previste dal GDPR. In caso di dubbi, contatta il Responsabile della Protezione Dati personali.	Il consenso è una delle possibili basi giuridiche per il trattamento dei dati personali. Ai sensi del regolamento esso deve essere libero, specifico, informato, inequivocabile, dimostrabile e revocabile. In altre parole l'interessato deve essere nella posizione di poter scegliere in maniera totalmente autonoma e di non subire pregiudizio dal suo mancato rilascio. È però evidente che, in molti casi, la mancata autorizzazione al trattamento dei propri dati impedisca materialmente la possibilità di acquisizione un bene o di fruizione di un servizio. In tali situazioni, non è possibile utilizzare il consenso quale base giuridica. Diviene quindi necessario individuare, all'interno dell'elenco tassativo previsto dal legislatore europeo, quali siano le condizioni atte a garantire la liceità del trattamento posto in essere. Effetto di tale considerazione è anche quello di sfatare un mito: quello in base al quale, laddove un titolare non sia in grado di individuare correttamente una base giuridica del trattamento, sia meglio, nel dubbio, richiedere il consenso. Quale suggerimento, è opportuno tener presente che, nella maggior parte dei casi, un'autorità pubblica, nell'esercizio delle sue funzioni istituzionali, effettua trattamento dati in base ad obblighi di legge ed in virtù dell'interesse pubblico perseguito. Quest'ultima voce in particolare è base giuridica del trattamento dei dati personali degli studenti in relazione alla loro carriera. Alla luce di tutto ciò, i moduli di richiesta del consenso possono essere utilizzati solo ed esclusivamente per quei trattamenti che non rientrano nelle finalità istituzionali dell'Ateneo o che sono da considerarsi complementari o sussidiari alle stesse.

4.4	Verifica della base giuridica dell'invio di comunicazioni a potenziali futuri studenti, futuri studenti, studenti, dottorandi, specializzandi **Chi: Responsabile di Dipartimento, Area, Ufficio** Se invii comunicazioni che non siano strettamente connesse alla carriera dello studente, dottorando o specializzando, o che non siano riferibili allo svolgimento e ai risultati di test di orientamento, di ammissione o di ingresso, assicurati che gli interessati abbiano effettivamente rilasciato il loro consenso. Nel caso poi si tratti di minori di 16 anni, assicurati che il consenso sia stato prestato dai genitori. In assenza del consenso esplicito a tale trattamento, non puoi inviare alcuna comunicazione che non sia strettamente connessa alla carriera dell'interessato. Per il futuro, ove necessario, modifica o chiedi che siano modificati i moduli di acquisizione dei dati personali affinché sia possibile raccogliere l'eventuale consenso a tali trattamenti. In caso di dubbi, contatta il Responsabile della Protezione Dati personali.	Il GDPR considera lecito il trattamento dei dati personali solo e nella misura in cui ricorrano determinate condizioni (artt. 5-11). In particolare un trattamento è lecito se ha come base giuridica una condizione tra consenso, obbligo contrattuale, obbligo legale, presenza di un interesse pubblico, legittimo interesse del titolare ove non prevalgano diritti o interessi dell'interessato. Alla luce di tutto questo l'invio di comunicazioni attinenti ai risultati di test di orientamento, di ammissione o di ingresso, è lecito nella misura in cui sia stata messa a disposizione dell'interessato una specifica informativa. Allo stesso modo l'invio di comunicazioni attinenti la carriera dello studente è lecito in virtù della messa a disposizione dell'informativa generale per gli studenti. Diversamente, il fatto che l'Ateneo conservi ad esempio gli indirizzi di posta elettronica di potenziali futuri studenti, futuri studenti, studenti, dottorandi e specializzandi, non costituisce automaticamente autorizzazione all'invio di mail non richieste. Ciò perché, è bene ricordare, ciascun trattamento è identificato in base alla finalità perseguita: se quindi si raccolgono dati di contatto per la partecipazione al test di ingresso per un determinato corso di studi (finalità specifica), ciò non implica che sia possibile utilizzarli anche per pubblicizzare altri corsi di studio o, in generale, altre attività dell'Ateneo. A maggior ragione ciò non autorizza all'invio di comunicazioni inerenti iniziative di terzi. Per maggiore chiarezza: l'invio di comunicazioni (e-mail, messaggi, etc.) relativi alla promozione di corsi di studio, master, corsi formazione, altre attività o eventi, si configura come azione di marketing diretto da parte dell'Ateneo e presuppone l'acquisizione del consenso al trattamento da parte degli interessati o dei loro genitori, laddove si tratti di interessati minori di 16 anni. È necessario acquisire un ulteriore consenso, distinto dal precedente, per l'invio comunicazioni relative ad attività di soggetti terzi (es. altri Atenei). Per l'invio di comunicazioni di questo genere, è quindi essenziale effettuare preventivamente una verifica sui consensi rilasciati dagli interessati. Ove il consenso sia stato rilasciato è possibile inviare la comunicazione, mentre ove esso sia stato negato o revocato o nelle situazioni dubbie, non è possibile procedere all'invio.

5 Laureati, ex studenti, partecipanti ad iniziative di Ateneo		
5.1	Verifica della base giuridica dell'invio di comunicazioni a laureati, ex studenti, partecipanti ad iniziative di Ateneo **Chi: Responsabile di Dipartimento, Area, Ufficio** Se invii comunicazioni a laureati, ex studenti, partecipanti a precedenti iniziative svolte dal nostro Ateneo, che non siano strettamente connesse al percorso di studi o all'attività cui si è preso parte, assicurati che gli interessati abbiano effettivamente rilasciato il loro consenso. Per il futuro, ove necessario, modifica o chiedi che siano modificati i moduli di acquisizione dei dati personali affinché sia possibile raccogliere l'eventuale consenso a tali trattamenti.	Il laureato, ancorché nel nostro Ateneo, l'ex studente o il partecipante a precedenti iniziative svolte dall'Ateneo non ha con noi alcun rapporto in essere che giustifichi l'invio di comunicazioni istituzionali. Pertanto, in assenza del consenso esplicito, noi non siamo autorizzati a farlo, indipendentemente se si tratti di iniziative promosse dall'Ateneo o da terzi. Possiamo invece inviare comunicazioni relative alla carriera conclusa o all'attività cui si è preso parte (ad esempio per il ritiro del diploma o dell'attestato di partecipazione). Ciò perché, in quest'ultimo caso, possiamo individuare quale base giuridica del trattamento la presenza di un rilevante interesse pubblico da tutelare. *Vedi 4.3 per ulteriori chiarimenti*
5.2	Verifica della concessione del consenso per le azioni di job-placement rivolte ai laureati **Chi: Responsabile di Dipartimento, Area, Ufficio** Se invii comunicazioni a laureati concernenti opportunità di lavoro, assicurati che gli interessati abbiano effettivamente rilasciato il loro consenso. Allo stesso modo se ti viene richiesto di segnalare uno o più potenziali candidati per posizioni lavorative, assicurati che sia stato rilasciato uno specifico consenso.	Sebbene il job-placement rappresenti oggi un'attività di primaria importanza per gli Atenei, essa non può essere considerata attività di interesse pubblico. In assenza di tale riconoscimento, non è possibile trattare i dati dei laureati per finalità connesse al job-placement in assenza del loro consenso. Peraltro, è opportuno distinguere il consenso alla ricezione di comunicazioni da parte dell'Ateneo dall'invio dei dati degli interessati ad enti ed aziende che ne facciano richiesta. È quindi essenziale che i consensi a tali trattamenti siano resi in maniera separata. *Vedi 4.3 per ulteriori chiarimenti*

5.3	Verifica e modifica dei moduli di partecipazione ad iniziative promosse dall'Ateneo **Chi: Responsabile di Dipartimento, Area, Ufficio** Assicurati che i moduli di partecipazione ad iniziative promosse dall'Ateneo contemplino o contengano un collegamento ad apposita informativa per il trattamento dei dati personali. Se ciò non si verifica, assicurati innanzi tutto dell'esistenza di una specifica informativa per l'attività in questione. Qualora l'informativa non sia stata prodotta, provvedi personalmente o chiedi che lo faccia il responsabile dell'attività. Prodotta o individuata l'informativa, intervieni modificando gli eventuali moduli cartacei, nel caso di moduli on-line contatta l'ufficio informatico competente e, ove necessario, chiedi il supporto del Responsabile della Protezione Dati personali.	L'informativa per la partecipazione ad una specifica iniziativa di Ateneo deve contemplare tutti gli elementi previsti dal GDPR e deve essere redatta in base al modulo standard ad uopo predisposto. Sarà necessario individuare la corretta base giuridica del trattamento che potrebbe variare a seconda della tipologia di attività svolta. È indispensabile che i partecipanti ad iniziative dell'Ateneo per le quali si procede alla raccolta di dati personali prendano visione dell'informativa, pertanto tutti i moduli di partecipazione devono contemplarne il testo o rinviare al relativo collegamento internet.

6 Concorsi, selezioni, gestione carriere di: personale docente, assegnisti di ricerca, collaboratori, personale tecnico amministrativo		
6.1	Verifica e modifica dei moduli per la partecipazione a concorsi e selezioni finalizzati all'assunzione **Chi: Responsabile di Dipartimento, Area, Ufficio** Assicurati che la modulistica impiegata allo scopo sia coerente con le informative rilasciate agli interessati al momento della compilazione. Verifica in particolare che, ove previsto, il modulo di consenso sia chiaro e non precompilato. Completata la revisione, cancella i precedenti moduli, onde evitare potenziali errori di pubblicazione. Ove dovessi avere dei dubbi, chiedi il supporto del Responsabile della Protezione Dati personali.	L'adeguamento della modulistica è essenziale perché permette di dimostrare innanzi tutto di aver preso atto della nuova normativa, poi di aver effettuato gli opportuni interventi per garantire la protezione dei dati personali degli interessati e infine di aver adempiuto agli obblighi di informazione.
6.2	Verifica e modifica dei moduli relativi ad attività connesse al rapporto di lavoro o di collaborazione **Chi: Responsabile di Dipartimento, Area, Ufficio** Assicurati che la modulistica impiegata allo scopo sia coerente con le informative rilasciate agli interessati al momento della compilazione. Verifica in particolare che, ove previsto, il modulo di consenso sia chiaro e non precompilato. Completata la revisione, cancella i precedenti moduli, onde evitare potenziali errori di pubblicazione. Ove dovessi avere dei dubbi, chiedi il supporto del Responsabile della Protezione Dati personali.	L'adeguamento della modulistica è essenziale perché permette di dimostrare innanzi tutto di aver preso atto della nuova normativa, poi di aver effettuato gli opportuni interventi per garantire la protezione dei dati personali degli interessati e infine di aver adempiuto agli obblighi di informazione.

7 Ricerca		
7.1	Predisposizione e adozione di linee guida per le attività di ricerca che prevedono il trattamento di dati personali **Chi: Gruppo di lavoro**	Il GDPR trova applicazione anche nel trattamento dei dati personali per scopi di ricerca scientifica, storica o a fini statistici. In particolare il rapporto tra GDPR e ricerca scientifica risulta essere uno degli aspetti più controversi della normativa europea, stante il rilievo costituzionale del rilevante interesse pubblico al suo svolgimento in maniera libera. È nei fatti necessario contemperare due distinte esigenze: da una parte la tutela dei dati personali dei soggetti i cui dati costituiscono base di partenza per l'attività di ricerca, dall'altra la possibilità di effettuare e portare a termine l'attività di ricerca. Allo scopo, il regolamento prevede l'adozione di garanzie adeguate per i diritti e le libertà degli interessati, con particolare riferimento a misure tecniche e organizzative finalizzate al rispetto del principio della minimizzazione dei dati e della pseudonimizzazione o anonimizzazione dei dati, a patto comunque che gli scopi in questione possano essere conseguiti in tal modo. Tutto il personale della ricerca avrà quindi bisogno di linee guida funzionali alla determinazione di quali aspetti del GDPR siano applicabili alla propria ricerca e dovranno impegnarsi al rispetto delle relative disposizioni.
7.2	Predisposizione e adozione della scheda di progetto finalizzata all'analisi di impatto sulla protezione dati personali **Chi: Gruppo di lavoro**	Ogni progetto di ricerca che preveda il trattamento di dati personali dovrà essere sottoposto, tra le altre cose, ad una valutazione del rischio. L'adozione di uno strumento quale la scheda di progetto può, da un lato, permettere di meglio identificare i dati di cui il ricercatore ha effettivamente bisogno, dall'altro consentire una corretta valutazione delle misure tecniche e organizzative da adottare ai fini del trattamento. Ciò si rivela di particolare importanza laddove oggetto del trattamento sono dati particolari quali, a titolo di esempio, lo stato di salute o l'identità e orientamento sessuale.

8 Attività gestionali e amministrative trasversali		
8.1	Individuazione dei ruoli e delle responsabilità ai sensi del GDPR **Chi: Vertice politico, Vertice amministrativo, Responsabile della Protezione Dati personali** Individua, anche per il tramite del gruppo di lavoro o del Responsabile della Protezione Dati personali, ruoli e responsabilità interne all'Ateneo. Provvedi, in sede di nomina oppure mediante atto separato, a dare evidenza dell'effettiva assegnazione di ogni specifico ruolo all'interno del sistema di protezione dei dati personali. Indipendentemente dalla scelta operata, inserisci nell'atto una descrizione puntuale delle attribuzioni in materia di privacy.	Il Codice Privacy, d.lgs. 196/2003, individuava la possibilità per il titolare di nominare responsabili interni del trattamento (ancorché esplicitamente non ammessi dalla normativa europea di riferimento) e incaricati del trattamento. Il GDPR non prevede figure di questo genere ed anzi, nelle indicazioni circa le caratteristiche di cui deve essere in possesso il responsabile del trattamento, di fatto esclude a priori la possibilità che questi sia una persona interna all'organizzazione. Menziona incidentalmente le persone fisiche autorizzate al trattamento sotto l'autorità diretta del titolare, concetto nell'ambito del quale è possibile ricondurre tutte le figure che, nell'organizzazione di un soggetto complesso, effettuano attività di trattamento dati personali. Tali figure devono essere adeguatamente istruite dal titolare. È possibile, adottando nozioni derivate dal decreto di adeguamento attualmente in discussione nel Parlamento italiano, individuare quali "soggetti designati al trattamento" i responsabili di area e quali "soggetti autorizzati al trattamento" gli operatori. Sebbene non esplicitamente previsto, pare opportuno avere traccia scritta di ogni assegnazione di ruolo all'interno del sistema di protezione dei dati personali. A tal proposito, è auspicabile che l'atto di assegnazione di nomina all'interno di un singolo ufficio contenga informazioni specifiche in merito agli obblighi derivanti dalla normativa sulla tutela dei dati personali. Questa opzione non è funzionale a sollevare il titolare dalle proprie responsabilità, bensì a dimostrare un approccio volto a distribuire consapevolezza tra i dipendenti rispetto agli obblighi derivanti dall'applicazione della normativa.

8.2.a	Predisposizione del piano di formazione per il personale di Ateneo **Chi: Vertice amministrativo, Responsabile della Protezione Dati personali, Responsabile ufficio formazione** Provvedi, anche con il supporto del Responsabile per la Protezione dei Dati personali, alla stesura di un piano di formazione sulla protezione dei dati personali. Adotta una metodologia che vada dal generale al particolare, differenziata in base alle responsabilità e alle funzioni ricoperte.	La formazione costituisce uno dei perni essenziali del sistema di protezione dei dati personali previsto dal GDPR. In particolare, il regolamento esplicita la necessità che chiunque operi sotto l'autorità del titolare debba essere da questi adeguatamente istruito. La formazione deve riguardare la conoscenza degli aspetti normativi, i comportamenti da tenere nello svolgimento dell'attività lavorativa, il corretto uso dei sistemi informatici, le misure organizzative e tecnologiche funzionali alla protezione dei dati personali. È possibile articolare un piano formativo in più livelli, a seconda delle mansioni e delle responsabilità dei dipendenti. Opportuno inoltre prevedere formazione specifica sulla sicurezza informatica per il personale IT e giuridica per il personale dell'ufficio legale. È auspicabile coniugare l'aggiornamento professionale in materia di privacy con quello legato alla gestione documentale. I due temi sono strettamente correlati e ciò indipendentemente dal fatto che si operi in ambiente tradizionale o digitale. Molte questioni legate alla sicurezza nel trattamento dei dati personali, possono infatti essere risolte con l'adozione di corrette procedure gestionali dei documenti che li contengono. È previsto anche l'obbligo di provvedere alla formazione del Responsabile della Protezione Dati personali mediante la partecipazione a corsi specifici finalizzati all'arricchimento delle conoscenze e delle competenze di questa nuova figura. La mancata formazione del personale costituisce elemento di valutazione ai fini della comminazione di sanzioni in caso di controllo da parte dell'Autorità Garante.

8.2.b	Attuazione del piano di formazione per il personale di Ateneo **Chi: Vertice amministrativo, Responsabile della Protezione Dati personali, Responsabile ufficio formazione** Attua il piano di formazione appositamente predisposto. Per i corsi di formazione in aula, organizza l'attività in maniera tale da conciliare le esigenze di lavoro di ufficio con quelle di apprendimento. Per i corsi di formazione in modalità e-learning, assicurati che essi siano effettivamente seguiti dai dipendenti e che al termine degli stessi sia previsto un test di autovalutazione. Procedi infine alla somministrazione di un test finale, concordando i contenuti dello stesso con il Responsabile della Protezione Dati personali.	L'attività di formazione in materia di protezione dei dati personali, che si ricorda essere obbligatoria, comporta l'impiego di tempo ed energie che sono sottratte al lavoro di ufficio. Fermo restando il legittimo interesse dell'amministrazione a che l'impatto sia minimo, non è ammissibile pensare ad una formazione svolta in maniera frammentaria o dispersiva. La conciliazione deve avvenire mettendo sullo stesso piano entrambe le esigenze. È necessario inoltre assicurarsi della partecipazione dei dipendenti alle attività formative. Qualora si prevedano corsi di formazione in aula, sarà necessario raccogliere le firme in entrata ed in uscita ed assicurarsi dell'effettiva presenza dei dipendenti durante l'attività. Qualora si prevedano corsi di formazione in e-learning, è opportuno adottare metodologie di controllo dell'effettiva frequenza delle attività. Nella maggior parte dei casi, ciò sarà reso possibile dalle piattaforme utilizzate. Ove ciò non sia possibile, è opportuno coinvolgere i responsabili delle aree e degli uffici nelle attività di controllo. Indipendentemente dalla formula adottata, è indispensabile procedere ad una o più verifiche dei risultati di apprendimento. A tal proposito si suggerisce, con riferimento alla formazione generale, la somministrazione di quesiti a risposta chiusa. Per la formazione specifica potrebbe invece rivelarsi più utile adottare la forma aperta o quantomeno quella mista.
8.3	Revisione del regolamento sulla protezione dati di Ateneo alla luce delle previsioni del GDPR **Chi: Organi collegiali** Procedete, tramite l'apposita commissione, alla revisione del regolamento di Ateneo sulla Privacy. Qualora il regolamento non sia mai stato redatto, procedete alla sua stesura e approvazione.	L'adeguamento al GDPR passa anche dalla revisione dei regolamenti interni all'Ateneo. Ove esistente, il regolamento per la protezione dei dati personali deve essere aggiornato, non solo in relazione ai riferimenti alla nuova normativa, ma anche nei contenuti. La revisione avrebbe dovuto essere effettuata prima della data del 25 maggio 2018, pertanto è opportuno procedere con celerità. Ove non esistente, il regolamento deve essere redatto con la massima urgenza.

8.4	Verifica e modifica delle procedure di gestione e conservazione documentale **Chi: Vertice amministrativo, Responsabile della Gestione Documentale, Responsabile della Conservazione, Responsabile della Protezione Dati personali** Procedi alla revisione delle procedure di gestione documentale, puntando ove possibile alla dematerializzazione. È essenziale che tutte le strutture si adeguino alle previsioni del Manuale di Gestione e del Manuale di Conservazione evitando da un lato l'accumulo di carte non necessarie, dall'altro la conservazione con modalità e tempi diversi dalle previsioni.	L'aggiornamento delle procedure di gestione documentale, con particolare riferimento alla dematerializzazione, costituisce un obbligo di legge sin dall'emanazione del Codice dell'Amministrazione Digitale. L'assenza di sanzioni ha, nei fatti, permesso un certo lassismo nell'adeguamento, lassismo che invece non è ammissibile in relazione al GDPR. La nuova normativa impatta sulla gestione documentale: le misure tecnologiche e organizzative attengono anche alla modalità di produzione, trasmissione e conservazione dei documenti in relazione ai dati che essi contengono. Per questa ragione è essenziale che il RGD e il RPD procedano alla revisione delle procedure e dei manuali di gestione e conservazione. Aspetto importante sarà quello relativo ai tempi di conservazione, posto l'obbligo previsto dal GDPR in base al quale non è consentito conservare i dati per un tempo superiore a quello necessario alle finalità del trattamento, fatto salvo obbligo di legge.
8.5	Verifica e modifica delle procedure di trasmissione / trasferimento dei dati personali **Chi: Responsabile di Dipartimento, Area, Ufficio** Effettua un controllo circa quali dati debbano essere trasmessi dall'Ateneo a soggetti terzi, con quali modalità e in quali momenti. Verifica l'effettiva adozione di misure organizzative, gestionali e tecniche funzionali a garantire la sicurezza dei dati nelle diverse fasi del trasferimento. In caso di trasferimento di dati personali all'estero, verifica che siano soddisfatte le condizioni previste dal regolamento. In presenza di dubbi, contatta il Responsabile per la Protezione dei Dati personali.	La trasmissione e il trasferimento di dati personali sono da considerarsi trattamenti ai sensi del GDPR e pertanto sono soggetti innanzi tutto alle condizioni di liceità di cui all'art. 6. Laddove avvengano in virtù di un obbligo di legge o del perseguimento di un rilevante interesse pubblico, non è necessario chiedere il consenso, che è invece necessario in tutti gli altri casi. Particolare attenzione va posta in relazione al Paese verso cui i dati sono trasmessi o trasferiti: se trattasi di Stato membro dell'UE non sussistono particolari problemi. Diversamente, grande attenzione si deve porre allorché il trasferimento di dati avvenga verso un Paese terzo (non UE) o un'organizzazione internazionale. Infatti il GDPR vieta espressamente questa tipologia di trasferimento, salvo che non si verifichino le condizioni di cui agli artt. 44 – 50.

8.6	Verifica e modifica dei contratti in essere con fornitori che trattano dati in nome e per conto dell'Ateneo, ai fini della loro nomina quali responsabili del trattamento ai sensi del GDPR **Chi: Responsabile di Dipartimento, Area, Ufficio** Effettua innanzi tutto una ricognizione dei contratti in essere. Tra questi, individua quelli che riguardano servizi relativi al trattamento dei dati personali. Verifica che, per ciascuno di questi ultimi, sia stata effettuata la nomina del fornitore quale responsabile del trattamento ai sensi del GDPR. Ove ciò non sia stato fatto, contatta il Responsabile della Protezione Dati personali.	Già il Codice Privacy prevedeva l'obbligo di nomina per iscritto del responsabile esterno del trattamento, laddove il titolare avesse stabilito di avvalersene. Il GDPR non solo conferma tale obbligo, ma stabilisce altresì che qualora un trattamento debba essere effettuato per conto del titolare del trattamento, questi debba ricorrere esclusivamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate alle previsioni del regolamento. L'obbligo in questione non riguarda solo i trattamenti effettuati a partire dall'introduzione del GDPR, ma anche quelli vigenti. Laddove un soggetto operi quale responsabile del trattamento in virtù di un contratto, ma non presenti le adeguate garanzie, è quindi necessario individuare, a tutela dell'Ateneo e dello stesso soggetto in questione, un percorso che porti alla rescissione del contratto.

8.7	*Introduzione, in sede di emanazione di bando di gara e/o di stipula di contratto, delle clausole di coerenza con le previsioni del GDPR per tutti i sistemi da acquisire in futuro*. **Chi: Responsabile di Dipartimento, Area, Ufficio** Adegua la modulistica relativa alla gestione delle procedure di gara e/o di stipula di contratto alle previsioni del GDPR. In particolare tanto la procedura, quanto il contratto dovranno presentare le seguenti indicazioni: - descrizione dell'oggetto, della durata, della natura e delle finalità del trattamento - descrizione della tipologia dei dati personali che saranno raccolti e delle categorie di soggetti interessati - clausole relative agli obblighi posti in capo al responsabile del trattamento: o di agire esclusivamente su indicazioni scritte del titolare, salvo diverse previsioni di legge o di garantire che il personale che accede ai dati sia soggetto all'obbligo di riservatezza o di adottare idonee misure tecniche e organizzative per garantire la sicurezza del trattamento o di incaricare eventuale sub-responsabile solo previo consenso del titolare e tramite contratto scritto o di assistenza al titolare nelle richieste di accesso da parte degli interessati o di assistenza al titolare con riferimento alle valutazioni di impatto e alle eventuali violazioni o di cancellazione o restituzione dei dati personali al titolare al momento della cessazione del contratto o di sottoporsi a verifiche e ispezioni da parte del titolare o di informare il titolare qualora riceva richieste in violazione delle disposizioni del GDPR o di assicurare, in caso abbia sede in un Paese extra-UE, che tale Paese offra un livello di protezione dei dati personali ritenuto adeguato dall'Unione Europea o di impegnarsi a sottoscrivere specifiche clausole contrattuali previste dall'Unione Europea	Già il Codice Privacy prevedeva l'obbligo di nomina per iscritto del responsabile esterno del trattamento, laddove il titolare avesse stabilito di avvalersene. Il GDPR non solo conferma tale obbligo, ma stabilisce altresì che qualora un trattamento debba essere effettuato per conto del titolare del trattamento, questi debba ricorrere esclusivamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate alle previsioni del regolamento. È quindi essenziale che, già in sede di emanazione di bando di gara, si faccia esplicito riferimento alla presentazione di garanzie in materia di misure tecniche e organizzative funzionali alla protezione dei dati personali. In alternativa sarebbe comunque possibile menzionare l'obbligo di accettazione, da parte del vincitore, della nomina quale responsabile del trattamento ai sensi del GDPR. In ogni caso, al momento della stipula del contratto, il fornitore dovrà accettare tale nomina e tutte le clausole che ne derivano.

9 Attività di Information technology		
9.1	Verifica e modifica dell'informativa sulla protezione dei dati personali presente sul sito internet di Ateneo e delle informative generali **Chi: Responsabile del sito internet di Ateneo, responsabili siti internet singole strutture** Rivedi e aggiorna l'informativa sulla protezione dati personali presente sul sito internet di Ateneo e su tutti i siti delle strutture di Ateneo. Redigi e procedi alla pubblicazione di una pubblicazione di una *cookie policy* dettagliata e dell'elenco completo dei servizi di terze parti che profilano gli utenti durante la navigazione del sito web. Quest'ultimo deve rimandare alle singole informative privacy di ciascuna delle terze parti. Procedi alla pubblicazione di tutte le informative generali di Ateneo nella specifica sezione e verifica la correttezza dei relativi collegamenti. Cancella infine le informative non più in vigore.	Il sito internet rappresenta, oggi come oggi, il principale punto di informazione di Ateneo e di tutte le strutture di cui esso si compone. È quindi essenziale che al suo interno si possa accedere almeno alle informative generali, suddivise per categorie di destinatari. Molta attenzione va posta rispetto all'aggiornamento delle stesse, in quanto è possibile che esse siano periodicamente sottoposte a revisione: sarà necessario che sul sito siano rinvenibili esclusivamente le informative vigenti. Sarebbe buona prassi eliminare quelle obsolete dal server che ospita il sito, anche al fine di non incorrere e non fare incorrere colleghi di altre strutture in errori di pubblicazione. La sezione che ospita le informative dovrebbe essere facilmente raggiungibile, ad esempio attraverso un collegamento presente nella homepage, e accessibile da parte di qualunque utente (niente area riservata). Il sito internet è certamente una vetrina, ma nei fatti è anche un sistema di trattamento dati in relazione alla navigazione. È quindi indispensabile procedere alla stesura o all'adeguamento della relativa informativa privacy, corredandola di una *cookie policy*, ovvero un regolamento sull'uso dei cookie, nonché dell'elenco di tutti i servizi di terze parti che raccolgono dati degli utenti durante la navigazione nel sito stesso. Tale elenco deve contemplare altresì i collegamenti alle informative di ciascun servizio. Sarebbe inoltre opportuno, in alcuni casi indispensabile, valutare quali tra questi servizi corrispondano alle esigenze dell'Ateneo, anche al fine di dismettere quelli di cui sia possibile, o necessario, fare a meno. Del resto, da una valutazione dell'impatto del trattamento sulla protezione dati personali, potrebbero emergere situazioni di non conformità, che obbligherebbero l'Ateneo a sospendere immediatamente il trattamento e a rimuovere il sistema incriminato.

9.2	Verifica e modifica il sito internet per renderlo conforme alle previsioni del GDPR **Chi: Responsabile del sito internet di Ateneo, responsabili siti internet singole strutture** Verifica la rispondenza del sito internet di Ateneo e dei siti delle singole strutture di Ateneo alle previsioni del GDPR. Controlla tutte le eventuali pagine statiche o le parti di contenuto statico di cui il sito si compone. Qualora dovessi riscontrare che i contenuti rientrino, anche solo in parte e in maniera marginale, nel campo di applicazione del regolamento, procedi con le opportune modifiche per renderli conformi alla nuova normativa. In caso di dubbi, contatta il Responsabile della Protezione Dati personali. Se raccogli dei dati, ad esempio tramite registrazione, assicurati di aver adottato i principi di minimizzazione, libera espressione del consenso, corretta informazione sui singoli trattamenti e sulle finalità perseguite. Se pubblichi dati personali, ad esempio per comunicare i risultati di un procedimento, assicurati di rendere pubblici solo i dati strettamente necessari e solo per i termini temporali previsti dalla legge. Laddove un dato personale o un documento contenente dati personali risulti essere visibile oltre i termini di legge, procedi alla sua deindicizzazione, contatta il Responsabile della Protezione Dati personali e verifica la possibilità di cancellare il dato dal sito. Se hai dei dubbi in merito ai termini di pubblicazione di un atto, consulta il Responsabile della Gestione Documentale. Qualora dovessi riscontrare lacune o difformità rispetto a quanto indicato, provvedi a colmare le stesse in maniera tempestiva. Ove ciò non fosse possibile, contatta il Responsabile per la Protezione Dati personali. Considera inoltre che il sito internet deve rispettare i requisiti di *privacy by design* e di *privacy by default*. Ove ciò non sia possibile, comunica al titolare la necessità di realizzare un nuovo sito internet.	Il sito internet rappresenta, oggi come oggi, il principale punto di informazione di Ateneo e di tutte le strutture di cui esso si compone. È una vetrina, uno strumento di informazione, un biglietto di presentazione dell'Ateneo. Al tempo stesso è un sistema di trattamento dati, che spesso sono dati personali, sicché esso deve essere conforme alle previsioni del regolamento. Se tramite il sito internet si provvede alla raccolta di dati personali (ad esempio attraverso la registrazione), sarà necessario innanzi tutto minimizzare i dati raccolti (limitandosi a quelli strettamente necessari per il perseguimento della o delle finalità previste), predisporre una o più informative ad hoc e adeguare i moduli alle previsioni del GDPR, con particolare riferimento alle modalità di rilascio del consenso. Su quest'ultimo punto, è bene ricordare che il consenso deve essere totalmente libero e che non è ammissibile che il suo mancato rilascio crei un pregiudizio nei confronti dell'interessato. Se tramite il sito internet si provvede alla pubblicazione di informazioni personali, ad esempio per adempiere ad obblighi di legge, è necessario porre particolare attenzione ai tempi di pubblicazione sia dei dati, sia degli eventuali documenti che li contengono: la visibilità di entrambi non deve eccedere i termini fissati dalle norme di legge. Si deve inoltre considerare che il sito internet, in quanto sistema di trattamento, deve rispettare le indicazioni in merito alla *privacy by design* e alla *privacy by default*. In altre parole il sito deve essere progettato a monte per garantire la protezione dei dati personali e, per impostazione, deve trattare solo ed esclusivamente i dati strettamente necessari al perseguimento delle finalità sottese ai trattamenti che, per il suo tramite, vengono effettuati. Una verifica in tal senso risulta essere oltremodo necessaria. In caso di esito negativo è imperativo implementare un nuovo sito internet.

9.3	Notifica agli interessati in merito alla pubblicazione di profili contenenti dati personali sul sito internet di Ateneo **Chi: Responsabile del sito internet di Ateneo, responsabili siti internet singole strutture** Se pubblichi profili di studenti o di dipendenti (ad esempio schede di contatto) su un sito internet accessibile dall'esterno, verifica la base giuridica del trattamento. In assenza di obblighi di legge o di interessi pubblici da tutelare, è necessario prevedere un modulo di consenso e comunque la possibilità di rendere non visibili i dati personali dall'esterno.	Il GDPR non considera, in linea di principio, illecita la pubblicazione di dati personali sul sito internet di Ateneo, che si tratti di studenti o di dipendenti. È però necessario assicurarsi di quale sia la base giuridica di tale trattamento. In particolare, laddove la pubblicazione non sia disposta in base ad obbligo di legge o interesse pubblico rilevante, è da presumere che il trattamento debba essere effettuato esclusivamente previo rilascio del consenso dell'interessato.
9.4	Verifica e modifica degli applicativi prodotti e utilizzati dall'Ateneo per renderli conformi alle previsioni del GDPR o dismetterli **Chi: Responsabile dell'area informatica di riferimento** Assicurati che il settore che realizza applicativi per le esigenze delle strutture di Ateneo, sia informato in merito alle previsioni del GDPR e proceda alla realizzazione di nuovi sistemi tenendo conto dei principi di *privacy by design* e *privacy by default*. Al tempo stesso, verifica o fai verificare la conformità dei sistemi autoprodotti in uso all'interno dell'Ateneo con le previsioni del GDPR e, in caso di difformità, adotta o fai adottare le misure correttive. Ove ciò non sia possibile, provvedi alla dismissione.	Ai sensi del GDPR è necessario che tutti gli applicativi, tramite i quali si effettua trattamento dati, prevedano sin dalla progettazione misure atte a garantire in maniera efficace la protezione dei dati personali. Inoltre è necessario che essi trattino, per impostazione predefinita, solo ed esclusivamente i dati strettamente necessari per ogni specifica finalità di trattamento. Nel caso in cui l'Ateneo decida di autoprodurre soluzioni informatiche, è quindi necessario tenere di conto delle suddette previsioni, procedendo altresì all'adeguamento di quanto esistente. In particolare per quanto riguarda i sistemi già in uso, è opportuno valutare anche la dismissione in favore di nuovi sistemi adeguati al GDPR.

9.5	Verifica e richiesta di modifica degli applicativi prodotti da terzi e utilizzati dall'Ateneo per renderli conformi alle previsioni del GDPR o dismetterli **Chi: Responsabile dell'area informatica di riferimento** Assicurati che tutti i sistemi prodotti da terzi e in uso presso le strutture di Ateneo siano conformi alle previsioni del GDPR. Ove ciò non si verifichi, contatta lo sviluppatore e chiedi le opportune modifiche. Laddove ciò non sia possibile, procedi con la dismissione.	Ai sensi del GDPR è necessario che tutti gli applicativi, tramite i quali si effettua trattamento dati, prevedano sin dalla progettazione misure atte a garantire in maniera efficace la protezione dei dati personali. Inoltre è necessario che essi trattino, per impostazione predefinita, solo ed esclusivamente i dati strettamente necessari per ogni specifica finalità di trattamento. Nel caso in cui l'Ateneo decida di acquisire nuove soluzioni informatiche, sarà necessario che si tenga conto di tali aspetti, escludendo ogni soluzione che per la quale non sia possibile dimostrare la conformità. Per quanto riguarda i sistemi già in uso, sarà necessario verificare se essi siano o meno adeguati alle previsioni del GDPR o se siano disponibili aggiornamenti che atti a garantire la conformità con la nuova normativa. Diversamente sarà necessario contattare il fornitore e chiedere un tempestivo intervento in questa direzione. Laddove dovesse risultare che l'adeguamento non sia possibile o che sia troppo oneroso, non resterà che dismettere il sistema in favore di soluzioni conformi al GDPR.
9.6	Verifica delle capacità di risposta rispetto alle richieste di accesso ai dati presenti all'interno dei server e dei database di Ateneo **Chi: Responsabile dell'area informatica di riferimento** Adotta una procedura atta a soddisfare le richieste di accesso ai dati personali conservati all'interno dei server e dei database di Ateneo e verifica, con riferimento ai modi e ai tempi, la tua capacità di risposta. Salvo casi ad elevata complessità, a fronte della richiesta di un singolo interessato, dovresti essere in grado di fornire tutte le informazioni in meno di 48 ore. Laddove verificassi che ciò non sia possibile, individua le cause ostative e procedi alla loro rimozione. Effettua altresì degli stress test atti a verificare la capacità di risposta in presenza di un elevato numero di richieste. Salvo casi ad elevata complessità, dovresti essere in grado di rispondere ad almeno 200 richieste entro 30 giorni dalla loro ricezione. Laddove verificassi che ciò non sia possibile, individua le cause ostative e procedi alla loro rimozione. Adotta altresì procedure di verifica dell'identità degli interessati.	È essenziale, a fronte di una richiesta di accesso ai dati effettuata da parte di un interessato, dare risposta in tempi brevi. Il termine di 48 ore è puramente indicativo e non previsto esplicitamente dal GDPR, che però sancisce l'obbligo di risposta senza ingiustificato ritardo. Tenuto conto del numero di richieste, il termine massimo che il regolamento concede per le risposte è di un mese dal momento della ricezione, estensibile per ulteriori due mesi nei casi di maggiore complessità. In caso di richieste semplici, è dunque opportuno procedere speditamente, anche al fine di evitarne l'accumulo e la sovrapposizione con richieste più complesse. Del resto, un ritardo motivato da negligenza o da neghittosità del titolare, non può essere considerato accettabile e costituisce comportamento sanzionabile. Lo svolgimento di uno stress-test potrebbe essere funzionale ad identificare preventivamente eventuali criticità, con particolare riferimento ai cosiddetti colli di bottiglia. In questa sede non è necessario entrare nel merito delle richieste, è però indispensabile testare le procedure di accertamento dell'identità degli interessati. In particolare si deve essere in grado di stabilire se il soggetto che formula la richiesta è effettivamente chi sostiene di essere, in particolare laddove la presentazione avvenga a mezzo di posta elettronica.

9.7	Verifica delle capacità di dare seguito alle richieste di esercizio dei propri diritti (rettifica, limitazione, cancellazione, portabilità, opposizione) da parte degli interessati **Chi: Responsabile dell'area informatica di riferimento** Adotta una procedura atta a soddisfare le richieste di esercizio dei diritti degli interessati relativamente ai dati personali conservati all'interno dei server e dei database di Ateneo e verifica, con riferimento ai modi e ai tempi, la tua capacità di risposta. Salvo casi ad elevata complessità, a fronte della richiesta di un singolo interessato, dovresti essere in grado di effettuare tutti gli interventi in meno di 48 ore. Laddove verificassi che ciò non sia possibile, individua le cause ostative e procedi alla loro rimozione. Effettua altresì degli stress test atti a verificare la capacità di risposta in presenza di un elevato numero di richieste. Salvo casi ad elevata complessità, dovresti essere in grado di rispondere ad almeno 200 richieste entro 30 giorni dalla loro ricezione. Laddove verificassi che ciò non sia possibile, individua le cause ostative e procedi alla loro rimozione. Adotta altresì procedure di verifica dell'identità degli interessati.	È essenziale, a fronte di una richiesta di accesso ai dati effettuata da parte di un interessato, dare risposta in tempi brevi. Il termine di 48 ore è puramente indicativo e non previsto esplicitamente dal GDPR, che però sancisce l'obbligo di risposta senza ingiustificato ritardo. Tenuto conto del numero di richieste, il termine massimo che il regolamento concede per le risposte è di un mese dal momento della ricezione, estensibile per ulteriori due mesi nei casi di maggiore complessità. In caso di richieste semplici, è dunque opportuno procedere speditamente, anche al fine di evitarne l'accumulo e la sovrapposizione con richieste più complesse. Del resto, un ritardo motivato da negligenza o da neghittosità del titolare, non può essere considerato accettabile e costituisce comportamento sanzionabile. Lo svolgimento di uno stress-test potrebbe essere funzionale ad identificare preventivamente eventuali criticità, con particolare riferimento ai cosiddetti colli di bottiglia. In questa sede non è necessario entrare nel merito delle richieste, sebbene sia indispensabile testare le procedure di accertamento dell'identità degli interessati. Si deve infatti essere in grado di stabilire se il soggetto che formula la richiesta è effettivamente chi sostiene di essere, in particolare laddove la presentazione avvenga a mezzo di posta elettronica.

9.8	Verifica delle misure tecnologiche e informatiche di sicurezza di Ateneo **Chi: Responsabile dell'area informatica di riferimento** Verifica che le misure tecniche e organizzative adottate nel piano di *disaster recovery* e *business continuity* siano effettivamente in uso e testane l'efficacia. Assicurati in particolare che siano individuate sia delle misure preventive, atte cioè ad anticipare eventi che impattano sulla protezione dei dati e sulla funzionalità dei sistemi, che reattive, ovvero di risposta al verificarsi di situazioni che espongono a violazione gli uni e gli altri. Laddove l'Ateneo non abbia redatto un piano in tal senso, procedi preventivamente alla sua stesura. Verifica il grado di protezione da accessi illeciti delle reti, dei sistemi e delle applicazioni utilizzate dall'Ateneo. Laddove le verifiche evidenziassero lacune, limiti o inefficienze, contatta immediatamente il Responsabile della Protezione Dati personali e valuta congiuntamente al titolare gli interventi da effettuare.	La cronaca insegna da tempo che tanto le violazioni, quanto le interruzioni di funzionamento dei sistemi informatici sono molto più frequenti di quanto si possa immaginare, possono presentarsi in qualsiasi momento e in diverse forme (ad esempio furto, cancellazione, sequestro, illecita diffusione di dati) e possono essere originate da vari fattori (errori umani, guasti interni e/o esterni, calamità naturali, attacchi intenzionali alle strutture fisiche o logiche dei sistemi). In situazioni di questo genere il coefficiente di rischio di perdita dei dati può assumere valori particolarmente alti, pertanto è necessario, ai fini della conformità alle previsioni del GDPR, adottare misure preventive e misure di recupero dei dati e di ripristino della funzionalità dei sistemi. In questo contesto, un ruolo primario spetta senza dubbio al piano di *business continuity* e di *disaster recovery*. Tra le misure preventive, è necessario disporre che l'accesso fisico ed informatico ai server di Ateneo sia consentito solo a soggetti autorizzati e che, nei locali che li ospitano, siano state adottate misure di prevenzione atte a garantire la sicurezza dell'infrastruttura, la sicurezza fisica dei dati, la sicurezza del personale che vi opera. Tra le misure reattive, si possono indicare misure atte a ripristinare sistemi, dati e infrastrutture necessarie all'erogazione dei servizi di Ateneo a fronte di gravi emergenze.
9.9	Verifica delle misure di sicurezza della strumentazione informatica messa a disposizione dei dipendenti e degli utenti **Chi: Responsabile dell'area informatica di riferimento** Verifica le misure tecniche e organizzative di sicurezza dei supporti informatici forniti dall'Ateneo e utilizzati dai dipendenti o dagli utenti. In caso di dubbi, contatta il Responsabile della Protezione Dati personali.	Il rispetto del GDPR passa anche dalla protezione dei dispositivi informatici concessi in uso ai dipendenti e agli utenti di Ateneo. Qualora tramite tali dispositivi sia possibile accedere a dati personali conservati dall'Ateneo è indispensabile che siano adottate misure tecniche di protezione atte a scongiurare le potenziali violazioni. Per i computer d'ufficio è essenziale prevedere almeno ad un sistema di controllo degli accessi, all'installazione di un firewall, di un antivirus, di un anti-malware e di un anti-spyware che devono essere mantenuti costantemente aggiornati, all'installazione di un sistema di cifratura delle cartelle destinate ad ospitare documenti contenenti dati personali. Opportuno prevedere l'introduzione di ulteriori misure alla luce dello stato dell'arte sulla sicurezza informatica. Azioni analoghe devono essere effettuate anche per i supporti mobile quali notebook, tablet, smartphone che l'Ateneo concede in uso ai dipendenti o agli studenti.

10 Azioni di monitoraggio		
10.1	*Monitoraggio sull'applicazione del piano di adeguamento* **Chi: Vertice politico, Vertice Amministrativo, Gruppo di lavoro, Responsabile della Protezione Dati personali** Verifica, con cadenza periodica, che le attività previste dal presente piano siano effettivamente svolte dai soggetti individuati. Laddove riscontrassi ritardi e/o criticità, effettua azioni di sollecito e, in caso di mancato riscontro, procedi all'espletamento delle azioni in via sussidiaria.	In linea di principio, l'attività di monitoraggio sull'applicazione del progetto dovrebbe rientrare esclusivamente tra le mansioni assegnate al gruppo di lavoro. È quindi opportuno che solo i componenti del gruppo procedano in questa direzione. È però indiscutibile, anche per le mansioni ricoperte, che tanto il Vertice politico, quanto il Vertice amministrativo abbiano il dovere di vigilare sul sistema di protezione dati personali e, di conseguenza, anche sull'andamento delle attività di adeguamento al GDPR. Infine, è opportuno precisare come il Responsabile della Protezione Dati personali possa agire sia come componente del gruppo di lavoro, sia in relazione alle mansioni correlate al proprio incarico.
10.2	Monitoraggio del sistema di protezione dati personali **Chi: Responsabile della Protezione Dati personali** Procedi al controllo periodico dello stato del sistema di protezione dati personali di Ateneo. Anche tramite la collaborazione di dipendenti ad uopo individuati, procedi alla verifica della sicurezza delle reti, dei server, della strumentazione informatica di Ateneo.	L'attività di monitoraggio del sistema di protezione dati rientra nel novero delle attività poste in capo al Responsabile della Protezione Dati personali. Il controllo deve riguardare ambivalentemente le misure organizzative e le misure tecniche di sicurezza: in particolare sarà necessario verificare la loro attuazione e il loro funzionamento rispetto all'obiettivo da perseguire. È necessario che di tale attività si tenga traccia scritta, anche al fine di dimostrare l'*accountability* di Ateneo.