

Università degli Studi di Messina

Piano per l'applicazione in Unime del Regolamento Europeo 679/2016 e del Codice in materia di protezione dei dati personali D.Lgs 196/2003 come modificato dal D.Lgs. 101/2018



Gruppo di lavoro Interno GDPR Privacy
D.D. 763 del 17 Aprile 2018

Responsabile della Protezione Dati
C.d.A. del 24 Maggio 2018

Indice

Premessa	Pag. 3
Organizzazione del documento	Pag. 4
I - Contesto normativo	Pag. 5
I nuovi principi e il cambio di prospettiva	Pag. 7
Circolare Unime <i>Disposizioni in materia di Protezione dei Dati Personali.</i> <i>Decreto legislativo del 10 agosto 2018 n. 101 e Regolamento (UE) 2016/679</i>	Pag. 8
II – Il Trattamento e la Protezione dei Dati Personali in Unime	Pag. 9
Fase I - Priorità e relative azioni	Pag. 11
Fase II - Interventi di mantenimento	Pag. 15
Azioni di revisione e miglioramento	
GANTT	Pag. 16
Allegati	Pag. 17

Premessa

Il Regolamento Europeo n. 679/2016 <<*Regolamento Generale sulla Protezione dei Dati*>> al quale si collega il D. Lgs. n. 101/2018, recante le disposizioni per l'adeguamento del <<*Codice in materia di protezione dei dati personali*>>, segna – per quel che attiene al **trattamento e alla protezione dei dati personali** – il passaggio da una tutela di tipo *remediale-reattivo-formale* ad una di tipo *preventivo-proattivo-sostanziale*.

Al centro di questo cambiamento devono essere posti: il trattamento dei dati personali e la responsabilità della sua gestione, alla quale sottende una marcata impostazione progettuale e preventiva, derivante dalla *positivizzazione* del principio di responsabilizzazione (c.d. *accountability*), e fortemente orientata alla *minimizzazione del rischio* e alla dimostrazione delle scelte assunte.

Questo approccio palesa quanto ormai sia da ritenersi obsoleta e fuorviante l'idea di associare la protezione dei dati personali alla c.d. *firmetta per la privacy*, oppure alla formale osservanza della norma, spesso percepita come un noioso adempimento burocratico.

Come per tutte le Amministrazioni pubbliche, anche per l'Università degli Studi di Messina si apre l'opportunità di progettare, attuare e mantenere un percorso di *compliance* al Regolamento Europeo e al "nuovo" Codice, considerando i processi istituzionali in gioco, coinvolgendo tutti gli attori che accedono e trattano dati personali.

La formulazione del piano nasce dall'esigenza di svolgere questo processo di *compliance* secondo una *strategia complessiva, strutturata e condivisa* e di esporne *dimostrazione*.

Il documento, infine, è proposto dalla Responsabile della Protezione dei Dati di Ateneo e raccoglie i contributi ad oggi condivisi nell'ambito delle attività del Gruppo di Lavoro *GDPR Privacy Unime*, anche al fine di valorizzarne le esperienze, definendo un metodo di lavoro riutilizzabile con continuità. Si tiene conto delle indicazioni e delle linee guida diffuse da GARANTE e dal Comitato Europeo *ex Working Party art. 29*.

Organizzazione del documento

Il documento si compone di 2 (due) parti oltre GANTT e Allegati.

1. Nella prima parte sono indicate alcune chiavi di lettura per una migliore interpretazione dei nuovi principi e delle novità introdotte dal Regolamento Generale, funzionali alla contestualizzazione delle azioni successivamente descritte; il dettaglio delle novità, introdotte dal Regolamento, sono rimandate alla Circolare Unime n. 33 del 29/10/2018 prot. 82783 <<Oggetto: *Disposizioni in materia di Protezione dei Dati Personali. Decreto legislativo del 10 agosto 2018 n. 101 e Regolamento (UE) 2016/679*>>, che illustra quelle di maggior interesse e ricaduta per l'Ateneo.
2. Nella seconda parte sono indicate le azioni di carattere tecnico e organizzativo che l'Ateneo, quale Titolare del Trattamento, pianifica di mettere in atto per la *compliance* dei propri trattamenti.

Le azioni individuate come prioritarie riguardano: la **Formazione**; **l'Organizzazione funzionale interna**; la **Gestione e misura del rischio**; la **Gestione e l'esecuzione del trattamento**; **le Informative e le misure di tutela**; il **Controllo sull'affidamento del trattamento a Responsabili (esterni)**; la **Regolamentazione interna** per precisare l'applicazione del RGPD.

Il GANTT descrive lo svolgimento temporale pensato per tali azioni. Gli Allegati, parte integrante del piano, includono: l'organigramma funzionale di Ateneo a supporto dell'attuazione del piano, lo schema di gestione del trattamento, il modello informativa del trattamento, il modello del Registro delle attività di trattamento, il modello del Registro di documentazione delle violazioni sui dati personali.

Per semplicità, nel seguito del documento, saranno adottate le seguenti abbreviazioni: <<RGPD>> indicherà il Regolamento Generale sulla Protezione dei Dati Personali n. 679/2016; <<CODICE>> indicherà l'adeguamento nazionale al suddetto Regolamento,

formulato dal D. Lgs 101/2018 (il “nuovo” Codice in materia di dati personali); e, infine, <<GARANTE>> indicherà l’Autorità Garante Italiana per la protezione dei dati personali.

I – Il contesto normativo.

Il Regolamento Generale sulla Protezione dei Dati n. 679/2016 stabilisce norme relative *alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati*, e protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali rientrando, quest’ultimo, tra i diritti fondamentali della persona.

Il Regolamento Generale – in vigore dal 25 Maggio 2016 e in piena efficacia e attuazione dal 25 Maggio 2018 – deve essere considerato, in materia, l’atto regolatorio fondamentale; trattandosi di un Regolamento e non di una Direttiva non necessita di leggi attuative fatta eccezione per alcuni ambiti sui quali il legislatore Europeo delega e rinvia alla disciplina dei singoli Stati Membri. Ciò premesso, sulla base del sistema di interconnessione delle fonti normative (comunitarie e nazionali), il Codice in materia di protezione di dati personali espresso dal D.Lgs. 196/2003, viene:

- 1) disapplicato, per le parti in cui contrasta con il RGPD;
- 2) adeguato, ove necessario, nelle parti che rientrano negli ambiti sui quali, ai sensi del RGPD, i singoli Stati possono adottare leggi nazionali.

In conseguenza il Governo ha emendato il D.Lgs. 10 Agosto 2018, n. 101 <<*Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016...*>> che esplicita, abrogandole, le parti del Codice disapplicate e che aggiorna quelle oggetto di adeguamento.

Tra queste ultime, per il trattamento che rientra negli ambiti istituzionali dell’Ateneo (Didattica, Ricerca, Terza Missione, attività trasversali di supporto) si distinguono:

- a) in ordine all’esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri (in cui è ricompresa la maggior parte dei trattamenti effettuati dall’Ateneo):
 - la configurazione della base di liceità del trattamento;

- l'interesse pubblico rilevante e il trattamento di categorie particolari di dati;
- le specifiche situazioni di trattamento che rientrano nell'ambito pubblico (Titolo IV), nell'ambito dell'istruzione (Titolo VI); dell'archiviazione nel pubblico interesse, della ricerca scientifica o storica o a fini statistici (Titolo VII); nell'ambito del rapporto di lavoro (Titolo VIII); nell'ambito delle comunicazioni elettroniche (Titolo X).

b) In ordine alle sanzioni:

- quelle amministrative e pecuniarie connesse alla violazione o alla mancata applicazione delle disposizioni del RGPD con riferimento agli ambiti di titolarità dell'Ateneo;

c) in ordine all'organizzazione interna a supporto della protezione dei dati personali:

- l'attribuzione di funzioni e compiti a soggetti designati.

Ciò premesso, l'atto normativo fondamentale rimane il RGPD. Il diritto alla protezione dei dati personali è un diritto fondamentale Europeo, si applica con le medesime modalità in tutto il territorio dell'Unione, incrementa la fiducia per favorire la diffusione di una società (e di un'economia) digitale. Le stesse clausole di flessibilità (considerando 8, 9, 10, 11 del RGPD) che raccolgono gli ambiti in cui i singoli stati possono intervenire per derogare, sostituire ed inserirsi nelle norme del Regolamento sono limitati e definiti, senza grosse differenze tra paese e paese.

La nuova normativa si applica immediatamente ai trattamenti di tutte le Pubbliche Amministrazioni, oltre che a quelli di Titolari non stabiliti nell'Unione ma che offrono servizi e prodotti all'interno del mercato europeo (ad esempio: *Google Inc.*, *Facebook Inc.*, *Drobox Inc.*; *Twitter Inc.*).

Recepire e applicare le nuove norme è fondamentale; in difetto, inosservanza o violazione potrebbero crearsi i presupposti non solo di rigide e pesanti sanzioni amministrative pecuniarie (fino a 20.000.000 euro o al 4% del fatturato annuo globale con intuibile pesante e negativo impatto sulle singole attività) ma, e non secondariamente, di perdita di immagine e di competitività.

I nuovi principi e il cambio di prospettiva.

Il Regolamento Generale 679/2016, per il tramite del trattamento e delle misure ad esso applicate per la tutela dei diritti e delle libertà delle persone fisiche, estende ed evolve il paradigma [*dato personale, risorsa*] a [*dato personale, risorsa, persone*], passando da una visione “individualistica/assoluta” (quella della Direttiva madre 95/46/CE e, per ricaduta, del Codice ex D.Lgs. 196/2003) ad una visione “sociale/relativa”.

In questa prospettiva si inseriscono l’approccio basato sul rischio (inteso come impatto negativo del trattamento per i diritti e le libertà delle persone) e le misure di *accountability* di titolari e responsabili (esterni); il ruolo del GARANTE si colloca “*ex post*” ed è successivo alle determinazioni assunte in autonomia dall’Ateneo (Titolare); quindi, in generale, senza che siano più necessarie autorizzazioni e notifiche preventive o verifiche preliminari, sostituiti da obblighi di tenuta di un registro dei trattamenti e di effettuazione di analisi del rischio e valutazioni di impatto, con eventuale successiva consultazione del GARANTE.

Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale (considerando 4 del RGPD); come tale va temperato e bilanciato con altri diritti fondamentali e relativi beni giuridici (ad es. la trasparenza, l’autodeterminazione informativa, la qualità dell’informazione, la riservatezza, i principi etici e morali quali la libertà di espressione e di informazione).

Nel RGPD il focus della tutela si sposta dal *dato personale statico* al *trattamento del dato personale* (dinamico). **L’elemento guida è il trattamento** le cui caratteristiche discriminano: la base giuridica; l’individuazione, l’attuazione e il riesame di tutte le misure di tutela tecniche e organizzative; l’applicazione dei principali strumenti metodologici prescritti dal RGPD (*Data Protection_by_Design_by Default*); la valutazione d’impatto e i relativi esiti; le due diverse tipologie di informative.

Infine, nel RGPD si rileva, il passaggio dal *consenso* al *controllo* quest’ultimo attuato, innanzitutto, per il tramite dell’informativa e dei diritti azionabili dal soggetto interessato.

Circolare Unime n. 33 del 29/10/2018 prot. 82783

<<Oggetto: Disposizioni in materia di Protezione dei Dati Personali. Decreto legislativo del 10 agosto 2018 n. 101 e Regolamento (UE) 2016/679>>

Nella circolare sono richiamate e illustrate le principali disposizioni in materia di protezione dei dati personali, disposte sia dal Regolamento Generale Europeo 679/2016 che dal decreto legislativo n. 196/2003, modificato dal decreto legislativo n. 101/2018. Di seguito si elencano i punti trattati nella circolare.

- a) Ambito di applicazione e territoriale (artt.2-3 del RGPD).
- b) Definizione di dati (art. 4 del RGPD)
- c) Definizione di trattamento (art. 4 del RGPD)
- d) Interessato, Titolare, Responsabile e “soggetto incaricato” (art. 4 del RGPD)
- e) Principi del trattamento (art. 5 del RGPD)
- f) Liceità del trattamento (art. 6 del RGPD)
- g) Consenso (art. 6 del RGPD)
- h) Informativa all’interessato (artt. 12- 13-14 RGPD)
- i) Diritti dell’interessato (artt. 15-22 RGPD)
- j) Il principio di Responsabilizzazione (c.d. accoutability)
- k) Protezione fin dalla progettazione e per impostazione predefinita (art. 25 del RGPD)
- l) Registro delle attività di trattamento (art. 30 del RGPD)
- m) Sicurezza del trattamento. (artt. 32 e 33 del RGPD)
- n) Valutazione d'impatto sulla protezione dei dati (art. 35 RGPD).
- o) Responsabile della protezione dei dati (RPD, artt. 37 - 39 del RGPD)
- p) Sanzioni (artt. 83 e 84 RGPD)
- q) Accesso a documenti amministrativi e accesso civico (artt. 59 e 60 del CODICE)
- r) Trattamento di dati relativi a studenti (art. 96 del CODICE)
- s) Trattamento di dati a fini di ricerca. (artt. da 100 a 110-bis del CODICE)
- t) Curriculum (art. 111-bis del CODICE)
- u) Divieto di indagini sui lavoratori (art. 113 del CODICE)
- v) Tutela dell’interessato (artt. da 140-bis a 152del CODICE)
- w) Illeciti penali (artt. da 167 a 172 del CODICE)
- x) Disposizioni transitorie del dlgs 101/2018.

II – Il trattamento e la protezione dei dati personali in Unime

Acquisita la consapevolezza sulla centralità del trattamento e sulla responsabilizzazione della sua gestione l'Università degli Studi di Messina punta a svolgere il processo di *compliance* al RGPD secondo una *strategia* il più possibile strutturata, sistemica e complessiva.

- Si fa riferimento, in particolare, alle disposizioni del CAPO II del RGPD recante i *Principi* e precisamente l'art. 5 (*Principi applicabili al trattamento dei dati personali*); alle disposizioni del CAPO IV del RGPD recante *Disposizioni relative al titolare del trattamento e al responsabile*, e precisamente: l'art.24 (*Responsabilità del Titolare del Trattamento*), l'art. 25 (*Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita*), l'art. 32 (*Sicurezza del Trattamento*) e art. 35 (*Valutazione d'impatto sulla protezione dei dati*) del RGPD; e all'art. 2 - quaterdecies (*Attribuzione di funzioni e compiti a soggetti designati*) del CODICE.

L'intero Ateneo nel suo complesso, quale Titolare del trattamento, è tenuto a *determinare ed eseguire* i trattamenti di dati personali ricompresi nei propri processi organizzativi istituzionali (di didattica, di ricerca, di terza missione basati su o formati da dati personali) mettendo in atto - fin dalla fase di progettazione del trattamento e della determinazione dei mezzi di trattamento (*by design*), *misure di tutela* - non solo tecniche ma anche organizzative, *adeguate* rispetto alle *caratterizzazione del trattamento* e al *livello di rischio*, **per garantire ed essere in grado di dimostrare che il trattamento è conforme al RGPD (e al CODICE).**

Il ciclo di gestione del trattamento, in schema descritto e riassunto nell'all. 2, può essere suddiviso nelle seguenti fasi. Si assume che il trattamento sia necessario e lecito, ovvero sia stata individuata la base giuridica (art. 6).

1. *Caratterizzazione sistematica del trattamento e livello di rischio*: l'Ateneo è tenuto – fin dalla fase di progettazione (*by_design*, art.25) e, quindi, prima della sua esecuzione – ad analizzare il trattamento tenendo conto della natura, dell'ambito, del contesto e delle finalità nonché dei rischi, costituiti dal trattamento, aventi probabilità, gravità e impatti negativi diversi per i diritti e le libertà delle persone fisiche; nonché a prevedere i dati personali oggetto del trattamento, i destinatari e il periodo di conservazione; a determinare la funzione e i mezzi di trattamento;

2. sempre nell'ambito della fase di progettazione, effettuata questa analisi e rilevati i rischi noti o evidenziabili, in caso di rischio ritenuto non elevato, l'Ateneo è tenuto a valutare (autonomamente) e, quindi ad attuare, misure di tutela sia di carattere tecnico che organizzativo, che siano *adeguate* al trattamento e alla mitigazione del rischio e che, come tali, **garantiscono** l'esecuzione del trattamento (punto 3). Alcune misure di tutela sono indicate esplicitamente dal RGPD (ad es. le misure di sicurezza, art.32). In caso di rischio elevato per i diritti e le libertà delle persone fisiche, l'Ateneo, prima di procedere al trattamento, è tenuto ad effettuare una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali (art. 35). In esito della valutazione di impatto l'Ateneo potrà decidere in autonomia se iniziare il trattamento (ritenendo di aver adottato le misure adeguate ad una sufficiente minimizzazione) ovvero consultare il GARANTE per ottenere indicazioni su come gestire il rischio residuale; il GARANTE non interviene per "autorizzare" il trattamento, bensì per indicare misure di tutela ulteriori, complementari o correttive ai sensi dell'art. 58.
3. in coerenza e in ragione alla progettazione e alle valutazioni di cui al punto 2), *nell'esecuzione* l'Ateneo è tenuto ad attuare nel trattamento, in modo efficace e per il tramite delle misure minimizzanti il rischio, i principi applicabili ai dati personali fissati dal RGPD (art. 5: liceità, correttezza e trasparenza; limitazione della finalità del trattamento; minimizzazione dei dati; esattezza; limitazione della conservazione, integrità e riservatezza) evitando, per impostazione predefinita *by_default*, art. 25), l'utilizzo di informazioni o il ricorso ad operazioni non necessarie rispetto alla finalità del trattamento; inoltre, l'Ateneo è tenuto, sempre per il tramite delle misure di tutela, a garantire un livello di sicurezza adeguato al rischio (art. 32); e, in genere, ad integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del RGPD e tutelare i diritti degli interessati.

Per l'Ateneo, quindi, il principio di responsabilizzazione si configura come una vera e propria assunzione di rischio (e della relativa gestione), distinta da una forte autonomia (in ordine alla configurazione della linea strategica da seguire per la gestione del trattamento, la valutazione e l'attuazione delle misure di tutela) ma, al contempo, bilanciata da un altrettanto forte onere di dimostrazione sul perché delle scelte compiute.

Le azioni di seguito descritte oltre a rappresentare le coordinate del piano di attuazione del RGPD e del CODICE si propongono di essere funzionali a tale onere.

Fase I: Priorità e relative azioni (Organizzative e tecniche)

Analizzato il contesto iniziale, il grado di conoscenza, di consapevolezza e di operatività interno all'Ateneo sulle questioni attinenti alla protezione dei dati personali – considerata la necessità di procedere in maniera graduale, sistemica e condivisa alle attività di adeguamento – si individuano le seguenti prioritarie misure/azioni di carattere sia tecnico che organizzativo, ritenute adeguate e concorrenti per la conformità al RGPD e al CODICE.

1. Formazione.

- 1.1 Istruire le risorse che partecipano alla gestione e al trattamento dei dati personali fornendo loro le conoscenze necessarie: a tal fine l'Ateneo ha formulato e attua apposito piano di formazione, di cui al Prot. 49869 del 29 Giugno 2018, che prevede: interventi formativi di carattere trasversale, applicati mediante un percorso di sensibilizzazione sui principi generali della disciplina e rivolto a tutto il personale; e, inoltre, interventi di carattere tecnico-operativo attuati mediante un percorso formativo specifico rivolto a chi accede e svolge attività di trattamento e controllo sui dati personali;
- 1.2 Utilizzare anche il portale di Ateneo come veicolo di in-formazione in argomento RGPD, CODICE, misure e iniziative per la protezione dei dati personali.

Le azioni precedenti concorrono a favorire, incrementare e diffondere la consapevolezza, l'attenzione e l'interesse di tutta la comunità accademica sulla protezione dei dati personali e sulle relative implicazioni.

2. Organizzazione funzionale interna.

- L'Ateneo ha già provveduto alla costituzione di un Gruppo di Lavoro GDPR Privacy¹ e alla nomina del Responsabile della Protezione dei Dati (RPD) la cui designazione, ruolo e compiti sono specificati agli artt. 37-39 del RGPD e richiamati nella delibera di nomina;
- 2.1 sulla base dell'organigramma delle strutture amministrative/didattiche vigente nell'Ateneo, ai sensi dell'art. 2 – quaterdecies del CODICE (*Attribuzione di funzioni e compiti a soggetti designati*), designare per tipologia di struttura, le figure del *Referente Interno del Trattamento* e dell'*Incaricato Istruito del Trattamento*. Entrambi possono essere considerati responsabili interni dello svolgimento del trattamento, si raccordano e sono supportati dal Responsabile della Protezione dei Dati di Ateneo e dal GdL GDPR Privacy, concorrono a configurare un'organizzazione efficiente ed efficace di supporto all'applicazione del RGPD. Il *Referente* è designato dal Rettore o dal Direttore

¹ Il Gruppo di Lavoro è stato istituito con D.D. n.29714 del 17 Aprile 2018 e il Responsabile della Protezione dei dati designato con delibera del CdA del 24 Maggio 2018.

Generale; l'*Incaricato* è designato dal Direttore Generale o dal *Referente Interno del Trattamento*.
L'all.1 descrive il diagramma delle relazioni funzionali, le competenze e i compiti.

- 2.2 applicare la circolare n.24/2018, Prot n. 60258 del 08/08/2018: *Normativa sulla protezione dei dati personali. Invito a raccordarsi con la Responsabile Protezione dei Dati di Ateneo*.

La costante e pro-attiva interazione di tutti gli attori coinvolti è condizione per l'efficace e positiva attuazione di tutte le rimanenti azioni.

3. Gestione e misura del rischio.

- 3.1 definire e utilizzare un sistema/criteri metodologici di supporto alla valutazione delle misure (sia di carattere tecnico e organizzativo, adeguate al rischio e alla relativa gestione) che preveda la gestione e la misurazione (anche quantitativa) del rischio, incrociando: i requisiti di conformità al RGPD, le misure previste (in generale) per il rispetto di questi requisiti, i fattori di rischio che ne ostacolano il rispetto; l'impatto negativo del trattamento. Prevedere riesame e aggiornamento dei criteri.
- per la definizione di questo sistema possono essere considerate: la linea guida WP 248 del Comitato Europeo: *Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679* e le indicazioni interpretative prodotte, in argomento, dal GARANTE: *Valutazione d'impatto sulla protezione dei dati - Individuazione e gestione del rischio, Ultimo aggiornamento 27 aprile 2018, Doc-Web: 8581408*.

4. Gestione ed esecuzione del trattamento.

Metodo e applicazione della protezione fin dalla progettazione per impostazione predefinita.

- 4.1 procedere alla mappatura dei trattamenti negli ambiti di didattica, ricerca, terza missione e servizi trasversali di supporto (ivi inclusi quelli formati da categorie particolari di dati e/o da dati personali relativi a condanne penali e reati; e i trattamenti di dati personali verso paesi terzi o organizzazioni internazionali), anche mediante l'utilizzo delle Linee Guida Codau² e considerando le procedure, i procedimenti e i processi in essere, assegnati alle singole strutture, nei quali i trattamenti possono essere ricompresi;
- 4.2 progettare ed eseguire il trattamento utilizzando il metodo illustrato nel precedente paragrafo II – *Il trattamento e la protezione dei dati personali in Unime* e riprodotto in schema

² Linee Guida in materia di Privacy e Protezione dei dati personali in ambito Universitario, versione 1.1 del Novembre 2017, esitate dal Gruppo di Lavoro CODAU nell'ambito dell'omonimo progetto al quale l'Università degli Studi di Messina ha operativamente partecipato insieme al Politecnico di Milano e alle Università Statale e Bicocca di Milano, di Bologna e di Firenze.
http://www.codau.it/sites/default/files/verbali/all_3_lineeguida_privacy_gdpr_ravera.pdf

nell'all. 2. Riesaminare il trattamento se necessario. L'attuazione del precedente punto 3.1 è propedeutica all'attuazione della presente azione;

- 4.3 per la gestione del trattamento a fini statistici o di ricerca scientifica riferirsi alle disposizioni degli artt. 105 (*Modalità di Trattamento*), 106 (*Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica*) e 110 (*Ricerca medica, biomedica ed epidemiologica*) del CODICE e considerare sempre l'impiego della valutazione di impatto tenuto conto dell'ampiezza, della potenziale invasività, dell'ri-utilizzo massivo di dati con l'impiego di nuove tecnologie; nonché dell'utilizzo di categorie particolari di dati personali o della ricorrenza di una o più specifiche indicate nel WP 248: *Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679.*

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

In conformità alle linee guida emanate o che saranno emanate dal GARANTE o dal Comitato Europeo, è necessario procedere, prevedendo nel tempo riesame e eventuale aggiornamento:

- 5.1 alla redazione delle informative ai sensi degli artt. 12-14, utilizzando il modello incluso nell'allegato 3; e alla prestazione del consenso (laddove configurante la liceità del trattamento);
- 5.2 alla revisione/adeguamento degli atti (es. delibere, bandi, o altri atti includenti o formati da dati personali) e della modulistica (sia interna che esterna);
- 5.3 alla corretta e conforme configurazione, rispetto al RGPD, di tutti i servizi Unime che utilizzano piattaforme sociali di Titolari non stabiliti nell'Unione ma che offrono servizi e prodotti all'interno del mercato europeo (ad esempio: *Google Inc., Facebook Inc., Dropbox Inc.; Twitter Inc.*);
- 5.4 in coerenza al precedente punto 3.1, alla ricognizione, alla verifica e all'eventuale integrazione e miglioramento delle misure tecniche e organizzative, già in uso nell'Ateneo con particolare riferimento a quelle connesse alla sicurezza del trattamento (art.32);
- 5.5 alla implementazione, validazione e tenuta del registro delle attività di trattamento del Titolare, anche in forma precompilata e sulla base del modello incluso nell'allegato 4. La definizione dei vocabolari semantici relativi ai campi previsti del RGPD (dominio delle finalità, dei dati personali, dei destinatari, delle attività di trattamento,...) è propedeutica allo svolgimento di questo punto;
- 5.6 alla tenuta del registro delle violazioni, sulla base del modello incluso nell'allegato 5;
- 5.8 alla definizione e utilizzo di una procedura di notifica e comunicazione delle violazioni (Data Breach).

6. Controllo sull'affidamento del trattamento a Responsabili (esterni) (Es. Cineca) e fornitori di servizi. Contratto/atto giuridico e RGPD.

- 6.1 Redigere e mantenere un elenco dei Responsabili esterni del trattamento (il cui ruolo, funzioni e i rapporti con l'Ateneo sono definiti all'art. 28 del RGPD);
- 6.2 predisporre e aggiornare nel tempo i relativi contratti ai sensi del suddetto articolo; considerati i trattamenti effettuati dal Responsabile per conto del Titolare, prevedere specificazioni contrattuali in ordine alla migliore configurazione delle misure tecniche e organizzative, richieste al Responsabile del trattamento e da questi attuate, adeguate per garantire la conformità al RGPD e la tutela dell'interessato; ciò, in particolare ma non solo, per quel che concerne: a) il livello di sicurezza adeguato al rischio derivante dalla possibile violazione dei dati personali accidentale o illecita (art. 4 del RGPD); b) l'attuazione, da parte del Responsabile del trattamento, delle metodologie di *data protection by design by default*; c) nell'ambito delle informazioni necessarie per dimostrare la conformità al RGPD, quelle concorrenti all'analisi e alla gestione del rischio, delle eventuali violazioni dei dati personali e - per i trattamenti compiuti con processi automatizzati - quelle attinenti lo schema applicato nei sistemi informativi utilizzati (persistenza delle informazioni, algoritmi e *business logic*);
- 6.3 prevedere clausole di salvaguardia con riguardo alla fattispecie sanzionatoria o risarcitoria per danni reclamati dai soggetti interessati;
- 6.4 considerare i precedenti punti anche per i fornitori di servizi, prevedendo il requisito di conformità al RGPD nella gestione della gara, nonché esplicita specifica nei capitolati d'appalto.

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

- 7.1 Aggiornare e/o modificare i regolamenti vigenti per l'utilizzo dei servizi e delle risorse ICT di Ateneo;
- 7.2 anche in previsione della possibile formulazione di codici di condotta del comparto universitario, redigere con riguardo agli ambiti istituzionali dell'Ateneo, propri Regolamenti e/o linee guida con riferimento alle specifiche dell'art.40 comma 2 lettere a), c), d) e), f), h), i), j), k); prioritariamente, precisare l'applicazione del RGPD in merito a: a) comunicazione e diffusione di dati personali (ex. Art.2-ter del CODICE), anche con riguardo al bilanciamento del diritto alla protezione dei dati con il principio della trasparenza e il diritto di accesso per quel che attiene, in particolare, alle informazioni pubblicate sul Web mediante il Portale di Ateneo; b) in argomento protezione dei dati fin dalla progettazione e per impostazione predefinita all'attuazione in Ateneo del principio di minimizzazione e limitazione della conservazione (*Policy di Data Quality: Data Minimisation e Data Retention*); c) esercizio dei diritti degli interessati.

Interventi di mantenimento - Azioni di revisione e miglioramento

Il piano è stato articolato per configurare le azioni e le priorità di intervento affinché non solo rispondano a esigenze puntuali e immediate di adeguamento, ma che – nel contesto di un’analisi preventiva e delle misure di tutela che da questa derivano – tali azioni possano concretizzarsi in una serie di attività specifiche e dimostrabili, riesaminate e aggiornate nell’ottica di un miglioramento continuo; ed inoltre, che tali attività possano concorrere ad affiancare all’osservanza delle regole l’attuazione e la dimostrazione di un approccio volto a valorizzare l’*adempimento*, integrandolo della necessaria flessibilità affinché, in coerenza con i processi organizzativi già in essere, diventi una *misura/azione* dinamica al variare delle caratteristiche del trattamento e del suo possibile grado di rischiosità.

La durata del piano è di 18 mesi (dall’approvazione) con verifiche interne trimestrali, riportate alla *Governance* di Ateneo dal Responsabile della Protezione dei Dati e dal Gruppo di Lavoro, in ordine agli esiti prodotti dall’attuazione dei punti indicati al precedente paragrafo, all’osservanza interna del Regolamento e alla conformità dei trattamenti al RGPD e al CODICE. Trascorsi i 18 mesi e in continuità il piano dovrà essere aggiornato e/o riformulato in coerenza all’attività di riesame e allo stato di attuazione.

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

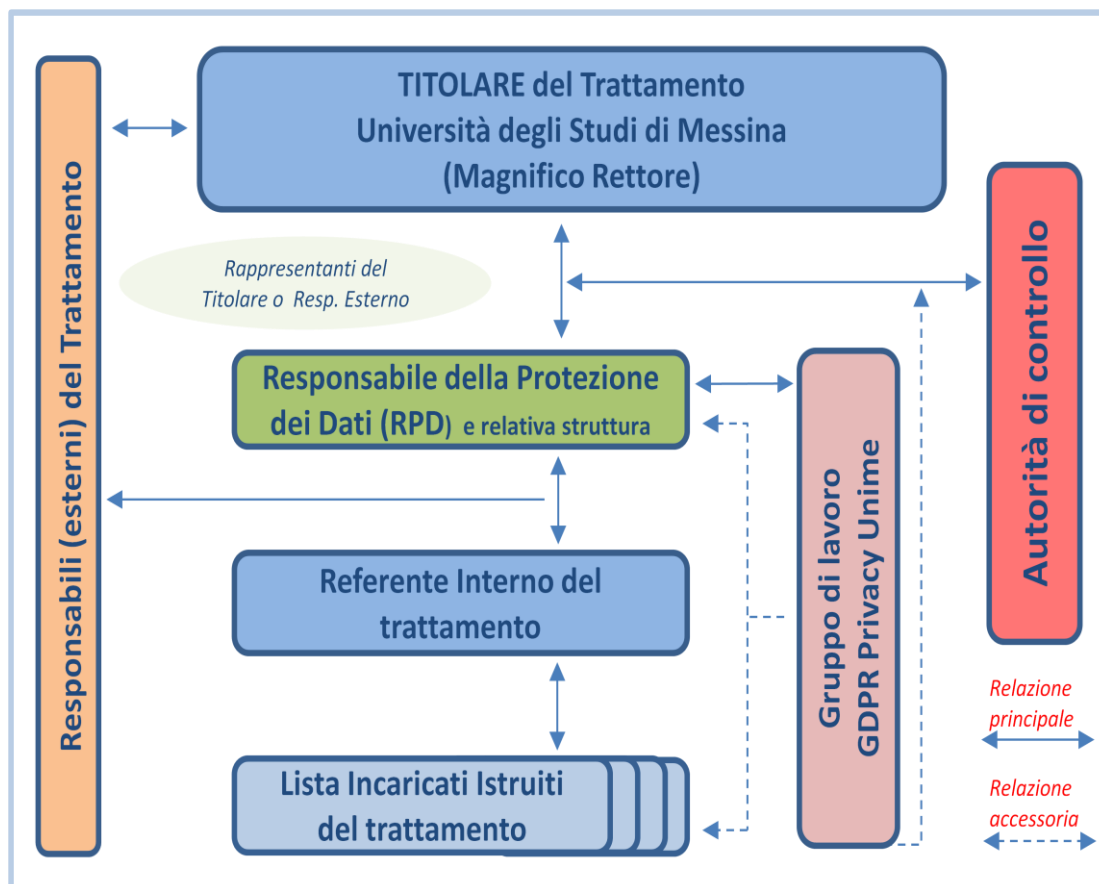
In itinere agli esiti del piano e del suo monitoraggio, l’Ateneo si riserva di valutare l’utilizzo di un sistema dedicato all’applicazione del RGPD per, ricorrendone le condizioni, agevolare tutti i soggetti coinvolti nello svolgimento del processo di *compliance*.

La diffusione e l’informazione sullo svolgimento del presente piano avvengono anche tramite l’aggiornamento periodico della sezione *privacy* di Ateneo (<http://www.unime.it/it/ateneo/privacy>).

PIANO UNIME Applicazione Regolamento Generale Protezione Dati Personali n.679/2016 e "Nuovo" Codice D.Lgs. 196/2003 e 101/2018																		
GANTT	18 Mesi																	
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Formazione	1.1 attuazione e aggiornamento piano Privacy																	
	1.2 In-formazione tramite portale di Ateneo																	
Organigramma	Designazioni						RPD											
Gestione e misura del rischio	3.1 Definizione Criteri						3.1 Utilizzo											
													3.1 Riesame e aggiornamento criteri					
Gestione ed esecuzione del trattamento	4.1 Mappatura																	
	4.2 Progettazione																	
	4.2 Esecuzione ed eventuale riesame																	
Informativa e misure di tutela	5.1 Informativa																	
	5.2 adeguamento doc. amm.vi																	
	5.3 conformità trattamenti piattaforme social																	
	5.4 Ricognizione e Verifica misure di tutela																	
	5.4 Integrazione e miglioramento																	
	5.4 Riesame e Aggiornamento misure di tutela																	
	5.5 Implementazione e validazione Registro attività trattamento																	
	5.5 tenuta Registro attività del trattamento																	
																5.5 Riesame e aggior. modello		
	5.6 Tenuta del registro delle violazioni																	
5.7 Definizione proc. Data Breach																		
5.7 Utilizzo Procedura Data Breach																		
												5.7 Riesame e aggior. proc. Data Breach						
Controllo affidamento Resp.	6.1 Ricognizione Resp. Tratt																	
	6.2 6.3 6.4 - Nomina Responsabili (esterni) del Trattamento																	
													6 Riesame e aggiornamento nomine					
Regolamenti Interni	7.1 Aggiornamento regolamenti vigenti																	
	7.2 Stesura nuovi regolamenti																	

Allegato 1

Organigramma funzionale di Ateneo a supporto dell'attuazione del piano
Rev. 1.1. del 26 Luglio 2018



Principio di responsabilizzazione e Organizzazione interna
Diagramma funzionale: Referenti e Incaricati Istruiti del Trattamento di Dati Personali

Legenda	<p>Responsabile (Esterno) del Trattamento (ad esempio, Cineca): così come definito dall'art. 28 del RGPD.</p>	<p>1) Referente Interno del trattamento di dati personali: Designazione del Rettore o Direttore Generale presso: Dipartimenti; Direzione Generale; Dipartimenti Amministrativi; Centri autonomi e non; SBA; SIR</p>
	<p>Responsabile della Protezione dei dati: così come definito degli art. 37, 38, 39 del RGPD e relativa struttura.</p>	<p>2) Incaricato Istruito del trattamento di dati personali: Designazione del Direttore Generale o del Referente Interno del Trattamento presso le strutture di supporto (didattiche o amministrative) di: Dipartimenti; Segreterie Generali e/o, Unità Organizzative e/o Unità Operative della Direzione Generale e delle Unità Speciali; dei Dip. Amm.vi; dei Centri; di SBA e SIR.</p>
<p>N.B il presente diagramma non complementa ne si sovrappone al vigente organigramma delle strutture di Ateneo, ma ad esso si aggancia per il tramite della designazione.</p>		

Competenze e compiti del Referente Interno

longa manus del Titolare del trattamento; non sostituisce il Titolare ma ne agevola l'applicazione e l'attuazione del principio di responsabilizzazione nelle varie strutture dell'Ateneo. Il Referente, avvalendosi del supporto del Responsabile Protezione dei Dati e del Gruppo di Lavoro GDPR Privacy di Ateneo concorre, per la struttura di afferenza, all'analisi del trattamento, all'analisi del rischio e alla relativa misurazione; all'attuazione delle misure adeguate; alla valutazione d'impatto se necessaria; alla progettazione del trattamento; al riesame del trattamento e delle misure di tutela. I compiti potranno essere specificati nel decreto di designazione. **Ruolo compatibile:** responsabili apicali delle strutture elencate in 1); ad ogni struttura corrisponde un solo Referente Interno del Trattamento.

Competenze e compiti dell'Incaricato:

è la risorsa che conosce le attività di trattamento, le esegue in maniera operativa, è autorizzato ad accedere ai dati personali dei soggetti interessati, svolge le attività di trattamento in maniera costante e distinguibile rispetto ad altri ruoli o responsabilità. L'incaricato, avvalendosi del supporto del Responsabile Protezione dei Dati e del Gruppo di Lavoro GDPR Privacy di Ateneo e del Referente, concorre, per la struttura di afferenza, alla progettazione e all'esecuzione del trattamento. I compiti potranno essere specificati nel decreto di designazione. **Ruolo compatibile:** risorse afferenti alle strutture di cui al punto 2)

Esempi di compiti

- **Informativa:** il Referente concorre alla formulazione dell'informativa e alla valorizzazione dei relativi campi, l'Incaricato ne cura l'utilizzo agganciandola, ove necessario, a bandi e/o moduli di raccolta dati e ad altri canali di diffusione;
- **Registro attività di Trattamento:** il Referente concorre alla progettazione e alla compilazione del Registro, l'Incaricato partecipa alla progettazione e ne cura l'aggiornamento e la tenuta;
- **Gestione delle violazioni:** l'Incaricato rileva una violazione, entrambi - Incaricato e Referente - valutano la probabilità di rischio, il Referente provvede alla notifica al GARANTE e/o alla comunicazione all'Interessato, l'Incaricato annota la violazione aggiornando il registro delle violazioni.

N.B. Per articolazione di struttura e tipologia dei trattamenti ad ogni Referente Interno del trattamento potrebbero corrispondere anche più Incaricati Istruiti senza prefissate precedenze di carattere gerarchico; i criteri di individuazione dell'Incaricato sono sostanziali, quindi, come tali, consistono nella non duplicazione del ruolo (per esempio la nomina dell'incaricato istruito non dovrebbe riguardare contemporaneamente Resp. e Vice-resp. di una struttura) e soprattutto nella effettiva competenza e operativa partecipazione al trattamento (che potrebbe incrociare gli specifici compiti di una risorsa incardinata, per esempio, in una Unità Operativa e non contestualmente o necessariamente nel responsabile gerarchico della struttura superiore). Nell'individuazione degli Incaricati Istruiti del trattamento, quindi, ciò che "guida" è il trattamento e le effettive competenze rispetto all'esecuzione delle operazioni/attività che lo compongono e non il ruolo e la relazione gerarchica della risorsa.

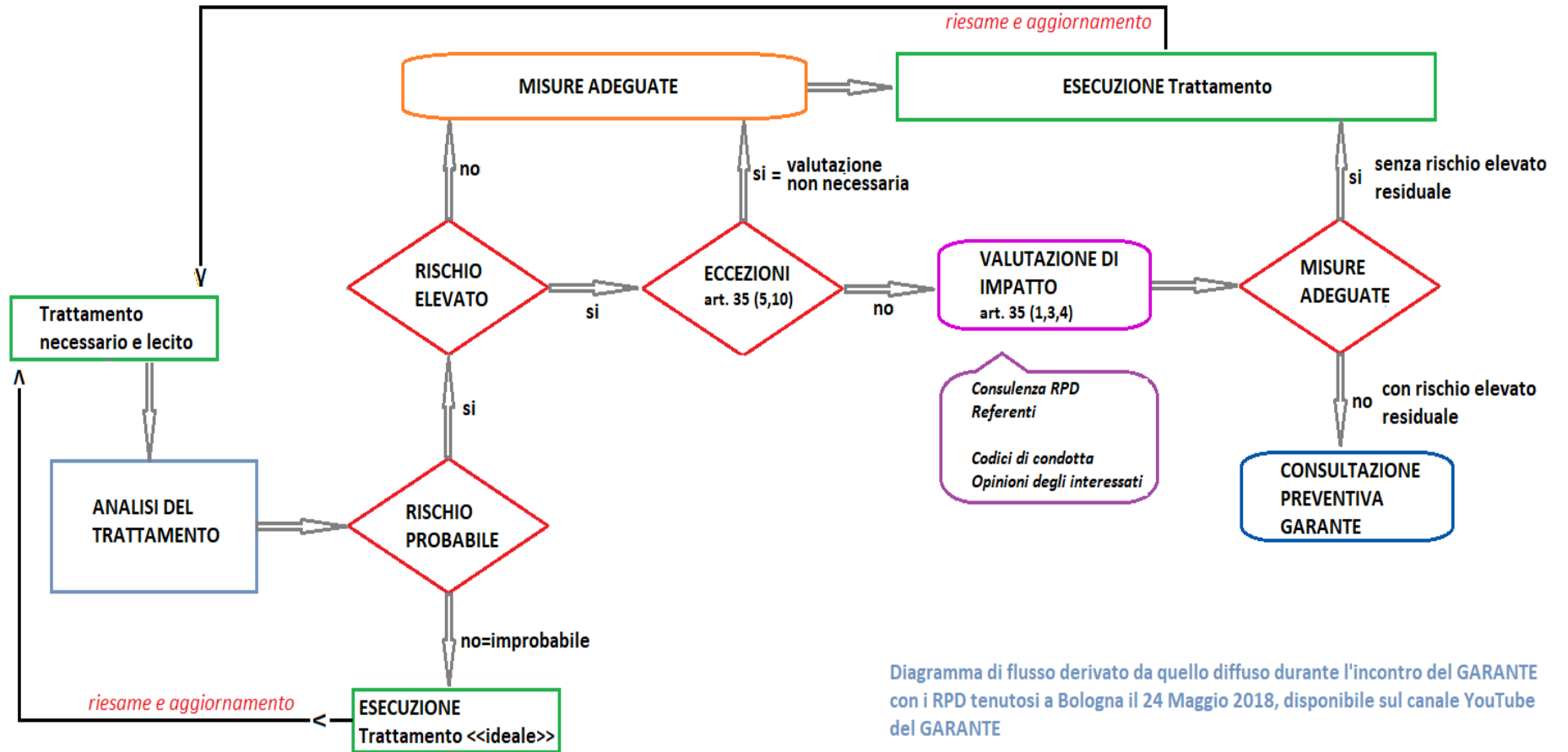


Diagramma di flusso derivato da quello diffuso durante l'incontro del GARANTE con i RPD tenutosi a Bologna il 24 Maggio 2018, disponibile sul canale YouTube del GARANTE



Contesto e natura del Trattamento

La presente informativa attiene il trattamento di [1], effettuato dall'Ateneo nell'ambito dello svolgimento della propria missione istituzionale. [2], ed è rivolta a coloro che, quali Soggetti Interessati, si relazionano con l'Università degli Studi di Messina per [3].

Oggetto/Ambito di applicazione del Trattamento

In particolare, i dati personali oggetto del trattamento, che identificano o possono identificare il Soggetto Interessato, sono: [4].

Corre l'obbligo di fornire i dati richiesti? No, il conferimento è facoltativo; l'assenza [5] l'impossibilità di fruire del servizio richiesto. Il Soggetto Interessato può esercitare il controllo sul trattamento dei propri dati personali trattati azionando i diritti indicati nella presente informativa.

Sono trattati ulteriori dati oltre quelli già indicati? [6].

I Soggetti del Trattamento

Titolare del trattamento: Università degli Studi di Messina
Plesso Centrale dell'Ateneo - Piazza Pugliatti 1, 98122 Messina

Telefono: 0906768900

Email: rettorato@unime.it;

PEC: protocollo@pec.unime.it

Responsabile della protezione dei dati (RPD) dell'Ateneo:

Telefono: 0906768355

Email: rpd@unime.it;

PEC: protezionedati@pec.unime.it

Responsabile del Trattamento: [7]

Inoltre, il *referente interno del trattamento* è/sono: [8]

Destinatari

L'Ateneo informa che i dati personali trattati potranno essere comunicati anche a: [9]

Base giuridica

Il trattamento descritto nella presente informativa è collegabile al [10].

Il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o perché connesso all'esercizio di pubblici poteri di cui è investito l'Ateneo, risultando, quindi, un trattamento lecito ai sensi dell'art. 6 comma 1 lettera e) del RGPD.

L'Università degli Studi di Messina, nella qualità di Titolare, assicura che i dati personali sono trattati secondo quanto

indicato dall'art. 5 del RGPD: in modo lecito, corretto e trasparente; per finalità determinate, esplicite e legittime; nel rispetto dei principi di qualità dei dati (minimizzazione, esattezza e limitazione della conservazione), e dei requisiti di sicurezza di cui all'art. 32 del RGPD (integrità e riservatezza; disponibilità e resilienza dei sistemi).

Finalità del trattamento – Per quale scopo, i dati personali raccolti, sono trattati? [11]

Caratteristiche e modalità del trattamento – Quali sono i mezzi e gli strumenti, le operazioni e le attività di trattamento? [12]

Trattamenti non effettuati sui dati personali raccolti

L'Ateneo ti informa che: non utilizza né si avvale di strumenti e servizi di *data analytics* esposti dalle piattaforme social o dai motori di ricerca; non effettua trattamenti di profilazione commerciale; e che non intende trasferire i dati raccolti ad un destinatario in un paese terzo o a un'organizzazione internazionale [13]

Periodo di conservazione - Per quanto tempo, i dati personali trattati, sono conservati presso l'Ateneo? [14]

Misure di tutela [15]

Diritti dell'interessato

Il soggetto interessato può azionare il controllo sulle proprie informazioni esercitando i diritti dichiarati al CAPO III del RGPD: di informazione e accesso (artt.12-15) ottenendone origine, finalità, copia, destinazione dei dati e base giuridica; potendone chiedere la rettifica (artt.16,19) e/o la cancellazione (artt.17, 19), la limitazione di trattamento (artt.18, 19) o l'esistenza di un processo decisionale automatizzato (art. 22).

Il Soggetto Interessato, in qualsiasi momento, può opporsi al trattamento (art. 21), revocare il consenso (senza tuttavia pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca, art. 7).

Inoltre può proporre reclamo all'Autorità di Controllo (art.15).

L'Autorità di Controllo nazionale italiana in materia di protezione dei dati personali è Il Garante per la protezione dei dati personali (Garante Privacy, <http://www.garanteprivacy.it>).

Per azionare i propri diritti l'Interessato può contattare il Titolare o il Responsabile della Protezione dei Dati ai punti di contatto che precedono.

Per Informazioni e aggiornamenti in argomento privacy, e per consultare le altre informative rese dall'Ateneo, è possibile consultare la sezione privacy che L'Università di Messina dedica all'argomento: <http://www.unime.it/privacy>

- [1] inserire categorizzazione dei dati personali;
- [2] se possibile specificare: didattica, ricerca, terza missione; amministrazione dei processi; informazione e comunicazione
- [3] nominare il/i servizio/i nel/i quale/i si contestualizza il trattamento
- [4] inserire elenco specificando se raccolti presso l'interessato o altra fonte. Se sono trattati dati personali rientranti in categorie particolari (art. 9 RGPD, es. dati relativi alla salute, o che rivelino l'origine razziale o etnica....) specificarne la base giuridica rispetto alle eccezioni
- [5] comporta/può comportare
- [6] valorizzare questa sezione nel caso in cui al trattamento, analizzato nel suo complesso, concorrono o sono coinvolti altri dati personali, accessori o trasversali, rispetto a quelli primari già specificati; tipico esempio: il caso di servizi amministrativi dematerializzati, in cui alla raccolta esplicita di dati anagrafici del Soggetto Interessato si affiancano identificativi di connettività per operazioni di logging di sistema o applicativo
- [7] se necessario, inserire la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, sulla base di un contratto o atto giuridico, tratta i dati per conto del titolare; es. Cineca
- [8] secondo l'attuazione del piano + organigramma privacy di Ateneo specificare il ruolo/i rispetto alla fase di trattamento
- [9] inserire la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che riceve comunicazione dei dati personali; non occorre inserire le Autorità Pubbliche alle quali i dati personali sono comunicati per obbligo legale o per consentirne l'esercizio della loro missione istituzionale
- [10] inserire e nominare il principale o più recente riferimento normativo
- [11] anche considerati i riferimenti normativi di cui alla precedente sezione, inserire il fine/obiettivo del trattamento non le modalità/operazioni/mezzi]. Esempi: Gestione selezioni di accesso all'Ateneo; Gestione amministrativa della carriera; Miglioramento e semplificazione dei Servizi e dei Processi (on-line, verso l'utenza interna ed esterna); Divulgazione e promozione; Orientamento;...;
- [12] considerato il flusso dei dati, in questa sezione deve essere descritto il trattamento e le sue fasi procedurali principali, descrivendo sinteticamente e con semplicità: a) le operazioni di trattamento secondo le specifiche dell'art. 4 comma 2, e, per ognuna di esse, il mezzo o il canale utilizzato; b) il flusso dei dati in termini di processo e procedure; c) la tipologia di sistemi interni all'Ateneo e, se utilizzati, anche quelli esterni (es. Cineca; Cloud, Social) inclusi eventuali strumenti di Data Analytics; d) la natura della divulgazione web/intranet Unime/interna;
- [13] se necessario variare questa impostazione di default.
- [14] specificare periodo e/o politica di conservazione, tenendo in considerazione i termini di massimario e scarto già applicati, i vincoli archivistici anche di natura storica; le tempistiche connesse all'applicazione del principio di trasparenza; se, eventualmente, l'Ateneo è configurabile come Service Provider]
- [15] con riferimento al trattamento a cui si riferisce l'informativa, indicare sommariamente le principali misure di tutela, rispetto, ad esempio, al mantenimento dei requisiti di sicurezza (integrità, riservatezza, la disponibilità e l'accesso) al fine di minimizzare il rischio derivante da accesso/divulgazione/modifica non autorizzata; perdita/distruzione dei dati comunque trattati.

Allegato 4

Registro (unico) delle attività di Trattamento Rev. 1.1 del 12 Luglio 2018

Art.30_RegistroAttivitàTrattamento_Titolare_Unime - Copia.xlsx - Excel

Info_Accessorie		Info_Accessorie								
Informazioni identificative del trattamento				Art. 30 1, a)			Art. 30 1, b)		Art. 30 2, b)	
ID_Treatmento	Riferimento	Validatore	Struttura	Titolare Trattamento	Responsabile Trattamento	Rappresentante	Finalità del trattamento	Categorie del trattamento	Descrizione e attività del trattamento	
//identificativo univoco del trattamento	// risorsa autorizzata a compilare il registro.	// risorsa autorizzata a validare il registro.	//collocazione amministrativa del trattamento.	//campi da valorizzare solo per i trattamenti eccezione rispetto alle informazioni inserite nel primo foglio.			//perché e per quale scopo i dati personali sono processati	// rispetto alla finalità, cosa si pone in essere per processare i dati personali oggetto di trattamento; come si utilizzano i mezzi fissati dal titolare in termini di attività e operazioni di trattamento		

Art.30_RegistroAttivitàTrattamento_Titolare_Unime - Copia.xlsx - Excel

Art. 30 1, c)		Art. 30 1, d)		Art. 30 1,e; Art. 44-46; 48-50		Art. 30 1, f)		Art. 30 1, g)	
Categorie dati personali	Categorie interessati	Categorie destinatari	Trasferimenti dati personali Paesi Terzi	Condizioni di Liceità		Termini di cancellazione	Criteria	Analisi dei rischi	Misure di sicurezza
//raggruppare i dati personali oggetto di trattamento	// raggruppare i soggetti identificati o identificabili dai dati personali	// raggruppare i soggetti che ricevono comunicazione dei dati (pur senza trattarli).	//...	//...		// indicare il termine di cancellazione.	// indicare modalità e periodo di conservazione e i relativi criteri (opzionale).	// segnalare indicatore quantitativo di rischio	//tecniche e organizzative

Allegato 5

Registro delle violazioni (Data Breach) Rev. 1.1 del 13 ottobre 2018

Accadimento e durata					Interessato									
Compromissione (Presunta)		Rilevazione e Diagnosi Blocco e Segnalazione			Ultimo accesso lecito, Ante Violazione (presunto)		Soggetto		Struttura di afferenza / Incarico		Contatti			
Data	Data	Ora	Tramite	Data	Tit.	Nome	Cognome	Matr.	Struttura/Unime/AOU	Ruolo/Incarico	@unime.it	@unime.it	@altro	tel.

Categorie Dati Pesonali (violati)			Violazione e Circostanze		Conseguenze		Rischio		Misure di tutela		Azioni e Provvedimenti	
Comuni	Riservati	Particolari	Descrizione con indicazione Sorgente violazione	Descrizione	Descrizione	Livello	Di sicurezza, Tecniche e Organizzative	Descrizione	Descrizione e gestione della violazione; Notifica e Comunicazione con inserimento di data e ora			