UNIVERSITÀ TELEMATICA
GIUSTINO FORTUNATO

REGOLAMENTO DI ATENEO PER LA PROTEZIONE DEI DATI PERSONALI

in attuazione del Regolamento UE 2016/679

"Regolamento generale per la protezione dei dati"

emanato con D.P. n. 15 del 2 maggio 2019

INDICE

ALLEGATO 1
Disciplinare per il trattamento dei dati senza l'ausilio di strumenti elettronici

ALLEGATO 2
Disciplinare per l'utilizzo della strumentazione informatica e della rete internet

CAPO I
DISPOSIZIONI GENERALI E PRINCIPI

Articolo 1
OGGETTO DEL REGOLAMENTO

1. Il presente Regolamento disciplina le misure procedimentali e le regole di dettaglio ai fini della migliore funzionalità ed efficacia dell'attuazione del Regolamento Europeo n. 679 del 27 aprile 2016 "Regolamento generale sulla protezione dei dati" (RGPD), relativo alla protezione delle persone fisiche con riguardo ai trattamenti dei dati personali nonché alla libera circolazione di tali dati.
2. Per quanto non previsto nel presente regolamento si rinvia al predetto Regolamento europeo 2016/679, alle vigenti fonti di diritto europee e nazionali in materia di protezione dei dati personali, alle linee guida e ai provvedimenti del "Gruppo di Lavoro 29" nonché del Garante della Privacy, alle direttive impartite dal Titolare del trattamento, dai Responsabili del trattamento, dall'Amministratore del sistema informatico e dal Responsabile della protezione dei dati.

Articolo 2
DEFINIZIONI
(artt. 4, 9, 10 RGPD)

1. Ai fini del presente regolamento si intende per:
   a) «**Ateneo**»: l'Università Telematica Giustino Fortunato, nella qualità il titolare del trattamento dei dati personali;
   b) «**Garante**»: l'Autorità di controllo ossia il Garante della Privacy;
   c) «**RGPD** o **REG. UE 2016/679**»: il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 "Regolamento generale sulla protezione dei dati";
   d) «**Codice**»: il d.lgs. 30 giugno 2003, n. 196 "Codice in materia di protezione di dati personali";
   e) «**dato personale**»: qualsiasi informazione riguardante una persona fisica identificata o identificabile. Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale; (**C26, C27, C30**)
   f) «**dati sensibili**»: i dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, dati genetici, dati biometrici, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona; (**C51)**
   g) «**dati giudiziari**»: i dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza;
   h) «**dati genetici**»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o

sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione; (**C34**)

i) «**dati biometrici**»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici; (**C51**)

j) «**dati relativi alla salute**»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute; (**C35**)

k) «**interessato**»: la persona fisica titolare dei dati personali oggetto di trattamento;

l) «**trattamento**»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

m) «**limitazione di trattamento**»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro; (**C67**)

n) «**profilazione**»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica; (**C24, C30, C71-C72**)

o) «**pseudonimizzazione**»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile; (**C26, C28-C29**)

p) «**archivio**»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico; (**C15**)

q) «**titolare del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri; (**C74**)

r) «**contitolari del trattamento**»: due o più titolari del trattamento che determinano congiuntamente, mediante un accordo interno, le finalità e i mezzi del trattamento;

s) «**responsabile del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

t) «**sub-responsabile del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali a cui fa ricorso il responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento;

u) «**autorizzato del trattamento**»: chiunque, agendo sotto l'autorità del responsabile del trattamento o del titolare del trattamento, abbia accesso a dati personali essendo stato autorizzato al loro trattamento;
l) «**responsabile della protezione dei dati**»: la persona fisica o giuridica estranea all'organizzazione del titolare o del responsabile del trattamento che svolge i compiti di cui all'art. 39 del REG. UE 2016/679 o ulteriori compiti affidati dal titolare del trattamento sulla base di un contratto di servizi;
m) «**amministratore del sistema**»: la figura professionale finalizzata alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti, nonché all'amministrazione di basi di dati, di reti e di apparati di sicurezza e di sistemi *software* complessi.
n) «**terzo**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile del trattamento;
o) «**destinatario**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento; (**C31**)
p) «**consenso dell'interessato**»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento; (**C32, C33**)
q) «**violazione dei dati personali**»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati; (**C85**)
r) «**Unione**»: l'Unione Europea;
s) «**Stato**»: lo Stato italiano.

3. Per le definizioni non riportate nel precedente comma si rinvia all'elenco definizioni previste dall'art. 4 del RGPD.

Articolo 3
FINALITÀ DEL TRATTAMENTO
(art. 3 RGPD)

1. I trattamenti dei dati personali sono eseguiti dall'Ateneo per le seguenti finalità:
   a) l'adempimento di un obbligo legale alla quale è soggetto l'Ateneo;
   b) l'esecuzione di un contratto con riguardo ai soggetti interessati;
   c) per specifiche finalità diverse da quelle di cui ai precedenti punti, purché l'interessato esprima il consenso al trattamento.

Articolo 4
PRINCIPI APPLICABILI AL TRATTAMENTO
(art. 5 – C39, C74 - RGPD)

1. I dati personali sono trattati nel rispetto dei principi di: (C39)
   a) «**liceità, correttezza e trasparenza**»: i dati personali sono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
   b) «**limitazione delle finalità»**: i dati personali sono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'art. 89, prf. 1 del RGDP, considerato incompatibile con le finalità iniziali;
   c) «**minimizzazione dei dati»**: i dati personali sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
   d) «**esattezza**»: i dati personali sono esatti e, se necessario, aggiornati; sono adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;
   e) «**limitazione della conservazione**»: i dati personali sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'art. 89, prf. 1 del RGPD, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato;
   f) «**integrità e riservatezza**»: i dati personali sono trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali;
   g) «**responsabilizzazione**»: il titolare del trattamento è competente per il rispetto dei principi di cui al comma 1 e deve essere in grado di comprovarlo. (C74)
2. Nelle ipotesi in cui disposizioni legislative, regolamentari o statutarie prevedano pubblicazioni obbligatorie, il responsabile del procedimento adotta le opportune misure atte a garantire la riservatezza dei dati personali a norma del RGPD, del "Codice della privacy" di cui al d.lgs. 30 giugno 2003.n. 196, del "Codice della trasparenza" di cui al d.lgs. 14 marzo 2013, n. 33 e dei provvedimenti del Garante della Privacy.

Articolo 5
LICEITÀ DEL TRATTAMENTO
(art. 6 – C40→C46 - RGPD)

1. Il trattamento dei dati personali effettuato dall'Ateneo é lecito soltanto per lo svolgimento le proprie funzioni e se:

a) l'interessato ha espresso il consenso al trattamento dei suoi dati personali per una o più specifiche finalità;
b) il trattamento é necessario all'esecuzione di un contratto di cui l'interessato é parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso interessato;
c) il trattamento é necessario per adempiere un obbligo legale alla quale é soggetto questo Ateneo;
d) il trattamento é necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica, se non trova applicazione alcuna delle altre predette condizioni;

2. La base su cui si fonda il trattamento dei dati di cui alle lettere c) del comma 1 deve essere stabilita dal diritto dell'Unione o dello Stato.
3. La finalità del trattamento è determinata in tale base giuridica; la stessa potrebbe contenere disposizioni specifiche per adeguare l'applicazione delle norme del RGPD, tra cui: le condizioni generali relative alla liceità del trattamento da parte del titolare del trattamento; le tipologie di dati oggetto del trattamento; gli interessati; i soggetti cui possono essere comunicati i dati personali e le finalità per cui sono comunicati; le limitazioni della finalità, i periodi di conservazione e le operazioni e procedure di trattamento, comprese le misure atte a garantire un trattamento lecito e corretto, quali quelle per altre specifiche situazioni di trattamento di cui al capo IX dello stesso RGPD. Il diritto dell'Unione o degli Stati membri persegue un obiettivo di interesse pubblico ed è proporzionato all'obiettivo legittimo perseguito.
4. Laddove il trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti non sia basato sul consenso dell'interessato o su un atto legislativo dell'Unione o dello Stato che costituisca una misura necessaria e proporzionata in una società democratica per la salvaguardia degli obiettivi di cui all'articolo 23, paragrafo 1, del RGPD al fine di verificare se il trattamento per un'altra finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il titolare del trattamento tiene conto, tra l'altro: (**C50**)
   a) di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto;
   b) del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il titolare del trattamento;
   c) della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'articolo 9 del RGPD, oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell'articolo 10 del RGPD;
   d) delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati;
   e) dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione.

Articolo 6
CONSENSO DELL'INTERESSATO
(art. 7 - da C40 a C46 – RGPD)

1. Questo Ateneo non deve richiedere agli interessati il consenso per il trattamento dei loro dati personali allorquando il trattamento dei dati è effettuato per l'adempimento di un obbligo legale alla quale è soggetta l'Ateneo per l'esecuzione di un contratto con riguardo a

soggetti interessati.

2. Nelle fattispecie diverse da quelle di cui al precedente comma 1, qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali.
3. Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante.
4. L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato.
5. Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto.

Articolo 7
TRATTAMENTO DEI DATI SENSIBILI
(art. 9 RGPD)

1. È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona. (**C51**)
2. Il divieto di cui al precedente comma non si applica se si verifica uno dei seguenti casi: (**C51, C52**)
   a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1;
   b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;
   c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
   d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso

dell'interessato;

e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;
f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato; (**C55, C56**)
h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3; (C53)
i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale; (**C54**)
j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, del RGPD sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

3. I dati personali di cui al paragrafo 1 possono essere trattati per le finalità di cui al paragrafo 2, lettera h), se tali dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti o da altra persona anch'essa soggetta all'obbligo di segretezza conformemente al diritto dell'Unione o dello Stato o alle norme stabilite dagli organismi nazionali competenti. (**C53**)

Articolo 8
TRATTAMENTO DEI DATI GIUDIZIARI
(art. 10 RGPD)

1. Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, del RGPD deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o dello Stato che preveda garanzie appropriate per i diritti e le libertà degli interessati.

CAPO II
DIRITTI DELL'INTERESSATO

Articolo 9
INFORMATIVA, COMUNICAZIONE E MODALITÀ TRASPARENTI PER L'ESERCIZIO DEI DIRITTI DELL'INTERESSATO
(art. 12 – C58, C60, C64 - RGPD)

1. L'Ateneo adotta misure appropriate per fornire all'interessato tutte le informazioni di cui ai successivi articoli 10 e 11 e le comunicazioni di cui agli articoli da 12 a 18 e all'articolo 29 relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.
2. L'Ateneo agevola l'esercizio dei diritti dell'interessato ai sensi degli articoli da 12 a 18. Nei casi di cui all'articolo 11, paragrafo 2, del RGPD l'Ateneo non può rifiutare di soddisfare la richiesta dell'interessato al fine di esercitare i suoi diritti ai sensi degli articoli da 12 a 18, salvo che l'Ateneo dimostri che non è in grado di identificare l'interessato.
3. L'Ateneo fornisce all'interessato le informazioni relative all'azione intrapresa riguardo a una richiesta ai sensi degli articoli da 12 a 18 senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste. L'Ateneo informa l'interessato di tale proroga, e dei motivi del ritardo, entro un mese dal ricevimento della richiesta. Se l'interessato presenta la richiesta mediante mezzi elettronici, le informazioni sono fornite, ove possibile, con mezzi elettronici, salvo diversa indicazione dell'interessato. Se non ottempera alla richiesta dell'interessato, L'Ateneo informa l'interessato senza ritardo, e al più tardi entro un mese dal ricevimento della richiesta, dei motivi dell'inottemperanza e della possibilità di proporre reclamo a un'autorità di controllo e di proporre ricorso giurisdizionale.
4. Le informazioni fornite ai sensi degli articoli 10 e 11 ed eventuali comunicazioni e azioni intraprese ai sensi degli articoli da 12 a 18 e dell'articolo 29 sono gratuite. Se le richieste dell'interessato sono manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo, il titolare del trattamento può:
   a) addebitare un contributo spese ragionevole tenendo conto dei costi amministrativi sostenuti per fornire le informazioni o la comunicazione o intraprendere l'azione richiesta; oppure
   b) rifiutare di soddisfare la richiesta. Incombe all'Ateneo l'onere di dimostrare il carattere manifestamente infondato o eccessivo della richiesta.
5. Fatto salvo l'articolo 11 del RGPD, qualora l'Ateneo nutra ragionevoli dubbi circa l'identità della persona fisica che presenta la richiesta di cui agli articoli da 12 a 17, può richiedere ulteriori informazioni necessarie per confermare l'identità dell'interessato.
6. Le informazioni da fornire agli interessati a norma degli articoli 10 e 11 possono essere fornite in combinazione con icone standardizzate per dare, in modo facilmente visibile, intelligibile e chiaramente leggibile, un quadro d'insieme del trattamento previsto. Se

presentate elettronicamente, le icone sono leggibili da dispositivo automatico.

Articolo 10
INFORMATIVA PER I DATI DA RACCOGLIERE PRESSO L'INTERESSATO
(art. 13 – C60, C62 - RGPD)

1. In caso di raccolta presso l'interessato di dati che lo riguardano, l'Ateneo fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni:
   a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
   b) i dati di contatto del responsabile della protezione dei dati;
   c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
   d) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali.
2. In aggiunta alle informazioni di cui al paragrafo 1, nel momento in cui i dati personali sono ottenuti, l'Ateneo fornisce all'interessato le seguenti ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente:
   a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
   b) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
   c) qualora il trattamento di dati non sensibili e non giudiziari sia basato sul consenso espresso dall'interessato per una o più specifiche finalità oppure il trattamento dei dati sensibili sia basato sul consenso espresso dall'interessato per una o più specifiche finalità e il diritto dell'Unione o dello Stato abbia disposto l'irrevocabilità del divieto di trattare gli stessi dati sensibili previsto dal paragrafo 1 dell'articolo 9 del RGPD, l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
   d) il diritto di proporre reclamo a un'autorità di controllo;
   e) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
   f) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, del RGPD, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.
3. Qualora l'Ateneo intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente di cui al paragrafo 2.
4. I commi 1, 2 e 3 non si applicano se e nella misura in cui l'interessato dispone già delle informazioni.

Articolo 11
INFORMATIVA PER I DATI DA OTTENERE DA SOGGETTI DIVERSI DALL'INTERESSATO
(art. 14 – C60, C62 - RGPD)

1. Qualora i dati non siano stati ottenuti presso l'interessato, il titolare del trattamento fornisce all'interessato le seguenti informazioni:
   a) l'identità e i dati di contatto dell'Ateneo;
   b) i dati di contatto del responsabile della protezione dei dati;
   c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
   d) le categorie di dati personali in questione;
   e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
2. Oltre alle informazioni di cui al comma 1, il titolare del trattamento fornisce all'interessato le seguenti informazioni necessarie per garantire un trattamento corretto e trasparente nei confronti dell'interessato:
   a) il periodo di conservazione dei dati oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
   b) l'esistenza del diritto dell'interessato di chiedere all'Ateneo l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento dei dati personali che lo riguardano e di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
   c) qualora il trattamento di dati non sensibili e non giudiziari sia basato sul consenso espresso dall'interessato per una o più specifiche finalità oppure il trattamento dei dati sensibili sia basato sul consenso espresso dall'interessato per una o più specifiche finalità e il diritto dell'Unione o dello Stato abbia disposto l'irrevocabilità del divieto di trattare gli stessi dati sensibili previsto dal paragrafo 1 dell'articolo 9 del RGPD, l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
   d) il diritto di proporre reclamo a un'autorità di controllo;
   e) la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico;
   f) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.
3. L'Ateneo fornisce le informazioni di cui ai commi 1 e 2:
   a) entro un termine ragionevole dall'ottenimento dei dati personali, ma al più tardi entro un mese, in considerazione delle specifiche circostanze in cui i dati personali sono trattati;
   b) nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, al più tardi al momento della prima comunicazione all'interessato; oppure
   c) nel caso sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati.
4. Qualora l'Ateneo intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati ottenuti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni informazione pertinente di

cui al comma 2

5. I commi da 1 a 4 non si applicano se e nella misura in cui:
   a) l'interessato dispone già delle informazioni;
   b) comunicare tali informazioni risulta impossibile o implicherebbe uno sforzo sproporzionato; in particolare per il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatte salve le condizioni e le garanzie di cui all'articolo 89, paragrafo 1, del RGPD o nella misura in cui l'obbligo di cui al comma 1 del presente articolo rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità di tale trattamento. In tali casi, l'Ateneo adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, anche rendendo pubbliche le informazioni;
   c) l'ottenimento o la comunicazione sono espressamente previsti dal diritto dell'Unione o dello Stato e che prevede misure appropriate per tutelare gli interessi legittimi dell'interessato; oppure
   d) qualora i dati personali debbano rimanere riservati conformemente a un obbligo di segreto professionale disciplinato dal diritto dell'Unione o dello Stato, compreso un obbligo di segretezza previsto per legge.

Articolo 12
DIRITTO DI ACCESSO DELL'INTERESSATO
(art. 15 – C63, C64 - RGPD)

1. L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:
   a) le finalità del trattamento;
   b) le categorie di dati personali in questione;
   c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
   d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
   e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
   f) il diritto di proporre reclamo a un'autorità di controllo;
   g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
   h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, del RGPD e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.
2. Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi, le cui tariffe sono determinate dall'Ateneo. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo

indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.

3. Il diritto di ottenere una copia di cui al comma 2 non deve ledere i diritti e le libertà altrui.
4. L'istanza é formulata dall'interessato per iscritto e inviata anche tramite posta elettronica.
5. Il Dirigente del settore competente per la materia relativa al trattamento dei dati ovvero, su delega di quest'ultimo, il Responsabile del servizio provvede a soddisfare la richiesta dell'interessato nel più breve tempo possibile e comunque non oltre trenta giorni.

Articolo 13
DIRITTO DI RETTIFICA E INTEGRAZIONE
(art. 16 – C65 – art. 19 RGPD)

1. L'interessato ha il diritto di ottenere dall'Ateneo la rettifica dei suoi dati personali inesatti nonché, tenuto conto delle finalità del trattamento, l'integrazione dei suoi dati personali incompleti, anche fornendo una dichiarazione integrativa. L'istanza di rettifica o integrazione é formulata dall'interessato per iscritto e inviata anche tramite posta elettronica.
2. Alla rettifica ovvero all'integrazione dei dati richiesta dall'interessato provvede, senza ritardo e comunque entro cinque giorni lavorativi dalla data di arrivo della predetta istanza, il Responsabile del procedimento amministrativo cui ineriscono i dati da rettificare o integrare.
3. Dell'eseguita rettifica o integrazione ovvero della motivata inammissibilità é data tempestiva comunicazione all'interessato con raccomandata con avviso di ricevimento o con notifica a mani o tramite p.e.c.
4. Il Responsabile del procedimento relativo al trattamento dei dati oggetto della richiesta deve comunicare, con tempestività, a ciascuno dei destinatari cui sono stati trasmessi i dati personali la rettifica del trattamento effettuata, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato; e, inoltre, dà comunicazione all'interessato di tali destinatari qualora l'interessato lo richieda.

Articolo 14
DIRITTO ALLA CANCELLAZIONE (DIRITTO ALL'OBLIO)
(art. 17 – C65, C66 – art. 19 - RGPD)

1. L'interessato ha il diritto di ottenere dall'Ateneo la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e l'Ateneo ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:
   a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
   b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), ovvero all'art. 9, prf. 2, lett. a), del RGPD e se non sussiste altro fondamento giuridico per il trattamento;
   c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, del RGPD e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si

oppone al trattamento ai sensi dell'articolo 21, paragrafo 2, del RGPD;
   d) i dati personali sono stati trattati illecitamente;
   e) i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato cui è soggetto il titolare del trattamento;
   f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1, del RGPD.
2. L'istanza é formulata dall'interessato per iscritto e inviata anche tramite posta elettronica.
3. L'Ateneo, se ha reso pubblici dati personali ed è obbligato, ai sensi del comma 1, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.
4. I commi 1 e 2 non si applicano nella misura in cui il trattamento sia necessario:
   a) per l'esercizio del diritto alla libertà di espressione e di informazione;
   b) per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
   c) per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3, del RGPD;
   d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, del RGPD nella misura in cui il diritto di cui al comma 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; o
   e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.
5. Il Responsabile del procedimento relativo al trattamento dei dati oggetto della richiesta deve comunicare, con tempestività, a ciascuno dei destinatari cui sono stati trasmessi i dati personali la rettifica del trattamento effettuata, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato; dà, inoltre, comunicazione all'interessato di tali destinatari qualora l'interessato lo richieda.

Articolo 15
DIRITTO DI LIMITAZIONE DI TRATTAMENTO
(artt. 18 e 19 – C67 – RGPD)

1. L'interessato ha il diritto di ottenere dall'Ateneo la limitazione del trattamento quando ricorre una delle seguenti ipotesi:
   a) l'interessato contesta l'esattezza dei dati personali, per il periodo necessario all'Ateneo per verificare l'esattezza di tali dati personali;
   b) il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;
   c) benché l'Ateneo non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
   d) l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1, del RGPD

in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

2. Se il trattamento è limitato a norma del comma 1, tali dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o dello Stato.
3. L'interessato che ha ottenuto la limitazione del trattamento a norma del comma 1 è informato dall'Ateneo prima che detta limitazione sia revocata.
4. Il Responsabile del procedimento relativo al trattamento dei dati oggetto della richiesta deve comunicare, con tempestività, a ciascuno dei destinatari cui sono stati trasmessi i dati personali la limitazione del trattamento effettuata, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato; e, inoltre, dà comunicazione all'interessato di tali destinatari qualora l'interessato lo richieda.

Articolo 16
DIRITTO ALLA PORTABILITÀ DEI DATI
(art. 20 – C68 - RGPD)

1. L'interessato ha il diritto di ottenere dall'Ateneo la portabilità dei dati quando ricorre una delle seguenti ipotesi:
   a) Il trattamento si basi sul consenso ai sensi dell'articolo 6 paragrafo 1, lettera a), o dell'articolo 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'articolo 6 paragrafo 1. Lettera b);l'interessato contesta l'esattezza dei dati personali, per il periodo necessario all'Ateneo per verificare l'esattezza di tali dati personali;
   b) Il trattamento sia effettuato con mezzi automatizzati;
2. Nell'esercitare i propri diritti relativamente alla portabilità dei dati a norma del paragrafo 1, l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali dall'Ateneo ad un altro titolare del trattamento, se tecnicamente fattibile
3. L'interessato che ha ottenuto la portabilità dei dati a norma del comma 1 è informato dall'Ateneo prima che detta portabilità sia effettuata.
4. Il Responsabile del procedimento relativo al trattamento dei dati oggetto della richiesta deve comunicare, con tempestività, a ciascuno dei destinatari cui sono stati trasmessi i dati personali la portabilità del trattamento effettuata, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato; e, inoltre, dà comunicazione all'interessato di tali destinatari qualora l'interessato lo richieda.

Articolo 17
DIRITTO DI OPPOSIZIONE
(art. 21 – C69, C70 - RGPD)

1. L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano, compresa la

profilazione sulla base di tali disposizioni. L'Ateneo si astiene dal trattare ulteriormente i dati personali salvo che dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

2. L'opposizione é formulata dall'interessato per iscritto ed é inviata all'Ateneo anche per posta elettronica.
3. Da parte del Responsabile del procedimento relativo al trattamento dei dati oggetto dell'opposizione il diritto di cui al comma 1 è esplicitamente portato all'attenzione dell'interessato ed è presentato chiaramente e separatamente da qualsiasi altra informazione al più tardi al momento della prima comunicazione con l'interessato.

Articolo 18
PROCESSO DECISIONALE AUTOMATIZZATO RELATIVO ALLE PERSONE FISICHE, COMPRESA LA PROFILAZIONE

(art. 22 – C71, C72 - RGPD)

1. L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.
2. Il comma 1 non si applica nel caso in cui la decisione:
   a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;
   b) sia autorizzata dal diritto dell'Unione o dello Stato, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato;
   c) si basi sul consenso esplicito dell'interessato.
3. Nei casi di cui al comma 2, lettere a) e c), l'Ateneo attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione.
4. Le decisioni di cui al comma 2 non si basano sulle categorie di dati sensibili di cui all'articolo 9, paragrafo 1, a meno che non sia d'applicazione l'articolo 9, paragrafo 2, lettere a) o g), del RGPD e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato.

CAPO III
SOGGETTI RESPONSABILI DEL TRATTAMENTO E DELLA SICUREZZA DEI DATI

Articolo 19
TITOLARE DEL TRATTAMENTO
(art. 24 – C74, C78 - RGPD)

1. L'Ateneo, è il titolare del trattamento dei dati personali raccolti in banche dati, automatizzate o cartacee, gestite dagli uffici dell'Ateneo. Per il trattamento di dati l'Ateneo può avvalersi anche di soggetti privati esterni tramite un contratto di servizio o altro atto giuridicamente valido nel quale sono specificati le finalità e le modalità del trattamento, le categorie di dati da trattare, le responsabilità e i doveri facenti carico al soggetto che svolgerà il trattamento determinandone la qualifica di contitolare o responsabile del trattamento.
2. L'Ateneo è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 RGPD: liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza.
3. L'Ateneo mette in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento di dati personali è effettuato in modo conforme al RGPD.
4. Le misure sono definite fin dalla fase di progettazione e messe in atto per applicare in modo efficace i principi di protezione dei dati e per agevolare l'esercizio dei diritti dell'interessato stabiliti dagli articoli 15-22 RGPD, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio.
5. Gli interventi necessari per l'attuazione delle misure sono considerati nell'ambito della programmazione operativa e di bilancio, previa apposita analisi preventiva della situazione in essere, tenuto conto dei costi di attuazione, della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi dallo stesso derivanti, aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.
6. Il Titolare adotta misure appropriate per fornire all'interessato:
   a) le informazioni indicate dall'art. 13 RGPD, qualora i dati personali siano raccolti presso lo stesso interessato;
   b) le informazioni indicate dall'art. 14 RGPD, qualora i dati personali non stati ottenuti presso lo stesso interessato.
7. Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, l'Ateneo deve effettuare una valutazione dell'impatto del trattamento sulla protezione dei dati personali (di seguito indicata con "DPIA") ai sensi dell' art.35, RGDP, considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento, tenuto conto di quanto indicato dal successivo articolo 31.
8. L'Ateneo provvede a:
   a) designare i Responsabili del trattamento nelle persone dei Dirigenti e/o dei Responsabili di P.O. e/o dei Funzionari Responsabili delle singole strutture o dei servizi in cui si articola l'organizzazione, che sono preposti al trattamento dei dati contenuti nelle banche dati esistenti nelle articolazioni organizzative di loro competenza;
   b) designare gli autorizzati del trattamento nelle persone dei Dirigenti e/o dei Responsabili

di P.O. e/o dei Funzionari Responsabili delle singole strutture o dei servizi in cui si articola l'organizzazione, che sono preposti al trattamento dei dati contenuti nelle banche dati esistenti nelle articolazioni organizzative di loro competenza;

c) nominare il Responsabile della protezione dei dati;
d) nominare l'Amministratore del sistema informatico;
e) a diramare le direttive necessarie per l'applicazione delle disposizioni del RGPD e del presente regolamento, sentito il CDA, il Responsabile della protezione dei dati, l'Amministratore del sistema informatico e i Responsabili del trattamento. Il Responsabile della protezione dei dati, é tenuto a sentire preventivamente l'Amministratore del sistema informatico e i Responsabili del trattamento.

9. L'Ateneo favorisce l'adesione ai codici di condotta elaborati dalle associazioni e dagli organismi di categoria rappresentativi, ovvero a meccanismi di certificazione della protezione dei dati approvati, per contribuire alla corretta applicazione del RGPD e per dimostrarne il concreto rispetto da parte del Titolare e dei Responsabili del trattamento.

Articolo 20
CONTITOLARI DEL TRATTAMENTO
(art. 26 – C79 - RGPD)

1. Nel caso di esercizio associato di funzioni e servizi fra due o più titolari del trattamento, gli stessi determinano congiuntamente e in modo trasparente, mediante accordo interno, le finalità ed i mezzi del trattamento, ai sensi dell'art. 26 RGPD.
2. L'accordo definisce le responsabilità di ciascun titolare in merito all'osservanza degli obblighi derivanti dal RGPD, con particolare riferimento all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli artt. 13 e 14 del RGPD, fermo restando eventualmente quanto stabilito dalla normativa europea o statale specificatamente applicabile. Tale accordo può individuare un punto di contatto comune per gli interessati.

Articolo 21
RESPONSABILI DEL TRATTAMENTO
(art. 28 – C81 - RGPD)

1. L'Ateneo si avvale obbligatoriamente di più Responsabili del trattamento. La designazione avviene con il decreto di attribuzione delle funzioni dirigenziali o con separata nomina, nel quale sono tassativamente previsti:
   - la materia trattata, la durata, la natura e la finalità del trattamento o dei trattamenti assegnati;
   - il tipo di dati personali oggetto di trattamento e le categorie di interessati;
   - gli obblighi ed i diritti del Titolare del trattamento.

   Tale disciplina può essere contenuta anche in apposita convenzione o contratto da stipularsi fra l'Ateneo e ciascun responsabile designato.

2. Sino alla designazione di cui al comma 1 si intende prorogata di diritto la designazione dei Responsabili del trattamento in carica al momento della predetta proclamazione.
3. Devono essere designati Responsabili del trattamento dei dati personali, i Dirigenti delle strutture di massima dimensione in cui si articola l'organizzazione dell'Ateneo. Possono essere designati, altresì, Responsabili del trattamento i Funzionari cui é attribuita la Posizione Organizzativa e i Funzionari responsabili di servizi o uffici limitatamente alle banche dati di propria competenza che abbiano una rilevante importanza per l'attività istituzionale dell'Ateneo.
4. Il Responsabile del trattamento deve essere in grado, anche attraverso una adeguata preventiva formazione, di offrire garanzie sufficienti in termini di conoscenza specialistica, esperienza, capacità ed affidabilità, per mettere in atto le misure tecniche e organizzative di cui al successivo articolo 28 rivolte a garantire che i trattamenti siano effettuati in conformità al RGPD.
5. L'Ateneo può avvalersi, per il trattamento di dati, anche sensibili, di soggetti privati che, in qualità di responsabili del trattamento, forniscano le garanzie di cui al comma 2, stipulando atti giuridici in forma scritta, che specifichino la finalità perseguita, la tipologia dei dati, la durata del trattamento, gli obblighi e i diritti del responsabile del trattamento e le modalità di trattamento.
6. Gli atti che disciplinano il rapporto tra il Titolare del trattamento e il Responsabile del trattamento devono in particolare contenere quanto previsto dall'art. 28, p. 3, del RGPD; tali atti possono anche basarsi su clausole contrattuali tipo adottate dal Garante per la protezione dei dati personali oppure dalla Commissione europea.
7. Qualora un Responsabile del trattamento si assenti o sia impedito o sospeso per un prolungato periodo di tempo superiore a trenta giorni l'Ateneo provvede alla sua sostituzione temporanea.
8. È consentita la nomina di sub-responsabili del trattamento da parte di ciascun Responsabile del trattamento per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano il Titolare del trattamento e il Responsabile del trattamento primario, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del RGPD. Se il sub-responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile primario conserva nei confronti del Titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi del sub-responsabile.
9. Le operazioni di trattamento possono essere effettuate solo da sub-responsabili o da incaricati che operano sotto la diretta autorità del Responsabile del trattamento attenendosi alle istruzioni loro impartite per iscritto dallo stesso Responsabile, le quali istruzioni individuano specificatamente l'ambito del trattamento consentito.
10. Il Responsabile del trattamento risponde, anche dinanzi al Titolare del trattamento, dell'operato del sub- responsabile del trattamento e degli incaricati del trattamento anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso non gli è in alcun modo imputabile e che ha vigilato in modo adeguato sull'operato del sub-responsabile e dell'incaricato del trattamento.
11. Il Responsabile del trattamento garantisce che chiunque agisca sotto la sua autorità ed abbia accesso a dati personali sia in possesso di apposita formazione ed istruzione e si sia impegnato alla riservatezza od abbia un adeguato obbligo legale di riservatezza.
12. Il titolare o il responsabile del trattamento provvede, per il proprio ambito di competenza, a tutte le attività previste dalla legge e a tutti i compiti affidatigli dal Titolare del trattamento,

analiticamente specificati per iscritto nell'atto di designazione, ed in particolare deve provvedere:

a) a tenere aggiornato il registro delle categorie di attività di trattamento svolte per conto del Titolare;
b) ad adottare le misure tecniche e organizzative adeguate a garantire la sicurezza dei trattamenti;
c) ad autorizzare i dipendenti appartenenti alla sua struttura ad accedere ai dati personali al fine di svolgere il trattamento afferente i rispettivi compiti istituzionali;
d) a sensibilizzare e formare il personale che partecipa ai trattamenti in materia di protezione dei dati personali, fornendo le istruzioni per il corretto trattamento dei dati personali, e a controllare che le attività di trattamento, con particolare riferimento alle operazioni di comunicazione e diffusione, svolte dagli incaricati siano conformi alle norme del RGPD;
e) a collaborare con il Titolare al fine di definire la valutazione dell'impatto sulla protezione dei dati (di seguito indicata con "DPIA") fornendo allo stesso ogni informazione di cui è in possesso;
f) a informare il Titolare, senza ingiustificato ritardo, della conoscenza di casi di violazione dei dati personali (cd. "data breach"), per la successiva notifica della violazione al Garante Privacy, nel caso in cui il Titolare stesso ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati.
g) a curare le informative di cui agli articoli 13 e 14 del RGPD da fornire agli interessati, predisponendo la necessaria modulistica o determinando altre forme idonee di informazione inerenti i trattamenti di competenza della propria struttura organizzativa, facendo, in presenza di dati sensibili, espresso riferimento alla normativa che prevede gli obblighi o i compiti in base alla quale è effettuato il trattamento;
h) a curare l'eventuale raccolta del consenso degli interessati per il trattamento dei dati sensibili qualora il loro trattamento non sia previsto da una specifica norma di legge;
i) adottare le misure necessarie per facilitare l'esercizio dei diritti dell'interessato di cui agli articoli da 15 a 22 del RGPD;
j) a stabilire le modalità di gestione e le forme di responsabilità relative a banche dati condivise da più articolazioni organizzative, d'intesa con gli altri responsabili; in caso di mancato accordo tra i responsabili, decide il Segretario Generale, sentiti gli stessi responsabili competenti;
k) a stipulare gli accordi con altri soggetti pubblici o privati per l'esercizio del diritto di accesso alle banche-dati nei limiti previsti dalle disposizioni legislative e regolamentari;

Articolo 22
AUTORIZZATI DEL TRATTAMENTO
(art. 29 – C81 - RGPD)

1. Autorizzati del trattamento sono i soggetti interni all'Ateneo che hanno accesso a dati personali ovvero agiscano sotto l'autorità del Titolare del trattamento o dei responsabili del trattamento.
2. Gli Autorizzati del trattamento non possono svolgere operazioni di trattamento dei dati personali se non istruiti in tal senso dal Titolare del trattamento o dal responsabile del

trattamento della struttura o servizio in cui svolge le proprie mansioni.

3. I dipendenti sono designati autorizzati del trattamento con formale atto di nomina del Titolare del trattamento. Nell'atto di nomina sono indicati: i procedimenti amministrativi per lo svolgimento dei quali è indispensabile il trattamento dei dati personali; le finalità del trattamento; le categorie di dati personali da trattare; le operazioni di trattamento eseguibili, con particolare riferimento alla comunicazione e alla diffusione dei dati sensibili e giudiziari; gli eventuali limiti al trattamento; le misure di sicurezza da adottare da parte degli stessi Incaricati. Le predette designazione e autorizzazione nonché le prefate indicazioni del trattamento possono essere stabilite anche con un atto distinto dal contratto individuale di lavoro. Tale atto deve essere notificato al dipendente interessato, il quale non può esimersi dalla sua accettazione e attuazione.
4. I dipendenti possono essere individuati quali autorizzati del trattamento nominativamente ovvero con riferimento alla categoria di inquadramento o al profilo professionale o alla collocazione nell'organizzazione del servizio o dell'ufficio.
5. I dipendenti autorizzati del trattamento operano sotto l'autorità dei Responsabili del trattamento, attenendosi alle istruzioni impartite per iscritto, con particolare riferimento alla custodia degli atti e documenti analogici e digitali contenenti dati personali sensibili e giudiziari e alle relative misure di sicurezza.
6. Agli autorizzati compete, in relazione al trattamento dei dati personali provvedere:
   - al trattamento dei dati personali per lo svolgimento delle funzioni dell'Ateneo, in conformità alle disposizioni del RGPD;
   - la raccolta e la registrazione per gli scopi inerenti l'attività istituzionale svolta da ciascuno;
   - la verifica in ordine alla loro pertinenza, completezza e non eccedenza delle finalità per le quali sono stati raccolti o successivamente trattati, secondo le indicazioni ricevute dal responsabile del trattamento;
   - la conservazione, rispettando le misure di sicurezza predisposte al riguardo.
7. Per ogni operazione di trattamento è da garantire la massima riservatezza.
8. Nel caso di allontanamento anche temporaneo dalla propria postazione di lavoro, l'autorizzato verifica che non vi sia possibilità per chiunque non sia autorizzato all'accesso ai dati di accedere alle banche-dati e/o ai dati personali per i quali è in corso un qualsiasi tipo di trattamento.
7. Le comunicazioni e le diffusioni a soggetti diversi dagli interessati devono essere svolte nel pieno rispetto delle norme che le disciplinano.
8. Il flusso di dati tra Titolare del trattamento, Responsabili del trattamento, Autorizzati del trattamento, Amministratore del sistema informatico e il Responsabile della protezione dei dati, non costituisce "comunicazione" in senso tecnico quale operazione di trattamento; ne consegue che tale flusso non é soggetto ai limiti previsti per tale operazione di trattamento.

Articolo 23
AMMINISTRATORE DEL SISTEMA INFORMATICO

(Garante Privacy provvedimento del 25.6.2009)

1. Al fine di ottemperare a quanto disposto dal Garante della Privacy con il provvedimento datato 27/11/2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con

strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" come modificato con successivo provvedimento datato 25/06/2009, l'Ateneo si avvale obbligatoriamente di un Amministratore del sistema informatico al fine di assicurare che il sistema informatico di questo Ateneo sia strutturato e gestito in modo da garantire le misure tecniche e organizzative adeguate per la necessaria protezione dei dati personali trattati attraverso lo stesso sistema.

2. L'Amministratore del sistema deve essere in possesso di titolo di studio specifico in informatica almeno di scuola media di secondo grado o laurea triennale oppure deve essere un soggetto dotato di comprovate conoscenze specialistiche tecniche e giuridiche in materia di sicurezza degli strumenti e dei programmi informatici per la protezione dei dati personali nonché della capacità di assolvere i compiti di competenza.
3. Amministratore del sistema informatico può essere designato un dipendente a tempo indeterminato ovvero, nel caso di mancanza di un dipendente con le competenze di cui al punto 2, un soggetto esterno, persona fisica o giuridica. La designazione da parte dell' Ateneo del soggetto esterno avviene tra quanti abbiano partecipato ad una apposita procedura ad evidenza pubblica e assolve i suoi compiti in base a un contratto di servizi. L'assenza di conflitti di interesse anche potenziali con l'esercizio dei propri compiti é strettamente connessa agli obblighi di autonomia e indipendenza dell'Amministratore di sistema.
4. Nell'atto ovvero nel contratto di servizio con cui é designato Amministratore di sistema il dipendente o il soggetto esterno all'Ateneo devono essere riportati, altresì, tutti gli adempimenti con tutto ciò che essi comportano sia sul piano delle procedure amministrative, che dell'organizzazione, che dell'adozione e verifica di ogni misura necessaria in materia di protezione dei dati personali dalle fonti di diritto europee e nazionali, dal "Gruppo di Lavoro europeo 29", dal Garante della Privacy, dalle disposizioni regolamentari e dalle direttive emanate dal Titolare del trattamento e dal Responsabile della protezione dei dati, nonché per conformarsi alla disciplina del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82/2004 e ss.mm.ii., in particolare la cura dei seguenti adempimenti:
    a) gestire l'hardware e i software dei server e delle postazioni di lavoro informatizzate;
    b) impostare e gestire un sistema di autenticazione informatica per i trattamenti di dati personali effettuati con strumenti elettronici;
    c) registrare gli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli altri amministratori di sistema (se designati); impostare e gestire un sistema di autorizzazione per i componenti degli organi di governo e di controllo interno, per il Responsabile per la protezione dei dati, per i Responsabili e gli Autorizzati dei trattamenti di dati personali effettuati con strumenti elettronici nonché di quanti siano autorizzati all'accesso ai dati personali contenuti nelle banche-dati informatizzati;
    d) verificare costantemente che il Titolare del trattamento abbia adottato le misure tecniche e organizzative adeguate per la sicurezza dei dati personali, secondo quanto disciplinato dall'art. 32 RGDP, provvedendo senza indugio agli adeguamenti eventualmente necessari e redigendo entro il 30 settembre di ogni anno una apposita relazione da inviare al Titolare del trattamento ed al Responsabile per la protezione dei dati in modo da attuare gli adempimenti amministrativi e contabili per la previsione nella successiva programmazione utile per la realizzazione delle ulteriori misure di sicurezza;

e) suggerire al Titolare del trattamento, ai Responsabili del trattamento l'adozione e l'aggiornamento delle misure di sicurezza adeguate per assicurare la sicurezza dei dati atte a che i dati personali oggetto di trattamento siano custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta secondo quanto disciplinato dall'art. 32 RGDP;

   Più specificamente, l'Amministratore di sistema dovrà:

   1) assegnare e gestire il sistema di autenticazione informatica e quindi generare, sostituire ed invalidare, in relazione agli strumenti e alle applicazioni informatiche utilizzate, le parole chiave ed i Codici identificativi personali da assegnare ai Responsabili e ai soggetti autorizzati del trattamento dei dati, svolgendo anche la funzione di custode delle copie delle credenziali; In particolare dovrà:
      - custodire le parole chiave attribuite dagli autorizzati del trattamento di dati personali con elaboratori elettronici e preservare con estrema attenzione il "cartellino delle credenziali di autenticazione" in modo da evitare accidentali aperture della busta ed evitare di aprire tali buste;
      - nel caso in cui il Responsabile del trattamento abbia la necessità indifferibile di accedere ad un elaboratore in caso di assenza o impedimento del soggetto autorizzato che lo utilizza abitualmente, consentire al Responsabile del trattamento con una nuova parola chiave l'accesso all'elaboratore sul quale egli possa intervenire unicamente per necessità di operatività e sicurezza del sistema informativo; informare l'Autorizzato del trattamento allorché rientri in servizio e consegnargli una nuova parola chiave diversa da quella consegnata al Responsabile del trattamento durante la sua assenza.
   2) procedere, più in particolare, alla disattivazione dei Codici identificativi personali, in caso di perdita della qualità che consentiva ai soggetti interessati l'accesso all'elaboratore, oppure nel caso di mancato utilizzo dei Codici identificativi personali per oltre 6 (sei) mesi;
   3) dotare e attivare nonché aggiornare adeguati programmi antivirus, firewall ed altri strumenti software o hardware atti a garantire la massima misura di sicurezza e protezione dei dati trattati attraverso gli elaboratori del sistema informativo contro il rischio di intrusione e contro l'azione dei virus informatici, ed utilizzando le conoscenze acquisite in base al progresso tecnico software e hardware, verificandone l'installazione, l'aggiornamento ed il funzionamento degli stessi;
   4) aggiornare periodicamente, con frequenza almeno annuale (oppure semestrale se si trattano dati sensibili o giudiziari), i programmi volti a prevenire la vulnerabilità degli strumenti elettronici e a correggerne i difetti;
   5) curare l'adozione e l'aggiornamento delle predette misure di sicurezza;
   6) impartire a tutti i soggetti che comunque svolgano trattamento dei dati istruzioni organizzative dirette al salvataggio quotidiano dei dati; prendere pertanto tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati e provvedere al ricovero periodico degli stessi con copie di back-up; assicurarsi della qualità delle copie di back-up dei dati e della loro conservazione in luogo adatto e sicuro;
   7) adottare procedure per la custodia delle copie di sicurezza dei dati e per il ripristino

della disponibilità dei dati e dei sistemi;

8) predisporre un piano di controlli periodici, da eseguirsi con cadenza almeno annuale, dell'efficacia delle misure di sicurezza;

9) indicare al personale competente o provvedere direttamente alla distruzione e smaltimento dei supporti informatici di memorizzazione logica o alla cancellazione dei dati allorché si provveda al loro reimpiego;

5. All'Amministratore del sistema informatico è:
   a) fatto assoluto divieto di leggere, copiare, stampare o visualizzare i documenti o i dati degli utenti memorizzati sul sistema a meno che questo sia strettamente indispensabile per le operazioni attinenti ai ruoli allo stesso assegnati; tale divieto vale anche nei confronti di quanti non siano stati autorizzati dal Titolare o dai Responsabili del trattamento a conoscere i dati personali oggetto di trattamento;
   b) obbligato a dare tempestiva comunicazione al Titolare e ai Responsabili del trattamento interessati nonché al Responsabile della protezione dei dati dei problemi di affidabilità sia dell'hardware che dei software eventualmente rilevati;
   c) obbligato a osservare scrupolosamente le informazioni e le disposizioni allo stesso impartite in merito alla protezione dei sistemi informatici, degli elaboratori e dei dati, sia da intrusioni che da eventi accidentali, il trattamento consentito, l'accesso e la trasmissione dei dati, in conformità ai fini della raccolta dei dati.
6. Il Responsabile della protezione dei dati procederà, alla verifica delle attività svolte dall'Amministratore del sistema informatico in modo da controllare la loro rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

Articolo 24
RESPONSABILE DELLA PROTEZIONE DEI DATI
(artt. 37, 38, 39 – C97 - RGPD)

1. L'Ateneo si avvale di un Responsabile della protezione dei dati (RPD), in possesso delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di competenza.
2. Il Responsabile della protezione è designato con specifico contratto sottoscritto con il Titolare del Trattamento.
3. L'Ateneo provvede, tempestivamente, a che i dati identificativi e di contatto del Responsabile della protezione dei dati siano:
   - pubblicati nel sito web dell'Ateneo;
   - comunicati al Garante della Privacy;
   - comunicati a tutti i dirigenti e dipendenti, ai componenti degli organi di controllo interni.
4. Nel contratto di servizio relativo all'affidamento dell'incarico di RPD devono essere riportati i compiti che lo stesso é tenuto a svolgere, tra cui almeno i seguenti:
   a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o dello Stato relative alla protezione dei dati; in tal senso il RPD può indicare al Titolare e/o ai

Responsabili del trattamento i settori funzionali ai quali riservare un audit interno o esterno in tema di protezione dei dati, le attività di formazione interna per il personale che tratta dati personali, e a quali trattamenti dedicare maggiori risorse e tempo in relazione al rischio riscontrato;

b) sorvegliare l'osservanza del RGPD, di altre disposizioni dell'Unione o dello Stato relative alla protezione dei dati nonché delle politiche del titolare del trattamento o dei responsabili del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo; fanno parte di questi compiti la raccolta di informazioni per individuare i trattamenti svolti, l'analisi e la verifica dei trattamenti in termini di loro conformità, l'attività di informazione, consulenza e indirizzo nei confronti del Titolare e del Responsabile del trattamento;
c) sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare e dai Responsabili del trattamento;
d) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del RGPD; il Titolare del trattamento, in particolare, si consulta con il RPD in merito a: se condurre o meno una DPIA; quale metodologia adottare nel condurre una DPIA; se condurre la DPIA con le risorse interne ovvero esternalizzandola; quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi delle persone interessate; se la DPIA sia stata condotta correttamente o meno e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi al RGPD;
e) verificare e relazionare, riguardo alle attività svolte dall'Amministratore del sistema informatico in modo da controllare la loro rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.
f) cooperare con il Garante per la protezione dei dati personali e fungere da punto di contatto per detta Autorità per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 del RGPD, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione.

5. Nell'eseguire i propri compiti il Responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo. A tali fini il RPD procede a mappare le aree di attività e ne valuta il grado di rischio in termini di protezione dei dati, determinandone un elenco in ordine decrescente di gravità in modo da definire un ordine di priorità nell'attività da svolgere - ovvero un piano annuale di attività - incentrandola sulle aree di attività che presentano maggiori rischi in termini di protezione dei dati, da comunicare al Titolare e ai Responsabili del trattamento.
6. Il Titolare del trattamento e i Responsabili del trattamento si assicurano che il RPD sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali. A tal fine:
   - il RPD è invitato a partecipare alle riunioni di coordinamento dei Responsabili del trattamento che abbiano per oggetto questioni inerenti la protezione dei dati personali;
   - il RPD deve ricevere tempestivamente, tramite posta elettronica, dal Titolare e dai Responsabili del trattamento tutte le informazioni pertinenti sulle decisioni che impattano sulla protezione dei dati, in modo da essere edotto sulla evoluzione della gestione in materia e da poter rendere una consulenza idonea, scritta od orale;

- é obbligatorio richiedere il parere del RPD sulle decisioni che impattano sulla disciplina e sulla prassi da seguire nell'Ateneo in materia di protezione dei dati; qualora la decisione assunta determina condotte difformi dal parere del RPD, è necessario motivare specificamente tale decisione;
- il RPD, consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente, con proprio parere indica quali provvedimenti debbano essere adottati per porre rimedio ovvero per prevenire il ripetersi di tali violazioni.

7. Il RPD è tenuto a manifestare il proprio dissenso alle decisioni o ai provvedimenti o ai comportamenti incompatibili con il RGPD adottati o tenuti dai componenti degli organi di governo e di controllo nonché degli organi di gestione e dei dipendenti ogni qual volta ne venga a conoscenza, dandone comunicazione al CDA, ai Responsabili del trattamento interessati dai rilievi e, ove necessario, all'Amministratore del sistema informatico. I Responsabili del trattamento qualora non condividano i rilievi formulati dal RPD, comunicano a quest'ultimo ed al CDA le proprie osservazioni. Il RPD dirama le direttive utili a prevenire il ripetersi delle violazioni rilevate.
8. Il Titolare del trattamento e i Responsabili del trattamento sostengono il Responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 39 del RGPD fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica. In particolare é assicurato al RPD:
   - supporto attivo per lo svolgimento dei compiti da parte dei Responsabili del trattamento, anche considerando l'attuazione delle attività necessarie per la protezione dati nell'ambito della programmazione operativa e di bilancio;
   - tempo sufficiente per l'espletamento dei compiti affidati al RPD;
   - supporto adeguato in termini di risorse strumentali (sede e attrezzature) e umane (dipendenti) costituite in gruppo di lavoro che lo coadiuvi nell'espletamento dei suoi compiti (se necessario);
   - accesso garantito ai settori funzionali dell'Ateneo così da fornirgli supporto, informazioni e input essenziali.
9. Il titolare del trattamento e i responsabili del trattamento si assicurano che il Responsabile della protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti.
10. Il Responsabile della protezione dei dati non può essere rimosso o penalizzato dal Titolare del trattamento per l'adempimento dei propri compiti.
11. Il Responsabile della protezione dei dati riferisce direttamente al Titolare del trattamento.
12. Gli interessati possono contattare direttamente il Responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento
13. Il Responsabile della protezione dei dati è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti, in conformità del diritto dell'Unione o dello Stato.
14. Il Responsabile della protezione dei dati può svolgere altri compiti e funzioni. L'Ateneo si assicura che lo svolgimento dei compiti e delle funzioni del RPD non diano adito a un conflitto di interessi.

Articolo 25
TRATTAMENTO DI DATI PERSONALI NEI SERVIZI ESTERNALIZZATI

1. Nella ipotesi che a soggetti privati esterni siano affidati tramite delega o concessione o contratto lo svolgimento di compiti e/o servizi di competenza di questo Ateneo, da cui debba conseguire il trattamento di dati personali, il provvedimento o contratto di affidamento deve prevedere norme specifiche attraverso le quali si provvede: a nominare il legale rappresentante del soggetto privato ovvero la persona fisica affidatario quale sub-responsabile del trattamento dei dati personali per la durata dell'affidamento; ad obbligare il soggetto affidatario ad osservare le prescrizioni di cui al RGPD e alle altre fonti di diritto dell'Unione e dello Stato in materia di protezione dei dati personali; a consentire le verifiche sul rispetto delle predette disposizioni normative.
2. Nelle ipotesi di trattamento dei dati personali di cui al precedente comma, il Responsabile del trattamento della massima struttura organizzativa dell'Ateneo competente per materia in relazione al compito e/o al servizio affidato ha il dovere di verificare che il soggetto esterno osservi le predette prescrizioni; e l'Amministratore del sistema informatico verifica che siano osservate le norme riferite all'attuazione delle misure minime di sicurezza.
3. La periodicità delle predette verifiche, previste nel provvedimento o contratto di affidamento, è determinata in funzione della natura dei dati, della probabile gravità dei rischi, dei mezzi da utilizzare per il trattamento e della durata dell'affidamento.
4. Le verifiche e i risultati delle stesse sono registrate in appositi distinti verbali, sottoscritti, in duplice originale, dal sub-responsabile del trattamento e dal soggetto che svolge ciascuna verifica.

Articolo 26
COMUNICAZIONE INTERNA DI DOCUMENTI CONTENENTI DATI PERSONALI

1. La comunicazione di documenti, secondo la definizione di cui all'art. 1, comma 1, lettera a). del DPR n. 445/2000, contenenti dati personali non è soggetta a limitazioni particolari, salvo quelle espressamente previste da leggi e regolamenti.
2. Il Responsabile del trattamento può tuttavia disporre, con adeguata motivazione, le misure necessarie per la protezione dei dati personali, qualora la comunicazione concerna dati sensibili e/o giudiziari

CAPO IV
SICUREZZA DEI DATI PERSONALI

Articolo 27
MISURE PER LA SICUREZZA DEI DATI PERSONALI
(art. 32 – C83 - RGPD)

1. Il Titolare e i Responsabili del trattamento nonché l'Amministratore del sistema informatico e il Responsabile della protezione dei dati provvedono, per quanto di rispettiva competenza, all'adozione e alla dimostrazione di attuazione concreta di misure tecniche ed organizzative adeguate per garantire un livello di sicurezza correlato al rischio tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche. Per il trattamento dei dati analogici, si rinvia alle specifiche di cui all'allegato A del presente regolamento, mentre per il trattamento dei dati informatici, si rinvia alle specifiche di cui all'allegato B del presente regolamento.
2. Le misure tecniche ed organizzative di sicurezza da mettere in atto per ridurre i rischi del trattamento ricomprendono: la pseudonimizzazione; la minimizzazione; la cifratura dei dati personali; la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi con cui sono trattati i dati personali; la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico; una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
3. Costituiscono misure tecniche ed organizzative che possono essere adottate dal servizio cui è preposto ciascun Responsabile del trattamento:
   - sistemi di autenticazione, autorizzazione e protezione (antivirus; firewall; antintrusione; altro);
   - misure antincendio; sistemi di rilevazione di intrusione; sistemi di sorveglianza; sistemi di protezione con videosorveglianza; registrazione accessi; porte, armadi e contenitori dotati di serrature e ignifughi; sistemi di copiatura e conservazione di archivi elettronici; altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico.
4. La conformità del trattamento dei dati al RGDP in materia di protezione dei dati personali è dimostrata attraverso l'adozione delle misure di sicurezza o l'adesione a codici di condotta approvati o ad un meccanismo di certificazione approvato.
5. Il Titolare e i Responsabili del trattamento nonché l'Amministratore del sistema informatico e il Responsabile della protezione dei dati provvedono, per quanto di rispettiva competenza, a impartire adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per loro conto ed abbia accesso a dati personali.
6. I nominativi e i dati di contatto del Titolare e dei Responsabili del trattamento nonché dell'Amministratore del sistema informatico e del Responsabile della protezione dei dati sono pubblicati sul sito web dell'Ateneo, nella sezione "privacy".
7. I responsabili del trattamento provvedono, nell'ambito dei propri poteri di controllo, a effettuare periodiche verifiche sulla corretta applicazione della normativa in materia di

trattamento dei dati personali nell'ambito delle articolazioni organizzative cui sono preposti, in accordo con i controlli specifici effettuati dal responsabile della protezione dei dati.

Articolo 28
REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO
(art. 30 – C82 - RGPD)

1. È istituito il Registro delle attività di trattamento svolte dal Titolare del trattamento, sul quale sono annotate almeno le seguenti informazioni:
   a) il nome ed i dati di contatto del Titolare del Trattamento ai sensi del precedente art. 2, eventualmente del Contitolare del trattamento, del RPD;
   b) le finalità del trattamento;
   c) la sintetica descrizione delle categorie di interessati, nonché le categorie di dati personali;
   d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
   e) l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;
   f) ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
   g) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate.
2. Il Registro è tenuto dal Titolare in forma telematica, unitamente al Registro delle categorie delle attività trattate dai Responsabili del trattamento di cui al successivo art. 29, secondo lo schema allegato A al presente Regolamento; nello stesso possono essere inserite ulteriori informazioni tenuto conto delle dimensioni organizzative dell'Ateneo. È in facoltà del Titolare del trattamento, sentiti i Responsabili del trattamento, l'Amministratore del sistema informatico e il Responsabile della protezione dei dati, estrapolare dal predetto schema i dati attinenti ai rischi rilevati, alla loro ponderazione e alle rispettive misure individuate, annotandoli in un distinto apposito registro.
3. Il Titolare del trattamento può delegare la tenuta del predetto Registro unitario e dell'eventuale distinto Registro dei rischi e delle misure al Responsabile a un solo Responsabile del trattamento ovvero al RPD, sotto la responsabilità del medesimo Titolare. Ciascun Responsabile del trattamento ha comunque la responsabilità di fornire prontamente e correttamente al soggetto preposto ogni elemento necessario alla regolare tenuta ed aggiornamento del Registro unico.
4. Il Registro deve essere aggiornato annualmente entro il termine e in conformità alle direttive diramate dal Responsabile della protezione dei dati, il quale è tenuto a comunicare, entro trenta giorni successivi al predetto termine, le eventuali inadempienze al Titolare del trattamento per le eventuali responsabilità dirigenziali e disciplinari che ne conseguono.

Articolo 29
VALUTAZIONI DI IMPATTO SULLA PROTEZIONE DEI DATI
(artt. 35 e 36 – C84, C89, C93, C94, C95, C96 - RGPD)

1. Nel caso in cui una tipologia di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare, prima di effettuare il trattamento, deve attuare una valutazione dell'impatto del medesimo trattamento (DPIA) ai sensi dell'art. 35 RGDP, considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento. La valutazione dell'impatto del medesimo trattamento (DPIA) è una procedura che permette di realizzare e dimostrare la conformità alle norme del trattamento di cui trattasi.
2. Ai fini della decisione di effettuare o meno la DPIA si tiene conto degli elenchi delle tipologie di trattamento soggetti o non soggetti a valutazione come redatti e pubblicati dal Garante Privacy ai sensi dell'art. 35, paragrafi 4- 6, del RGDP.
3. Fermo restando quanto indicato dall'art. 35, paragrafo 3, del RGDP, i criteri in base ai quali sono evidenziati i trattamenti determinanti un rischio intrinsecamente elevato, sono i seguenti:
   a) trattamenti valutativi o di scoring, compresa la profilazione e attività predittive, concernenti aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato;
   b) decisioni automatizzate che producono significativi effetti giuridici o di analoga natura, ossia trattamenti finalizzati ad assumere decisioni su interessati che producano effetti giuridici sulla persona fisica ovvero che incidono in modo analogo significativamente su dette persone fisiche;
   c) monitoraggio sistematico, ossia trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o la sorveglianza sistematica di un'area accessibile al pubblico;
   d) trattamenti di dati sensibili o dati di natura estremamente personale, ossia le categorie particolari di dati personali di cui all'art. 9 del RGDP;
   e) trattamenti di dati su larga scala, tenendo conto: del numero di numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento; volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento; durata o persistenza dell'attività di trattamento; ambito geografico dell'attività di trattamento;
   f) combinazione o raffronto di insiemi di dati, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato;
   g) dati relativi a interessati vulnerabili, ossia ogni interessato particolarmente vulnerabile e meritevole di specifica tutela per il quale si possa identificare una situazione di disequilibrio nel rapporto con il Titolare del trattamento, come i dipendenti dell'Ateneo, soggetti con patologie psichiatriche, richiedenti asilo, pazienti, anziani e minori;
   h) utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;
   i) tutti quei trattamenti che, di per sé, impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.

   Nel caso in cui un trattamento soddisfi almeno due dei criteri sopra indicati occorre, in via generale, condurre una DPIA, salvo che il Titolare, sentito il Responsabile della protezione

dei dati e l'Amministratore del sistema informatico, ritenga motivatamente che non può presentare un rischio elevato; il Titolare può motivatamente ritenere che per un trattamento che soddisfa solo uno dei criteri di cui sopra occorra comunque la conduzione di una DPIA.

4. Il Titolare del trattamento garantisce l'effettuazione della DPIA ed è responsabile della stessa. Il Titolare può affidare la conduzione materiale della DPIA al Responsabile della protezione dei dati ovvero ad altro soggetto, interno o esterno all'Ateneo. Il Titolare deve consultarsi con il RPD anche per assumere la decisione di effettuare o meno la DPIA; tale consultazione e le conseguenti decisioni assunte dal Titolare devono essere documentate nell'ambito della DPIA. Il RPD, se gli viene affidato tale incombenza da parte del Titolare del trattamento, provvede allo svolgimento della DPIA ovvero, se non gli compete la predetta incombenza, monitora lo svolgimento della DPIA.
   I Responsabili del trattamento collaborano e assistono il Titolare del trattamento e il Responsabile della protezione dei dati nella conduzione della DPIA, redigendo per quanto di competenza il Registro unitario di cui ai precedenti articoli 29 e 30 e fornendo ogni informazione necessaria. L'Amministratore del sistema informatico fornisce il necessario supporto al Titolare per lo svolgimento della DPIA.
5. Il Responsabile della protezione dei dati può proporre lo svolgimento di una DPIA in rapporto a uno specifico trattamento, collaborando al fine di mettere a punto la relativa metodologia, definire la qualità del processo di valutazione del rischio e l'accettabilità o meno del livello di rischio residuale. L'Amministratore del sistema informatico può proporre di condurre una DPIA in relazione a uno specifico trattamento, con riguardo alle esigenze di sicurezza od operative.
6. La DPIA non è necessaria nei casi seguenti:
   a) se il trattamento non può comportare un rischio elevato per i diritti e le libertà di persone fisiche ai sensi dell'art. 35, paragrafo 1, del RGDP;
   b) se la natura, l'ambito, il contesto e le finalità del trattamento sono simili a quelli di un trattamento per il quale è già stata condotta una DPIA. In questo caso si possono utilizzare i risultati della DPIA svolta per l'analogo trattamento;
   c) se il trattamento è stato sottoposto a verifica da parte del Garante Privacy prima del 25 maggio 2018 in condizioni specifiche che non hanno subito modifiche;
   d) se un trattamento trova la propria base legale nella vigente legislazione che disciplina lo specifico trattamento, ed è già stata condotta una DPIA all'atto della definizione della base giuridica suddetta.

   Non è necessario condurre una DPIA per quei trattamenti che siano già stati oggetto di verifica preliminare da parte del Garante della Privacy o dal RDP e che proseguano con le stesse modalità oggetto di tale verifica. Inoltre, occorre tener conto che le autorizzazioni del Garante Privacy basate sulla direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite od abrogate.
7. La DPIA è condotta prima di dar luogo al trattamento, attraverso i seguenti processi:
   a) descrizione sistematica del contesto, dei trattamenti previsti, delle finalità del trattamento e tenendo conto dell'osservanza di codici di condotta approvati. Sono altresì indicati: i dati personali oggetto del trattamento, i destinatari e il periodo previsto di conservazione dei dati stessi; una descrizione funzionale del trattamento; gli strumenti coinvolti nel trattamento dei dati personali (hardware, software, reti, persone, supporti cartacei o canali di trasmissione cartacei);
   b) valutazione della necessità e proporzionalità dei trattamenti, sulla base:
      - delle finalità specifiche, esplicite e legittime;

- della liceità del trattamento;
- dei dati adeguati, pertinenti e limitati a quanto necessario;
- del periodo limitato di conservazione;
- delle informazioni fornite agli interessati;
- del diritto di accesso e portabilità dei dati;
- del diritto di rettifica e cancellazione, di opposizione e limitazione del trattamento;
- dei rapporti con i responsabili del trattamento;
- delle garanzie per i trasferimenti internazionali di dati;
- consultazione preventiva del Garante privacy;

c) valutazione dei rischi per i diritti e le libertà degli interessati, valutando la particolare probabilità e gravità dei rischi rilevati. Sono determinati l'origine, la natura, la particolarità e la gravità dei rischi o, in modo più specifico, di ogni singolo rischio (accesso illegittimo, modifiche indesiderate, indisponibilità dei dati) dal punto di vista degli interessati;

d) individuazione delle misure previste per affrontare ed attenuare i rischi, assicurare la protezione dei dati personali e dimostrare la conformità del trattamento con il RGPD, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

8. Il Titolare del trattamento può raccogliere le opinioni degli interessati o dei loro rappresentanti, se gli stessi possono essere preventivamente individuati. La mancata consultazione è specificatamente motivata, così come la decisione assunta in senso difforme dall'opinione degli interessati.
9. Il Titolare deve consultare il Garante Privacy prima di procedere al trattamento se le risultanze della DPIA condotta indicano l'esistenza di un rischio residuale elevato. Il Titolare consulta il Garante Privacy anche nei casi in cui la vigente legislazione stabilisce l'obbligo di consultare e/o ottenere la previa autorizzazione della medesima autorità, per trattamenti svolti per l'esecuzione di compiti di interesse pubblico, fra cui i trattamenti connessi alla protezione sociale ed alla sanità pubblica.
10. La DPIA deve essere effettuata - con eventuale riesame delle valutazioni condotte - anche per i trattamenti in corso che possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, nel caso in cui siano intervenute variazioni dei rischi originari tenuto conto della natura, dell'ambito, del contesto e delle finalità del medesimo trattamento.

Articolo 30
VIOLAZIONE DEI DATI PERSONALI
(artt. 33 e 34 – C85, C86, C87, C88 - RGPD)

1. Per violazione dei dati personali (in seguito "data breach") si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati dall'Ateneo.
2. Il Titolare, ove ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, provvede alla notifica della violazione al Garante Privacy.

La notifica dovrà avvenire entro 72 ore e comunque senza ingiustificato ritardo. Il Responsabile del trattamento è obbligato ad informare il Titolare, senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione.

3. I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al considerando 75 del RGPD, sono i seguenti:
   a) danni fisici, materiali o immateriali alle persone fisiche;
   b) perdita del controllo dei dati personali;
   c) limitazione dei diritti, discriminazione;
   d) furto o usurpazione d'identità;
   e) perdite finanziarie, danno economico o sociale.
   f) decifratura non autorizzata della pseudonimizzazione;
   g) pregiudizio alla reputazione;
   h) perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari).
4. Se il Titolare ritiene che il rischio per i diritti e le libertà degli interessati conseguente alla violazione rilevata è elevato, allora deve informare questi ultimi, senza ingiustificato ritardo, con un linguaggio semplice e chiaro al fine di fare comprendere loro la natura della violazione dei dati personali verificatesi. I rischi per i diritti e le libertà degli interessati possono essere considerati "elevati" quando la violazione può, a titolo di esempio:
   - coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;
   - riguardare categorie particolari di dati personali;
   - comprendere dati che possono accrescere ulteriormente i potenziali rischi (ad esempio dati di localizzazione, finanziari, relativi alle abitudini e preferenze);
   - comportare rischi imminenti e con un'elevata probabilità di accadimento (ad esempio rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito);
   - impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (ad esempio utenti deboli, minori, soggetti indagati).
5. La notifica deve avere il contenuto minimo previsto dall'art. 33 del RGPD, ed anche la comunicazione all'interessato deve contenere almeno le informazioni e le misure di cui al su citato art. 33.
6. Il Titolare del trattamento deve opportunamente documentare le violazioni di dati personali subite, anche se non comunicate alle autorità di controllo, nonché le circostanze ad esse relative, le conseguenze e i provvedimenti adottati o che intende adottare per porvi rimedio. Tale documentazione deve essere conservata con la massima cura e diligenza in quanto può essere richiesta dal Garante Privacy al fine di verificare il rispetto delle disposizioni del RGPD.

Articolo 31
ENTRATA IN VIGORE, PUBBLICAZIONE E DIVULGAZIONE DEL REGOLAMENTO

1. L'efficacia del presente regolamento e dei relativi allegato A e B decorre dal giorno in cui diviene esecutiva la deliberazione con cui è stato approvato.
2. Il presente regolamento è pubblicato sul sito web dell'Ateneo affinché tutti i Responsabili del trattamento e chiunque vi abbia interessa ne prenda cognizione.

ALLEGATO 1
Disciplinare per il trattamento dei dati senza l'ausilio di strumenti elettronici

CAPO I
I PRINCIPI

Articolo 1
INTRODUZIONE, DEFINIZIONI E FINALITÀ

Il presente disciplinare interno ha l'obiettivo di definire l'ambito di applicazione, le modalità e le norme sull'utilizzo della gestione di dati analogici da parte degli utenti (dipendenti, collaboratori, etc.), al fine di tutelare i beni dell'Ateneo ed evitare condotte inconsapevoli e/o scorrette che potrebbero esporre l'Ateneo a problematiche di sicurezza, di immagine e patrimoniali per eventuali danni cagionati anche a terzi.
L'insieme delle norme comportamentali ivi incluse, pertanto, è volto a conformare l'Ateneo ai principi di diligenza, informazione e correttezza nell'ambito dei rapporti di lavoro, con l'ulteriore finalità di prevenire eventuali comportamenti illeciti dei dipendenti, pur nel rispetto dei diritti ad essi attribuiti dall'ordinamento giuridico italiano.
A tal fine, pertanto, si rileva che gli eventuali controlli ivi previsti escludono finalità di monitoraggio diretto ed intenzionale dell'attività lavorativa e sono disposti sulla base della vigente normativa, con particolare riferimento al *Regolamento UE n. 2016/679*, alla *Legge n. 300/1970* (c.d. Statuto dei Lavoratori) ed ai provvedimenti appositamente emanati dall'Autorità Garante (si veda in particolare *Provv. 1 marzo 2007*).

Articolo 2
AMBITO DI APPLICAZIONE

Il presente disciplinare interno si applica ad ogni Utente nella possibilità di interagire con qualsiasi dato analogico di pertinenza dell'Ateneo.
Per Utente si intende, pertanto, a titolo esemplificativo e non esaustivo, ogni dipendente, collaboratore (interno o esterno), nonché i componenti degli organi di controllo, i consulenti, fornitori e/o terzi che in modo continuativo e non occasionale operino all'interno della struttura accademica avente accesso ai locali nei quali sono conservati dati analogici.
Per Ateneo si intende, invece, l'organizzazione e/o comunque il Titolare dei beni e dei dati ivi disciplinate, il quale opererà per mezzo dei soggetti che ne possiedono la rappresentanza.

Articolo 3
TITOLARITÀ DEI BENI E DELLE RISORSE

I beni dove sono custodi i dati analogici costituiscono beni di Ateneo e sono da considerarsi di

esclusiva proprietà dell'Università.
Il loro accesso, pertanto, è consentito solo per finalità di adempimento delle mansioni lavorative affidate ad ogni Utente in base al rapporto in essere (ovvero per scopi professionali afferenti l'attività svolta per l'Ateneo), e comunque per l'esclusivo perseguimento delle finalità di pubblico interesse.

Articolo 4
RESPONSABILITÀ' PERSONALE DELL'UTENTE

Ogni Utente è personalmente responsabile dell'accesso in locali ove presenti dati analogici su indicazione dell'Ateneo nonché dei relativi dati trattati per finalità di pubblico interesse.
A tal fine ogni Utente, nel rispetto dei principi di diligenza sottesi al rapporto instaurato con l'Ateneo, è tenuto a tutelare (per quanto di propria competenza) i dati analogici da utilizzi impropri e non autorizzati, danni o abusi anche derivanti da negligenza, imprudenza o imperizia.
Ogni Utente, pertanto, è tenuto, in relazione al proprio ruolo ed alle mansioni in concreto svolte, ad operare a tutela della sicurezza fisica, riportando al proprio responsabile e senza ritardo eventuali rischi di cui è a conoscenza ovvero violazioni del presente disciplinare interno.
Sono vietati comportamenti che possano creare un danno, anche di immagine, all'Ateneo.

CAPO II
CRITERI DI UTILIZZO DEI DATI PERSONALI ANALOGICI

Articolo 5
CRITERI DI UTILIZZO

I trattamenti di dati personali effettuati senza l'ausilio di strumenti elettronici devono essere effettuati secondo i seguenti criteri:

- L'Ateneo definisce quali siano le mansioni inerenti al trattamento di dati analogici, oltre a definire chi possa avere accesso ai locali ove questi conservati.
- Non è consentito fare copia di questi dati.
- L'accesso a tali dati può avvenire unicamente su indicazione dell'Ateneo stesso.
- L'Ateneo ricorda che le persone coinvolte nella manipolazione, riproduzione, occultamento e/o distruzione illegale di tali dati sono responsabili sia civilmente che penalmente e quindi possono essere condannate al pagamento dei danni e anche alla reclusione.

Articolo 6
DIVIETI

Per i trattamenti di dati personali effettuati senza l'ausilio di strumenti elettronici è fatto divieto di trattare dati, se non preventivamente autorizzati dall'Ateneo;

CAPO III
DISPOSIZIONI FINALI

Articolo 7
SANZIONI

L'eventuale violazione di quanto previsto dal presente disciplinare interno – rilevante anche ai sensi degli art. 2104 e 2105 c.c. - potrà comportare l'applicazione di sanzioni disciplinari in base a quanto previsto dall'art. 7 dello Statuto dei Lavoratori.
L'Ateneo avrà cura di informare senza ritardo (e senza necessità di preventive contestazioni e/o addebiti formali) le autorità competenti, nel caso venga commesso un reato, o la cui commissione sia ritenuta probabile o solo sospettata, tramite l'utilizzo illecito o non conforme dei beni e degli strumenti informatici.

Articolo 8
INFORMATIVA AGLI UTENTI EX ART. 13 Regolamento UE n. 2016/679

Il presente disciplinare interno, nella parte in cui contiene le regole per l'utilizzo dei beni e degli strumenti di ateneo, e relativamente ai trattamenti di dati personali svolti dall'Ateneo e finalizzati alla effettuazione di controlli leciti, così come definiti nell'art. 5, vale quale informativa ex. art. 13 del Regolamento UE n. 2016/679.

Articolo 9
COMUNICAZIONI

Il presente disciplinare interno è messo a disposizione degli utenti, per la consultazione, al momento dell'assegnazione di un account Utente. Sulla intranet di Ateneo, ovvero presso la bacheca di ateneo è pubblicata la versione più aggiornata dello stesso allo scopo di facilitarne la conoscibilità a tutti gli interessati.
Ad ogni aggiornamento del presente documento, ne sarà data comunicazione sulle bacheche di ateneo e tramite l'invio di apposito messaggio e-mail. Tutti gli utenti sono tenuti a conformarsi alla versione più aggiornata del presente disciplinare.
Le autorizzazioni e/o concessioni richieste dal presente disciplinare ovvero poste nella facoltà degli utenti potranno essere comunicate all'Ateneo per mezzo di qualsiasi strumento che ne garantisca la tracciabilità (es: e-mail).

ALLEGATO 2
Disciplinare per l'utilizzo della strumentazione informatica e della rete internet

CAPO I
I PRINCIPI

Articolo 1
INTRODUZIONE, DEFINIZIONI E FINALITÀ

Il presente disciplinare interno ha l'obiettivo di definire l'ambito di applicazione, le modalità e le norme sull'utilizzo della strumentazione informatica da parte degli utenti assegnatari (dipendenti, collaboratori etc.), al fine di tutelare i beni di ateneo ed evitare condotte inconsapevoli e/o scorrette che potrebbero esporre l'Ateneo a problematiche di sicurezza, di immagine e patrimoniali per eventuali danni cagionati anche a terzi.
L'insieme delle norme comportamentali ivi incluse, pertanto, è volto a conformare l'Ateneo ai principi di diligenza, informazione e correttezza nell'ambito dei rapporti di lavoro, con l'ulteriore finalità di prevenire eventuali comportamenti illeciti dei dipendenti, pur nel rispetto dei diritti ad essi attribuiti dall'ordinamento giuridico italiano.
A tal fine, pertanto, si rileva che gli eventuali controlli ivi previsti escludono finalità di monitoraggio diretto ed intenzionale dell'attività lavorativa e sono disposti sulla base della vigente normativa, con particolare riferimento al *Regolamento UE n. 2016/679*, alla *Legge n. 300/1970* (c.d. Statuto dei Lavoratori) ed ai provvedimenti appositamente emanati dall'Autorità Garante (si veda in particolare *Provv. 1 marzo 2007*).

Articolo 2
AMBITO DI APPLICAZIONE

Il presente disciplinare interno si applica ad ogni *Utente* assegnatario di beni e risorse informatiche di ateneo ovvero utilizzatore di servizi e risorse informative di pertinenza dell'Ateneo.
Per Utente si intende, pertanto, a titolo esemplificativo e non esaustivo, ogni dipendente, collaboratore (interno o esterno), nonché i componenti degli organi di controllo, i consulenti, fornitori e/o terzi che in modo continuativo e non occasionale operino all'interno della struttura accademica avente accesso ai locali nei quali sono conservati dati digitali e che siano previamente autorizzati dal Titolare del trattamento.
Per Ateneo si intende, invece, l'organizzazione e/o comunque il Titolare dei beni e dei dati ivi disciplinate, il quale opererà per mezzo dei soggetti che ne possiedono la rappresentanza.

Articolo 3
TITOLARITA' DEI BENI E DELLE RISORSE INFORMATICHE

I beni e le risorse informatiche, i servizi ICT e le reti informative costituiscono beni dell'Università rientranti nel patrimonio di ateneo e sono da considerarsi di esclusiva proprietà dell'Università.
Il loro utilizzo, pertanto, è consentito solo per finalità di adempimento delle mansioni lavorative affidate ad ogni Utente in base al rapporto in essere (ovvero per scopi professionali afferenti l'attività svolta per l'Ateneo), e comunque per l'esclusivo perseguimento degli obiettivi di ateneo.
A tal fine si precisa sin d'ora che qualsivoglia dato e/o informazione trattato per mezzo dei beni e delle risorse informatiche di proprietà dell'Ateneo, sarà dallo stesso considerato come avente natura interna e non riservata.

Articolo 4
RESPONSABILITA' PERSONALE DELL'UTENTE

Ogni Utente è personalmente responsabile dell'utilizzo dei beni e delle risorse informatiche affidatigli dall'Ateneo nonché dei relativi dati trattati per finalità di ateneo.
A tal fine ogni Utente, nel rispetto dei principi di diligenza sottesi al rapporto instaurato con l'Ateneo, è tenuto a tutelare (per quanto di propria competenza) il patrimonio di ateneo da utilizzi impropri e non autorizzati, danni o abusi anche derivanti da negligenza, imprudenza o imperizia. L'obiettivo è quello di preservare l'integrità e la riservatezza dei beni, delle informazioni e delle risorse di ateneo.
Ogni Utente, pertanto, è tenuto, in relazione al proprio ruolo e alle mansioni in concreto svolte, ad operare a tutela della sicurezza informatica, riportando al proprio responsabile e senza ritardo eventuali rischi di cui è a conoscenza ovvero violazioni del presente disciplinare interno.
Sono vietati comportamenti che possano creare un danno, anche di immagine, all'Ateneo.

Articolo 5
I CONTROLLI

I principi
L'Ateneo, in linea con quanto prescritto dall'ordinamento giuridico italiano (art. 4, Statuto dei Lavoratori), esclude la configurabilità di forme di controllo aventi direttamente ad oggetto l'attività lavorativa dell'Utente.
Ciononostante non si esclude che, per ragioni organizzative e produttive ovvero per esigenze dettate dalla sicurezza del lavoro, si utilizzino sistemi informatici, impianti o apparecchiature dai quali derivi la possibilità di controllo a distanza dell'attività dei lavoratori.

I controlli non autorizzati
In ogni caso l'Ateneo non può in alcun caso utilizzare sistemi da cui derivino forme di controllo a distanza dell'attività lavorativa che permettano di ricostruire l'attività del lavoratore.

Per tali s'intendono, a titolo meramente esemplificativo e non esaustivo:

- la lettura e la registrazione sistematica dei messaggi di posta elettronica, al di là di quanto necessario per fornire e gestire il servizio di posta elettronica stesso;
- la memorizzazione sistematica delle pagine internet visualizzate da ciascun Utente, dei contenuti ivi presenti, e del tempo di permanenza sulle stesse;
- la lettura e la registrazione dei caratteri inseriti dal lavoratore tramite tastiera o dispositivi analoghi;
- l'analisi dei dispositivi per l'accesso alla rete internet;

CAPO II
MISURE ORGANIZZATIVE

Articolo 6
AMMINISTRATORE DEL SISTEMA

L'Ateneo conferisce all'amministratore di sistema il compito di sovrintendere i beni e le risorse informatiche di ateneo. I compiti dell'amministratore di sistema sono indicati nell'art. 23 del Regolamento per la protezione dei dati personali in attuazione del Regolamento UE 2016/679 "Regolamento generale per la protezione dei dati"

Articolo 7
ASSEGNAZIONE DEGLI ACCOUNT E GESTIONE DELLE PASSWORD

Creazione e gestione degli Account

Un account Utente consente l'autenticazione dell'utilizzatore e di conseguenza ne disciplina l'accesso alle risorse informatiche, per singola postazione lavorativa.

Gli account utenti vengono creati dagli amministratori di sistema e sono personali, ovvero associati univocamente alla persona assegnataria;

L'accesso al proprio account avviene tramite l'utilizzo delle "credenziali di autenticazione" (es. "Username" e "Password"), comunicate all'Utente dall'amministratore di sistema, che le genera, attraverso modalità che ne garantiscano la segretezza (Es: busta chiusa e sigillata);

Le credenziali di autenticazioni costituiscono dati di ateneo da mantenere strettamente riservati e non è consentito comunicarne gli estremi a terzi (seppur soggetti in posizione apicale all'interno dell'Ateneo).

Se l'Utente ha il sospetto che le proprie credenziali di autenticazione siano state identificate da qualcuno, o il sospetto di un utilizzo non autorizzato del proprio account e delle risorse a questo associate, lo stesso è tenuto a modificare immediatamente la password e/o a segnalare la violazione all'amministratore del sistema nonché al Responsabile privacy di riferimento;

Ogni Utente è responsabile dell'utilizzo del proprio account Utente;

In caso di assenza improvvisa o prolungata del lavoratore e per improrogabili necessità legate all'attività lavorativa, per le esigenze produttive di ateneo o per la sicurezza ed operatività delle risorse informatiche dell'Ateneo, lo stesso si riserva la facoltà di accedere a qualsiasi dotazione e/o

apparato assegnato in uso all'Utente per mezzo dell'intervento dell'Amministratore di sistema.
Si ricorda, infine, che i beni e la strumentazione informatica oggetto del presente disciplinare interno rimane di esclusivo dominio dell'Ateneo, il quale, in virtù dei rapporti instaurati con gli utenti, ne disciplina l'affidamento.

Gestione e utilizzo delle password.
Dopo la prima comunicazione delle credenziali di autenticazione da parte dell'amministratore di sistema, l'Utente ha il compito di modificare, al suo primo utilizzo, la propria password, procedendo allo stesso modo ogni 6 mesi. In caso di trattamento di categorie particolari di dati, di cui agli artt. 9 e 10 del Regolamento UE 2016/679, la parola chiave è modificata ogni 3 mesi.
L'Utente, nel definire il valore della password, deve rispettare le seguenti regole:

- utilizzare almeno 8 caratteri alfanumerici, inclusi i caratteri speciali (#, %, etc.), di cui almeno uno numerico;
- la password deve contenere almeno un carattere maiuscolo, un carattere minuscolo, un numero o un carattere non alfanumerico tipo "@#§£$%...";
- evitare di includere parti del nome, cognome e/o comunque elementi a lui agevolmente riconducibili;
- evitare l'utilizzo di password comuni e/o prevedibili;
- proteggere con la massima cura la riservatezza della password ed utilizzarla entro i limiti di autorizzazione concessi.

Si ricorda che scrivere la password su post-it o altri supporti non è conforme alla normativa e costituisce violazione del presente disciplinare interno.

Cessazione degli Account
In caso di interruzione del rapporto di lavoro con l'Utente, le credenziali di autenticazione di cui sopra verranno disabilitate entro un periodo massimo di 30 giorni da quella data; entro 6 mesi, invece, si disporrà la definitiva e totale cancellazione dell'account Utente.

Articolo 8
POSTAZIONI DI LAVORO

Per postazione di lavoro si intende il complesso unitario di Personal Computer (di seguito, PC), notebook, accessori, periferiche e ogni altro *devices* concesso, dall'Ateneo, in utilizzo all'Utente. L'assegnatario di tali beni e strumenti informatici, pertanto, ha il compito di farne un uso compatibile con i principi di diligenza sanciti nel codice civile.
Al fine di disciplinare un corretto utilizzo di tali beni, l'Ateneo ha adottato le regole tecniche, che di seguito si riportano:

- Ogni PC, notebook (accessori e periferiche incluse), e altro *devices*, sia esso acquistato, noleggiato, o affidato in locazione, rimane di esclusiva proprietà dell'Ateneo, ed è concesso all'Utente per lo svolgimento delle proprie mansioni lavorative e comunque per finalità strettamente attinenti l'attività svolta;
- È dovere di ogni Utente usare i computer e gli altri dispositivi a lui affidati responsabilmente

e professionalmente;

- Il PC e gli altri dispositivi di cui sopra devono essere utilizzati con hardware e software autorizzati dall'Ateneo. Per utilizzare software o applicativi non presenti nella dotazione standard fornita, si necessita di espressa richiesta scritta dell'Utente indirizzata all'amministratore di sistema, il quale ne valuterà i requisiti tecnici e l'aderenza alle policy interne;
- Le postazioni di lavoro non devono essere lasciate incustodite con le sessioni utenti attive;
- Quando un Utente si allontana dalla propria postazione di lavoro, deve bloccare tastiera e schermo con un programma salvaschermo (screensaver) protetto da password o effettuare il log-out dalla sessione;
- L'Utente deve segnalare con la massima tempestività all'amministratore del sistema ovvero al proprio Responsabile di riferimento eventuali guasti tecnici, problematiche tecniche o il cattivo funzionamento delle apparecchiature;
- È fatto divieto di cedere in uso, anche temporaneo, le attrezzature e i beni informatici a soggetti terzi;
- L'Ateneo si riserva la facoltà di rimuovere qualsiasi elemento hardware e/o software la cui installazione non sia stata appositamente e preventivamente prevista o autorizzata.

Gli apparecchi di proprietà personale dell'Utente quali computer portatili, telefoni cellulari, agende palmari (PDA), hard disk esterni, penne USB, lettori musicali o di altro tipo, fotocamere digitali, ecc. non potranno essere collegati ai computer o alle reti informatiche di ateneo, salvo preventiva autorizzazione scritta dell'Ateneo.

Articolo 9
BACKUP DATI

Al fine di garantire la sicurezza dei dati, sono previste operazioni di backup dei dati, effettuate periodicamente, con cadenza settimanale.
È unicamente designato a tale attività l'amministratore di sistema nominato, il quale effettuerà le copie di backup dei dispositivi in dotazione dell'Ateneo, su cui vengono registrati tutti i dati acquisiti, strettamente necessari per lo scopo perseguito.

CAPO III
CRITERI DI UTILIZZO DEGLI STRUMENTI INFORMATICI

Articolo 10
PERSONAL COMPUTER E COMPUTER PORTATILI

Gli utenti utilizzano per l'espletamento delle proprie mansioni dispositivi di proprietà dell'Ateneo; ne consegue che gli stessi sono tenuti al rispetto delle seguenti regole:

- Non è consentito modificare la configurazione hardware e software del proprio PC, se

non previa esplicita autorizzazione dell'Ateneo che la esegue per mezzo dell'amministratore del sistema;
- Non è consentito rimuovere, danneggiare o asportare componenti hardware;
- Non è consentito installare autonomamente programmi informatici, software ed ogni altro applicativo non autorizzato espressamente dall'Ateneo;
- È onere dell'Utente, in relazione alle sue competenze, eseguire richieste di aggiornamento sulla propria postazione di lavoro derivanti da software antivirus nonché sospendere ogni attività in caso di minacce *virus* o altri malfunzionamenti, segnalando prontamente l'accaduto all'amministratore del sistema;
- è onere dell'Utente spegnere il proprio PC o computer portatile al termine del lavoro.

Per quanto concerne, invece, la gestione dei computer portatili, l'Utente ha l'obbligo di custodirli con diligenza e in luogo protetto durante gli spostamenti, rimuovendo gli eventuali *files* elaborati prima della sua riconsegna.
Non è consentito all'Utente caricare o inserire all'interno del portatile qualsiasi dato personale non attinente con l'attività lavorativa svolta. In ogni caso, al fine di evitare e/o ridurre al minimo la possibile circolazione di dati personali sull'apparecchio, si ricorda agli utenti di cancellare tutti i dati eventualmente presenti prima di consegnare il portatile agli uffici competenti per la restituzione o la riparazione.

Articolo 11
SOFTWARE

Premesso che l'installazione di software privi di regolare licenza non è consentita in nessun caso, gli utenti dovranno ottenere espressa autorizzazione dell'Ateneo per installare o comunque utilizzare qualsiasi programma o software dotato di licenza non proprietaria ("freeware" o "shareware").
L'Ateneo richiama l'attenzione del proprio personale su alcuni aspetti fondamentali che l'Utente è tenuto ad osservare per un corretto utilizzo del software nell'Ateneo;

- L'Ateneo acquista le licenze d'uso dei software da vari fornitori esterni. L'Utente, pertanto, è soggetto a limitazioni nell'utilizzo di tali programmi e della relativa documentazione e non ha il diritto di riprodurlo in deroga ai diritti concessigli. Tutti gli utenti sono quindi tenuti a utilizzare il software entro i limiti specificati nei contratti di licenza.
- Non è consentito fare né il download né l'upload tramite internet di software non autorizzati.
- L'Ateneo, sulla scorta di quanto disposto dalle normative a tutela della proprietà intellettuale e del diritto d'autore, ricorda che le persone coinvolte nella riproduzione illegale del software sono responsabili sia civilmente che penalmente e quindi possono essere condannate al pagamento dei danni e anche alla reclusione.
- L'Ateneo non tollererà la duplicazione illegale del software.

Articolo 12
DISPOSITIVI DI MEMORIA PORTATILI

Per dispositivi di memoria portatili si intendono tutti quei dispositivi che consentono di copiare o archiviare dati, files, o documenti esternamente al computer. Sono considerati tali CD-ROM, DVD, penne o chiavi di memoria USB, riproduttori musicali MP3, fotocamere digitali, dischi rigidi esterni, etc.
L'utilizzo di tali supporti risponde alle direttive che di seguito si riportano:

- non è consentito utilizzare supporti rimovibili personali, se non preventivamente autorizzati per iscritto dall'Ateneo;
- è onere dell'Utente custodire i supporti magnetici contenenti dati sensibili e giudiziari in armadi chiusi a chiave, onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto.
- Si precisa che, ove autorizzati in base a quanto sopra disposto, una volta connessi all'infrastruttura informatica dell'Ateneo, i dispositivi saranno soggetti (ove compatibili) al presene disciplinare interno.

Articolo 13
STAMPANTI, FOTOCOPIATRICI, SCANNER E FAX

L'utilizzo dei suddetti strumenti deve avvenire sempre per scopi professionali. Non è consentito un utilizzo per fini diversi o privati, salvo una specifica autorizzazione da parte dell'Ateneo.
È richiesta una particolare attenzione quando si invia su una stampante condivisa documenti aventi ad oggetto dati personali o informazioni riservate; ciò al fine di evitare che persone non autorizzate possano venirne a conoscenza. Si richiede quindi di evitare di lasciare le stampe incustodite e ritirarne immediatamente le copie non appena uscite dalla stampa.
L'utilizzo dei fax per l'invio di documenti che hanno natura strettamente confidenziale, è generalmente da evitare. Nei casi in cui questo sia necessario, si deve preventivamente avvisare il destinatario, in modo da ridurre il rischio che persone non autorizzate possano venirne a conoscenza, e successivamente chiedere la conferma telefonica di avvenuta ricezione.
L'utilizzo della funzione di scannerizzazione di documenti analogici in digitale, comporta l'immediato trasferimento del file dalla cartella di destinazione condivisa da ciascun PC all'inserimento delle apposite cartelle presenti su ciascuna postazione.

CAPO IV
GESTIONE DELLE COMUNICAZIONI TELEMATICHE

Articolo 14
GESTIONE UTILIZZO DELLA RETE INTERNET

Ogni Utente potrà essere abilitato, dall'Ateneo, alla navigazione Internet. Col presente disciplinare

interno si richiama gli utenti ad una particolare attenzione nell'utilizzo di Internet e dei servizi relativi, in quanto ogni operazione posta in essere è associata all' "Indirizzo Internet Pubblico" assegnato all'Ateneo stesso.
Internet è uno strumento messo a disposizione degli utenti per uso professionale. Ciascun utente, pertanto, deve usare la rete Internet in maniera appropriata, tenendo presente che ogni sito web può essere governato da leggi diverse da quelle vigenti in Italia; l'Utente deve, quindi, prendere ogni precauzione a tale riguardo.

Le norme di comportamento da osservare nell'utilizzo delle connessioni ad Internet sono le seguenti:

a. L'utilizzo è consentito esclusivamente per scopi accademici e, pertanto, non è consentito navigare in siti non attinenti allo svolgimento delle proprie mansioni lavorative.
b. Non è consentita l'effettuazione di ogni genere di transazione finanziaria, ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo casi espressamente autorizzati dall'Ateneo.
c. È vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.
d. Non sono permesse, se non per motivi professionali, la partecipazione a forum, l'utilizzo di chat-line o di bacheche elettroniche e le registrazioni in *guest-book*, anche utilizzando pseudonimi (o nicknames).
e. Non è consentita la navigazione in siti e la memorizzazione di documenti informatici di natura oltraggiosa, pornografica, pedopornografica e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.
f. È consentito l'utilizzo di soluzioni di Instant Messanger e/o chat esclusivamente per scopi professionali ed attraverso gli strumenti ed i software messi a disposizione dall'Ateneo.
g. Non è consentito l'utilizzo di sistemi di social networking sul luogo di lavoro o durante l'orario lavorativo.
h. Non è consentito lo scambio e/o la condivisione (es. i c.d. sistemi di Peer-to-Peer) a qualsiasi titolo, anche se non a scopo di lucro, di materiale audiovisivo, cinematografico, fotografico, informatico, etc., protetto da copyright.
i. Non è consentito sfruttare i marchi registrati, i segni distintivi e ogni altro bene immateriale di proprietà dell'Ateneo in una qualsiasi pagina web o pubblicandoli su Internet, a meno che tale azione non sia stata approvata espressamente;

Per facilitare il rispetto delle predette regole, l'Ateneo si riserva, per mezzo dell'amministratore di sistema, la facoltà di configurare specifici filtri che inibiscono l'accesso ai contenuti ivi non consentiti (con esclusione dei siti istituzionali) e che prevengono operazioni non correlate all'attività lavorativa (es. upload, restrizione nella navigazione, download di *file* o software).

Articolo 15
GESTIONE E UTILIZZO DELLA POSTA ELETTRONICA

Principi guida
Ad ogni Utente titolare di un account, l'Ateneo provvede ad assegnare una casella di posta elettronica individuale.

I servizi di posta elettronica devono essere utilizzati a scopo professionale: si ricorda a tutti gli utenti che l'account e-mail è uno strumento di proprietà dell'Ateneo ed è conferito in uso per l'esclusivo svolgimento delle mansioni lavorative affidate.
Ad uno stesso Utente possono essere assegnate più caselle di posta elettronica che non possono essere condivise con altri utenti dello stesso gruppo/dipartimento. Tali caselle devono essere utilizzate esclusivamente per la ricezione dei messaggi, mentre per le risposte o gli invii, si deve sempre utilizzare la casella di posta assegnata.
L'Ateneo valuterà caso per caso e previa richiesta dell'Utente, la possibilità di attribuire allo stesso un diverso indirizzo destinato ad uso privato.
Attraverso l'e-mail, gli utenti rappresentano pubblicamente l'Ateneo e per questo motivo viene richiesto di utilizzare tale sistema in modo lecito, professionale e comunque tale da riflettere l'immagine dell'Ateneo.
Gli utenti sono responsabili del corretto utilizzo delle caselle di posta elettronica di ateneo e sono tenuti ad utilizzarla in modo conforme alle presenti regole. Gli stessi, pertanto, devono:

- conservare la password nella massima riservatezza e con la massima diligenza;
- mantenere la casella in ordine, cancellando documenti inutili e allegati ingombranti;
- utilizzare, la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario;
- prestare attenzione alla dimensione degli allegati per la trasmissione di file all'interno della struttura nonché alla posta ricevuta. Gli allegati provenienti da mittenti sconosciuti non devono essere aperti in quanto possono essere utilizzati come veicolo per introdurre programmi dannosi (es. virus).
- inviare preferibilmente *files* in formato PDF;
- accertarsi dell'identità del mittente e controllare a mezzo di software antivirus i files attachment di posta elettronica prima del loro utilizzo;
- rispondere ad e-mail pervenute solo da emittenti conosciuti e cancellare preventivamente le altre;
- collegarsi a siti internet contenuti all'interno di messaggi solo quando vi sia comprovata sicurezza sul contenuto degli stessi.

Non è consentito agli utenti, al contrario:

- diffondere il proprio indirizzo e-mail di ateneo attraverso la rete internet;
- utilizzare la casella di posta elettronica di ateneo per inviare, ricevere o scaricare allegati contenenti video, brani musicali, etc., salvo che questo non sia funzionale all'attività prestata in favore dell'Ateneo (es: presentazioni o materiali video).

Si ricorda che, salvo l'utilizzo di appositi strumenti di cifratura, i sistemi di posta elettronica non possono garantire la riservatezza delle informazioni trasmesse. Pertanto, si richiede agli utenti di valutare con attenzione l'invio di informazioni classificabili quali "riservate" o aventi comunque carattere "strettamente confidenziale".
Occorre inoltre che i messaggi di posta elettronica contengano un avvertimento ai destinatari, nel quale sia dichiarata l'eventuale natura non personale dei messaggi stessi e precisato che le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente.
Nei casi in cui l'Ateneo si doti di posta elettronica certificata si applicheranno, ove compatibili, le presenti disposizioni.

Cessazione dell'indirizzo di posta elettronica

In caso di interruzione del rapporto di lavoro con l'Utente, l'indirizzo di posta elettronica verrà

disabilitato entro un periodo massimo di 30 giorni da quella data; entro 6 mesi, invece, si disporrà la definitiva e totale cancellazione dello stesso. In ogni caso, l'Ateneo si riserva il diritto di conservare i messaggi di posta elettronica che riterrà rilevanti.

Articolo 16
SANZIONI

L'eventuale violazione di quanto previsto dal presente disciplinare interno – rilevante anche ai sensi degli art. 2104 e 2105 c.c. - potrà comportare l'applicazione di sanzioni disciplinari in base a quanto previsto dall'art. 7 dello Statuto dei Lavoratori.
L'Ateneo avrà cura di informare senza ritardo (e senza necessità di preventive contestazioni e/o addebiti formali) le autorità competenti, nel caso venga commesso un reato, o la cui commissione sia ritenuta probabile o solo sospettata, tramite l'utilizzo illecito o non conforme dei beni e degli strumenti informatici.
Si precisa, infine, che in caso di violazione accertata da parte degli utenti delle regole e degli obblighi esposti in questo disciplinare, l'Ateneo si riserva la facoltà di sospendere, bloccare o limitare gli accessi di un account, quando appare ragionevolmente necessario per proteggere l'integrità, la sicurezza e/o la funzionalità dei propri beni e strumenti informatici.

Articolo 17
INFORMATIVA AGLI UTENTI EX ART. 13 Regolamento UE n. 2016/679

Il presente disciplinare interno, nella parte in cui contiene le regole per l'utilizzo dei beni e degli strumenti informatici di ateneo, e relativamente ai trattamenti di dati personali svolti dall'Ateneo e finalizzati alla effettuazione di controlli leciti, così come definiti nell'art. 5, vale quale informativa ex. art. 13 del Regolamento UE n. 2016/679.

Articolo 18
COMUNICAZIONI

Il presente disciplinare interno è messo a disposizione degli utenti, per la consultazione, con pubblicazione sul sito web di ateneo.
Ad ogni aggiornamento del presente documento, ne sarà data comunicazione con le medesime modalità. Tutti gli utenti sono tenuti a conformarsi alla versione più aggiornata del presente disciplinare.
Le autorizzazioni e/o concessioni richieste dal presente disciplinare ovvero poste nella facoltà degli utenti potranno essere comunicate all'Ateneo per mezzo di qualsiasi strumento che ne garantisca la tracciabilità (es: e-mail).