Disciplina per il trattamento dei dati personali da parte del Responsabile del trattamento

Versione 1.0 del 13/05/2017

ART. 1 - FINALITÀ

Il presente documento ha lo scopo di definire le modalità con le quali il Responsabile del trattamento (ai sensi dell'art. 28 del Regolamento UE 2016/679 - GDPR) (di seguito RESPONSABILE), formalmente nominato dall'Università degli Studi di Roma "La Sapienza" in qualità di Titolare del trattamento (di seguito TITOLARE) nell'ambito di un rapporto contrattuale fra le parti, si impegna ad effettuare operazioni di trattamento dei dati personali per conto del TITOLARE.

ART. 2 - OBBLIGHI GENERALI DEL RESPONSABILE

Il RESPONSABILE è tenuto a trattare i dati personali solo ed esclusivamente ai fini della prestazione dei servizi specificati nell'atto di nomina, nel rispetto di quanto disposto dalla normativa applicabile e vigente in materia di protezione dei dati personali, nonché delle istruzioni del TITOLARE riportate nei successivi punti, e di ogni altra indicazione scritta che potrà essergli dallo stesso fornita, nei limiti delle prestazioni contrattualmente dovute in suo favore.
Il RESPONSABILE nei limiti delle prestazioni contrattualmente dovute, si impegna a:

- trattare i dati in modo lecito, corretto e trasparente nei confronti dell'interessato, nell'ambito esclusivo delle finalità per le quali eroga i propri servizi in favore del TITOLARE;
- trattare i dati personali solamente su istruzione documentata del TITOLARE, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale;
- formare adeguatamente i propri dipendenti e collaboratori rispetto all'applicazione del Regolamento e della presente Disciplina e vigilare sull'operato dei propri incaricati, amministratori di sistema ed eventuali sub-responsabili, facendo sottoscrivere a costoro un apposito impegno di riservatezza;
- garantire che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza, anche somministrando agli autorizzati un accordo di riservatezza redatto per tale precipuo scopo;
- adottare le misure richieste ai sensi dell'art. 32 del GDPR, come meglio descritto al successivo art. 3 "Misure di Sicurezza";
- tenere un registro dei trattamenti in qualità di RESPONSABILE, ex art. 30 del GDPR;
- rispettare le condizioni previste dal GDPR nel ricorrere ad un altro RESPONSABILE, come meglio descritto all'art. 11 "Altri Responsabili del Trattamento";
- assistere il TITOLARE, tenendo conto della natura del trattamento stesso, con misure tecniche e organizzative adeguate, al fine di soddisfare l'obbligo del TITOLARE di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III del GDPR;
- assistere il TITOLARE nel garantire il rispetto degli obblighi di cui agli artt. da 32 a 36 del GDPR, tenendo conto della natura del trattamento e delle informazioni a disposizione del RESPONSABILE;
- garantire la cancellazione o la restituzione di tutti i dati personali, su richiesta del TITOLARE, al termine della prestazione dei servizi relativi al trattamento, nonché la cancellazione delle copie esistenti, salvo che la legge non preveda la conservazione di tali dati;
- mettere a disposizione del TITOLARE tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'art. 28 del GDPR;
- consentire e contribuire alle attività di revisione e ispezione realizzate dal TITOLARE o da soggetto da questi delegato.

Il RESPONSABILE, altresì, si impegna affinché i dati personali relativi alle attività di trattamento poste in essere in virtù dell'atto di nomina:

- vengano trattati per scopi determinati, espliciti e legittimi, e, se utilizzati in altre operazioni di trattamento, questi debbono essere processati in termini compatibili con tali scopi, ed in ogni caso nei limiti in cui il trattamento sia necessario per l'erogazione dei servizi, nel rispetto dei principi di pertinenza e necessità;
- siano esatti e, se necessario, aggiornati;
- siano pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono trattati;
- siano archiviati in una forma che ne consenta la cancellazione, la rettifica (nonché la conseguente notificazione agli eventuali destinatari a cui sono stati trasmessi i dati personali oggetto di richiesta di rettifica o cancellazione), nonché la limitazione o l'opposizione al relativo trattamento;
- siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali gli stessi sono stati raccolti e successivamente trattati.

ART. 3 - MISURE DI SICUREZZA

Il RESPONSABILE si impegna a individuare e adottare misure tecniche e organizzative appropriate ed adatte a garantire un livello di sicurezza adeguato al rischio, tenendo conto, fra l'altro, della tipologia di trattamento, delle finalità perseguite, del contesto e delle specifiche circostanze in cui avviene il trattamento, nonché della tecnologia applicabile e dei costi di attuazione. Tali misure comprendono:

I. la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali;
II. la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati personali in caso di incidente fisico o tecnico;
III. una procedura adeguata (messa a disposizione del TITOLARE su richiesta) per provare, verificare e valutare regolarmente l'efficacia delle misure adottate al fine di garantire la sicurezza del trattamento;
IV. ove espressamente richieste dal TITOLARE, l'anonimizzazione, la pseudonimizzazione o la cifratura dei dati personali, previa valutazione dei rischi con il RESPONSABILE.

Il RESPONSABILE dovrà in particolare attenersi scrupolosamente alle disposizioni emanate da AgID con Circolare 18 aprile 2017, n. 2/2017 relativa alle Misure minime di sicurezza ICT per le pubbliche amministrazioni.

ART. 4 - VIOLAZIONE DI DATI PERSONALI (cd. DATA BREACH)

Il RESPONSABILE si impegna ad informare tempestivamente il TITOLARE (inviando una comunicazione a mezzo PEC all'indirizzo rpd@cert.uniroma1.it) di ogni violazione della sicurezza che comporti 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, ed a prestare ogni necessaria collaborazione al TITOLARE in relazione all'adempimento dei propri obblighi di notifica delle suddette violazioni al Garante ai sensi dell'art. 33 del GDPR o di comunicazione della stessa agli interessati ai sensi dell'art. 34 del GDPR.

La comunicazione dovrà pervenire entro e non oltre le 24 (ventiquattro) ore dalla violazione, quale termine perentorio.

Nel caso di omessa e/o tardiva comunicazione da parte del RESPONSABILE, il TITOLARE si riserva la facoltà di valutare eventuali danni patrimoniali da commisurare all'entità ed alle conseguenze del Data Breach, ai fini di esercitare un diritto di rivalsa nei confronti del RESPONSABILE.

La comunicazione al TITOLARE conterrà almeno le seguenti informazioni:

I. la natura della violazione dei dati personali,
II. la categoria degli interessati,
III. contatto presso cui ottenere più informazioni,
IV. interventi attuati o che si prevede di attuare.

Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

ART. 5 - VALUTAZIONE D'IMPATTO (cd. DATA PROTECTION IMPACT ASSESSMENT)
Il RESPONSABILE si impegna a fornire al TITOLARE ogni elemento utile all'effettuazione, da parte di quest'ultimo, della valutazione di impatto sulla protezione dei dati, qualora lo stesso sia tenuto ad effettuarla ai sensi dell'art. 35 del GDPR, nonché ogni collaborazione nell'effettuazione della eventuale consultazione preventiva al Garante ai sensi dell'art. 36 del GDPR.

ART. 6 - SOGGETTI AUTORIZZATI AL TRATTAMENTO
Il RESPONSABILE è tenuto a fornire ai propri dipendenti e collaboratori deputati a trattare i dati personali per conto del titolare le istruzioni idonee allo scopo, vincolandoli alla riservatezza su tutte le informazioni acquisite nello svolgimento della loro attività, anche per il periodo successivo alla cessazione del rapporto di lavoro o collaborazione.

ART. 7 - AMMINISTRATORI DI SISTEMA
Nel caso in cui il RESPONSABILE eroghi i servizi attraverso sistemi informativi diversi da quelli forniti dal TITOLARE, il RESPONSABILE si impegna a conformarsi al Provvedimento generale del Garante per la protezione dei dati personali del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", così come modificato dal Provvedimento del Garante del 25 giugno 2009 "Modifiche del provvedimento del 27 novembre 2008 recante prescrizioni ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di amministratore di sistema e proroga dei termini per il loro adempimento" e da successive modifiche o integrazioni, e ad ogni altro pertinente provvedimento dell'Autorità.
Nello specifico, qualora tra gli autorizzati al trattamento vi siano degli amministratori di sistema, questi, oltre a quanto elencato nel presente articolo, dovranno conformarsi anche ai controlli di sicurezza ABSC5 della Circolare AgID 18 aprile 2017, n. 2/2017.
Il RESPONSABILE si impegna, in particolare, a:

I. designare quali amministratori di sistema le figure professionali dedicate alla gestione e alla manutenzione di impianti di elaborazione, o di loro componenti, con cui vengono effettuati trattamenti di dati personali;
II. predisporre e conservare l'elenco contenente gli estremi identificativi delle persone fisiche qualificate quali amministratori di sistema e le funzioni ad essi attribuite;
III. comunicare, ove richiesto dal TITOLARE, l'elenco aggiornato degli amministratori dei sistemi;
IV. verificare annualmente l'operato degli amministratori di sistema;
V. mantenere i file di log in conformità a quanto previsto nel suddetto Provvedimento.

Nei casi in cui venga richiesta un'attività di supporto tecnico presso i sistemi del TITOLARE, il TITOLARE conferisce al RESPONSABILE il ruolo di Amministratore di Sistema, previa apposita nomina per il tempo necessario all'intervento.

ART. 8 - ISTANZE DEGLI INTERESSATI
Tenendo conto della natura del trattamento, il RESPONSABILE si obbliga ad assistere il TITOLARE nell'adempimento dei propri obblighi di dar seguito alle richieste di esercizio dei diritti degli interessati di cui al capo III del GDPR.
Nell'eventualità in cui gli interessati rivolgessero le proprie istanze direttamente al RESPONSABILE, questi ha l'onere di trasmettere le istanze al TITOLARE entro e non oltre il termine di 10 (dieci) giorni dalla richiesta, avendo cura di corredare tale trasmissione di tutte le informazioni e documenti relativi ai servizi di propria competenza, al fine di adempiere al proprio obbligo di assistere il TITOLARE nel riscontrare la richiesta dell'interessato.

ART. 9 - ULTERIORI OBBLIGHI
Il RESPONSABILE mette a disposizione del TITOLARE tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui alla normativa vigente ed applicabile in materia di protezione dei dati personali e/o delle istruzioni del TITOLARE di cui all'atto di nomina, e consente al TITOLARE l'esercizio del potere di controllo e ispezione, prestando ogni necessaria

collaborazione alle attività di audit effettuate dal TITOLARE stesso o da un altro soggetto da questi incaricato o autorizzato allo scopo.
Resta inteso che qualsiasi verifica condotta ai sensi del presente articolo dovrà essere eseguita in maniera tale da non interferire con il normale corso delle attività del RESPONSABILE e fornendo a quest'ultimo un ragionevole preavviso.
Il RESPONSABILE si impegna altresì a:

I. collaborare, se richiesto dal TITOLARE, con altri Responsabili del trattamento, al fine di armonizzare e coordinare l'intero processo di trattamento dei dati personali;
II. realizzare quant'altro sia ragionevolmente utile e/o necessario al fine di garantire l'adempimento degli obblighi previsti dalla normativa applicabile in materia di protezione dei dati, nei limiti dei compiti affidati nell'atto di nomina;
III. effettuare, su richiesta del TITOLARE, anche con cadenza annuale, un rendiconto in ordine all'esecuzione delle istruzioni ricevute dal TITOLARE, agli adempimenti eseguiti e alle conseguenti risultanze;
IV. informare prontamente il TITOLARE di ogni questione rilevante ai fini di legge, in particolar modo, a titolo esemplificativo e non esaustivo, nei casi in cui abbia notizia, in qualsiasi modo, che risulti violata la normativa in materia di protezione dei dati personali, ovvero che il trattamento presenti rischi specifici per i diritti, le libertà fondamentali e/o la dignità dell'interessato, nonché qualora, a suo parere, un'istruzione violi la normativa, nazionale o dell'Unione Europea, relativa alla protezione dei dati.

ART. 10 - RAPPORTI CON LE AUTORITÀ
Il RESPONSABILE, su richiesta del TITOLARE, si impegna a coadiuvare quest'ultimo nella difesa in caso di procedimenti dinanzi alle autorità di controllo o giudiziarie che riguardino il trattamento dei dati personali oggetto dell'atto di nomina.

ART. 11 - ALTRI RESPONSABILI DEL TRATTAMENTO
Il TITOLARE autorizza il RESPONSABILE a ricorrere ad altri Responsabili (di seguito "sub-responsabili") per l'esecuzione delle attività di trattamento (o parte delle stesse) oggetto dell'atto di nomina, imponendo agli stessi i medesimi obblighi in materia di protezione dei dati a cui è soggetto il RESPONSABILE, compreso il rispetto, ove possibile, dell'applicazione delle Misure minime di sicurezza ICT per le pubbliche amministrazioni emanate da AgID; nello specifico dovrà garantire il rispetto delle Misure minime anche qualora il sub-responsabile nominato sia un soggetto non tenuto *ex lege* al rispetto della richiamate misure.
Trattandosi di autorizzazione generale, il RESPONSABILE informa preventivamente e per iscritto il TITOLARE di ogni cambiamento ravvisato riguardante l'aggiunta o la sostituzione di altri Responsabili.
Il TITOLARE ha il diritto di opporsi alla nomina e/o alla sostituzione del sub-responsabile effettuata dal RESPONSABILE entro il termine di 5 (cinque) giorni dal ricevimento della comunicazione scritta.
Il RESPONSABILE ha la facoltà di indicare un nome ulteriore o di trattenere le relative competenze con comunicazione scritta entro il termine dei successivi 5 (cinque) giorni. In ogni caso la nomina diviene effettiva qualora il TITOLARE non abbia sollevato obiezioni nel termine a lui concesso.
In particolare:

- il RESPONSABILE informa il TITOLARE circa i soggetti che provvede a nominare quali sub-responsabili del trattamento, specificandone altresì i relativi compiti assegnati;
- il RESPONSABILE si impegna a far rispettare ai sub-responsabili del trattamento gli stessi obblighi imposti dal TITOLARE in materia di protezione dei dati;
- il RESPONSABILE prende atto di conservare nei confronti del TITOLARE l'intera responsabilità dell'adempimento degli obblighi posti in capo ai sub-responsabili nominati dallo stesso RESPONSABILE.

ART. 12 - RESPONSABILITÀ
Ai sensi dell'art. 82 paragrafo 2 del GDPR, il RESPONSABILE risponde per il danno causato dal trattamento solo se non ha adempiuto agli obblighi del GDPR specificatamente diretti ai

Responsabili del trattamento, ovvero ha agito in modo difforme o contrario rispetto alle legittime istruzioni del TITOLARE ed alla presente Disciplina.
Qualora il TITOLARE e il RESPONSABILE siano coinvolti nello stesso trattamento e siano, secondo le previsioni dei paragrafi 2 e 3 dell'art. 82 del Regolamento UE 2016/679, responsabili dell'eventuale danno causato dal trattamento, ogni TITOLARE o RESPONSABILE è responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato.
Nel caso in cui il TITOLARE o il RESPONSABILE abbia pagato, conformemente al paragrafo 4 dell'art. 82, l'intero risarcimento del danno, tale soggetto ha il diritto di reclamare dall'altra parte coinvolta nello stesso trattamento la quota del risarcimento corrispondente alla parte di responsabilità di quest'ultima per il danno, conformemente alle condizioni di cui al paragrafo 2 dell'art. 82 del GDPR.

ART. 13 - CANCELLAZIONE DEI DATI
Alla cessazione del trattamento dei dati o alla revoca per iscritto dell'atto di nomina, il RESPONSABILE dovrà mantenere la massima riservatezza sui dati e le informazioni relative al TITOLARE delle quali sia venuto a conoscenza nell'adempimento delle sue obbligazioni. Il RESPONSABILE, all'atto di cessazione – per qualunque causa – dell'efficacia dell'atto di nomina, salvo la sussistenza di un obbligo di legge o di regolamento nazionale e/o dell'Unione Europea che preveda la conservazione dei dati personali, dovrà interrompere ogni operazione di trattamento degli stessi e dovrà provvedere, a scelta del TITOLARE, all'immediata restituzione allo stesso dei dati personali oppure alla loro integrale cancellazione, in entrambi i casi rilasciando contestualmente un'attestazione scritta che presso lo stesso RESPONSABILE non ne esiste alcuna copia. In caso di richiesta scritta del TITOLARE, il RESPONSABILE è tenuto ad indicare le modalità tecniche e le procedure utilizzate per la cancellazione/distruzione. Con riferimento all'obbligo di restituzione dei dati, il RESPONSABILE si obbliga ad utilizzare formati standard ed interfacce che facilitino l'interoperabilità e la portabilità dei dati.

ART. 14 - DIRITTO DI INFORMAZIONE DELLE PERSONE INTERESSATE
Spetta al TITOLARE, nella propria qualità, l'obbligo di fornire agli interessati le informazioni di cui agli Artt. 13 e 14 del GDPR.

ART. 15 - DISPOSIZIONI FINALI
Resta inteso che l'atto di nomina non comporta alcun diritto per il RESPONSABILE a uno specifico compenso o indennità o rimborso per l'attività svolta né ad un incremento del compenso spettante allo stesso in virtù delle relazioni contrattuali con il TITOLARE.
Per tutto quanto non previsto dalla presente Disciplina e dall'atto di nomina si rinvia alle disposizioni generali vigenti ed applicabili in materia di protezione dei dati personali.
Il TITOLARE si riserva in ogni caso la facoltà di rivedere le condizioni della presente disciplina e dell'atto di nomina laddove la normativa subisse una significativa riforma, dandone tempestiva comunicazione al RESPONSABILE.