

AII. ORTD

OBBLIGHI DEL RESPONSABILE DEL TRATTAMENTO DEI DATI

1. Con la sottoscrizione del contratto relativo all'affidamento del servizio di telecomunicazione (telefonia fissa e dati) per l'Università degli Studi di Padova, (nel seguito anche "Contratto"), il Contraente è nominato Responsabile del trattamento ai sensi dell'art. 28 del Regolamento UE n. 2016/679 (nel seguito anche "Regolamento UE"), secondo le disposizioni del presente allegato.
2. Il Contraente si impegna a presentare su richiesta dell'Ente garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse per l'adozione di misure tecniche ed organizzative adeguate volte ad assicurare che il trattamento sia conforme alle prescrizioni della normativa in tema di trattamento dei dati personali.
3. Le finalità del trattamento sono: quelle strettamente necessarie all'esecuzione delle prestazioni oggetto degli accordi contrattuali tra il Titolare del trattamento (l'Università) e il Responsabile del trattamento (contraente aggiudicatario), da intendersi espressamente richiamati, complessivamente e in ogni loro parte.
4. Il tipo di dati personali trattati in ragione delle attività oggetto del contratto sono:
 - i) dati comuni (es. dati anagrafici e di contatto ecc.);
 - ii) dati particolari;
 - iii) dati giudiziari.
5. Le categorie di interessati sono:
 - a) dipendenti e collaboratori
 - b) utenti dei servizi,
 - c) fornitori di beni e servizi e operatori economici, loro dipendenti e consulenti
6. Nell'esercizio delle proprie funzioni, il Responsabile si impegna a:
 - a) rispettare la normativa vigente in materia di trattamento dei dati personali, comprese le norme che saranno emanate nel corso della durata del contratto;
 - b) trattare i dati personali per le sole finalità specificate e nei limiti dell'esecuzione delle prestazioni contrattuali;
 - c) trattare i dati personali conformemente alle istruzioni impartite dall'Università e di seguito indicate, che il Contraente si impegna a far osservare anche alle persone da questi autorizzate ad effettuare il trattamento dei dati personali oggetto del presente contratto, d'ora in poi "persone autorizzate"; nel caso in cui ritenga che un'istruzione costituisca una violazione del Regolamento UE sulla protezione dei dati o delle altre disposizioni di legge relative alla protezione dei dati personali, il Contraente deve informare immediatamente il Titolare del trattamento;
 - d) garantire la riservatezza dei dati personali trattati nell'ambito del presente contratto e verificare che le persone autorizzate a trattare i dati personali in virtù del presente contratto:
 - si impegnino a rispettare la riservatezza o siano sottoposti ad un obbligo legale appropriato di segretezza;
 - ricevano la formazione necessaria in materia di protezione dei dati personali;
 - trattino i dati personali osservando le istruzioni impartite dal Titolare al Responsabile;
 - e) adottare politiche interne e attuare misure che soddisfino i principi della protezione dei dati personali fin dalla progettazione di tali misure (privacy by design), nonché adottare misure tecniche ed organizzative adeguate per garantire che i dati personali siano trattati, in ossequio al principio di necessità ovvero che siano trattati solamente per le finalità previste e per il periodo strettamente necessario al raggiungimento delle stesse (privacy by default);
 - f) adottare tutte le misure tecniche ed organizzative che soddisfino i requisiti del Regolamento UE anche al fine di assicurare un adeguato livello di sicurezza dei trattamenti, in modo tale da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, modifica, divulgazione non autorizzata, nonché di accesso non autorizzato, anche accidentale o illegale, o di trattamento non consentito o non conforme alle finalità della raccolta;
 - g) su eventuale richiesta dell'Amministrazione, assistere quest'ultima nello svolgimento della valutazione d'impatto sulla protezione dei dati personali, conformemente all'articolo 35 del Regolamento UE e nella

eventuale consultazione del Garante per la protezione dei dati personale, prevista dall'articolo 36 del medesimo Regolamento UE;

h) ai sensi dell'art. 30 del Regolamento UE e nei limiti di quanto esso prescrive, tenere un Registro delle attività di trattamento effettuate sotto la propria responsabilità e cooperare con l'Amministrazione e con l'Autorità Garante per la protezione dei dati personali, mettendo il predetto Registro a disposizione del Titolare e dell'Autorità, laddove ne venga fatta richiesta;

i) adottare le misure minime di sicurezza ICT per le PP.AA. di cui alla Circolare AgID n. 2/2017 del 18 aprile 2017.

l) rispettare la Circolare. 3 del 9 aprile 2018 Criteri per la qualificazione di servizi SaaS per il Cloud della PA;

m) rispettare le Linee guida AGID su acquisizione e riuso di software per le pubbliche amministrazioni del 9 maggio 2019;

n) rispettare tutte le altre Linee Guida Agid, ove applicabili;

o) conservare i dati personali, trattati per conto del Titolare, fino alla cessazione degli effetti del contratto per l'erogazione dei relativi servizi, provvedendo, alla scadenza, ai sensi del successivo punto 15

p) designare per iscritto gli incaricati o i soggetti autorizzati al trattamento per l'erogazione del servizio, impartendo loro precise disposizioni e vigilando sulla loro attività nel rispetto di quanto previsto dal Regolamento UE e dalle altre norme relative alla protezione dei dati personali.

7. Tenuto conto della natura, dell'oggetto, del contesto e delle finalità del trattamento, il Contraente si impegna a fornire all'Amministrazione un piano di misure tecniche e organizzative di sicurezza rimesse all'approvazione della stessa, che saranno concordate al fine di assicurare un adeguato livello di sicurezza dei trattamenti, in modo tale da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, modifica, divulgazione non autorizzata, nonché di accesso non autorizzato, anche accidentale o illegale, o di trattamento non consentito o non conforme alle finalità della raccolta, per garantire il rispetto degli obblighi di cui all'art. 32 del Regolamento UE. Tali misure comprendono tra le altre, se del caso:

- la pseudonimizzazione e la cifratura dei dati personali;
- la capacità di assicurare, su base permanente, la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi che trattano 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 testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Di tipo tecnico:

autenticazione degli utenti;
gestione delle autorizzazioni;
tracciamento degli accessi;
sicurezza delle postazioni fisiche di lavoro;
protezione dei locali fisici.

Di tipo organizzativo:

sensibilizzazione e formazione del personale;
istruzioni chiare e precise;
adozione di procedure standard;
pianificazione di controlli interni periodici;
adesione a codice di condotta o meccanismi di certificazione.

La valutazione circa l'adeguatezza del livello di sicurezza deve tenere conto, in particolare, dei rischi del trattamento derivanti da: distruzione o perdita anche accidentale, modifica, divulgazione non autorizzata, nonché accesso non autorizzato, anche accidentale o illegale, o trattamento non consentito o non conforme alle finalità del trattamento dei dati personali conservati o comunque trattati.

8. Il Responsabile del trattamento deve mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al Regolamento UE, oltre a contribuire e consentire al Titolare - anche tramite soggetti terzi dal medesimo autorizzati, dandogli piena collaborazione - verifiche periodiche circa l'adeguatezza e l'efficacia delle misure di sicurezza adottate ed il pieno e

scrupoloso rispetto delle norme in materia di trattamento dei dati personali. A tal fine, il Titolare informa preventivamente il Responsabile del trattamento con un preavviso minimo di tre giorni lavorativi, fatta comunque salva la possibilità di effettuare controlli a campione senza preavviso; nel caso in cui all'esito di tali verifiche periodiche, ispezioni e audit le misure di sicurezza dovessero risultare inadeguate rispetto al rischio del trattamento o, comunque, inadeguate ad assicurare l'applicazione del Regolamento, o risulti che il Contraente agisca in modo difforme o contrario alle istruzioni fornite dall'Amministrazione, quest'ultima applicherà la penale prevista nel contratto e diffiderà il Contraente ad adottare tutte le misure più opportune o a tenere una condotta conforme alle istruzioni entro un termine congruo che sarà all'occorrenza fissato. In caso di mancato adeguamento a seguito della diffida, resa anche ai sensi dell'art. 1454 cc, l'Amministrazione, in ragione della gravità dell'inadempimento, potrà risolvere il contratto ed escutere la garanzia definitiva, salvo il risarcimento del maggior danno.

Il Responsabile del trattamento può avvalersi di ulteriori Responsabili per delegargli attività specifiche, previa autorizzazione scritta del Titolare del trattamento.

10. Il Sub-responsabile del trattamento deve rispettare obblighi analoghi a quelli forniti dal Titolare al Responsabile Iniziale del trattamento, riportate in uno specifico contratto o atto di nomina. Spetta al Responsabile Iniziale del trattamento assicurare che il sub-Responsabile del trattamento presenti garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse, per l'adozione di misure tecniche ed organizzative appropriate di modo che il trattamento risponda ai principi e alle esigenze del Regolamento UE. In caso di mancato adempimento da parte del Sub-responsabile del trattamento degli obblighi in materia di protezione dei dati, il Responsabile Iniziale del trattamento è interamente responsabile nei confronti del Titolare del trattamento di tali inadempimenti; l'Amministrazione potrà in qualsiasi momento verificare le garanzie e le misure tecniche ed organizzative del Sub-responsabile, tramite audit e ispezioni anche avvalendosi di soggetti terzi. Nel caso in cui tali garanzie risultassero insussistenti o inadeguate l'Amministrazione potrà chiedere la presentazione di garanzie sufficienti entro un termine congruo ed in caso di mancato riscontro risolvere il contratto con il Responsabile iniziale.

Nel caso in cui all'esito delle verifiche, ispezioni e audit le misure di sicurezza dovessero risultare inapplicate o inadeguate rispetto al rischio del trattamento o, comunque, inadeguate ad assicurare l'applicazione del Regolamento UE 2016/679 o risulti che il Sub-responsabile agisca in modo difforme o contrario alle istruzioni fornite dall'Amministrazione, quest'ultima applicherà al Contraente/Responsabile Iniziale del trattamento la penale prevista nel Contratto e diffiderà lo stesso a far adottare al Sub-responsabile del trattamento tutte le misure più opportune o a tenere una condotta conforme alle istruzioni entro un termine congruo che sarà all'occorrenza fissato. In caso di mancato adeguamento a tale diffida, resa anche ai sensi dell'art. 1454 cc, l'Amministrazione potrà, in ragione della gravità dell'inadempimento, risolvere il contratto con il Responsabile Iniziale ed escutere la garanzia definitiva, salvo il risarcimento del maggior danno.

11. Il Responsabile del trattamento deve assistere il Titolare del trattamento al fine di dare seguito alle richieste per l'esercizio dei diritti degli interessati. Qualora gli interessati esercitino tale diritto presso il Responsabile del trattamento, quest'ultimo è tenuto ad inoltrare tempestivamente, e comunque dalla richiesta nel più breve tempo possibile (entro e non oltre 3 giorni), le istanze al Titolare del Trattamento, supportando quest'ultimo al fine di fornire adeguato riscontro agli interessati nei termini prescritti.

12. Il Responsabile del trattamento informa tempestivamente e, comunque entro e non oltre le 48 ore dall'avvenuta conoscenza, il Titolare di ogni violazione di dati personali (cd. *data breach*); tale notifica è accompagnata da ogni documentazione utile, ai sensi degli artt. 33 e 34 del Regolamento UE, per permettere al Titolare del trattamento, ove ritenuto necessario, di notificare questa violazione all'Autorità Garante per la protezione dei dati personali, senza ingiustificato ritardo e, ove possibile, entro il termine di 72 ore da quando il Titolare ne viene a conoscenza; nel caso in cui il Titolare debba fornire informazioni aggiuntive all'Autorità di controllo, il Responsabile del trattamento si impegna a supportare il Titolare nell'ambito di tale attività.

13. Il Responsabile del trattamento deve avvisare tempestivamente e comunque entro e non oltre le 24 ore successive al loro ricevimento il Titolare in caso di ispezioni, di richiesta di informazioni e di documentazione da parte dell'Autorità Garante per la protezione dei dati personali; inoltre, deve assistere il Titolare nel caso di richieste formulate dall'Autorità Garante o dall'Autorità Giudiziaria in merito al trattamento dei dati personali effettuate in ragione del presente contratto.

14. Il Responsabile del trattamento deve comunicare al Titolare del trattamento il nome ed i dati del proprio "Responsabile della protezione dei dati", qualora, in ragione dell'attività svolta, ne abbia designato uno conformemente all'articolo 37 del Regolamento UE; il Responsabile della protezione dei dati personali del Contraente/Responsabile collabora e si tiene in costante contatto con il Responsabile della protezione dei dati del Titolare.

15. La nomina a Responsabile del trattamento decorre dalla data in cui il contratto è sottoscritto dalle parti ed è valida fino alla cessazione di ogni suo effetto, compresa l'eventuale proroga dello stesso, ovvero fino alla revoca anticipata della nomina per qualsiasi motivo da parte del Titolare, fermo restando che, anche successivamente alla cessazione degli effetti del contratto, compresa l'eventuale proroga o l'eventuale revoca per iscritto del presente atto di nomina, il Responsabile del trattamento dovrà mantenere la massima riservatezza sui dati personali e sulle informazioni relative al Titolare delle quali sia venuto a conoscenza nell'adempimento delle sue obbligazioni.

Al termine della prestazione dei servizi oggetto del contratto, il Responsabile, su richiesta del Titolare, si impegna a:

- i) restituire al Titolare del trattamento i supporti rimovibili eventualmente utilizzati su cui sono memorizzati i dati;
- ii) distruggere tutte le informazioni registrate su supporto fisso, documentando per iscritto l'adempimento di tale operazione.

Nel caso in cui il Responsabile del trattamento eroghi servizi nel proprio Data Center, questo 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", così come eventualmente modificato o sostituito dallo stesso Garante, e ad ogni altro pertinente provvedimento dell'Autorità.

Il Responsabile del trattamento si impegna, in particolare, a:

- designare quali amministratori di sistema le figure professionali dedicate alla gestione e alla manutenzione di impianti di elaborazione o di loro componenti, alla gestione di database e allo sviluppo di software, che effettuano trattamenti di dati personali;
- predisporre e conservare l'elenco contenente gli estremi identificativi delle persone fisiche qualificate quali amministratori di sistema e le funzioni ad essi attribuite;
- comunicare, ove richiesto dal Titolare, l'elenco aggiornato degli amministratori dei sistemi;
- verificare annualmente l'operato degli amministratori di sistema;
- mantenere i file di log in conformità a quanto previsto nel suddetto provvedimento.

Nei casi dove venga richiesta una attività di supporto tecnico presso i sistemi del Titolare, questo conferisce al Responsabile del trattamento, previa apposita nomina per il tempo necessario all'intervento, il ruolo di Amministratore di Sistema.

17. Il Responsabile del trattamento si impegna ad operare adottando tutte le misure tecniche e organizzative, le attività di formazione, informazione e aggiornamento ragionevolmente necessarie per garantire che i Dati Personali trattati in esecuzione del presente contratto, siano precisi, corretti e aggiornati nel corso della durata del trattamento - anche qualora il trattamento consista nella mera custodia o attività di controllo dei dati - eseguito dal Responsabile, o da un sub-Responsabile.

18. Il Responsabile non può trasferire i dati personali verso un paese terzo o un'organizzazione internazionale salvo che non abbia preventivamente ottenuto l'autorizzazione scritta da parte del Titolare.

19. Sarà obbligo del Titolare del trattamento vigilare durante tutta la durata del trattamento, sul rispetto degli obblighi previsti dal presente documento e dal Regolamento UE sulla protezione dei dati da parte del Responsabile del trattamento, nonché a supervisionare l'attività di trattamento dei dati personali effettuando audit, ispezioni e verifiche periodiche sull'attività posta in essere dal Responsabile del trattamento.

20. Durante l'esecuzione del Contratto, nell'eventualità di qualsivoglia modifica della normativa in materia di Trattamento dei Dati Personali che generi nuovi requisiti (ivi incluse nuove misure di natura fisica, logica, tecnica, organizzativa, in materia di sicurezza o trattamento dei dati personali), il Responsabile del trattamento si impegna a collaborare - nei limiti delle proprie competenze tecniche, organizzative e delle proprie risorse - con il Titolare affinché siano sviluppate, adottate e implementate misure correttive di adeguamento ai nuovi requisiti.

21. Il Responsabile del trattamento manleverà e terrà indenne il Titolare da ogni perdita, contestazione, responsabilità, spese sostenute nonché dei costi subiti (anche in termini di danno reputazionale) in relazione anche ad una sola violazione della normativa in materia di Protezione dei Dati Personali e/o della disciplina sulla protezione dei dati personali contenuta nel Contratto (inclusi gli Allegati) comunque derivata dalla condotta (attiva e/o omissiva) sua e/o dei suoi agenti e/o subappaltatori e/o sub-contraenti e/o sub-fornitori. Si rinvia altresì all'art. 82 del Regolamento UE.

22. L'incarico di Responsabile del trattamento non comporta uno specifico compenso o indennità o rimborso per l'attività svolta, né un incremento del compenso spettante allo stesso in virtù delle relazioni contrattuali con il Titolare. Per tutto quanto non previsto dal presente documento si rinvia alle disposizioni generali vigenti ed applicabili in materia di protezione dei dati personali.