



ISTRUZIONI ALL'AUTORIZZATO AL TRATTAMENTO DEI DATI PERSONALI.

Destinatari delle presenti istruzioni: componenti di Senato Accademico, Consiglio di Amministrazione, Nucleo di Valutazione, Collegio di Disciplina e altre cariche accademiche.

L'Autorizzato svolge per conto del Titolare le operazioni di trattamento di dati personali connesse alla propria carica. Lo stesso, pertanto, è autorizzato a trattare dati personali esclusivamente entro tale ambito di operatività.

L'Autorizzato potrà accedere ai dati personali legati alle attività connesse al mandato, come, a titolo esemplificativo ma non limitativo, dati del personale tecnico-amministrativo, del personale docente, di docenti a contratto, di studenti e di collaboratori esterni all'Ateneo. L'Autorizzato potrà eventualmente accedere ai contenuti delle banche dati in uso presso la struttura o l'ufficio di riferimento (ad esempio Dipartimento o Segreteria Organi) e ogni altra banca dati, anche futura, connessa al mandato che implichi trattamento per le categorie di interessati di dati.

Nello svolgimento della suddetta attività l'autorizzato dovrà:

- a. attenersi scrupolosamente alle istruzioni a lui impartite dal titolare del trattamento;
- b. rispettare i principi di necessità, adeguatezza, pertinenza e non eccedenza nello svolgimento delle attività di trattamento dei dati personali;
- c. svolgere con correttezza le operazioni di raccolta dei dati;
- d. comunicare con prontezza al titolare qualsiasi circostanza rilevante ai fini dell'applicazione della normativa in materia di protezione dei dati personali in vigore (come ad esempio la violazione dei dati personali, etc.) scrivendo all'indirizzo di posta elettronica privacy@uninsubria.it;
- e. osservare con diligenza tutte le prescrizioni impartite dal titolare in materia di sicurezza e utilizzo degli strumenti informatici con particolare riferimento al Regolamento per l'accesso e l'utilizzo delle infrastrutture centrali di *information e communication technology* (ICT) dell'Ateneo.

In particolare, il soggetto autorizzato al trattamento dovrà attenersi alle seguenti istruzioni:

1. nelle sedute degli Organi collegiali dell'Università il trattamento dei dati avviene in conformità ai regolamenti per il funzionamento degli Organi pubblicati sul sito di Ateneo e al solo fine delle attività istruttorie e per le finalità deliberative di competenza degli organi.
2. la pubblicazione dei dati personali contenuti nelle deliberazioni degli organi collegiali di governo, del nucleo di valutazione e dell'organismo indipendente di valutazione è ammessa solo ove costituisca un'operazione strettamente necessaria al perseguimento delle finalità assegnate all'Ateneo da specifiche leggi o regolamenti e riguardanti informazioni utili a far conoscere ai destinatari le sue attività e il suo funzionamento o a favorire l'accesso ai servizi prestati dall'amministrazione;





3. non è mai consentito al soggetto Autorizzato del Trattamento condividere la componente riservata delle proprie credenziali di autenticazione ai sistemi informativi con soggetti terzi. Le credenziali attribuite al soggetto Autorizzato non possono mai essere riprodotte su supporto cartaceo, né archiviate in altro modo in luoghi o supporti accessibili a terzi oppure salvate in file non cifrati;
4. i dispositivi di proprietà dell'Ateneo in uso esclusivo del soggetto Autorizzato (ad es. personal computer, notebook, tablet, smartphone, smart card, etc.) devono sempre essere protetti da sistemi di autenticazione che, dove previsto, devono essere attivati automaticamente a seguito del loro prolungato inutilizzo (ad es. screensaver) e, per quanto possibile, non devono mai essere lasciati incustoditi se non temporaneamente per esigenze documentabili;
5. i dati personali trattati devono essere salvati esclusivamente in banche dati, dispositivi di memorizzazione e servizi cloud forniti dall'Ateneo e destinati a tale scopo;
6. gli allegati ai messaggi di posta elettronica non devono essere salvati su dispositivi mobili se non estremamente necessario e devono essere cancellati appena possibile;
7. gli atti e i documenti contenenti dati personali devono essere utilizzati e custoditi con diligenza. Gli stessi non devono mai essere lasciati incustoditi, se non temporaneamente per esigenze documentabili, e al termine del loro utilizzo devono essere riposti in luoghi accessibili solo al personale autorizzato e protetti da misure di sicurezza fisiche;
8. deve essere mantenuto il più stretto riserbo sui dati personali e su qualsiasi altro tipo di informazione di cui si sia venuti a conoscenza in ambito lavorativo. È consentito comunicare solo ad altri soggetti autorizzati informazioni e dati personali conosciuti a seguito dello svolgimento nell'ambito delle proprie attività lavorative ed esclusivamente per scopi professionali, salvo che ciò non sia previsto da un obbligo stabilito dal diritto dell'Unione o dal diritto nazionale applicabile. Tale obbligo di osservare i doveri di riservatezza e segretezza permane anche successivamente alla cessazione del rapporto di lavoro con l'Università.
9. prendere visione dei Regolamenti di Ateneo in materia di protezione dei dati personali ed in particolare:
 - Regolamento per l'attuazione delle Leggi in materia di protezione dei dati personali disponibile al link:
<https://www.uninsubria.it/sites/default/files/2023-04/Reg.%20dati%20personali%202021.pdf>
 - Regolamento per il trattamento dei dati appartenenti a categorie particolari e relativi a condanne penali e reati in attuazione delle leggi in materia di protezione dei dati personali disponibile al link:
https://www.uninsubria.it/sites/default/files/2023-04/Reg_dati_categ_particolari.pdf
 - Regolamento per l'accesso e l'utilizzo delle infrastrutture centrali di information e communication technology (ICT) dell'ateneo disponibile al link:
<https://www.uninsubria.it/sites/default/files/2023-04/Reg ICT modifica all.F.pdf> e dell'"estratto normativo" disponibile al link <https://www.uninsubria.it/protezione-dati-personali>.



La violazione degli obblighi di riservatezza ex art. 2105 c.c. e della protezione dei dati personali costituisce anche violazione degli obblighi contrattuali gravanti sull'autorizzato in ragione del Suo rapporto di lavoro. Tali violazioni, infatti, sono punibili ai sensi e per gli effetti dell'art. 7 della L. 300/1970. Inoltre, che alla luce dell'art. 82 del GDPR, l'interessato al trattamento ha facoltà di chiedere il risarcimento di qualsiasi danno dallo stesso patito in ragione di un illecito trattamento dei propri dati personali.

Il titolare del trattamento si riserva il diritto di aggiornare le istruzioni impartite al soggetto autorizzato o di assegnarne nuove.

Il titolare del Trattamento, inoltre, eseguirà regolari controlli, attraverso ispezioni o attività di audit, sull'effettivo svolgimento delle attività affidate al soggetto autorizzato del trattamento secondo le istruzioni ricevute e le disposizioni di legge.