

Allegato: Vademecum *“Nozioni generali in materia di protezione dei dati personali”*

Vademecum “Nozioni generali in materia di protezione dei dati personali”

DATI PERSONALI	
Cos'è un dato personale?	Qualsiasi informazione che permette di identificare una persona fisica direttamente (es. attraverso nome e cognome) o indirettamente, tramite qualsiasi altra informazione relativa ad esempio alle abitudini, alle relazioni personali, allo stato di salute, alla situazione economica o lavorativa (es. il Dirigente dell'Area Finanza e Risorse Umane dell'Università), ivi compreso un numero d'identificazione personale (come il codice fiscale e il numero di matricola).
Dati personali comuni	Informazioni riferite a una persona fisica quali, per esempio, i dati anagrafici (nome, cognome, data di nascita, codice fiscale e indirizzo di residenza), la partita IVA, il numero di telefono e l'indirizzo e-mail.
CATEGORIE DI DATI PERSONALI CHE, PER LA LORO PARTICOLARE NATURA, NECESSITANO DI TUTELE RAFFORZATE	
Dati particolari	Si tratta dei cosiddetti " <i>dati sensibili</i> ", cioè quelli che rivelano l'origine razziale od etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, relativi alla salute o alla vita sessuale (“dati sanitari”); in questa categoria rientrano anche i dati genetici (relativi cioè alle caratteristiche genetiche ereditarie), i dati biometrici (relativi alle caratteristiche fisiche, fisiologiche o comportamentali di un individuo rilevate attraverso tecnologie innovative, come la scansione della retina o il riconoscimento facciale) e quelli relativi all'orientamento sessuale.
Dati giudiziari	Informazioni relative a provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitiva, la liberazione condizionale, il divieto od obbligo di soggiorno), condanne penali, reati, alla qualità di imputato o di indagato.
I SOGGETTI PRIVACY	
 Titolare	La persona fisica, l'autorità pubblica, l'impresa, l'ente pubblico o privato, l'associazione, ecc., che adotta le decisioni sugli scopi e sulle modalità del trattamento. <i>Per l'Ateneo, il Titolare è l'Università stessa in persona del Rettore.</i>
 Responsabile	La persona fisica o giuridica alla quale il Titolare affida la gestione di un qualsiasi servizio avente ad oggetto dati personali. <i>Per l'Ateneo, i Responsabili sono tutti i soggetti che forniscono all'Università servizi che comportano il trattamento di dati personali per conto della stessa. Con tali soggetti deve essere sottoscritto apposito contratto (atto di nomina a Responsabile del trattamento).</i>
 Interessato	La persona fisica alla quale si riferiscono i dati personali. Quindi, se un trattamento riguarda, ad esempio, l'indirizzo e il codice fiscale di Mario Rossi, questa persona è l'Interessato. <i>Per l'Ateneo, gli interessati sono, per esempio, gli studenti, il personale PTA e docente, i partecipanti a progetti di ricerca, ecc.</i>
IL TRATTAMENTO	
Che cosa si deve intendere per “trattamento”?	Qualsiasi attività, operazione o insieme di operazioni aventi ad oggetto dati personali effettuate con o senza l'ausilio di strumenti elettronici (supporti cartacei) come la

	raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca dati.	
Raccolta: è la prima operazione di trattamento e consiste nell'attività di acquisizione del dato.	Registrazione: l'annotazione cartacea o memorizzazione dei dati su un qualsiasi supporto.	Organizzazione/Strutturazione: la classificazione e catalogazione dei dati secondo un metodo prescelto e condiviso.
Visualizzazione: il leggere/prendere visione dei dati. Es. accesso a documenti, file o applicativi e piattaforme informatiche contenenti dati personali.	Modifica: la parziale trasformazione o variazione dei dati trattati. Es. correzione, aggiornamento, alterazione di dati.	Conservazione: la custodia in archivi cartacei o memorizzazione di informazioni digitali su un qualsiasi supporto informatico. Es. archivi, magazzini di fascicoli, hard disk, pendrive, back-up, copie di sicurezza.
Distruzione: l'attività di eliminazione definitiva dei dati trattati mediante strumenti cartacei utilizzando strumenti (per es. trita documenti) o servizi specializzati.	Cancellazione: l'eliminazione di dati raccolti mediante strumenti elettronici. Es. cancellazione, in modo irreversibile, di file, database o parte di essi.	Comunicazione: il dare conoscenza di dati personali ad uno o più soggetti determinati diversi dall'Interessato, dal Responsabile del trattamento e dagli autorizzati, anche mediante la loro messa a disposizione o consultazione. Es. invio dei dati dei dipendenti all'INPS o invio di e-mail contenenti dati personali a consulenti o avvocati.
Diffusione: il dare conoscenza dei dati trattati ad un numero di soggetti indefinito, in qualunque forma anche mediante la loro messa a disposizione o consultazione. Es. pubblicazione delle graduatorie sul sito web.		
QUALI PRINCIPI GENERALI DEVONO "GUIDARE" IL MIO TRATTAMENTO?		
Need to know	I dati devono essere conosciuti solo da chi ha l'effettiva necessità di accedervi per svolgere i propri compiti (es. un dipendente dell'area Risorse Umane, potrà aver accesso ai dati dei dipendenti e collaboratori necessari per lo svolgimento della propria attività, ma <u>non</u> dovrà aver accesso ai dati degli studenti dell'Ateneo, salvo che ciò non sia necessario, per esempio, nell'ambito di un procedimento disciplinare).	
Integrità, Riservatezza e Disponibilità	I dati devono essere trattati in modo da garantire un livello di sicurezza adeguato al rischio.	
Liceità del trattamento	I dati devono essere trattati sulla base di una idonea base giuridica (l'Università può trattare i dati personali solo per finalità istituzionali sulla base di un obbligo di legge).	
Correttezza del trattamento	Rispettare tutte le norme che regolano quel trattamento specifico (es. nel caso di progetti di ricerca rispettare le Regole Deontologiche per i trattamenti a fini statistici o di ricerca scientifica emanate dal Garante per la protezione dei dati personali).	
Trasparenza	Prima di raccogliere i dati, informare l'interessato con un linguaggio semplice e chiaro (ossia verificare che sia stata resa idonea informativa).	

Finalità Determinate, Esplicite e Legittime	Prima dell'inizio del trattamento stabilire per quali scopi si intende raccogliere i dati e dichiararlo chiaramente agli interessati.
Principio Di Necessità	Evitare di identificare l'interessato quando il trattamento non lo richiede o non è necessario (es. in caso di questionario da compilare a fini statistici) e di raccogliere dati superflui per il raggiungimento della finalità perseguita.
Esattezza	I dati trattati devono essere esatti e costantemente aggiornati (es. dare riscontro alle richieste di rettifica dei dati avanzate dagli interessati).
Limitazione Della Conservazione	I dati devono essere conservati solo per il tempo strettamente necessario al raggiungimento della finalità per la quale sono stati raccolti salvo sussista una base giuridica per il trattamento per ulteriori finalità (es. i dati raccolti per la partecipazione ad eventi di orientamento, dovranno essere cancellati decorso il periodo di conservazione stabilito).

QUALI SONO LE REGOLE RELATIVE ALLA PASSWORD DELL' ACCOUNT IUAV?

L'accesso all'account Iuav avviene tramite username e password.

La password **deve**:

- essere modificata al primo accesso e, successivamente, ogni 180 giorni;
- essere composta da almeno 8 caratteri alfanumerici e presentare almeno: un numero, una lettera maiuscola, almeno un carattere speciale all'interno di un insieme definito e indicato all'utente in fase di inserimento. Di seguito i caratteri speciali ammessi:
! ? _ () : + = “
- essere diversa dalle 5 password usate in precedenza;
- essere modificata immediatamente ogni qualvolta sussista il rischio che questa sia facilmente conoscibile o sia stata effettivamente conosciuta da terzi ovvero su richiesta esplicita di AT (Area Tecnica) ove vengano rilevate compromissioni della password.

La password **non deve**:

- contenere parole o parti di parola di uso comune (es. venez123) o sequenze comuni di caratteri o numeri (es. 123456 qwerty aaaaa);
- contenere elementi agevolmente riconducibili all'utente o riferimenti basati su informazioni facilmente deducibili, quali il proprio nome, il nome dei famigliari, la data di nascita, il codice fiscale;
- essere divulgata a terzi né trascritta su supporti fisici (es. fogli, post-it, agende, ecc...);
- essere condivisa con altri (es. colleghi, familiari, ecc...) che operino con tale identificativo.

QUALI SONO LE REGOLE RELATIVE ALL'UTILIZZO DELLA CASELLA DI POSTA ELETTRONICA ISTITUZIONALE?

La casella di posta istituzionale (dominio @iuav.it e relativi sottodomini come ad es. @community.iuav.it, @alumni.iuav.it) deve essere utilizzata esclusivamente per lo svolgimento dell'attività lavorativa. È tollerato un limitato utilizzo a fini privati, che non dovrà però in alcun modo interferire con il normale svolgimento dell'attività lavorativa.

La casella di posta elettronica è strettamente personale: le credenziali di accesso (username e password) non possono essere rivelate a terzi e l'account non può essere condiviso o ceduto ad altri.

Quando si utilizza la casella di posta elettronica si **deve**:

- prestare attenzione nell'aprire gli allegati

La casella di posta elettronica **non deve** essere utilizzata per:

- inviare messaggi in forma anonima o sotto

<p>ricevuti, dato che rappresentano un mezzo molto diffuso per la trasmissione di virus e <i>malware</i>;</p> <ul style="list-style-type: none"> • mantenere i file ricevuti nella casella di posta elettronica o salvati nei server preposti e non nell'<i>hard disk</i> dei <i>personal computer</i>; • inserire gli indirizzi dei destinatari nel campo "ccn" quando vengono inviate comunicazioni ad indirizzi plurimi e non deve essere resa conoscibile l'identità degli altri destinatari. 	<p>mentite spoglie;</p> <ul style="list-style-type: none"> • inviare messaggi il cui contenuto sia lesivo dell'immagine dell'Ateneo o sia di natura oltraggiosa, minacciosa, oscena, intimidatoria, diffamatoria, molesta e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica, o altrimenti illegali; • violare la normativa sui diritti di autore, di proprietà intellettuale e/o industriale o, in generale, altri diritti tutelati dalla normativa vigente; • inviare <i>spam</i> o comunicazioni di simile natura; • inviare materiali contenenti dati particolari, salvo previa criptazione secondo le istruzioni impartite dall'Ateneo.
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

QUALI SONO LE REGOLE RELATIVE ALL'UTILIZZO DELLE CARTELLE CONDIVISE E DEGLI SPAZI DI ARCHIVIAZIONE PERSONALI (ad es. Dropbox)?

<p>Si deve:</p> <ul style="list-style-type: none"> • utilizzare tali spazi per finalità istituzionale; • procedere al salvataggio dei documenti di lavoro. 	<p>Non si deve:</p> <ul style="list-style-type: none"> • utilizzare tali spazi per salvare documenti personali, nemmeno per breve tempo. Durante le attività di controllo, questi documenti potrebbero essere rimossi.
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

QUALI SONO LE REGOLE RELATIVE ALL'UTILIZZO DEI DEVICE E DELLE POSTAZIONI DI LAVORO?

<p>Si deve:</p> <ul style="list-style-type: none"> • custodire qualunque tipo di dispositivo rimovibile in luogo protetto (es. armadi e cassettiere chiusi a chiave); • crittografare i dati particolari prima di salvarli su supporti rimovibili; • verificare il contenuto informativo dei supporti di memoria prima: (i) della loro consegna a terzi per il riutilizzo del supporto ovvero della loro eliminazione/distruzione (in questo caso il dispositivo non dovrà più contenere dati leggibili o comunque in qualsiasi modo recuperabili); (ii) della loro consegna a terzi per il trasferimento dei dati (in questo caso il dispositivo deve contenere esclusivamente i dati a cui il terzo ha diritto di accedere); • cancellare i dati contenuti nei supporti rimovibili, quando non più necessari. 	<p>Non si deve:</p> <ul style="list-style-type: none"> • installare alcun tipo di software senza preventiva autorizzazione da parte di AT; • installare strumenti hardware e/o software atti a intercettare e a modificare le comunicazioni informatiche oppure ad aggirare o a neutralizzare sistemi di protezione; • sviluppare programmi informatici che interferiscano con l'attività di altri utenti o che modifichino parti dei sistemi informatici esistenti; • trasmettere, scaricare, stampare o diffondere in qualunque altro modo contenuti di carattere indecente, osceno, razzista, sessualmente esplicito, illegale, immorale o discriminatorio; • lasciare incustodita la propria postazione durante una sessione di lavoro, anche in caso di breve assenza senza proteggerla tramite le funzionalità di sistema (Ctrl+Alt+Canc); al termine dell'attività lavorativa le sessioni di lavoro devono essere chiuse (<i>log-off</i>).
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

QUALI SONO LE REGOLE RELATIVE UTILIZZO DELLA RETE INTERNET DELL'UNIVERSITA'?

<p>La rete internet dell'Università deve essere utilizzata per finalità istituzionali, ma è consentito l'uso sporadico od occasionale della stessa per motivi personali o non collegati alle attività lavorative.</p>	
<p>L'uso istituzionale della rete internet:</p> <ul style="list-style-type: none"> • è concesso a persone che hanno un rapporto di 	<p>L'uso personale della rete internet non deve:</p> <ul style="list-style-type: none"> • interferire con la produttività o con la prestazione

<p>lavoro, studio o collaborazione con l'Ateneo;</p> <ul style="list-style-type: none">• non può essere finalizzato a scopi illeciti, quali la violazione di norme di legge e/o di regolamento.	<p>professionale dell'utente o di qualsiasi altro dipendente;</p> <ul style="list-style-type: none">• incidere negativamente sul buon funzionamento del computer;• violare le norme oggetto del Regolamento interno.
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------