



**UNIVERSITÀ DEGLI STUDI
DELL'INSUBRIA**

REGOLAMENTO PER L'ATTUAZIONE DELLE LEGGI IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

*Emanato con Decreto rettorale 29 dicembre 2021, n. 1215
In vigore dal 14 gennaio 2022*



UFFICIO ORGANIZZAZIONE, TRASPARENZA E PREVENZIONE DELLA CORRUZIONE

Via Ravasi, 2 – 21100 Varese (VA) – Italia

Tel. +39 0332 21 9040-9043-9047

Email: ufficio.organizzazione@uninsubria.it – PEC: ateneo@pec.uninsubria.it

Web: www.uninsubria.it

P.I. 02481820120 - C.F. 95039180120

Chiaramente Insubria!



**REGOLAMENTO
PER L'ATTUAZIONE DELLE LEGGI
IN MATERIA DI PROTEZIONE DEI DATI PERSONALI**

INDICE

PARTE I – PRINCIPI GENERALI	3
Art. 1 - Oggetto del Regolamento	3
Art. 2 - Definizioni.....	3
Art. 3 - Circolazione dei dati all'interno dell'Università.....	6
Art. 4 - Circolazione dei dati all'esterno dell'Università (Art. 96 del Codice).....	6
Art. 5 - Diritto di accesso ai dati.....	6
PARTE II – I SOGGETTI.....	7
Art. 6 - Titolare.....	7
Art. 7 - Autorizzati di primo livello del trattamento (Delegati)	7
Art. 8 - Responsabile della Protezione dei dati.....	8
Art. 12 - Responsabilità.....	10
PARTE III – IL TRATTAMENTO DEI DATI PERSONALI	10
Art. 13 - Modalità di raccolta e requisiti dei dati personali	10
Art. 14 - Valutazione di impatto sulla protezione dei dati (DPIA)	10
Art. 15 - Tipologie dei dati trattati dall'Università	11
Art. 16 - Informativa.....	11
Art. 17 - Diritti dell'interessato	12
Art. 18 - Forma della richiesta di comunicazione e diffusione dei dati	12
PARTE IV – LA SICUREZZA DEI DATI.....	12
Art. 19 - Misure di sicurezza.....	12
PARTE V – DISPOSIZIONI FINALI.....	13
Art. 20 - Disposizioni finali	13
Art. 21 - Entrata in vigore.....	13



PARTE I – PRINCIPI GENERALI

Art. 1 - Oggetto del Regolamento

1. Il presente Regolamento è emanato in attuazione delle Leggi in materia di protezione dei dati personali, intendendosi con tale termine (i) il Regolamento EU 2016/679 “GDPR” (ii) il D.Lgs 196/2003, come emendato dal D.lgs 101/2018 “Codice in materia di protezione dei dati personali”, (iii) le linee guida e i provvedimenti emessi dall’Autorità Garante per la protezione dei dati personali e infine (iv) le linee guida e i provvedimenti applicabili del Comitato Europeo per la protezione dei dati personali (“EDPB”, ex Gruppo di lavoro Art. 29) e disciplina il trattamento, la comunicazione e la diffusione da parte dell’Università degli Studi dell’Insubria dei dati personali, trattati sia con sistemi automatizzati che non automatizzati, per il perseguimento dei propri fini istituzionali.
2. L’Università provvede al trattamento dei dati personali per lo svolgimento dei propri fini istituzionali, nei limiti stabiliti dallo Statuto, dalle leggi e dai regolamenti e in ogni caso nel rispetto dei diritti, delle libertà fondamentali e della dignità dell’interessato, con riferimento particolare alla riservatezza, all’identità personale e al diritto alla protezione dei dati personali.
3. Le disposizioni del presente Regolamento garantiscono il trattamento di informazioni a carattere personale, acquisite dall’Amministrazione Universitaria o ad essa rese, riguardanti persone fisiche secondo criteri coerenti con la normativa in materia di protezione dei dati personali.
4. Sono esclusi dalla disciplina del presente Regolamento i trattamenti dei dati appartenenti a categorie particolari e relativi a condanne penali e reati che sono oggetto di altro specifico Regolamento di Ateneo.

Art. 2 - Definizioni

1. Ai fini del presente Regolamento si applicano le definizioni elencate nelle Leggi in materia di protezione dei dati personali. Si intende per:

<i>Trattamento:</i>	Qualunque operazione o complesso di operazioni, svolte con o senza l'ausilio di mezzi elettronici o comunque automatizzati, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, 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.
<i>Dato personale:</i>	qualsiasi informazione riguardante una persona fisica identificata o identificabile; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, a titolo esemplificativo mediante il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
<i>Dati particolari:</i>	i dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale; i dati genetici; i dati biometrici; i dati relativi alla salute, alla vita sessuale e all'orientamento sessuale.
<i>Dati identificativi:</i>	I dati personali che permettono l'identificazione diretta dell'interessato.
<i>Dati relativi a condanne penali o reati:</i>	I dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002,



	n. 313 in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale
<i>Dato anonimo:</i>	Il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile, può essere trattato senza il consenso da parte dell'interessato.
<i>Profilazione:</i>	qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo dei dati 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.
<i>Processo decisionale automatizzato:</i>	decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produce effetti nella sfera giuridica dell'interessato o che incide in modo analogo significativamente sullo stesso.
<i>Pseudonimizzazione:</i>	il trattamento dei dati personali in modo tale che 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 i dati personali non siano attribuiti a una persona fisica identificata o identificabile.
<i> Titolare:</i>	La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.
<i>Responsabile:</i>	La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali.
<i>Autorizzati:</i>	Le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile.
<i>Interessato:</i>	La persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali.
<i>Comunicazione:</i>	Il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
<i>Diffusione:</i>	Il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
<i>Blocco:</i>	La conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento.



<i>Banca di dati:</i>	Qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti.
<i>Garante:</i>	Autorità garante per la protezione dei dati personali istituita ai sensi dell'art. 30 della Legge 675/1996.
<i>Misure di sicurezza:</i>	Il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello di protezione richiesto ai sensi dell'articolo 32 del GDPR in relazione al livello di rischio di ogni attività di trattamento.
<i>Strumenti elettronici:</i>	Gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento.
<i>Sistema di autenticazione informatica:</i>	L'insieme degli strumenti elettronici e delle procedure per la verifica dell'identità o della dichiarazione di identità.
<i>Credenziali di autenticazione:</i>	I dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati dal sistema di autenticazione informatica per la verifica dell'identità o di una dichiarazione di identità.
<i>Parola chiave:</i>	Componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica.
<i>Profilo di autorizzazione:</i>	L'insieme dei dati cui una persona può accedere, nonché dei trattamenti ad essa consentiti.
<i>Sistema di autorizzazione:</i>	L'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.
<i>Amministratori di sistema</i>	I soggetti cui è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e di consentirne l'utilizzazione (art. 1 c1 lett. c del DPR 318/99).
<i>Archivio</i>	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.
<i>Responsabile della protezione dei dati personali» o «DPO» (Data Protection Officer)</i>	Figura specializzata nel supporto al Titolare, che svolge funzioni di raccordo con il Garante e di tutela degli interessati.
<i>Destinatario</i>	La persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali.
<i>Terzo</i>	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo diversi dall'interessato, dal Titolare del trattamento, dal Responsabile del trattamento e dalle persone Autorizzate al trattamento; Università degli Studi dell'Insubria – Via Ravasi, 2 – 21100 Varese www.uninsubria.it
<i>Valutazione d'impatto sulla protezione dei dati</i>	Procedura atta a descrivere il trattamento, a valutarne la necessità e proporzionalità e a garantire la gestione dei rischi per i diritti e le libertà degli interessati.
<i>Amministratori di sistema</i>	La figura professionale dedicata alla gestione e alla manutenzione degli impianti di elaborazione con cui vengono effettuati trattamenti di dati



	personali, compresi i sistemi di gestione delle basi di dati, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali.
<i>Scopi statistici</i>	Le finalità di indagine statistica o di produzione di risultati statistici.
<i>Scopi scientifici</i>	Le finalità di studio e di indagine sistematica finalizzata allo sviluppo delle conoscenze scientifiche in uno specifico settore.

Art. 3 - Circolazione dei dati all'interno dell'Università

1. Le disposizioni contenute negli articoli che seguono s'intendono riferite al trattamento, alla diffusione ed alla comunicazione dei dati a terzi. L'accesso ai dati personali da parte delle strutture amministrative, di servizio, didattiche e scientifiche e dei dipendenti dell'Università è limitato ai casi in cui sia finalizzato al perseguimento dei fini istituzionali ed è ispirato al principio della libera circolazione delle informazioni.
2. L'accesso ai dati personali da parte delle strutture e dei dipendenti dell'Università deve essere debitamente motivato e connesso con lo svolgimento dell'attività inerente alla loro specifica funzione, e viene valutato in via diretta e senza formalità nella misura necessaria al perseguimento dell'interesse istituzionale. Qualora invece l'accesso sia giustificato per un utilizzo ulteriore e/o diverso dei dati, i soggetti già indicati devono presentare esplicita e formale richiesta; questa ultima viene esaminata dal Responsabile del trattamento dei dati, e l'autorizzazione viene concessa o negata a seconda che il fine della richiesta rientri o meno nell'attività istituzionale dell'Università. Il richiedente deve adottare tutte le misure necessarie a garantire la sicurezza dei dati a lui trasmessi.
3. Ai fini dell'accesso ai dati sono equiparati alle strutture dell'Università gli organismi sindacali, gli organismi di controllo e di valutazione ed ogni altro organo a cui espresse disposizioni normative affidano tali compiti.

Art. 4 - Circolazione dei dati all'esterno dell'Università (Art. 96 del Codice)

1. Al fine di favorire l'inserimento nel mondo del lavoro e della ricerca degli studenti che hanno conseguito il titolo conclusivo dei corsi di studi di ogni tipologia prevista nel proprio ordinamento didattico, l'Università può comunicare e diffondere all'esterno i dati personali attinenti alla carriera degli studenti medesimi, alle loro competenze ed aspirazioni professionali, su richiesta di soggetti pubblici, aziende private, associazioni di categoria e altri soggetti privati ovvero di propria iniziativa, anche mediante inserimento in sito Internet o in altri circuiti informativi.
2. L'Università avrà cura di chiedere il preventivo consenso scritto degli studenti interessati, previa informativa ai sensi dell'art. 13 del GDPR.

Art. 5 - Diritto di accesso ai dati

1. L'esercizio del diritto di accesso è subordinato alla sussistenza di un interesse per la tutela di situazioni giuridicamente rilevanti.
2. Oggetto del diritto di accesso è il documento amministrativo. Come stabilito dalle Leggi in materia di protezione dei dati personali, il diritto all'accesso a documenti amministrativi contenenti dati personali resta disciplinato dalla Legge 7 agosto 1990, n. 241 e dal decreto legislativo n. 97 del 2016 che ha modificato il decreto legislativo n. 33 del 2013 (FOIA - Il Freedom of Information Act) e successive modificazioni ed integrazioni.



3. L'esercizio del diritto d'accesso, se implica la comunicazione di dati personali di terzi, deve essere limitato unicamente ai dati necessari a soddisfare il diritto stesso.
4. Quando la richiesta di accesso concerne dati idonei a rivelare lo stato di salute o la vita sessuale, il trattamento è consentito solo se il diritto sottostante che il terzo intende far valere, sulla base del materiale documentale al quale chiede di accedere, è di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile.

PARTE II – I SOGGETTI

Art. 6 - Titolare

1. L'Università degli Studi dell'Insubria nella persona del Rettore, in qualità di legale rappresentante, è Titolare del trattamento dei dati personali trattati dalla stessa.
2. Tutti i Responsabili del trattamento e gli Autorizzati dell'Università degli Studi dell'Insubria sono tenuti ad attenersi alle prescrizioni dell'Ateneo. Il mancato rispetto delle suddette prescrizioni potrebbe infatti comportare che sia i Responsabili del trattamento sia gli Autorizzati si trovino ad agire quali Titolari autonomi del trattamento, assumendone così i conseguenti obblighi e responsabilità.
3. Quando l'Università determina finalità e mezzi del trattamento congiuntamente con un altro Titolare, assume, unitamente a quest'ultimo, il ruolo di Contitolare del trattamento.
4. I Contitolari definiscono in modo trasparente, mediante un accordo interno, i rispettivi ruoli e responsabilità in merito all'osservanza degli obblighi derivanti dal Regolamento UE, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle Informazioni di cui ai successivi artt. 16-17. Il contenuto essenziale dell'accordo di Contitolarità è messo a disposizione dell'interessato, dietro richiesta.
5. L'interessato può esercitare i propri diritti nei confronti di ciascun Contitolare del trattamento.
6. Il Titolare predispone ed approva il documento riassuntivo delle misure di sicurezza, organizza le attività di vigilanza e di controllo, verifica la rispondenza dei trattamenti effettuati alle modalità prescritte dal Regolamento ed attua gli eventuali adattamenti.

Art. 7 - Autorizzati di primo livello del trattamento (Delegati)

1. Il Titolare individua gli Autorizzati di primo livello del trattamento nei responsabili apicali di struttura (Direttori di Dipartimento, Presidente della Scuola di Medicina, Direttore Generale, Dirigenti e Direttori di Centro Servizio), i quali hanno il compito di vigilare, monitorare e garantire, all'interno della struttura cui sono preposti, il rispetto delle norme vigenti e delle istruzioni del Titolare in materia di protezione dei dati personali.
2. Il Titolare, nella persona del Rettore pro-tempore, può comunque designare, con provvedimento formale, uno o più Autorizzati di primo livello diversi dai soggetti sopra indicati.
3. Gli Autorizzati di primo livello del trattamento possono individuare, all'interno della propria struttura, un Referente che avrà il compito di interfacciarsi con il Responsabile per la protezione dei dati personali di Ateneo per ogni comunicazione legata all'applicazione della normativa in materia di protezione dei dati personali e supportare il designato nella gestione delle attività relative al trattamento dei dati personali. All'Autorizzato di primo livello del trattamento sono attribuite le responsabilità di indirizzo, vigilanza e controllo sull'operato del Referente. L'individuazione del soggetto Referente non libera l'Autorizzato di primo livello del trattamento in relazione ai suoi compiti di cui al comma 1.



4. I Referenti sono individuati dall'Autorizzato di primo livello tra il personale tecnico-amministrativo della struttura, in possesso delle necessarie competenze professionali. Per i Dipartimenti, in base alla complessità ed eterogeneità dei dati trattati, l'Autorizzato di primo livello può individuare il Referente anche tra il personale docente o ricercatore. I nominativi dei Referenti individuati devono essere comunicati, per via telematica, al Titolare e al Responsabile della Protezione dei dati personali.
5. Gli Autorizzati di primo livello del trattamento provvedono a identificare e segnalare al Titolare eventuali ulteriori trattamenti di dati, diversi da quelli sensibili e giudiziari già oggetto di specifico regolamento di Ateneo, che presentano rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura degli stessi, alle modalità o agli effetti del trattamento.
6. Gli Autorizzati di primo livello del trattamento, su espressa delega del Titolare, designano, con propri atti scritti, gli autorizzati al trattamento dei dati operanti all'interno della struttura di competenza. Ciascun Autorizzato di primo livello del trattamento provvede, altresì, alla custodia delle parole chiave degli autorizzati dallo stesso designati.
7. Qualora i dati siano trattati su sistemi informatici amministrati centralmente dall'Area Sistemi informativi, il Dirigente della stessa Area, oltre che come Autorizzato di primo livello del trattamento, agisce anche come Referente.

Art. 8 - Responsabile della Protezione dei dati

1. Il Titolare designa un Responsabile della Protezione dei Dati (DPO), figura individuata sulla base 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 cui al successivo comma 3, che svolge funzioni di raccordo con il Garante e di tutela degli interessati.
2. Il DPO può essere un soggetto interno all'Università, nominato con decreto rettorale, oppure un soggetto esterno, nel qual caso assolve i propri compiti in base a un contratto di servizi.
3. Il DPO, considerando i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo, svolge i seguenti compiti:
 - a. informa e fornisce consulenza al Titolare, al Responsabile e ai soggetti Autorizzati in merito agli obblighi derivanti dal Regolamento UE e dalle altre disposizioni normative in materia di protezione dei dati personali;
 - b. sorveglia l'osservanza della normativa e delle politiche dell'Università in materia di protezione dei dati personali - comprese l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
 - c. fornisce, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e ne sorveglia lo svolgimento;
 - d. coopera con il Garante fungendo da punto di contatto per lo stesso per questioni connesse al trattamento, tra cui la consultazione preventiva, ed effettua, se del caso, consultazioni relativamente a qualunque altra questione;
 - e. collabora alla redazione e all'aggiornamento dei Registri di trattamento;
 - f. tiene i contatti con gli interessati, in relazione all'esercizio dei loro diritti.

Art. 9 - Soggetti autorizzati al trattamento

1. Sono soggetti Autorizzati al trattamento tutti coloro i quali svolgono le operazioni inerenti al trattamento sotto la diretta autorità del Titolare e, in quanto tali, sono autorizzati a trattare i dati personali nel pieno rispetto delle istruzioni del Titolare.



2. Il personale dell'Ateneo è Autorizzato al trattamento nell'ambito definito dalle mansioni attribuite con contratto di lavoro o atto di nomina, dalle competenze della struttura di assegnazione o afferenza e dalle attività assegnate dal Responsabile di struttura.
3. Tutti i dipendenti dell'Ateneo sono tenuti a seguire le indicazioni e le disposizioni dell'Ateneo in materia di protezione dei dati personali e sicurezza informatica e ad agire in modo conforme alla normativa vigente anche quando svolgono attività lavorativa da remoto (*smart working*, lavoro agile o telelavoro).

Art. 10 - Amministratori di sistema

1. Sono Amministratori di sistema ai sensi del Provvedimento del Garante del 27 novembre 2008 e s.m.i. le figure professionali finalizzate alla gestione e manutenzione di un impianto di elaborazione o di sue componenti. Ai fini del presente regolamento sono da considerarsi tali anche gli amministratori di basi di dati, gli amministratori di rete, gli amministratori di apparati di sicurezza, gli amministratori di sistemi software complessi.
2. L'Amministratore di sistema sviluppa e gestisce l'impianto di elaborazione o i suoi componenti hardware e software mediante i quali vengono effettuati i trattamenti di dati personali applicando per i profili relativi alla sicurezza le direttive del Titolare.
3. Il Titolare o un Autorizzato di primo livello del trattamento, su espressa delega dello stesso, individua gli amministratori di sistema con atto di designazione individuale che definisce analiticamente i compiti e gli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

Art. 11 - Responsabile del trattamento

1. Il Responsabile del trattamento è il soggetto esterno all'organizzazione dell'Università che esegue trattamenti per conto dell'Università stessa. L'Università, per il trattamento di dati personali, ricorre unicamente a Responsabili che presentino garanzie idonee, in particolare in relazione alle misure tecniche e organizzative adeguate a consentire il rispetto delle disposizioni del Regolamento UE, ivi compresa la tutela dei diritti degli interessati.
2. L'Università designa il Responsabile del trattamento mediante un contratto o altro atto giuridico che determina la natura, la durata e la finalità del trattamento o dei trattamenti assegnati, il tipo di dati trattati, le categorie di interessati, gli obblighi e i diritti del Titolare e del Responsabile, le responsabilità e le misure tecniche e organizzative adeguate a consentire il rispetto delle istruzioni impartite dal Titolare e delle disposizioni normative.
3. Obblighi specifici del Responsabile sono:
 - a. la tenuta del Registro dei trattamenti svolti per conto del Titolare del trattamento;
 - b. l'adozione di idonee misure tecniche e organizzative per garantire la sicurezza dei trattamenti;
 - c. la designazione di un Responsabile della Protezione Dati, se prevista dalla legge o se ritenuta necessaria;
 - d. la designazione di un rappresentante in Italia (nel caso di Responsabile non stabilito nella UE);
 - e. il rispetto delle istruzioni fornite dal Titolare del trattamento.
4. Per specifiche attività di trattamento, nel rispetto degli obblighi contrattuali che lo legano all'Università, il Responsabile può nominare sub-responsabili del trattamento esclusivamente previa autorizzazione scritta, specifica o generale, dell'Università e con attribuzione al sub-responsabile dei medesimi obblighi in materia di protezione dei dati personali derivanti dal contratto – o altro atto giuridico – tra Università e Responsabile. Qualora un sub-responsabile ometta di adempiere ai propri obblighi in



materia di protezione dei dati, il Responsabile conserva nei confronti dell'Università l'intera responsabilità dell'adempimento degli obblighi del sub-responsabile, anche ai fini del risarcimento di eventuali danni causati dal trattamento.

5. L'Università può essere nominata Responsabile di uno o più trattamenti per conto di un altro Titolare.

Art. 12 - Responsabilità

1. Il soggetto che richiede, riceve, tratta, o semplicemente ha notizia di dati è vincolato al rispetto del segreto d'ufficio di cui all'art. 15 del D.P.R. 10 Gennaio 1957 n. 3, come sostituito dall'art. 28 della Legge 7 Agosto 1990 n. 241.
2. Le attività di trattamento dei dati personali sono state equiparate alle attività pericolose, pertanto, chiunque cagioni un danno ad altri per effetto delle operazioni di trattamento è tenuto al risarcimento del danno ai sensi dell'articolo 2050 del codice civile.
3. Le responsabilità dei soggetti di cui agli artt. 7 e 11 comprendono anche quella relativa alla mancata vigilanza sull'attività degli autorizzati al trattamento dei dati, all'omessa o inidonea informativa fornita all'interessato.
4. La responsabilità, anche penale, espressamente prevista dal Decreto Legislativo 30 giugno 2003, n. 196 per un eventuale utilizzo illecito o non corretto dei dati personali conosciuti è a carico della singola persona, titolare, responsabile o autorizzato, cui l'uso illegittimo sia riferibile.

PARTE III – IL TRATTAMENTO DEI DATI PERSONALI

Art. 13 - Modalità di raccolta e requisiti dei dati personali

1. I dati personali oggetto di trattamento sono:
 - a. trattati in modo lecito e secondo correttezza;
 - b. raccolti e registrati per scopi determinati, espliciti e legittimi, utilizzati in altre operazioni del trattamento in termini non incompatibili con tali scopi;
 - c. esatti e, se necessario, aggiornati;
 - d. pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono stati raccolti e successivamente trattati;
 - e. conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario per gli scopi per i quali i dati sono stati raccolti o successivamente trattati.
2. Il trattamento di dati personali per scopi storici, di ricerca scientifica o di statistica è compatibile con gli scopi per i quali i dati sono raccolti o successivamente trattati e può essere effettuato anche oltre il periodo necessario a questi ultimi scopi.

Art. 14 - Valutazione di impatto sulla protezione dei dati (DPIA)

1. Il Titolare, prima di procedere ad un nuovo trattamento di dati personali, provvederà, ove ne ricorrano le condizioni, a sottoporre il trattamento a DPIA.
2. Per consentire al Titolare il corretto svolgimento della DPIA chi intende procedere, nell'ambito delle funzioni universitarie, ad un nuovo trattamento di dati personali per i quali è previsto l'obbligo della DPIA deve comunicarlo al responsabile della struttura organizzativa, tra quelle indicate al precedente art. 7 del presente Regolamento. La comunicazione contiene:
 - a. le finalità e le modalità del trattamento;



- b. la natura dei dati, il luogo ove sono custoditi e le categorie di interessati cui i dati si riferiscono;
- c. l'ambito di comunicazione e di diffusione dei dati;
- d. gli eventuali trasferimenti di dati previsti verso Paesi non appartenenti all'Unione Europea o, qualora si tratti di dati sensibili e di dati relativi ai provvedimenti di cui all'art. 686 c.p.p., fuori del territorio nazionale;
- e. una descrizione delle misure di sicurezza adottate;
- f. l'eventuale connessione con altri trattamenti o banche di dati, e comunque ogni altra informazione utile al Titolare per procedere allo svolgimento della DPIA.

Art. 15 - Tipologie dei dati trattati dall'Università

1. Il trattamento dei dati personali è consentito soltanto per lo svolgimento delle funzioni istituzionali, nei limiti stabiliti dalle Leggi in materia di protezione dei dati personali dal presente Regolamento.
2. L'Università degli Studi dell'Insubria è un'istituzione pubblica di alta cultura che ha per finalità lo sviluppo del sapere critico e della sua trasmissione. L'Università opera per attuare il diritto allo studio con particolare riguardo ai capaci e meritevoli, anche di concerto con gli enti competenti in materia. Favorisce la qualità e l'efficacia dell'attività di formazione degli studenti e ne cura la preparazione professionale. Nel perseguimento dei suoi fini, assicura il rispetto della libertà di ricerca e della libertà di insegnamento costituzionalmente protetti. Individua, coordina e predispone i mezzi materiali e finanziari a ciò necessari, in rapporto alle esigenze ed alle risorse. L'Università garantisce il raggiungimento delle proprie finalità istituzionali per mezzo delle sue strutture didattiche, ed attraverso la conclusione di apposite convenzioni con istituzioni ed organismi di alta cultura nazionali ed esteri, operanti nel campo della didattica e della ricerca, e con enti pubblici e privati.
3. Per il perseguimento dei propri fini istituzionali l'Università tratta principalmente le seguenti tipologie di dati personali:
 - a. dati relativi al personale dipendente ed a contratto;
 - b. dati relativi a studenti, inclusi coloro che hanno già terminato gli studi;
 - c. dati relativi al personale operante a vario titolo nell'Università (borsisti, tirocinanti, visitatori ecc.);
 - d. dati raccolti per fini amministrativi e contabili;
 - e. dati raccolti per fini di didattica e ricerca.

Art. 16 - Informativa

1. L'interessato deve essere debitamente informato, prima del trattamento dei dati personali, circa:
 - a. le finalità e le modalità del trattamento cui sono destinati i dati richiesti;
 - b. la natura obbligatoria o facoltativa del conferimento di dati richiesti;
 - c. i soggetti o le categorie di soggetti ai quali i dati possono essere comunicati e l'ambito di diffusione dei dati medesimi;
 - d. i diritti di cui agli articoli da 15 a 22 del GDPR;
 - e. i dati relativi al titolare e, se designato, del responsabile.
2. L'informativa può essere resa individualmente, attraverso modalità orali o scritte, oppure collettivamente, mediante informative di massa od annunci sulle pagine Web.



Art. 17 - Diritti dell'interessato

1. Il soggetto i cui dati sono contenuti in una banca di dati ha il diritto di ottenere, senza ritardo, ai sensi degli articoli da 15 a 22 del GDPR:
 - a. la conferma dell'esistenza o meno di trattamenti che lo riguardano, anche se non ancora registrati, e la comunicazione in forma intelligibile dei medesimi dati e della loro origine, nonché della logica e delle finalità del trattamento;
 - b. la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge;
 - c. l'aggiornamento, la rettificazione, ovvero, qualora vi abbia interesse, l'integrazione dei dati;
 - d. l'attestazione che le operazioni di cui alle lett. b e c sono state portate a conoscenza dei terzi.
2. L'interessato ha, inoltre, il diritto di opporsi, per motivi legittimi, al trattamento dei dati che lo riguardano, ancorché pertinenti allo scopo della raccolta, l'interessato può esercitare tali diritti con una richiesta scritta al responsabile della banca dati.
3. L'interessato può conferire, per iscritto, delega o procura a persone fisiche o ad associazioni.

Art. 18 - Forma della richiesta di comunicazione e diffusione dei dati

1. La comunicazione e la diffusione dei dati sono permesse quando:
 - a. siano previste da una norma di legge o di regolamento;
 - b. siano necessarie per finalità di ricerca scientifica o di statistica, e si tratti di dati anonimi;
 - c. siano richieste dai soggetti quali forze di polizia, autorità giudiziaria, organismi di informazione e sicurezza o da altri soggetti pubblici per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione di reati;
 - d. sia stata espressamente autorizzata dagli interessati.
2. Al fine di ottenere la comunicazione dei dati, i richiedenti presentano una richiesta scritta e motivata al Titolare o al Responsabile del trattamento, indicando oltre che i dati cui essa fa riferimento:
 - a. il nome, la denominazione o la ragione sociale;
 - b. le finalità e le modalità di utilizzo dei dati richiesti. I dati vengono rilasciati a condizione che il richiedente si impegni ad utilizzarli esclusivamente per le finalità e nell'ambito delle modalità indicate, e ad adottare tutte le misure necessarie a garantirne la sicurezza.
3. L'Università, dopo avere valutato che la diffusione e la comunicazione dei dati sono compatibili con i propri fini istituzionali, provvede alla trasmissione dei dati stessi nella misura e secondo le modalità strettamente necessarie a soddisfare la richiesta.
4. Le richieste provenienti da soggetti pubblici, esclusi gli enti pubblici economici, finalizzate alla comunicazione dei dati sono soddisfatte quando necessarie al perseguimento dei fini istituzionali dell'ente richiedente.

PARTE IV – LA SICUREZZA DEI DATI

Art. 19 - Misure di sicurezza

1. Il Titolare ed i Responsabili del trattamento dei dati provvedono, per quanto di loro competenza così come indicato agli artt. 6 e 11 del presente Regolamento, in relazione alla disciplina disposta all' art. 32 del GDPR all'adozione di idonee e adeguate misure di sicurezza al fine di prevenire:



- a. i rischi di distruzione, perdita anche accidentale di dati o danneggiamento delle banche dati o dei locali ove esse sono custodite;
 - b. l'accesso non autorizzato ai dati stessi;
 - c. modalità di trattamento dei dati non consentite rispetto alla legge o al presente Regolamento;
 - d. modalità di trattamento dei dati non conformi rispetto alle finalità della raccolta.
2. I dati personali oggetto di trattamento devono essere custoditi e controllati, anche in relazione alle conoscenze rese disponibili dal progresso tecnico e allo stato dell'arte, 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.

PARTE V – DISPOSIZIONI FINALI

Art. 20 - Disposizioni finali

1. Per quanto non previsto nel presente Regolamento, si applicano le disposizioni del Decreto Legislativo 30 giugno 2003 n. 196 e le successive modificazioni ed integrazioni.

Art. 21 - Entrata in vigore

1. Il presente Regolamento entra in vigore dal quindicesimo giorno successivo alla pubblicazione dell'albo ufficiale di Ateneo. di emanazione all'albo dell'Università.