VADEMECUM DEL REGOLAMENTO SUL TRATTAMENTO, LA COMUNICAZIONE E LA DIFFUSIONE DA PARTE DELL'UNIVERSITÀ DEGLI STUDI DI PARMA DEI DATI PERSONALI, IVI COMPRESI QUELLI SENSIBILI E GIUDIZIARI, AI SENSI DEL REGOLAMENTO UE N. 679/2016

Il Regolamento in epigrafe, adottato ai sensi del Regolamento UE n. 679/2016 e del D.lgs 30.06.2003 n. 196 "Codice in materia di protezione dei dati personali" così come recentemente modificato dal D.lgs n. 101/2018 di adeguamento al GDPR, risponde alla necessità di fornire ai dipendenti uno strumento interpretativo, condiviso, valido e concreto, finalizzato ad uniformare all'interno dell'Università l'applicazione del vigente quadro normativo.

In ossequio al principio di *accountability*, dunque, sono state fissate talune regole per un duplice intento:

- evitare il rischio di violazioni del GDPR[1];
- garantire agli utenti/collaboratori/esterni che vengano in contatto con l'Ateneo il miglior controllo possibile sul trattamento dei loro dati personali.

Il presente documento è puramente riepilogativo e intende offrire, evidentemente senza pretesa di esaustività, una sintesi del GDPR e di tutte le più importanti novità ivi introdotte e, conseguentemente, una sintesi del Regolamento di Ateneo in materia.

Per maggiore comodità dei destinatari, si riporta il testo del Regolamento Europeo 679/2016 al seguente collegamento:

- https://www.garanteprivacy.it/il-testo-del-regolamento

Preliminarmente, occorre chiarire che, per **dato personale**, si intende qualunque informazione riguardante una **persona fisica identificata o identificabile**.

Tra le principali **novità** introdotte dal GDPR rispetto alla normativa previgente (Direttiva 95/46/EC), emergono:

a) La tutela dei dati personali oltre i confini nazionali. Il Regolamento UE 679/2016 tutela i dati personali dei cittadini europei e viene applicato a tutte le aziende, ivi comprese le Pubbliche Amministrazioni, che operano all'interno dell'Unione Europea e che trattano i dati personali di individui residenti nell'UE;

b) La regola di chiarezza sul consenso. Il GDPR introduce una nuova disciplina per l'acquisizione del consenso al trattamento dei dati personali all'insegna della chiarezza. Il consenso, dunque, dovrà essere libero, specifico, informato ed esplicito. Tutte le aziende sia pubbliche che private, ivi compresi gli Atenei, pertanto, sono tenute a spiegare in maniera chiara e senza possibilità di equivoco, tutte le condizioni che

[1] Il **regolamento europeo**, è un vero e proprio atto legislativo vincolante in tutte le sue parti. Ciò comporta che gli Stati membri sono obbligati a **rispettarlo per intero**. Non occorre un provvedimento nazionale di recepimento, dato che il regolamento è **immediatamente vincolante ed obbligatorio verso tutti i soggetti pubblici o privati**, tenuti al rispetto del diritto dell'UE (si tratta infatti di norme anche dette **self-executing**).

regolano la raccolta e il trattamento dei dati. Ciò significa che occorre necessariamente rivedere e riorganizzare, sulla base delle prescrizioni del GDPR, l'intera *policy privacy* interna, come ha fatto e continua a fare il nostro Ateneo, mediante la predisposizione di nuovi strumenti (V. Regolamento di Ateneo) e l'aggiornamento e l'adeguamento di quelli già esistenti (V. informative ex art. 13 e 14 specifiche per tipologia di trattamento).

Affinché il consenso per l'elaborazione dei dati sia legittimo, ai sensi del GDPR, l'individuo deve essere posto nella condizione di effettuare una scelta informata e consapevole con possibilità di revoca del consenso eventualmente già reso.

c) Il principio di a*ccountability*. È uno dei principi fondamentali introdotti dal GDPR e va inteso come "principio di responsabilità" del titolare del trattamento. Quest'ultimo, infatti, deve adottare politiche e attuare misure adeguate per garantire ed essere in grado di dimostrare che il trattamento dei dati personali effettuato è conforme al Regolamento Europeo.

d) Il criterio di *data protection by design e by default.* Ovvero protezione dei dati fin dalla progettazione e protezione per impostazione predefinita.

Data protection by design è un metodo innovativo che impone ai soggetti pubblici e privati che trattano dati personali l'**obbligo di avviare qualsiasi progetto introducendo fin dall'inizio idonei strumenti a tutela dei dati personali**, quali ad esempio, tecniche di pseudonimizzazione o minimizzazione dei dati.

Data protection by default prevede, invece che, per impostazione predefinita, i soggetti dovrebbero trattare solo i dati personali nella **misura necessaria e sufficiente per le finalità previste e per il periodo strettamente necessario a tali fini**. Occorre, quindi, progettare il sistema di trattamento di dati garantendo la non eccessività dei dati raccolti (ad es. non deve essere obbligatorio compilare un campo di un form il cui conferimento di dati è facoltativo) in modo che l'interessato riceva un alto livello di protezione anche se non si attiva per limitare la raccolta dei dati (ad es. tramite *opt out* ossia la possibilità di rinunciare con un semplice clik alla ricezione di informazioni su prodotti e servizi non desiderati).

L'introduzione dei suddetti due principi obbliga, ovviamente, a predisporre una valutazione di impatto privacy ogni volta che si avvia un progetto che prevede un trattamento di dati.

e) Le sanzioni in caso di violazione delle disposizioni del Regolamento europeo. Le sanzioni possono arrivare fino al 4% del "fatturato" annuale o a 20 milioni di euro.

***

Il GDPR, oltre a definire le misure da adottare per proteggere i dati personali, introduce una serie di **nuovi diritti a tutela degli utenti**.

1) Diritto di essere informato. L'interessato ha il diritto di ottenere dal titolare del trattamento le informazioni elencate nell'articolo 13 o 14 del GDPR, a seconda che i dati personali siano o meno raccolti presso l'interessato stesso.

2) Diritto di accesso. L'interessato ha il diritto di ottenere dal titolare del trattamento l'accesso ai dati personali che lo riguardano e alle informazioni elencate nell'articolo 15 del GDPR.

3) Diritto di rettifica. L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano, senza ingiustificato ritardo, e l'integrazione dei dati personali incompleti.

4) Diritto di cancellazione. L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano, senza ingiustificato ritardo, in caso sussista uno dei motivi elencati nell'articolo 17 del GDPR.

5) Diritto di limitazione del trattamento. L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento dei dati personali che lo riguardano, in caso sussista uno dei motivi elencati nell'articolo 18 del GDPR.

6) Diritto di notifica. L'interessato ha il diritto di ricevere comunicazione da parte del titolare del trattamento riguardo eventuali rettifiche, cancellazioni o limitazioni del trattamento dei propri dati.

7) Diritto di portabilità. L'interessato ha il diritto di riottenere i propri dati personali (in formato di uso comune e leggibile da dispositivo automatico) da un titolare del trattamento e di trasmetterli a un altro senza alcun impedimento.

8) Diritto di opposizione. L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano, ai sensi dell'articolo 21 del GDPR.

Anche l'Università, in qualità di titolare del trattamento dei dati di dipendenti, studenti, ecc., deve essere in grado di garantire tali diritti.

Il GDPR, infine, conferma un approccio "responsabilizzante" mediante l'introduzione della figura del **Responsabile della Protezione dei Dati (DPO o *Data Protection Officer*)**, ovvero un soggetto altamente qualificato che affianca il titolare nella gestione delle questioni connesse al trattamento dei dati personali e lo supporta nel rispetto della normativa.

*** * ***

Il Regolamento interno di Ateneo sul trattamento, la comunicazione e la diffusione dei dati personali, sensibili e giudiziari, è articolato in quattro capi, un allegato e un'appendice.

- Il capo I riprende i principi e le definizioni contenute nel GDPR;
- Il capo II contiene le linee guida per la conformità in materia di tutela dei dati personali;

- Il capo III contiene le linee guida per i trattamenti nelle Aree di specifico interesse dell'Ateneo;
- Il capo IV contiene le disposizioni finali e di attuazione;
- L'allegato 1 contiene l'elenco delle strutture competenti a svolgere le funzioni di cui all'art. 4 comma 1 del Regolamento di Ateneo (Compliance, ICT, Security);
- L'Appendice contiene considerazioni in ordine al bilanciamento tra accesso civico generalizzato e riservatezza dei dati personali e in ordine al diritto di cronaca, nonché istruzioni concernenti la compilazione e la tenuta del registro dei trattamenti e indicazione relative alla *data retention* ovvero ai tempi di conservazione dei dati.

PRECISAZIONI SU TALUNI CONCETTI CONTENUTI NEL REGOLAMENTO INTERNO

I dati personali si distinguono in "comuni", "particolari" (ex sensibili) e giudiziari

Sono dati personali comuni (art. 4 comma 1 GDPR), il nome, la data e il luogo di nascita, l'indirizzo, il numero di telefono, il codice fiscale, l'indirizzo IP (quando collegato ad altri dati), una fotografia, la firma, l'identità digitale, le informazioni genetiche, ecc., ovvero qualunque informazione relativa a persona fisica identificata o identificabile (interessato).

Sono dati particolari (art. 9 comma 1 GDPR) l'origine razziale ed 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 o all'orientamento sessuale. Rispetto a questi dati la regola generale è il divieto di trattamento, salvo talune eccezioni tassativamente elencate dall'art. 9 paragrafo 2 del GDPR.

Sono dati giudiziari (art. 10 GDPR) i dati personali relativi alle condanne penali, ai reati o a connesse misure di sicurezza. Il trattamento di questi dati deve avvenire sotto il controllo dell'Autorità Pubblica.

Tipologie di trattamento dei dati

Sono operazioni di trattamento con o senza strumenti automatizzati, che soggiacciono all'applicazione dei principi e delle regole imposte dal GDPR oltre che alla normativa italiana in materia: la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento, la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, la diffusione, l'elaborazione, il raffronto, l'interconnessione, la limitazione, la cancellazione e la distruzione.

Distinzione tra comunicazione e diffusione dei dati personali

L'art. 4 del GDPR nonché l'art. 2 ter del D.Lgs n.196/2003 (Codice Privacy italiano) così come aggiornato e modificato dal D. Lgs n. 101/2018 di attuazione del testo italiano a quello europeo, distinguono tra comunicazione e diffusione dei dati personali.

La **comunicazione** (o cessione) consiste nel dare conoscenza di 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 caso di comunicazione il dato viene trasferito a terzi, ed è quindi attività particolarmente delicata. L'Università può comunicare a finanziatori di borse di dottorato e assegni di ricerca dati comuni relativi a dottorandi e assegnisti che abbiano usufruito dei finanziamenti; può comunicare le opinioni degli studenti sulla didattica al Nucleo di Valutazione e/o al Presidio della Qualità; può comunicare alle Aziende sanitarie in convenzione dati inerenti al personale dell'Università che eserciti la propria attività nell'ambito della convenzione, ecc.
Per **diffusione**, invece, si intende il dare conoscenza dei dati a soggetti indeterminati, in qualunque forma anche mediante la loro messa a disposizione o consultazione. Si ha, quindi, diffusione anche quando, in ottemperanza ai principi di trasparenza, l'Università pubblica, sui siti web di Ateneo, dati inerenti le valutazioni d'esame mediante diffusione del numero di matricola dello studente e del voto conseguito.

Principali soggetti del trattamento

- L**'interessato**, definibile impropriamente come il "proprietario" dei dati oggetto di trattamento;
- Il t**itolare** (Università degli Studi di Parma, nella persona del Magnifico Rettore) che determina le finalità e i mezzi del trattamento;
- Il **responsabile del trattamento** (Dirigenti delle Aree amministrative e Direttori di Centri e Dipartimenti) che tratta dati senza stabilire finalità e mezzi del trattamento ma attenendosi scrupolosamente alle istruzioni in tal senso ricevute dal titolare. Per particolari necessità, può essere nominato anche un responsabile esterno all'Ateneo.
- Il **responsabile per la protezione dei dati personali** (DPO, ruolo attualmente ricoperto dall'Ing. Mauro Amigoni) con compiti di sensibilizzazione e formazione del personale, sorveglianza sullo svolgimento della valutazione d'impatto, e di punto di contatto per gli interessati e per il Garante per ogni questione attinente l'applicazione del Regolamento.
- L'**incaricato al trattamento** è la persona fisica designata o autorizzata al trattamento dal Titolare o dal Responsabile del trattamento;
- L'a**mministratore di sistema** è la figura professionale che mantiene, configura e gestisce un sistema centrale di elaborazione dati o sue componenti.

Funzioni di supporto

Al fine di meglio garantire l'applicazione del Regolamento di Ateneo in materia, vengono individuati specifici ruoli e strutture competenti a svolgere funzioni di supporto:

- **Funzione *Compliance*** (attualmente in capo all'ambito legale di Ateneo), preposta all'assistenza legale e giuridica agli Organi Accademici e alle Strutture di Ateneo, e competente anche per le tematiche legali in materia di *privacy* e protezione dei dati personali;
- **Funzione *ICT*** (attualmente in capo all'Area Sistemi Informativi ASI) con responsabilità di indirizzo e di controllo delle attività relative al processo ICT, di adozione delle misure di sicurezza identificate, di aggiornamento delle istruzioni agli incaricati e di designazione degli Amministratori di Sistema;
- **Funzione *Security*** (attualmente in capo all'U.O. Sicurezza e Processi IT afferente all'ASI) definisce le misure di sicurezza da adottare, supporta il responsabile del trattamento per la determinazione del tempo di conservazione dei dati, per la valutazione d'impatto (DPIA), in caso di analisi ed eventuale denuncia di violazioni, ecc.

Base giuridica dei trattamenti da parte dell'Università di Parma

Può essere costituita esclusivamente da una norma di legge o, nei casi previsti dalla legge, di Regolamento.
Il trattamento è lecito se è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito l'Ateneo.

Valutazione di impatto *(DPIA – Data Protection Impact Assessement)*

Novità prevista dal Regolamento europeo, secondo cui la DPIA, ovvero la valutazione di impatto del trattamento sui diritti degli interessati, è un elemento essenziale.
I responsabili del trattamento opportunamente supportati dalla funzione di *compliance*, dalla funzione *security* e quando necessario dalla funzione ICT, sentito il DPO, infatti, procedono alla valutazione d'impatto in presenza di almeno due condizioni tra quelle indicate all'art. 22 del Regolamento di Ateneo in materia di trattamento dati, individuando, nei casi di rischio elevato, misure specifiche per l'eliminazione o attenuazione del rischio.

Denuncia di violazione dei dati personali *(data breach)*

Il personale di Ateneo deve agire con la massima diligenza al fine di prevenire episodi di violazione dei dati personali, ossia accessi non autorizzati – da parte di altre persone dell'Ateneo e/o terzi – ai dati oggetto dei trattamenti facenti capo all'Ateneo o comunque incidenti al corretto svolgimento dei trattamenti medesimi.
Chiunque venga a conoscenza, direttamente o indirettamente, o abbia anche solo il sospetto di una violazione, deve comunicare immediatamente, tramite l'indirizzo email databreach@unipr.it al DPO, alla funzione security, al responsabile del trattamento competente, ove noto, e, in ogni caso, alla funzione di *compliance* tale possibile violazione.

Le funzioni coinvolte valuteranno se ricorrono i presupposti per considerare l'evento come violazione dei dati personali e, se del caso, informeranno dell'avvenuta violazione l'Autorità di controllo (Garante Privacy) e/o gli interessati i cui dati sono stati oggetto di violazione.

Informative e consenso degli studenti al trattamento dei dati personali

L'Università, nello svolgimento delle proprie funzioni istituzionali, non deve richiedere il consenso al trattamento dei dati personali (art. 6 lett. e del GDPR).

I dati forniti dagli studenti iscritti, sono trattati dall'Ateneo, in qualità di Titolare del trattamento, per finalità istituzionali connesse all'organizzazione e alla realizzazione dei Corsi di studio.

Il trattamento è necessario per il perseguimento del proprio fine istituzionale e avviene nel rispetto dei principi generali di trasparenza, correttezza e non eccedenza previsti dall'art. 5 del GDPR, con particolare riguardo alla liceità, all'utilizzo dei dati per finalità determinate, esplicite, legittime, in modo pertinente rispetto al trattamento, rispettando i principi di minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza, responsabilità.

L'Università è, invece, sempre tenuta a fornire l'informativa ai sensi degli artt. 13 e 14 del GDPR, i cui modelli sono reperibili nella sezione Privacy del sito web di Ateneo al link: https://www.unipr.it/ateneo/elezioni-statuto-e-regolamenti/privacy.

Non è necessario ottenere una presa visione della consegna dell'informativa, che è anche pubblicata sul sito elettronico dell'Ateneo.

Per le attività che non rientrano strettamente nei fini istituzionali è sempre necessario ottenere il consenso al trattamento dei dati da parte dell'interessato o di chi ne è tutore.

Registro dei trattamenti

Si tratta di uno strumento fondamentale che ciascun responsabile del trattamento è tenuto a redigere e aggiornare, al fine di disporre di un quadro completo dei trattamenti in essere. I contenuti minimi sono indicati all'art. 30 del GDPR nonché all'art. 28 del Regolamento interno di Ateneo. Deve avere forma scritta, anche elettronica e va esibito al Garante su richiesta.

Obbligo formativo

La normativa vigente impone in maniera esplicita una adeguata preparazione dei soggetti attivi nel trattamento, a seconda del preciso ruolo da questi ricoperto.

L'obbligo formativo ricade sul Titolare del Trattamento, che vi provvede tramite i competenti uffici, e sul Responsabile della Protezione dei Dati (DPO) sul quale ricade, altresì, il dovere di verifica dell'efficacia della formazione e il suo mantenimento nel corso del tempo**.**

L'Università di Parma ha già avviato il previsto percorso formativo con il corso "Privacy e sicurezza dei dati" tenutosi in data 29 maggio 2019. Il corso, obbligatorio per tutti i dipendenti, verrà somministrato, a breve, anche in modalità e-learning per consentire la formazione di coloro i quali non abbiano potuto partecipavi personalmente.
Per i soggetti che rivestono particolari ruoli, inoltre, l'Ateneo ha già programmato iniziative formative specifiche.

Per qualunque dubbio o perplessità derivante dall'applicazione pratica della normativa comunitaria e nazionale in materia di protezione dei dati personali, oltre che dall'applicazione del Regolamento interno di Ateneo in materia, si potrà richiedere il supporto della funzione *Compliance,* via mail, all'indirizzo legaleprivacy@unipr.it e del DPO all'indirizzo dpo@unipr.it