POLITICA DI CLASSIFICAZIONE DEI DATI

Approvazione
Data: **03/11/2021**
Dirigente ASI: **Dott.ssa Francesca Pruneti**
Firmato digitalmente ai sensi del D.Lgs. n. 82/2005

Informazioni sul documento		
Redazione a cura di: *U.O. Sicurezza IT* *U.O. Legale e compliance* *U.O. Programmazione e controllo di gestione*	**Destinatari:** *Utenti dell'Università di Parma e chiunque debba trattare i dati dell'Università di Parma*	**Deposito del documento:** *www.unipr.it/regolamento-sicurezza-IT*

Sommario

1. Scopo del documento

Lo scopo di questo documento è fornire un metodo di classificazione dei dati trattati dall'Università di Parma in base al loro valore e criticità per l'organizzazione, con l'obiettivo di individuare le misure di protezione più adeguate.

2. Ambito di applicazione

La politica descritta in questo documento si applica a qualsiasi forma di dati, inclusi documenti cartacei e dati digitali memorizzati su qualsiasi tipo di supporto, che siano soggetti a trattamento da parte di dipendenti, collaboratori dell'Ateneo e/o persone o società autorizzate al trattamento stesso.

3. Classificazione delle tipologie di dati

I dati trattati si distinguono in:

1. Dati personali
2. Dati non personali

3.1 Dati personali

Per **dato personale** si intende qualsiasi informazione riconducibile, in modo univoco, a una persona vivente identificata o identificabile.

Anche **le diverse informazioni che, raccolte insieme, possono portare all'identificazione di una determinata persona** costituiscono i dati personali. Ad esempio, un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online, uno o più elementi caratteristici dell'identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

I dati personali sottoposti a **deidentificazione, cifratura o pseudonimizzazione**, ma che possono essere utilizzati per reidentificare una persona, rimangono dati personali

Esempio di dati personali:

- nome e cognome;
- indirizzo di casa;
- indirizzo e-mail come nome.cognome@azienda.com;
- numero della carta d'identità;
- dati sulla posizione (ad es. la funzione di posizionamento su un telefono cellulare);
- indirizzo IP;
- ID cookie
- …

3.1.1 Categorie particolari di dati personali

Costituiscono categorie **particolari** di dati personali quelli che rivelino l'**origine razziale o etnica**, le **opinioni politiche**, le **convinzioni religiose o filosofiche**, o l'**appartenenza sindacale**, nonché i **dati genetici**, i **dati biometrici** intesi a identificare in modo univoco una persona fisica, i **dati relativi alla salute** o alla vita sessuale o **all'orientamento sessuale** della persona.
Anche i dati personali relativi alle **condanne penali e ai reati** o a connesse misure di sicurezza sono da considerarsi particolari e possono essere trattati soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati.

3.2 Dati non personali

I **dati non personali** sono dati che **non identificano né rendono identificabile una persona fisica.**
Esempi di dati non considerati personali:

- numero di iscrizione al registro delle imprese di una società;
- indirizzo e-mail impersonale come info@azienda.com;
- dati resi anonimi in modo irreversibile;
- dati statistici
- dati aggregati
- brevetti
- piani aziendali
- bilanci
- …

Partendo da queste due categorie sono state definite dieci tipologie di dati ognuna con un livello di protezione adeguato al rischio associato a quei dati. Le tipologie di dati elencate di seguito sono in ordine di rilevanza crescente sotto il profilo dell'impatto in caso di perdita di riservatezza, disponibilità e integrità dei dati.

Il livello di protezione associato a ciascuna tipologia di dato può assumere uno di questi cinque valori: basso, medio, alto, molto alto, critico. I livelli di protezione, descritti in un paragrafo successivo, sono definiti da un insieme di strumenti, procedure e sistemi di controllo adeguati a quel livello.

Tipo di dato	Descrizione	Livello di protezione	Esempio
Dati non personali tipo 1	Sono dati non personali solitamente destinati alla divulgazione pubblica, specialmente attraverso applicativi web propri o di terze parti.	1 – Basso	• Bandi, • informazioni sull'ente, • dati aggregati, • mappe, • …
Dati personali tipo 1	Rientrano in questa categoria i dati personali che a seguito degli obblighi di trasparenza applicabili all'ente, sono oggetto di pubblicazione sul portale di Ateneo e altre sedi pubblicamente accessibili.	1 – Basso	• Nome e cognome di assegnisti o collaboratori, • compensi delle figure apicali, • …
Dati non personali tipo 2	Rientrano in questa categoria i dati che generalmente non sono pubblicabili o accessibili senza un controllo dell'identità di chi li consulta. La perdita di riservatezza, integrità o disponibilità di questi dati potrebbe avere un impatto negativo moderato sulla missione aziendale in termini di sicurezza, reputazione o sotto l'aspetto economico-finanziario.	2 – Medio	• Dati dei processi aziendali, • materiale didattico per gli studenti iscritti, • contenuti didattici a pagamento, • …

Dati personali **tipo 2**	Rientrano in questa categoria i dati personali per i quali non è prevista la pubblicazione.	2 – Medio	• Documenti d'identità, • indirizzo del domicilio privato, • numero di cellulare • …
Dati non personali tipo 3	Rientrano in questa categoria i dati la cui protezione è richiesta per legge o da regolamenti di categoria. Dalla perdita di riservatezza, integrità o disponibilità dei dati o del sistema potrebbe derivarne un impatto negativo significativo sulla missione aziendale in termini di sicurezza, reputazione o sotto l'aspetto economico-finanziario.	3 – Alto	• Risultati di ricerche non ancora pubblicati, • pianificazione del budget, • bilanci, • strategie aziendali, • proprietà intellettuale, • …
Dati particolari (ad esclusione di quelli riferibili a tipologie successive)	Sono dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare l'orientamento sessuale.	3 – Alto	• Adesione sindacale, • adesione a organizzazioni universitarie, • …
Dati biometrici	I dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali i dati dell'immagine facciale o i dati dattiloscopici.	4 – Molto alto	• Immagini del volto, • impronte digitali, • timbro vocale, • qualsiasi elemento fisico idoneo ad essere letto e interpretato da programmi di riconoscimento automatizzato, • …
Dati sulla salute	I dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.	4 – Molto alto	• Temperatura corporea, • patologie pregresse o in corso, • referti medici, • …
Dati giudiziari	I dati che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale o la qualità di imputato o indagato. Il Regolamento UE 2016/679 (art. 10) ricomprende in tale nozione i dati relativi alle condanne penali e ai reati o a	4 – Molto alto	• Provvedimenti penali di condanna definitivi, • libertà condizionale, • il divieto od obbligo di soggiorno, le misure alternative alla detenzione,

	connesse misure di sicurezza. In particolare, rientrano in questa categoria i dati personali idonei a rivelare provvedimenti di cui all'art. 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.		• …
Dati genetici	I dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che conferiscono informazioni univoche sulla fisiologia di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione.	5 – Critico	• Risultati di esami genetici, • Risultati di test pre-sintomatici o predittivi, • …

4. Livelli di protezione dei dati

Per proteggere i dati con le adeguate misure di sicurezza, sono stati definiti dei livelli di protezione in termini di strumenti informatici, procedure e sistemi di controllo.

Livello di protezione 1 – Basso

Strumenti
Strumenti informatici che rispondono alle Misure Minime di Sicurezza ICT – livello minimo
Portali web e applicazioni senza autenticazione e cifratura delle informazioni in transito
Supporti mobili senza cifratura
Backup su dispositivi personali

Livello di protezione 2 – Medio

Oltre alle misure previste dal livello di protezione precedente, si adottano le seguenti.

Strumenti
Strumenti informatici che rispondono alle Misure Minime di Sicurezza ICT – livello standard
Portali web e applicazioni con autenticazione e cifratura delle informazioni in transito (OneDrive, Sharepoint etc.)

Supporti mobili con cifratura
Backup su dispositivi di Ateneo

Livello di protezione 3 – Alto

Oltre alle misure previste dal livello di protezione precedente, si adottano le seguenti.

Strumenti
Strumenti informatici che rispondono alle Misure Minime di Sicurezza ICT – livello avanzato
File server di Ateneo cifrato
Backup su dispositivi di Ateneo centralizzati

Procedure
Accesso ai dati solo a un elenco individuato di autorizzati

Livello di protezione 4 – Molto alto

Oltre alle misure previste dal livello di protezione precedente, si adottano le seguenti.

Strumenti
Applicazioni con algoritmi di crittografia forte per le informazioni in transito e basi di dati cifrate
Sistemi Operativi installati e mantenuti secondo le linee guida del CIS
Sistemi di posta elettronica con cifratura dei messaggi
Il software utilizzato deve avere analisi mensili delle vulnerabilità e aggiornamento continuo

Livello di protezione 5 – Critico

Oltre alle misure previste dal livello di protezione precedente, si adottano le seguenti.

Strumenti
Sistemi ICT certificati e applicazioni certificate per la gestione di dati genetici

5. Procedura di classificazione dei dati

Il responsabile dei dati, o il referente se nominato (art. 12 - Regolamento d'Ateneo sul trattamento dei dati personali), compila una tabella per ogni trattamento dati che deve gestire. Nella tabella elenca i singoli insiemi di dati che costituiscono il trattamento etichettandoli ognuno con un nome, poi barra con una "X" in corrispondenza della corretta tipologia di dati per quell'insieme. Il livello di protezione da applicare all'intero trattamento corrisponde al livello di protezione più alto fra quelli degli insiemi di dati inseriti. Per esempio, l'ufficio che si occupa di accoglienza e orientamento degli studenti deve gestire un trattamento con tre insiemi di dati: il primo sono le anagrafiche dei nuovi studenti iscritti con i loro contatti personali, il secondo è costituito dalle eventuali disabilità cognitive o motorie, mentre il terzo l'eventuale partecipazione a organizzazioni studentesche dell'Ateneo. Gli insiemi vengono etichettati (Anagrafiche, Disabilità e Organizzazioni) e poi viene scelto il tipo di dato corrispondente a ciascun insieme. Siccome il livello di protezione più alto corrisponde all'insieme "Disabilità", il trattamento deve essere gestito con gli strumenti, le procedure e i sistemi di controllo contenuti nel livello di protezione 4 – Molto alto.

Tipo di dato	**Livello di protezione**	**Insieme 1: Anagrafiche**	**Insieme 2: Disabilità**	**Insieme 3: Organizzazioni**
Dati non personali - tipo 1	1 – Basso			
Dati personali - tipo 1	1 – Basso			
Dati non personali - tipo 2	2 – Medio			
Dati personali - tipo 2	2 – Medio	X		
Dati non personali - tipo 3	3 – Alto			
Dati particolari	3 – Alto			X
Dati biometrici	4 – Molto alto			
Dati salute	4 – Molto alto		X	
Dati giudiziari	4 – Molto alto			
Dati genetici	5 – Critico			

6. Riferimenti

Elenco dei documenti utilizzati e risorse utili per la comprensione o l'approfondimento.

Nome	Contenuti e indirizzi
Regolamento UE 2016/679 (GDPR)	*https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6264597*
"Codice in materia di protezione dei dati personali" D.lgs. 30 giugno 2003, n.196	*https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9042678*

Misure Minime di Sicurezza ICT	*https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict*
Regolamento d'Ateneo sul trattamento dei dati personali	*https://www.unipr.it/node/26898*
Center for Internet Security (CIS)	*https://www.cisecurity.org/*

Revisioni del documento

Ver.	Descrizione modifiche	Autore	Data modifica
1.0	*Versione iniziale*	*U.O. Sicurezza IT*	*10/12/2020*