UNIVERSITÀ
DI PARMA

AREA AFFARI GENERALI E LEGALE
U.O. LEGALE

Prot. n.____ Parma,

Tit.__ Cl. __

Pregiatissimi Sig.ri:

- **Responsabili di strutture apicali**
- **Responsabili U.O.**
- **Personale docente**
- **Personale tecnico amministrativo**

e, p.c. **Parte Sindacale**:

- R.S.U.
- OO.SS.

Circolare n. 1 di *Compliance* al Reg. UE n. 679/2016 sulla protezione dei dati personali (GDPR), avente ad oggetto istruzioni tecniche concernenti l'utilizzo di strumenti informatici finalizzati a promuovere la sicurezza dei dati e della rete informatica di Ateneo, nonché la protezione della proprietà intellettuale.

Nel far seguito all'evento formativo di carattere obbligatorio in materia di *"Privacy e sicurezza dei dati"*, organizzato dal nostro Ateneo in data 29 maggio 2019, e, attualmente, fruibile in modalità e-learning fino alla data del 31 dicembre 2020, con la presente, **in costante attuazione dell'obbligo formativo di cui al Regolamento Europeo n. 679/2016 sulla protezione dei dati personali (GDPR)**, nonché allo scopo di mitigare le possibili minacce alla sicurezza dei dati di Ateneo derivanti dall'inesatto o imprudente utilizzo di dispositivi, che contengono dati, siano essi rimovibili (ad es. chiavette USB, DVD, dischi esterni…), o mobili (ad es. pc portatili, laptop), ed in risposta a recenti episodi di uso improprio e di inutile esposizione al rischio, si forniscono alla SS.LL. le sotto riportate

disposizioni:

Modalità di utilizzo supporti per salvataggio dati

1. E' fortemente **sconsigliato** l'utilizzo di dispositivi di memorizzazione e/o archiviazione dati esterna (ad es. chiavette USB, CD, memory card, hard disk esterni, ecc.); poiché il furto o la perdita accidentale del supporto stesso potrebbe consentire a chiunque di accedere agevolmente ai dati in esso contenuti, siano essi personali o relativi a proprietà intellettuale, con conseguente perdita di riservatezza e di controllo del dato stesso e suo possibile utilizzo anche a scopi illeciti. Si ricorda che, nel caso di violazione di dati personali, potrebbe rendersi necessario procedere con la notifica all'Autorità Garante della protezione dei dati personali;

2. Le necessarie attività di memorizzazione e archiviazione dei dati devono essere espletate utilizzando le aree strettamente personali negli spazi di cloud computing già messi a disposizione dall'Ateneo su cui esistono misure di sicurezza, riservatezza e disponibilità adeguate, quali: Onedrive, Sharepoint* (vedi nota in fondo al documento)

3. Per il personale tecnico-amministrativo è altresì vivamente **consigliata** l'archiviazione di file e/o informazioni di carattere lavorativo sui fileserver (disco S e disco U) di rete. Ciò poiché, in caso di perdita di dati, sarà sempre possibile richiedere il recupero del relativo file così come salvato nell'ultima versione di backup;

Cifratura

4. Qualora, per lo svolgimento delle attività lavorative, si renda strettamente necessario l'utilizzo del dispositivo esterno di archiviazione, ad esempio se il dispositivo rimovibile è utilizzato per trasportare file di grandi dimensioni, **è obbligatorio proteggere i dati cifrandoli** con programmi adeguati.

Rispettivamente:

1) per chiavette che si utilizzeranno solo con PC Windows: si può usare **BitLocker To Go (già presente nel sistema operativo nel Pannello di Controllo)**
2) per chiavette che si utilizzeranno solo con PC Macintosh: si può usare **Utility Disco** (https://support.apple.com/it-it/guide/disk-utility/dskutl35612/mac)
3) per chiavette che si utilizzeranno in ambienti misti: Windows, Macintosh e Linux: si può usare **VeraCrypt**

5. In caso di invio, a mezzo mail, di contenuti riservati, o comunque relativi a **categorie particolari di dati personali** (cioè dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona), si consiglia di procedere a criptare il file, prima dell'invio, con la crittografia con password o di livello superiore. Sarà necessario aver cura di comunicare, con discrezione e MAI unitamente all'invio del file stesso e comunque con un mezzo differente (es: sms, telefono), la password al destinatario del file. La password dovrà essere accuratamente conservata dal mittente e dal destinatario. Un software adatto allo scopo è 7ZIP che è liberamente installabile da tutti gli utenti in dominio Microsoft mediante Software center (dalla barra di Windows: pulsante Start -> Microsoft Endpoint Center -> Software Center).

Minimizzazione

6. È importante ricordare che i dati salvati nei dispositivi esterni, e più in generale quelli estratti e salvati sui propri dispositivi di elaborazione, devono rispondere ai **principi di minimizzazione**, pertanto è richiesto che vengano salvati e trattati solo i dati necessari e non eccedenti, rispetto all'espletamento delle attività per cui sono stati ottenuti, sia in termini di estensione e qualità dei dati (dati non necessari, es: elenchi di dati personali degli studenti con indirizzi personali, telefono cellulare, indirizzo email, ecc) che in termini temporali (dati non più necessari);

Custodia dei dispositivi

7. In caso di salvataggio, anche solo temporaneo, di dati su supporti rimovibili cifrati e non, gli stessi dovranno essere custoditi con la massima cura, prudenza e diligenza e non dovranno essere lasciati incustoditi o resi accessibili ad altri incaricati non autorizzati al trattamento dei dati ivi contenuti, in special modo qualora il dispositivo dovesse uscire dai locali di pertinenza dell'Ateneo;

8. I dispositivi esterni, come anche i dispositivi di elaborazione portatili (es: *laptop, smartphone*), devono essere sempre presidiati dagli incaricati e, quando non temporaneamente utilizzati devono essere

conservati con cura in luoghi sicuri, e, ove possibile, la loro archiviazione dovrà avvenire mediante strumenti dotati di misure di sicurezza (armadi o contenitori dotati di serratura);

9. I supporti rimovibili possono essere utilizzati e ceduti solamente tra gli incaricati autorizzati al trattamento dei dati in essi contenuti;
10. L'utente Responsabile o incaricato del trattamento richiamato rispettivamente agli artt. 12 e 14 del "*Regolamento* di Ateneo *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 679/2016*", **è responsabile della custodia dei supporti e dei dati aziendali in essi contenuti**.

Cancellazione dati o termine utilizzo dispostivi di archiviazione

11. I supporti rimovibili **non riscrivibili** quali CD-ROM / DVD i cui dati non possono essere eliminati attraverso procedure di formattazione del supporto, devono essere distrutti fisicamente se si ritiene che non debbano essere più utilizzati per il trattamento. Se gli obblighi di conservazione (c.d. *data retention*) dei dati contenuti in detti supporti non consentono la loro definitiva cancellazione (si faccia riferimento al Regolamento sul trattamento dei dati personali), il supporto – ove possibile - dovrà essere archiviato con le modalità di cui ai punti 7 e 8 della presente circolare;
12. Ferme restando le necessità di conservazione dei dati, nel rispetto delle indicazioni contenute nell'Appendice al 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 679/2016 | Università degli Studi di Parma , **i supporti rimovibili riscrivibili** (ad es. chiavetta USB, disco esterno) contenenti dati personali comuni e/o particolari, se non più utilizzati, dovranno essere formattati in modo sicuro. Al fine di assicurare la distruzione e/o inutilizzabilità di detti supporti magnetici rimovibili contenenti dati personali comuni o particolari, ciascun utente potrà aprire un ticket scrivendo a helpdesk.informatico@unipr.it

13 Al termine dell'utilizzo di un dispositivo di elaborazione portatile (ad es. pc portatile, laptop, smartphone) l'utente deve richiederne il ritiro attraverso l'apertura di un ticket a helpdesk.informatico@unipr.it. Il Supporto Utenti si farà carico della completa cancellazione dei dati

Smarrimento o perdita di supporti

14. L'utente è tenuto a comunicare immediatamente all'indirizzo databreach@unipr.it l'eventuale furto, smarrimento, perdita dei supporti rimovibili e/o di strumenti di elaborazione portatili (inclusi quelli personali se utilizzati per assolvere ad attività connesse all'Ateneo) e, ad attenersi alle istruzioni all'uopo ricevute;

*Spazi di cloud computing:

OneDrive è uno spazio in cluod di 50 GB, collegato al proprio account, che consente di archiviare i propri file personali in un'unica posizione, condividerli con altri e accedervi da qualsiasi dispositivo connesso a Internet.

Per accedere al proprio spazio di archiviazione su Onedrive è sufficiente cliccare il seguente link: https://univpr-my.sharepoint.com/

Nella sezione *Azienda o istituto di istruzione* di questa pagina potete trovare una guida all'utilizzo di tale strumento

https://support.office.com/it-it/article/video-di-formazione-su-onedrive-1f608184-b7e6-43ca-8753-2ff679203132?ocmsassetID=1f608184-b7e6-43ca-8753-2ff679203132&wt.mc_id=otc_home&ui=it-IT&rs=it-IT&ad=IT

Sono in corso di calendarizzazione eventi formativi specifici anche per consentire a tutto il personale di utilizzare al meglio gli strumenti consigliati.
Le istruzioni e disposizioni contenute nella presente circolare, in quanto concernenti la disciplina datoriale dell'attività di lavoro, hanno efficacia precettiva in ordine alle modalità di comportamento che i destinatari devono adottare; pertanto, i dipendenti sono tenuti ad osservarne le prescrizioni con diligenza.

Parma,

Il Rettore
Paolo Andrei

R.P.A. Responsabile del procedimento amministrativo	*U.O. Legale*	*Avv. Riccardo Marini*
	U.O. Sicurezza e Processi IT	*Dott.ssa Ilaria Comelli*