ISTRUZIONI PER LA PROTEZIONE DEI DATI PERSONALI

Formazione

Tutti i Soggetti Designati al trattamento dei dati personali di cui l'Università degli Studi di Modena e Reggio Emilia è titolare, sono tenuti a frequentare i corsi di formazione e aggiornamento organizzati dall'Ateneo sulle procedure e sui sistemi di sicurezza organizzativi, logici e fisici atti a tutelare il trattamento, la conservazione e l'integrità dei dati personali affidatigli per il trattamento e ad attenersi alle seguenti istruzioni.

Istruzioni per il trattamento dei dati personali

Ciascuno ha la responsabilità dei dati detenuti sulla propria stazione di lavoro e della loro protezione. I Soggetti Designati al trattamento dei dati detenuti dall'Ateneo, per il corretto e puntuale svolgimento del trattamento, dovranno:
1) prendere visione del Regolamento in materia di protezione dei dati personali di Ateneo e rispettare le prescrizioni in esso contenute;
3) prendere visione della procedura per la segnalazione del *data breach* e rispettare le prescrizioni in essa contenute.
Nel caso di trasferimento, anche temporaneo, ad altra struttura/ufficio, o nell'ipotesi di cessazione del rapporto di lavoro, il Soggetto Designato perde i privilegi di accesso ai dati personali riconosciuti all'ufficio di provenienza. L'autorizzazione al trattamento dei dati si intenderà revocata con la cancellazione del soggetto dall'elenco dei dipendenti e collaboratori afferenti alla struttura interessata dal trattamento come risultante dal Registro delle attività di trattamento.

Regole generali per tutti i trattamenti

Nello svolgimento del trattamento devono essere osservate le norme di legge e di regolamento in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali. In particolare:

- il trattamento dei dati personali, ai sensi dell'art. 5 del GDPR, deve rispettare i principi di liceità, correttezza e trasparenza nei confronti dell'interessato, e di limitazione delle finalità che devono essere determinate, esplicite e legittime;

- i dati trattati devono essere pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattate (minimizzazione dei dati) e devono essere esatti, se necessario aggiornati. I Soggetti Designati al trattamento, nello svolgimento di qualunque operazione di trattamento (raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento, modifica, estrazione, consultazione, uso, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto, interconnessione, limitazione, cancellazione, distruzione compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali) sono tenuti a:
  - ✓ prima di procedere alla raccolta dei dati, consegnare agli interessati la relativa informativa;
  - ✓ consentire l'esercizio dei diritti e delle facoltà previste dagli artt.15, 16, 17, 18, 20, 21 del GDPR (diritto di accesso, di cancellazione, di limitazione del trattamento, diritto alla portabilità dei dati, diritto di opposizione) nel rispetto delle indicazioni fornite dal Titolare e dai Referenti per la protezione dei dati;
  - ✓ collaborare, con gli altri Soggetti Designati al medesimo trattamento, esclusivamente per i fini dello stesso e nel rispetto delle indicazioni fornite dal Titolare e dai Referenti per la protezione dei dati;
  - ✓ non trasmettere all'esterno ed a soggetti terzi, informazioni circa i dati personali conosciuti in ragione del proprio ufficio, salvo che si tratti di comunicazione funzionale allo svolgimento dei compiti affidati, previa autorizzazione del Referente per la protezione dei dati.
  - ✓ rispettare il suddetto obbligo di riservatezza anche nel periodo successivo all'eventuale cessazione del rapporto di lavoro o al trasferimento ad altra unità organizzativa, fino a quando le suddette informazioni non vengano divulgate da parte del Titolare, oppure divengano di dominio pubblico;
  - ✓ accertarsi dell'identità del diretto interessato, prima di fornire informazioni circa i dati personali o il trattamento effettuato.
  - ✓ segnalare qualsiasi anomalia e stranezza da cui si possa desumere una anche solo presunta violazione di dati personali al Referente per la protezione dei dati.
- Nel caso di presenza in ufficio di un ospite o altro personale di servizio:
  - ✓ farlo attendere in luoghi in cui non sono presenti informazioni riservate o dati personali;
  - ✓ evitare di allontanarsi dalla scrivania in loro presenza, riporre i documenti e attivare il salvaschermo del PC prima di allontanarsi;

Trattamenti senza strumenti elettronici

Per quanto riguarda la eventuale documentazione cartacea, compresi i supporti non informatici contenenti la riproduzione di informazioni relative al trattamento di dati personali, i Soggetti Designati al trattamento sono tenuti a:

- conservare gli atti e i documenti contenenti dati personali per la durata del trattamento e successivamente riporli in archivi ad accesso controllato al fine di escludere l'accesso, agli stessi, da parte di persone non autorizzate al trattamento. A questo proposito sono tenuti a segnalare le eventuali necessità di dotazioni e arredi, in modo da poter adempiere a quanto prescritto;
- non lasciare gli atti e i documenti contenenti dati personali incustoditi su scrivanie o tavoli di lavoro e riporli nei relativi archivi a fine giornata;
- utilizzare gli appositi apparecchi "distruggi documenti" qualora si renda necessario distruggere i documenti contenenti dati personali; in assenza di tali strumenti, i documenti dovranno essere sminuzzati in modo da non essere più ricomponibili;
- adottate misure organizzative idonee per salvaguardare la riservatezza dei dati personali nei flussi di documenti cartacei all'interno degli uffici (es. trasmettere documenti in buste chiuse);
- se si è in attesa di un documento contenente informazioni riservate via fax, non lasciare incustodito l'apparecchio del fax ma rimuovere immediatamente il documento.

Trattamenti concernenti particolari categorie di dati personali
(origine razziale, etnica, opinioni politiche, convinzioni religiose, convinzioni filosofiche, appartenenza sindacale, dati genetici, dati biometrici intesi a identificare in modo univoco la persona fisica, dati relativi allo stato di salute, alla vita sessuale, all'orientamento sessuale della persona) o dati relativi a condanne penali e reati.

Nel caso di trattamento delle suddette categorie di dati ai Soggetti Designati al trattamento è richiesto il rispetto di norme di sicurezza aggiuntive quali:

- ✓ non fornire dati o informazioni di carattere sensibile per telefono, qualora non si abbia certezza assoluta sull'identità del destinatario;
- ✓ evitare di inviare, per fax o e- mail, documenti in chiaro contenenti dati sensibili: si suggerisce, in tal caso, di inviare la documentazione, senza alcun esplicito riferimento all'interessato (ad esempio, contrassegnando i documenti semplicemente con un codice);
- conservare, anche in corso di trattamento, i documenti, ancorché non definitivi, ed i supporti contenenti tali categorie di dati, in elementi di

arredo muniti di serratura e non lasciarli incustoditi in assenza del soggetto autorizzato al trattamento;

- conservare i supporti ed i documenti recanti dati relativi alla salute e alla vita sessuale nei predetti contenitori muniti di serratura, separatamente da ogni altro documento;
- non memorizzare mai tali particolari categorie di dati su supporti removibili (pennette usb, hard disk esterni, pc portatili).

Trattamenti con strumenti elettronici

Per quanto riguarda, in particolare, le elaborazioni e le altre fasi dei trattamenti effettuate attraverso strumenti informatici, ai Soggetti Designati al trattamento dei dati è richiesto il rispetto delle c.d. buone pratiche per la sicurezza informatica come da normativa vigente. In particolare, si dovranno seguire le precise indicazioni contenute nelle Istruzioni per i trattamenti con strumenti elettronici di Ateneo, in relazione alla:

- ✓ Gestione delle credenziali (utente e password)
- ✓ Scelta della password
- ✓ Difesa da attacchi informatici (virus, phishing, malware, ecc)
- ✓ Gestione delle postazioni di lavoro (pc, telefoni, tablet, stampanti, ecc.)
- ✓ Utilizzo degli applicativi e degli strumenti informatici
- ✓ Gestione delle apparecchiature dismesse

Gestione del materiale

Gestione del materiale di output

- se non utilizzati e quando ci si assenta dall'ufficio, provvedere a custodire in armadio o cassetto muniti di serratura i supporti removibili (es. chiavette USB, cd) contenenti informazioni riservate o strategiche;
- controllare attentamente lo stato delle stampe di documenti riservati e rimuovere immediatamente tali copie dalla stampante, onde evitare che personale non autorizzato abbia accesso alle informazioni;
- provvedere a rendere inintelligibili eventuali stampe non andate a buon fine.

Gestione del materiale cartaceo

- conservare i supporti cartacei contenenti dati personali in modo da evitare che detti documenti siano accessibili a persone non autorizzate al trattamento dei dati stessi (stanze, armadi, cassetti chiusi a chiave);