Regolamento europeo sulla Privacy

Corso di formazione 12 dicembre 2018

Collegio Geometri e Geometri Laureati

Pordenone

Ing. Tiziano Sinigaglia

Tiesse Informatica – Padova

www.tiesseinformatica.it

Regolamento europeo della Privacy

- Il Regolamento europeo 2016/679 sulla tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione dei dati è entrato in vigore il 24 maggio 2016 ed è diventato direttamente applicabile in tutti gli Stati membri a partire dal **25 maggio 2018**.

Dati personali, sensibili e giudiziari

- **Dati personali** : qualunque informazione relativa a persona fisica, («interessato»), che permette di identificarla direttamente o indirettamente. Ad esempio cognome e nome, codice fiscale, dati di nascita, indirizzo, telefono, e-mail, ecc.
- **Dati sensibili** : dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute fisica o mentale o alla vita sessuale o all'orientamento sessuale della persona
- **Dati personali relativi a condanne penali e reati :** il trattamento dei dati può avvenire soltanto sotto il controllo dell'autorità pubblica

Trattamento dei dati e incaricati

- **Trattamento** : qualsiasi operazione compiuta con o senza l'ausilio di strumenti elettronici (quindi compresi i supporti cartacei) effettuata su dati personali, come la raccolta, la registrazione, l'organizzazione, la conservazione, la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, la cancellazione o la distruzione.
- Gli **incaricati** sono le persone fisiche autorizzate ad operare sui dati. Devono avere un incarico scritto dal parte del titolare o del responsabile e **devono aver ricevuto una adeguata formazione**. Devono avere **sottoscritto un adeguato obbligo legale di riservatezza**. Hanno le responsabilità che derivano dal contratto di lavoro, o di collaborazione.

Titolare, responsabile, incaricati

- Il **titolare** è la persona fisica o giuridica che è responsabile di fronte alla legge del trattamento dei dati. Determina le finalità e i mezzi del trattamento di dati personali. Si assume tutte le responsabilità civili e penali.
- Il **responsabile** è la persona fisica o giuridica che tratta dati personali per conto del titolare del trattamento. Tramite un contratto scritto gli viene delegato uno specifico trattamento dei dati, con tutte le responsabilità di sicurezza correlate. Condivide le responsabilità con il titolare limitatamente al proprio incarico.
- **Esempi di responsabili :** commercialista, consulente del lavoro, RSPP, medico del lavoro, altri studi con i quali si collabora

Responsabile della Protezione dei dati

- Il Responsabile della Protezione dei dati (indicato anche come Data Protection Officer) è una nuova figura introdotta dalla normativa con i seguenti compiti :
  - informare e fornire consulenza in merito agli obblighi derivanti dal Regolamento europeo
  - sorvegliare l'osservanza del Regolamento europeo, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo
  - fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento
- La nomina di questa figura **è facoltativa** per gli Studi Tecnici
- Il nominativo va notificato al Garante e i suoi dati di contatto devono essere indicati nell'informativa privacy e nel sito Internet

Amministratori e manutentori di sistema

- L'amministratore di sistema è la persona o la ditta incaricata di impostare, gestire, controllare e mantenere le misure di sicurezza attivate sulle apparecchiature informatiche
- Il manutentore di sistema è la persona o la ditta incaricata di aggiornare, mantenere e assistere una specifica apparecchiatura informatica, o software gestionale (ad esempio software di contabilità)
- Se viene affidato l'incarico ad una ditta o persona esterna l'incarico deve essere nominativo e deve riportare il cognome e nome della persona incaricata, oltre a quello della ditta
- Per gli amministratori e i manutentori deve essere creato un utente specifico (con relativa password), oppure fatti operare sotto il proprio controllo e responsabilità
- Qualora le misure minime di sicurezza siano messe in atto con l'ausilio di ditte esterne, è consigliabile farsi rilasciare una descrizione di quanto effettuato e una dichiarazione di conformità con quanto prescritto dalla normativa

Informativa e consenso al trattamento dei dati

- L'**informativa** è una comunicazione che deve essere rilasciata alla persona fisica di cui si vogliono trattare i dati personali, di qualunque tipo essi siano
- Può essere data in forma scritta o orale, ma è consigliabile la forma scritta con l'apposizione di una firma che ne attesti la ricevuta
- Nel caso di trattamento di dati sensibili è obbligatorio anche il **consenso**, che deve essere libero, esplicito e inequivocabile. Non è ammesso il consenso tacito o presunto.
- Il consenso dei minori è valido a partire dai 16 anni, prima di tale età occorre raccogliere il consenso dei genitori o di chi ne fa le veci

Contenuti dell'informativa privacy

- Deve avere forma concisa, trasparente, comprensibile per l'interessato; occorre utilizzare un linguaggio chiaro e semplice
- L'informativa deve essere fornita all'interessato prima di effettuare la raccolta dei dati e deve contenere i seguenti dati :
  - l'identità e i dati di contatto del titolare del trattamento
  - i dati di contatto del **responsabile della protezione dei dati**, se nominato
  - le categorie dei dati personali oggetto di trattamento
  - le finalità del trattamento
  - gli eventuali destinatari dei dati personali
  - il **periodo di conservazione** dei dati personali

Contenuti dell'informativa privacy

- l'intenzione di trasferire dati personali fuori dell'Unione Europea (**servizi cloud**). In tal caso deve essere dichiarata l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o il riferimento alle garanzie appropriate rilasciate dal fornitore del servizio.
- l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al **diritto alla portabilità dei dati**
- l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca
- il diritto di proporre reclamo a un'autorità di controllo
- se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati

Adeguamento delle informative già raccolte e delle lettere di nomina

- Se le informative e le richieste di consenso non contengono i dati sopra indicati, o sono state rilasciate e raccolte in modo incompleto, è necessario **adeguarle e farle firmare nuovamente**.
- Inoltre si deve controllare che la nomina degli incaricati e dei responsabili del trattamento dati sia conforme alla nuova normativa.

Consenso alle foto e alle riprese audio e video

La legge sulla tutela dell'immagine personale richiede uno specifico consenso per :

- Fotografare le persone o effettuare riprese audio e video
- Pubblicare le foto in calendari, poster, notiziari, giornalini, ecc.
- Pubblicare le foto in Internet (sito dello Studio, Facebook, ecc.)
- Per ognuno di questi punti è **necessario chiedere un consenso esplicito**

Informativa sui siti Internet

- Se il sito Internet utilizza i «cookies» (piccoli file che vengono memorizzati nel computer) si ha l'obbligo di inserire nel sito una specifica informativa.
- E' richiesto l'esplicito consenso nei cookies di profilazione, ossia in quelli che memorizzano le scelte e le opzioni del visitatore, per poi proporre promozioni e messaggi pubblicitari
- Se all'interno del sito Internet sono previsti moduli di richiesta contatto, è necessario inserire l'informativa privacy e chiederne l'accettazione prima di procedere

Videosorveglianza

- Se viene installato un sistema di videosorveglianza (telecamere) bisogna :
  - Esporre i cartelli con l'informativa
  - Fare una specifica lettera d'incarico per chi controlla le telecamere
  - Cancellare le eventuali registrazioni entro 24 ore
- La videosorveglianza degli ambienti di lavoro è proibita dallo Statuto dei lavoratori

Diritto all'oblio

- Viene introdotto il diritto all'oblio, ossia il diritto di ogni persona di chiedere la cancellazione dei propri dati quando non più necessari per gli scopi in base ai quali sono stati raccolti.
- Questo riguarda anche la pubblicazione di notizie o foto sul sito Internet o sulla pagina Facebook.
- Tale diritto, tuttavia, viene meno quando la diffusione di determinate informazioni sia necessaria per l'adempimento di un obbligo legale o per l'esecuzione di un compito svolto nel pubblico interesse o nell'esercizio di pubblici poteri, per motivi di interesse pubblico nel settore della sanità pubblica, a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Portabilità dei dati

- Viene introdotto il diritto alla portabilità dei propri dati personali, ossia alla possibilità di trasferirli da un titolare del trattamento ad un altro.

- Ad esempio si potrà cambiare il gestore della posta elettronica senza perdere i messaggi salvati e la rubrica.

Trasferimento dati fuori dell'Unione Europea (servizi cloud)

- E' vietato trasferire i dati personali fuori dell'Unione Europea, salvo che il fornitore del servizio non sia stato «certificato» dalla Commissione Europea, o non vengano date specifiche garanzie contrattuali.
- In mancanza di certificazione o delle garanzia contrattuali, i dati potranno essere trasferiti solo con un esplicito consenso dell'interessato.
- Questo riguarda soprattutto i servizi cloud, inclusi Dropbox (Stati Uniti e Australia), Google Drive (stati Uniti), Onedrive (Microsoft).
- Il trasferimento dei dati fuori dell'Unione Europea va comunque indicato nell'informativa sul trattamento dei dati personali.

Cosa fare in caso di violazione dei dati personali

- Per «violazione dei dati personali» si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, il furto, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati
- Il titolare dovrà notificare al Garante della Privacy le violazioni di dati personali senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, ma soltanto se ritiene probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati
- Pertanto, la notifica all'Autorità dell'avvenuta violazione non è obbligatoria, essendo subordinata alla valutazione del rischio per gli interessati che spetta, ancora una volta al titolare. Se la probabilità di tale rischio è elevata, si dovrà informare delle violazione anche gli interessati, sempre senza ingiustificato ritardo

Cosa fare in caso di violazione dei dati personali

- Il titolare del trattamento dovrà in ogni caso documentare le violazioni di dati personali subite, anche se non notificate all'autorità di controllo e non comunicate agli interessati, nonché le relative circostanze e conseguenze e i provvedimenti adottati .
- Si raccomanda, pertanto, di **predisporre il modulo necessario a documentare eventuali violazioni**, essendo tenuti a fornire tale documentazione, su richiesta, al Garante in caso di accertamenti.

Principio di responsabilizzazione

- Viene affermato il principio di responsabilizzazione del titolare dei dati («accountability»), che sostituisce l'osservazione di alcune regole formali spesso non più al passo con l'evoluzione tecnologica (ex misure minime di sicurezza)
- Le misure di sicurezza devono garantire un livello di sicurezza adeguato al rischio
- La valutazione sull'adozione di misure di sicurezza viene rimessa al titolare e al responsabile del trattamento dati in rapporto ai rischi specificamente individuati
- In altre parole il titolare del trattamento dei dati deve essere in grado di dimostrare di avere adottato tutte le misure organizzative e tecniche per la protezione dei dati personali, anche attraverso l'elaborazione di specifici modelli organizzativi: deve dimostrare in modo positivo e proattivo di trattare i dati in modo conforme al regolamento europeo.

Misure di sicurezza consigliate

- **L'accesso ai computer deve essere protetto da password**
- Ogni utente deve avere delle credenziali diverse (nome utente e password)
- La password deve essere lunga almeno 8 caratteri e non può contenere riferimenti agevolmente riconducibili alla persona. Deve essere diversa per ogni incaricato del trattamento e va cambiata ogni 3 mesi
- Se il computer lo permette, predisporre un sistema automatico di cambio password periodico ogni 3 mesi
- Se il computer non tiene memoria dei cambi password, è bene mantenere per ogni utente una busta chiusa all'interno della quale vengono registrati tutti i cambi password
- Le credenziali di accesso vanno disattivate nel caso non vengano utilizzate per più di sei mesi
- Va attivato un **salvaschermo ("screen saver") con password** per evitare intrusioni mentre si è assenti (impostare un tempo di attesa di 10-15 minuti)

Misure di sicurezza consigliate

- **Il sistema operativo** (software che permette di avviare il computer) deve permettere anche di impostare delle autorizzazioni o delle limitazioni di accesso ai dati diversificate per ogni utente
- Questa funzionalità è disponibile nei sistemi Windows 7,8,10 di tipo Professional o in quelli di categoria server. Per altri sistemi operativi (Mac, Linux) chiedere la verifica al proprio tecnico informatico
- Deve essere impostato l'aggiornamento automatico del sistema operativo. Nel caso dei sistemi Windows deve essere attivata la funzione **Windows Update**, che avviene tramite Internet ed è gratuita
- I computer devono essere protetti da un **sistema antivirus** con aggiornamento automatico tramite Internet
- Deve essere presente anche un dispositivo di tipo software o hardware che blocchi i tentativi di intrusione dall'esterno ("firewall"). Anche questo va aggiornato periodicamente (almeno ogni 6 mesi).

Misure di sicurezza consigliate

- Il salvataggio ("backup") degli archivi contenenti dati personali deve essere eseguito almeno una volta la settimana
- Nel caso in cui non esista una notifica automatica è consigliabile compilare un registro dei backup con la data, l'esito e la firma dell'incaricato
- E' consigliato che l'incaricato del backup riceva una specifica lettera di nomina, con l'indicazione della procedura da seguire
- I supporti di backup (pen-drive, dischi USB, CD o DVD, ecc..) vanno custoditi in un luogo riservato, meglio se chiuso a chiave. Se si vuole riutilizzarli per altri scopi, vanno preventivamente cancellati con un software di cancellazione sicura, ossia essere resi non leggibili e non tecnicamente ricostruibili
- E' consigliabile la presenza di un gruppo di continuità per proteggere i computer in caso di black-out o sbalzi di corrente

Misure di sicurezza consigliate

- Capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico (ad es. contratto di assistenza con una ditta informatica o estensione di garanzia)
- Procedura per testare, verificare e valutare periodicamente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento
- La cifratura dei dati personali è una tecnica che permette di poter leggere i dati solo se in possesso della password. Quindi protegge contro eventuali furti o smarrimento di dati. E' una funzionalità presente in Windows 10/8.1 Professional o può essere attivata con appositi software. Si può cifrare sia il computer, che eventuali supporti rimovibili
- I dati personali, soprattutto quelli sensibili, inviati tramite posta elettronica vanno preventivamente cifrati, ossia codificati in modo tale da non essere leggibili da terze persone (es. ZIP con password)

Misure di sicurezza consigliate per gli archivi cartacei

- Anche in caso di trattamento solo cartaceo dei dati personali gli incaricati devono ricevere una lettera di incarico da parte del titolare e ricevere una adeguata formazione
- I dati personali, soprattutto quelli, vanno conservati in armadi o contenitori chiusi a chiave, o comunque in locali con accesso controllato
- Gli incaricati sono responsabili dei dati su supporto cartaceo per tutta la durata del trattamento, avendo cura di riporli nel loro raccoglitore al termine dello stesso.
- Particolare cura va posta nel caso di locali aperti al pubblico

Registro dei trattamenti

- Nel caso di trattamenti di dati sensibili viene introdotto l'obbligo di redigere un Registro dei trattamenti, che assomiglia molto al vecchio DPS.
- Il registro deve essere tenuto in forma scritta, anche in formato elettronico, e deve essere esibito su richiesta al Garante. Deve contenere obbligatoriamente le seguenti informazioni :
  - il nome e i dati di contatto del titolare del trattamento, dei rappresentanti del trattamento e del responsabile della protezione dei dati
  - le finalità del trattamento

Registro dei trattamenti

- una descrizione delle categorie di interessati e delle categorie di dati personali
- le categorie di destinatari a cui i dati personali saranno comunicati
- i trasferimenti di dati personali verso Stati al di fuori della Comunità Europea e la documentazione delle garanzie adeguate
- i termini previsti per la cancellazione delle diverse categorie di dati
- una descrizione generale delle misure di sicurezza tecniche e organizzative

- Il Registro dei trattamenti va tenuto aggiornato. SI consiglia comunque una revisione almeno una volta l'anno

Privacy «by design» e «by default»

- Viene introdotto l'obbligo di «privacy by design», ossia di considerare le problematiche privacy fin dalla progettazione di un nuovo trattamento o di un nuovo sistema.
- Devono essere garantite la correttezza, l'integrità, la riservatezza e la sicurezza dei dati, nonché l'effettiva cancellazione quando richiesta.
- Vien ribadito, poi, il concetto di «privacy by default», ossia la necessità che la salvaguardia dei dati personali sia sempre presente (non è un optional)

Aumento delle sanzioni

- Le sanzioni per l'inosservanza delle norme sulla Privacy sono state notevolmente aumentate e adesso arrivano fino a 20 milioni di euro, o al 4% del fatturato (se superiore) nel caso di un'impresa.
- I controlli si concentreranno sull'adozione delle misure di sicurezza da parte di pubbliche amministrazioni e di imprese che trattano dati sensibili, il rispetto delle norme sull'informativa e il consenso, la durata della conservazione dei dati da parte di soggetti pubblici e privati. L'attività ispettiva verrà svolta anche in riferimento a segnalazioni e reclami con particolare attenzione alle violazioni più gravi.

Decalogo degli adempimenti

- Informativa e consenso privacy
- Consenso alle foto e riprese audio e video
- Eventuale informativa cookies del sito Internet
- Eventuale informativa videosorveglianza e lettera di nomina degli incaricati della videosorveglianza
- Lettera di nomina degli incaricati al trattamento dati
- Lettera di nomina dei responsabili del trattamento dati
- Lettera di nomina degli incaricati del backup
- Lettera di nomina dell'amministratore e/o manutentore di sistema

Decalogo degli adempimenti

- Attivazione delle misure di sicurezza
- Scheda di verifica periodica delle misure di sicurezza
- Registro dei trattamenti
- Predisposizione del modulo da usare in caso di violazione dei dati

Per saperne di più …

www.garanteprivacy.it/pacchettoprotezionedati

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI