2 TERMINI E DEFINIZIONI (ordine alfabetico)

(**R**if. Associati a UNI EN ISO 9000, UNI CEI ISO/IEC 27001, UNI ISO 31000, EU Reg. 2016/679, UNI ISO/IEC 25012, UNI CEI EN ISO/IEC 17065)

Amministratori di Sistema

Professionisti che in ambito ITC, gestiscono e manutengono un impianto di elaborazione o di sue componenti.

Analisi del rischio

Utilizzo sistematico di informazioni per identificare le cause e stimare il rischio.

Archivio

Qualsiasi insieme organizzato e sistematico di dati personali disponibili su supporto cartaceo o digitale, accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o distribuito geograficamente.

Audit interno

Esame sistematico ed indipendente per determinare se l'attività svolta ed i risultati ottenuti sono in accordo con quanto pianificato e se quanto pianificato e predisposto risulta congruo al raggiungimento degli obiettivi.

Autenticazione Informatica

Insieme degli strumenti elettronici e delle procedure di verifica anche indiretta dell'identità dell'utente di un sistema informatico ed elettronico che anche solo potenzialmente fornisca un mezzo di accesso ai dati personali sia esso diretto o indiretto.

Autorità capofila

Autorità di controllo disciplinata dall'art. 56, EU Reg. 2016/679

Azione correttiva

Azione da intraprendere per eliminare la causa di non *compliance* rilevata o di particolari situazioni che si presentano all'esame.

Azione preventiva

Azione per eliminare la causa di una non compliance potenziale o di situazioni non desiderabili. L 'azione preventiva si adotta per evitare il verificarsi di non *compliance*.

Carta di Nizza

Carta dei diritti fondamentali dell'unione europea proclamata a Nizza il 7 dicembre 2000 e pubblicata i 18.12.2000 (2000/C 364/01)

Credenziali di autenticazione

Dati e/o dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica.

Dati

Forme classificabili e reinterpretabile dell'informazione che è possibile processare in modo formalizzato, sia cartaceo che elettronico-digitale, per essere controllato e reso idoneo alla comunicazione, alla interpretazione e alla loro elaborazione.

Dati Anonimi

Dato che in origine, o a seguito di trattamento, non può essere assodato ad un interessato identificato o identificabile.

Dati Identificativi:

Dati personali che permettono l'identificazione diretta dell'interessato.

Dati Particolari

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 lo stato di salute e la vita sessuale.

Dato Biometrico

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 l'immagine facciale o i dati dattiloscopici.

Dato Genetico

I dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione.

Dato Personale

Qualunque informazione riguardante una persona fisica identificata o identificabile.

Dato relativo alla 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.

Disponibilità

Le informazioni devono essere disponibili entro i tempi stabiliti a coloro che le richiedono e sono autorizzati ad accedervi

Integrità

Proprietà di salvaguardia dell'accuratezza e completezza dei dati.

ISO (International Organization for Standardisation)

Ente internazionale con sede e Ginevra, che ha il compito di armonizzare le norme emanate dagli enti di normazione delle varie nazioni relativamente alle procedure tecniche e metrologiche.

Misurazione di qualità dei Dati

Variabile a cui è assegnato un valore come il risultato di misurazione di una caratteristica di qualità dei dati o indicante un loro livello di sicurezza richiesto.

Misure di sicurezza

Complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che garantiscono un livello di protezione adeguato a quello richiesto dalla valutazione dei rischi connessi al trattamento secondo la norma di riferimento e la base giuridica secondo finalità.

Misure opportune di compliance

Elementi di valutazione della *compliance* al Regolamento da parte del *Titolare* per attenuare il rischio.

Non *compliance*

Mancato soddisfacimento di un requisito, valutazione in luogo di inadempienza.

Norme vincolanti d'impresa

Politiche in materia di protezione dei dati personali applicate da un *Titolare* del trattamento o Responsabile stabilito in uno stato membro per regolare il trasferimento o il complesso di trasferimenti di dati personali a un responsabile in un paese terzo fuori dall'unione.

Organizzazione internazionale

Un'organizzazione e gli organismi di diritto internazionale pubblico ad essa subordinati o qualsiasi altro organismo istituito sulla base di un accordo fra due o più stati.

Parola chiave

Componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica.

Principio di esattezza

Obbligo del *Titolare* di agire sui dati inesatti rispetto alla finalità dichiarate, di garantire e verificare l'esattezza, l'aggiornamento e la completezza dei dati trattati, i dati inesatti o rettificando con tempestività le anomalie riscontrate.

Principio di finalità

Trattamento di un Archivio che avviene in termini chiari determinati e manifestati all'atto della raccolta.

Principio di liceità e correttezza

Trattamento di un Archivio nel rispetto delle norme vigenti, a regolamenti o a normativa comunitaria e comunque in modo trasparente nei confronti dell'Interessato.

Principio di non eccedenza

Utilizzo dei soli dati sufficienti al perseguimento dei legittimi fini dichiarati, pertinenti e non eccedenti i fini stessi ("minimizzazione dei dati").

Principi di Pertinenza e Trasparenza

Pertinenza - dei dati rispetto alla finalità per cui vengono trattati.

Trasparenza - informazioni destinate al pubblico o all'interessato siano concise, facilmente accessibili e di facile comprensione e che sia usato un linguaggio semplice e chiaro.

Profilazione

Qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o calcolare metricamente caratteristiche e/o aspetti di rendimento professionale, di situazione economica, di salute, di preferenze personali, di interessi, di affidabilità, di comportamento, di ubicazione, o di spostamenti della persona fisica resi georeferenziabili.

Profilo di autorizzazione

Insieme degli attributi, univocamente associati ad una persona, che consentono di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti.

Pseudonimizzazione

Trattamento di dati personali che rendono identificabile l'interessato o possono essere a lui associati solo con ulteriori informazioni aggiuntive, separatamente conservate e sottoposte ad adeguate misure tecniche e organizzative che non ne consentano l'attribuzione univoca ad una persona.

Qualità dei Dati

La valutazione metrica del livello di sicurezza delle caratteristiche dei dati quando soddisfano coerentemente condizioni prestabilite e/o implicite alle condizioni di trattamento dichiarate nelle politiche del sistema di Qualità e Sicurezza.

Responsabilizzazione (Accountability)

Obbligo *Titolare* nel garantire ed essere in grado di dimostrare il rispetto degli obblighi derivanti dai principi previsti nella normativa di riferimento.

Riesame

Valutazione sistematica e regolare dell'efficacia ed efficienza degli elementi atti a conseguire gli obiettivi pianificati e stabiliti. Il riesame può comprendere un adattamento a nuove esigenze per azioni di miglioramento

Rischio elevato

E' una condizione ci rischio di pregiudizio dei diritti e delle libertà delle persone fisiche.

Sistema

Insieme di strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

Strumenti elettronici

Elaboratori, programmi per elaboratori, e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento.

Struttura HLS

Struttura generale ad alto livello, cioè struttura comune a gli standard ISO definita nel 2012 al fine di migliorare l'interoperabilità degli standard normativi. Si basa principalmente su terminologie, testi, definizioni e sequenza comuni.

Terzo

La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il *Titolare* del trattamento, il Responsabile del trattamento, il Delegato al trattamento e una Soggetto Autorizzati al trattamento dei dati personali sotto l'autorità diretta del Responsabile o del *Titolare*.

TFEU

Trattato sul funzionamento dell'Unione Europea (trattato di Lisbona)

Titolare del Trattamento

Persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli stati membri, il *Titolare* del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal dritto dell'Unione o dagli stati membri.

Tracciabilità

Grado in cui i dati hanno attributi che forniscono una registrazione degli accessi ai dati e a tutte le modifiche effettuate ai dati in un contesto di utilizzo specifico.

Trattamento

Qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di strumenti elettronici, processi automatizzati e applicate a dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, memorizzazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

Trattamento a rischio

Trattamento di dati personali suscettibile di cagionare un danno fisico, materiale o morale in particolar modo se il trattamento comporta discriminazione, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione o qualsiasi altro danno economico o sociale importante. Viene inoltre considerato trattamento particolarmente a rischio il trattamento di categorie particolari di dati, la valutazione della personalità, preferenze ed interessi personali, affidabilità o comportamento. Infine, è trattamento a rischio il trattamento di una notevole quantità di dati personali per un vasto numero di interessati.

Valutazione del rischio

Processo atto a determinare la probabilità e la gravità del rischio del trattamento, in funzione della natura, dell'oggetto, del contesto e delle finalità del trattamento dei dati personali. La valutazione deve essere basata su elementi di valutazione oggettivi.

Valutazione d' Impatto

E' la valutazione che si rende obbligatoria, qualora un tipo di trattamento presenti un rischio elevato per i diritti e le libertà dei interessati.