



DISCLAIMER

Il materiale contenuto nel drive è stato raccolto e richiesto tramite autorizzazione ai ragazzi frequentanti il corso di studi di Informatica dell'Università degli Studi di Salerno. Gli appunti e gli esercizi nascono da un uso e consumo degli autori che li hanno creati e risistemati per tanto non ci assumiamo la responsabilità di eventuali mancanze o difetti all'interno del materiale pubblicato.

Il materiale sarà modificato aggiungendo il logo dell'associazione, in tal caso questo possa recare problemi ad alcuni autori di materiale pubblicato, tale persona può contattarci in privato ed elimineremo o modificheremo il materiale in base alle sue preferenze.

Ringraziamo eventuali segnalazioni di errori così da poter modificare e fornire il miglior materiale possibile a supporto degli studenti.



CoScienze
Associazione

Norme e Formati della Firma Digitale - Introduzione Norme

Un **regolamento** è una legge europea di diretta applicazione, cioè una volta approvato è applicabile negli stati membri senza una diretta ratifica.





Una **direttiva** europea non è immediatamente vincolabile ma deve essere approvata dai vari parlamenti. eIDAS è un regolamento europeo del 2014 che definisce il panorama per l'autenticazione della firma.

E' stato recepito nella normativa italiana con delle opportune modifiche nel codice dell'amministrazione digitale. Fondamentalmente è la normativa di riferimento per la digitalizzazione della pubblica amministrazione con ripercussioni sul settore privato. Del CAD (Codice dell' Amministrazione Digitale) ci interessa la definizione di documento elettronico, ovvero un documento elettronico è un artefatto che contiene la rappresentazione informatica di atti, fatti e dati giuridicamente rilevanti.

Il quadro normativo nazionale ed internazionale definisce chiaramente cosa sia una firma digitale e quali caratteristiche debba avere. I vari tipi di firme elettroniche sono necessarie per conferire validità legale ai documenti informatici quando per esempio si sottoscrivono contratti o atti amministrativi. Questo implica che devono avere lo stesso valore della firma autografa.

- Firma elettronica (semplice o debole) FES o FEC - "dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare" (una scansione della firma olografa);
- Firma elettronica avanzata FEA - "una firma elettronica che soddisfi i requisiti di cui all'articolo 26":
 - è connessa unicamente al firmatario;
 - è idonea a identificare il firmatario;
 - è creata mediante dati che il firmatario può utilizzare sotto il proprio esclusivo controllo;
 - è collegata ai dati per identificare ogni successiva modifica.
- Firma elettronica qualificata FEQ - "una firma elettronica avanzata creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche"
- Firma digitale FD - "un particolare tipo di firma qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare di firma elettronica tramite la chiave privata e a un soggetto terzo tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici".

Il titolo V del D.P.C.M. 22 febbraio 2013 indica all'art. 55 che "la realizzazione di soluzioni di firma elettronica avanzata è libera e non è soggetta ad alcuna autorizzazione preventiva" e non è vincolata all'adozione di particolari piattaforme.

	Tipologia	Definizione	Valore probatorio	Tecnologia	Esempi
	Firma Elettronica	Insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica	Efficacia probatoria valutabile dal giudice caso per caso	Neutra	PIN, firma biometrica, UserID e Password
	Firma Elettronica Avanzata	Insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati	Efficacia probatoria della scrittura privata integra la forma scritta od substantiam tranne che per i contratti immobiliari	Neutra	Firma grafometrica su tablet, PEC verso la PA.
	Firma Elettronica Qualificata	Particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma	Efficacia probatoria della scrittura privata integra la forma scritta od substantiam	Non neutra, certificato qualificato e dispositivo sicuro	Smart-card, token USB
	Firma Elettronica Digitale	Particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico	Efficacia probatoria della scrittura privata integra la forma scritta od substantiam	Non neutra, certificato qualificato chiavi asimmetriche e dispositivo sicuro	Smart-card, token USB, MicroSD, Firma remota

Dal punto di vista dell'efficacia giuridica delle firme elettroniche sussiste il principio definito di "non discriminazione" dove:

- Una FEQ ha effetti giuridici equivalenti a quelli di una firma autografa. E' riconosciuta in tutti Stati membri dell'UE.

Il CAD estende questa norma europea e stabilisce che nei casi di sottoscrizione con FES "l'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, in relazione alle caratteristiche di sicurezza, integrità e immodificabilità". In caso di contenzioso il giudice dovrà valutare, se in sede di generazione della firma sono state adottate idonee misure, tecnologiche e procedurali, atte a garantire in modo certo ed univoco la connessione tra il firmatario e il documento. Il titolare della firma digitale a dover dimostrare l'esistenza di un abuso nell'uso del dispositivo.

Le sospensioni e le revoche dei certificati qualificati sono giornalmente registrate dai prestatori di servizi fiduciari sulle CRL (Certificate Revocation List) che vengono consultate dai software in sede di verifica della firma digitale proprio con lo scopo di verificare se il certificato è valido o meno.

Il momento della pubblicazione deve inoltre essere attestato mediante adeguato riferimento temporale. L'apposizione ad un documento informatico di una firma digitale o di un altro tipo di firma basata su un certificato qualificato revocato, scaduto o sospeso equivale a mancata sottoscrizione. Pertanto c'è l'obbligo di attribuire a tutti i documenti informatici un riferimento temporale rappresentato dall'informazione contenente la data e l'ora sincronizzata con il tempo coordinato universale. Quando si firma un documento è pertanto necessario accertarsi circa la validità del proprio certificato e sapere come agire per preservare l'autenticità dello stesso oltre il termine di scadenza. Per quanto riguarda la firma digitale, quando apponiamo la firma ad un documento andiamo a realizzare quella che è definita busta crittografica, Essa contiene sia la firma del documento che il documento stesso.

I formati di realizzazione di busta crittografica dovrebbero sempre essere:

- "aperti" cioè conformi a specifiche pubbliche disponibili a chiunque;
- "non proprietari" cioè formati che sono indipendenti dalle piattaforme tecnologiche utilizzate per la formazione dei documenti;
- "robusti" in grado di recuperare in tutto o in parte il contenuto del file eventualmente corrotto o danneggiato;
- "stabili" cioè compatibili con le versioni precedenti e future;
- "sicuri" in relazione al grado di protezione dai virus;
- non contenenti macroistruzioni.

Formati

I formati da privilegiare per la conservazione a lungo termine sono i seguenti in relazione alla diversa tipologia documentale:

- PDF, PDF/A, TIFF utilizzato per la memorizzazione delle immagini;
- ODF-OOXML-XML-TXT, RFC 2822/MIME per i messaggi di posta elettronica.

Con l'apposizione di una firma digitale si crea la "busta crittografica" che è un file che racchiude il documento originale, la firma digitale e la chiave di verifica che è contenuta nel certificato del sottoscrittore.

- La busta che si crea utilizzando una firma CAdES è un file con estensione .p7m con formato pkcs#7, il cui contenuto è visualizzabile solo utilizzando idonei software in grado di "sbustare" il documento sottoscritto. Presenta il vantaggio di essere in grado di firmare qualsiasi formato di documento ma

ha lo svantaggio che il destinatario del documento avrà bisogno dell'installazione sul pc di un software specifico.

- La firma digitale PAdES genera un file con estensione .pdf secondo lo standard ISO/IEC 32000 leggibile con i comuni reader disponibili per questo formato, ma può essere utilizzata solo per firmare file con estensione pdf.
- XAdES (XML Advanced Electronic Signature) rappresenta un nuovo standard di firma digitale basato su file XML (formato già definito dal W3C)

I Sigilli Elettronici

Nella normativa e nella pratica c'è distinzione tra persona fisica e persona giuridica. La persona fisica è una qualunque persona, una persona giuridica è una persona che rappresenta un'organizzazione. La firma può essere apposta da una persona giuridica e in questo caso non si parla di firma digitale perchè non è certificata l'identità ma si parla di **Sigillo elettronico**. Il sigillo elettronico è l'equivalente del timbro apposto sui documenti.

Sigillo elettronico	Firma digitale
Garantisce l'origine e l'integrità dei documenti digitali.	Garantisce l'identità del firmatario di un documento digitale e conferisce piena validità legale a un documento digitale.
Si riferisce a una persona giuridica (un organismo unitario composto da una pluralità di individui o un complesso di beni, al quale vengono riconosciuti diritti e doveri).	Si riferisce a una persona fisica (un soggetto di diritto, dotato di capacità giuridica, con degli obblighi e dei diritti fin dalla sua nascita).

Similmente alle firme, è previsto un sigillo elettronico (semplice), uno avanzato ed uno qualificato.

- Un sigillo elettronico avanzato è tale se consente:
 1. Connessione esclusiva, univoca e diretta con il creatore;
 2. Idoneità a identificare il creatore;
 3. Creazione di un sigillo elettronico che possa essere controllato/utilizzato esclusivamente dal titolare;
 4. Collegamento a dati con cui garantirne l'originalità e l'integrità.

Un sigillo elettronico qualificato è un sigillo elettronico avanzato che sia stato creato utilizzando un dispositivo dotato di certificato qualificato.

Il sigillo elettronico è la forma digitale del "timbro" su carta, l'apposizione di un sigillo elettronico dovrebbe rendere immediatamente evidente l'origine di un documento elettronico riportando i dati identificativi della persona giuridica, un po' come la carta intestata della società.

Posta Elettronica Certificata - La Posta Elettronica

La posta elettronica (Electronic mail, o e-mail) è un servizio a cui possono accedere gli utenti collegati a Internet per spedire e ricevere messaggi 'elettronici'. Per usufruire di questo servizio è necessario disporre di un indirizzo. Ci sono due possibilità per ottenere un indirizzo di posta elettronica:

- attraverso l'iscrizione a un provider (pubblico o privato), che permette di ricevere, oltre a un 'account', un indirizzo di posta elettronica;
- attraverso l'iscrizione ai servizi di posta elettronica basati su Web (Web-based e-mail) offerti da alcune società (Hotmail, Yahoo, Kataweb...).

Per la gestione della posta elettronica gli utenti possono scaricare appositi software applicativi, come Microsoft Outlook, oppure avvalersi di servizi web accessibili da un browser e gestiti dal proprio provider.

La Posta Elettronica - Sicurezza

La posta elettronica è intrinsecamente un metodo di comunicazione non sicuro. Per offrire sicurezza abbiamo 2 strategie:

- prendere SMTP e costruirlo su SSL/TLS e fare SMTPS
- prendere MIME ed estenderlo per aspetti di sicurezza per la cifratura dei documenti

SMTPS usa sicurezza a livello di trasporto tra le entità di una firma digitale(tra utente e client di posta e tra client di posta e un altro client di posta)

MIMES offre sicurezza a livello applicativo, ovvero cifra e protegge un messaggio che va su un canale e raggiunge il destinatario che può decifrarlo o verificare la firma. I due possono essere usati assieme ma quello che manca in questo sistema è la certificazione della consegna.

La Posta Elettronica Certificata

La posta elettronica certificata o PEC è un tipo particolare di posta elettronica che permette di dare a un messaggio di posta elettronica lo stesso valore legale di una tradizionale raccomandata con avviso di ricevimento, garantendo così la prova dell'invio e della consegna.

Tutti i flussi documentali all'interno della pubblica amministrazione hanno validità legale mediante PEC.

Per il servizio di PEC si devono usare solamente domini dedicati, cioè domini il cui compito esclusivo è quello di gestire la PEC. Pertanto non possono esistere domini promiscui che al contempo gestiscono la posta elettronica "classica", e la PEC; infatti se ciò accadesse risulterebbe più facile un'eventuale compromissione del servizio PEC.

- Ricevuta di avvenuta consegna, che attesta che il messaggio è giunto a buon fine e che il destinatario ne ha piena disponibilità nella sua casella (anche se non ha ancora ricevuto il messaggio).

Il Gestore può emettere tre differenti tipologie di Ricevute di Avvenuta Consegna, che possono soddisfare differenti esigenze dell'utenza.

- La Ricevuta Completa è costituita da un messaggio di posta elettronica inviato al mittente che riporta in formato leggibile i dati di certificazione (mittente, destinatario, oggetto, data e ora di avvenuta consegna, codice identificativo del messaggio). Gli stessi dati sono inseriti all'interno di un allegato in XML.
- La Ricevuta Breve ha lo scopo di ridurre i flussi di trasmissione della PEC, e contiene il messaggio originale e gli hash crittografici di eventuali allegati. Per permettere la verifica dei contenuti, il mittente deve conservare gli originali non modificati degli allegati inseriti nel messaggio originale.
- La Ricevuta Sintetica segue le regole di emissione della ricevuta completa solo che l'allegato contiene esclusivamente il file XML con i dati di certificazione descritti.

Tutti i processi documentali, sia nel privato che nella pubblica amministrazione, hanno sostituito la posta elettronica normale con la posta elettronica certificata.

L'AGID (Agenzia per l'Italia Digitale) è l'ente che statale che sovrintende a questo organismo. Ha una serie di registri per sapere i gestori, casellari della pubblica amministrazione, necessari per riconoscere ad esempio qual'è la posta elettronica certificata di un dato comune.

- le comunicazioni elettroniche trasmesse ad uno dei domicili digitali mediante PEC hanno gli stessi effetti giuridici delle comunicazioni a mezzo raccomandata con ricevuta di ritorno ed equivalgono

alla notificazione per mezzo della posta salvo che la legge disponga diversamente [sentenza n. 4 del 3 gennaio 2019 la Corte di Appello di Brescia].

- l'utilizzo della posta elettronica certificata va inteso nei casi per i quali è necessaria l'evidenza dell'avvenuto invio e ricezione di un documento informatico [art.48].

Il valore aggiunto della PEC rispetto ad altri canali di comunicazione		
	Valore aggiunto della PEC	
PEC	<ul style="list-style-type: none"> ✓ certezza consegna ✓ valore legale ✓ certezza casella mittente 	E-mail
PEC	<ul style="list-style-type: none"> ✓ velocità e semplicità ✓ valore legale ✓ ubiquità 	Fax
PEC	<ul style="list-style-type: none"> ✓ certezza del contenuto ✓ velocità e semplicità ✓ tracciabilità mittente 	<ul style="list-style-type: none"> ✓ ubiquità ✓ costi Raccomandata A/R
PEC	<ul style="list-style-type: none"> ✓ velocità e semplicità ✓ costi ✓ ubiquità 	Consegna brevi manu

Norme Protezione dei Dati Personali

Quando si parla di privacy bisogna conoscere il quadro normativo, che ci definisce i diritti e i doveri e quindi che cosa deve garantire un sistema che deve preservare la privacy. Avere un sistema sicuro non garantisce la privacy e avere un sistema che è compliant con il GDPR non vuol dire avere un sistema sicuro.

Il termine "protezione dei dati" è un termine un po' fuorviante in quanto la privacy non protegge i dati. Questo termine deriva dal tedesco Datenschutz ed è il primo termine utilizzato in contesto privacy in un quadro normativo, risale al 1970, la Legge sulla protezione dei dati (Datenschutzgesetz) del Land tedesco dell'Assia, redatta dal "padre della protezione dei dati", il Professore Spiros Simitis.

- Il titolo utilizzava un termine "improprio, dal momento che [la Legge] non proteggeva i dati, ma il diritto degli individui i cui dati [venivano] trattati."
- il termine reale è "protezione delle persone fisiche con riguardo al trattamento dei dati personali"

La protezione dei dati presenta sia aspetti attinenti alle libertà individuali che aspetti sociali, quello che si va a tutelare sono i diritti delle persone e le loro libertà.

Inizialmente essendo un diritto della libertà, in legislatura viene chiamato **diritto fondamentale o proto-diritto**. Agli inizi degli anni '60 la Privacy era nelle costituzioni degli stati o era un diritto derivato da quelli costituzionali, quindi non si sentiva la necessità di avere una legge ad hoc per la privacy.

Con l'arrivo e diffusione dei computer, la problematica della protezione dei dati è diventata molto più cruciale. Questo perché mentre con i dati cartacei bastava proteggere gli archivi per proteggere le informazioni, con gli archivi digitali invece la problematica della protezione dei dati è diventata predominante.

Dalla legge degli anni '70 sono state emanate una serie di leggi in tutti gli stati europei che trattano la protezione dei dati. Queste leggi in giurisprudenza vengono chiamate leggi "leggi omnibus", ovvero non sono leggi specifiche ma sono leggi che sanciscono i diritti fondamentali (non sono leggi costituzionali). Queste leggi non dicono cosa fare per garantire la protezione dei dati, ma dicono che il cittadino ha il diritto ad esempio alla non divulgazione dei suoi dati.

Quindi essendo enunciati di principio, spesso rimanevano lettera morta. Quindi quando si è iniziato ad avere il processo di unificazione e omogeneizzazione europea, si è sentito il problema di avere molti stati membri con leggi completamente diverse tra loro o leggi omnibus che non venivano applicate.

Il Consiglio d'Europa quindi si è iniziato a porre la questione di dover avere dei regolamenti sulla protezione dei dati.

- 1973: Risoluzione del Consiglio d'Europa (73) sulla Tutela della riservatezza delle persone in rapporto alle banche dati elettroniche nel settore privato;
- 1974: Risoluzione del Consiglio d'Europa (74) sulla Tutela della riservatezza delle persone in rapporto alle banche dati elettroniche nel settore pubblico.

Nota: il Consiglio d'Europa è il consiglio dei capi di stato e di governo dell'Unione Europea, è un organo legislativo ma intergovernativo. Sono strumenti non vincolanti in cui si vanno ad emanare una serie di diritti che poi gli stati membri devono applicare. L'UE ci dice che abbiamo una serie di principi "fondamentali" che gli stati dovrebbero garantire attraverso leggi ad hoc.

Anche l'ONU e l'OSCE hanno emanato una serie di regolamenti in materia, ma tutti non vincolanti. Ovvero erano tutte leggi omnibus comuni transnazionali che però dovevano essere implementate; il problema è che molte di queste leggi rimasero sulla carta. Dalle risoluzioni del consiglio d'Europa, l'Italia nell'89 ha emanato la **legge 98** che ratifica i regolamenti e le direttive del consiglio d'Europa. Questa legge è stata quella fondamentale e iniziale per la protezione dei dati in Italia.

Con l'introduzione dell'UE e del parlamento Europeo, l'Europa si è dotata di una direttiva univoca, la **direttiva 95** sulla protezione dei dati. Non è una convenzione del Consiglio d'Europa ma è una direttiva, vuol dire che è una legge del Parlamento Europeo. Una direttiva va approvata, ovvero i parlamenti degli stati membri la devono approvare e quindi ratificare.

La direttiva 95 è stata approvata in Italia nel 96 ed è stata una delle prime nazioni a farlo; la direttiva 95 sostituiva la legge 98. La legge 675 che recepiva la direttiva è stata ulteriormente modificata nel 2003, questo per restringere quelli che erano i principi della direttiva europea.

Tale legge in Italia ha anticipato il GDPR, infatti nel 2016 l'Italia aveva già nel proprio organigramma organizzativo molte delle norme che hanno costituito il GDPR. Il GDPR non è una direttiva ma un regolamento, questo vuol dire che viene attuato immediatamente dall'entrata in vigore senza essere controfirmato dal parlamento nazionale.

Quando si parla di protezione dei dati, un contesto particolarmente critico è Internet. Dalla direttiva 95 si è sentita la necessità di fare una verticalizzazione dei diritti fondamentali, da cui ne è scaturita la direttiva 58 che è la direttiva e-Privacy specifica per il settore delle comunicazioni elettroniche.

Le due direttive viaggiano a braccetto, la prima dava i diritti fondamentali e la seconda prendeva quei diritti e li verticalizza nel settore delle comunicazioni elettroniche (vale solo su internet e il settore delle comunicazioni).

Ad esempio se ho un sito web sono subordinato alla prima direttiva in quanto un sito non è un sistema di comunicazione. Il problema dell'e-Privacy è che è molto limitata, si pensi ai dispositivi smart Home come Alexa e Google assistant; su tali dispositivi, la normativa e-Privacy non viene applicata in quanto non sono dispositivi di comunicazione, quindi va sul GDPR. Il Parlamento Europeo ha in discussione anche il regolamento e-Privacy che sostituirà la direttiva e-Privacy. Ogni strumento giuridico dell'UE (in passato CE) è, per sua natura, limitato alle materie di competenza del diritto dell'UE.

Le Direttive CE si limitavano a materie nell'ambito del cosiddetto Primo Pilastro, e non si applicavano alle attività del Secondo o Terzo Pilastro, per i quali sono stati elaborati a parte degli strumenti di protezione dei dati personali.

- **Pilastro 1:** Sono le politiche dell'UE che impattano i cittadini
- **Pilastro 2:** Sono gli aspetti di sicurezza comune
- **Pilastro 3:** Sono gli aspetti di potere giudiziario e di pene.

I tre pilastri dell'Unione Europea, istituiti con il Trattato di Maastricht del 1992, sono stati un modo di dividere le politiche dell'Unione Europea in tre aree fondamentali. Sono stati successivamente aboliti con l'entrata in vigore del Trattato di Lisbona nel 2009.

La direttiva 95 verteva sul primo pilastro e non sugli altri 2, quindi se dovevo garantire la privacy in ambito militare e in ambito giudiziario, la direttiva 95 non veniva applicata, ma c'erano direttive specifiche sugli altri pilastri.

La Direttiva ha ampliato le definizioni di base della Convenzione del 1981 (convenzione sulla protezione dei dati collegata alla direttiva 95)

Direttiva e-Privacy

La Direttiva che ci interessa conoscere è la 58, abitualmente definita "Direttiva e-Privacy" in quanto è più recente e spesso indicata come "la norma sui cookie" perché ha principalmente disciplinato i cookie.

La Direttiva e-Privacy è ancora in vigore, anche se la Direttiva sulla protezione dei dati del 1995 è stata sostituita dal Regolamento Generale sulla Protezione dei Dati (GDPR). Nelle materie specificamente disciplinate dalla direttiva e-Privacy, quest'ultima si applica in luogo del GDPR. Pertanto, le basi giuridiche contemplate nel GDPR non trovano applicazione qualora la Direttiva e-Privacy contenga norme più specifiche per il trattamento di dati personali.

Mentre la Direttiva del 1995 prevedeva un ampio campo di applicazione a tutti i trattamenti di dati personali da parte di organismi pubblici o privati operanti nel "Primo Pilastro" della Comunità Europea, la Direttiva e-Privacy, in quanto strumento sussidiario, ha un campo di applicazione molto più ristretto, relativo alla [fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione]. Sussistono però delle ambiguità relative al campo di applicazione materiale e le disposizioni nazionali hanno spesso un campo di applicazione diverso da quello previsto all'Art. 3 della direttiva e-Privacy. Fin quando la Direttiva e-Privacy non sarà sostituita dal Regolamento e-Privacy sussisterà questo deficit di chiarezza anche rispetto alla legge nazionale applicabile.

Il GDPR dice che bisogna avere un'autorità per la privacy, la direttiva e-Privacy invece dice che per tutto ciò che riguarda le reti bisogna avere un'autorità (garante delle comunicazioni). Poiché la Direttiva e-Privacy è stata espressamente concepita quale *lex specialis* rispetto alla *lex generalis* della Direttiva del 95, le definizioni relative alla protezione dei dati della Direttiva 95 erano applicabili anche alla Direttiva e-Privacy, ora sostituite da quelle del GDPR.

La Direttiva e-Privacy aggiunge ulteriori definizioni, quali quelle di "utente", "dato relativo al traffico", "dato relativo all'ubicazione", "servizio a valore aggiunto", e "violazione dei dati personali". La modifica più importante concernente i concetti-chiave del GDPR rispetto alla Direttiva 95 riguarda la definizione di "consenso" in quanto è una delle basi giuridiche per il trattamento di dati personali.

La Direttiva e-Privacy prevede che il "consenso" è la base giuridica principale per alcuni trattamenti ma non per tutti quanti. Ho tutti i riferimenti al GDPR e tutte le basi giuridiche del GDPR, però la direttiva e-Privacy richiede il consenso ad esempio per la raccolta di informazioni dal terminale dell'utente o dell'abbonato. Se

però c'è la necessità di raccogliere informazioni per far pagare un servizio, non bisogna chiedere il consenso. Questo perché un'altra base giuridica è il "legittimo uso".

Il punto di contatto tra questa direttiva e il GDPR è l'obbligo di garantire la sicurezza, ma soprattutto di notificare violazioni dei dati personali. Questa è una caratteristica propria del GDPR che introduce il principio accountability, ovvero il monitoraggio dell'uso dei dati. Se avviene una violazione di privacy, la devo valutare e **notificare**.

Le notifiche possono essere **all'utente**: se c'è stata una violazione di libertà, ovvero hanno rubato i miei dati e devo saperlo; **all'autorità competente**.

Non occorre informare di una violazione dei dati gli abbonati e altre persone interessate se il fornitore è in grado di dimostrare "all'autorità competente" che i dati oggetto della violazione erano stati resi totalmente "incomprensibili" a chiunque abbia potuto accedervi a seguito della violazione, attraverso opportune misure tecnologiche di protezione.

Riservatezza delle comunicazioni: assicurare, mediante disposizioni di legge nazionali, la riservatezza delle comunicazioni effettuate tramite la rete pubblica di comunicazione e i servizi di comunicazione elettronica accessibili al pubblico, nonché dei relativi dati sul traffico. In particolare essi vietano l'ascolto, la captazione, la memorizzazione e altre forme di intercettazione o di sorveglianza delle comunicazioni, e dei relativi dati sul traffico, ad opera di persone diverse dagli utenti, senza consenso di questi ultimi, eccetto quando sia autorizzato legalmente.

GDPR

Il vecchio impianto normativo si fondava sulla centralità del consenso dell'interessato, a garanzia della legittimità dei trattamenti effettuati dal titolare, mentre il GDPR ha mutato tale assetto, prevedendo il consenso dell'interessato solo come uno dei casi che rendono leciti i nostri trattamenti; l'art.6 GDPR definisce le basi giuridiche.

- La necessità di dare esecuzione a un contratto di cui l'interessato è parte o a misure precontrattuali adottate su richiesta dello stesso;
- L'adempimento di un obbligo legale al quale è soggetto il titolare del trattamento, come ad esempio il trattamento dei dati dei dipendenti compiuto dal datore di lavoro per motivi di previdenza sociale e fiscalità;
- La salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica, come il caso di epidemie o emergenze umanitarie;
- L'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
- il legittimo interesse privato, se ho un'azienda che emette ricevute, devo poter monitorare l'uso della risorsa che ti sto dando, quindi posso monitorare l'uso che fai di quel servizio senza chiedere il consenso.

Il GDPR sancisce molto bene qual'è il legittimo interesse di un'azienda dal marketing. Con la vecchia direttiva, il marketing, veniva visto come una delle possibili attività che rientravano nel legittimo interesse. Quindi lo scambio dati per marketing, veniva visto come legittimo interesse, con il GDPR questo non è più possibile. Il marketing diretto e indiretto è opportunamente disciplinato, quindi se io raccolgo informazioni su una fascia di utenti, non posso trasmettere le informazioni raccolte a terzi per il marketing.

Il Comitato Europeo per la Protezione dei Dati (EDPB), ha osservato che se il titolare del trattamento sceglie il consenso quale propria base giuridica per legittimare un trattamento di dati personali. Il titolare, in base alla base giuridica scelta può fare determinati trattamenti. Se cambia la finalità deve cambiare anche la base giuridica, altrimenti quel trattamento non è lecito.

Diversi sono gli attori del trattamento dei dati personali:

- Il titolare è definito dal GDPR (Art. 4) come quel soggetto che determina le finalità e i mezzi del trattamento di dati personali. Se due o più titolari determinano congiuntamente le finalità e i mezzi del trattamento, sono da considerarsi contitolari del trattamento
- Il responsabile del trattamento, invece, è la persona fisica o giuridica che tratta i dati per conto del titolare del trattamento, seguendo istruzioni precise, contenute in un contratto o altro atto giuridico vincolante. Il responsabile del trattamento, come il titolare, ha degli obblighi specifici che spesso si affiancano a quelli del titolare stesso. Deve tenere un **Registro** di tutte le categorie di attività relative al trattamento (Art. 30), mettere in atto misure tecniche e organizzative adeguate per garantire la sicurezza del trattamento (Art. 32), designare, in determinate situazioni, un responsabile della protezione dei dati (Art. 37).
- Il responsabile per la protezione dei dati (RPD), con il compito di fornire un supporto consulenziale (al titolare o al responsabile che lo ha nominato) sul rispetto delle norme in materia di protezione dei dati, agendo al contempo da punto di contatto con l'autorità di controllo.

L'Art. 37 del GDPR prevede l'obbligo di nominare un RPD in tre casi:

- se il trattamento è svolto da un'autorità pubblica o da un organismo pubblico;
- se le attività principali del titolare del trattamento o del responsabile consistono in trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
- se le attività principali del titolare o del responsabile del trattamento consistono nel trattamento di categorie particolari di dati personali di cui all'Art. 9 o di dati relativi a condanne penali e a reati di cui all'Art. 10 (art 9: minori o persone fragili, art 10 parte penale)

L'RPD è in genere un professionista esterno all'organizzazione, che ricopre tale ruolo in base a un contratto di servizi, ma può anche essere un dipendente del titolare o del responsabile del trattamento

L'Art. 39 del GDPR specifica i compiti e le funzioni degli RPD.

- informare e fornire consulenza al titolare (o al responsabile) che l'ha nominato, nonché al personale dello stesso che esegue le attività di trattamento (autorizzati al trattamento), in merito ai loro obblighi,
- sorvegliare l'osservanza delle norme dell'Unione europea o dell'ordinamento nazionale sulla protezione dei dati attraverso attività di controllo e la formazione del personale che partecipa ai trattamenti,
- cooperare con l'autorità di controllo e fungere da punto di contatto per quest'ultima per questioni connesse al trattamento dei dati come, per esempio, un'eventuale violazione dei dati personali.

Per assicurare l'indipendenza dell'RPD, il GDPR stabilisce alcune garanzie:

- I titolari e i responsabili del trattamento devono assicurare che gli RPD non ricevano alcuna istruzione. Essi non possono essere rimossi o penalizzati in alcun modo per l'adempimento dei compiti propri di RPD.

Per quanto riguarda lo svolgimento delle attività di controllo, in una grande azienda non è detto che faccia tutto l'RPD, ma egli può individuare dei dipendenti che lo coadiuvano e supervisionano i trattamenti in essere nell'azienda.

Il legislatore italiano ha ritenuto opportuno introdurre una nuova figura:

- Designato: persona fisica individuata dal titolare (o dal responsabile del trattamento) nell'ambito del proprio assetto organizzativo e alla quale sono attribuiti specifici compiti, tra l'organizzazione e coordinamento delle attività di trattamento.

I dati personali, una volta raccolti dal titolare, possono essere comunicati ad altri soggetti appartenenti o meno all'organizzazione del titolare

- Si definisce "destinatario" «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che riceve comunicazioni di dati personali, che si tratti o meno di terzi». È terzo, quindi, «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 e le persone autorizzate al trattamento dei dati sotto l'autorità diretta del titolare o del responsabile»

La protezione dei dati personali ha bisogno di una serie di diritti, che sono 15-22 del GDPR.

L'interessato è messo nelle condizioni di esercitare i propri diritti attraverso le informazioni che il titolare è tenuto a fornirgli nel momento in cui raccoglie i suoi dati personali (Art. 13) o lo fa mediante altre fonti (Art. 14).

Il primo diritto che ha un interessato e che è Prodromico all'esercizio di tutti gli altri diritti, è il **diritto di accesso**, ovvero posso richiedere i miei dati in qualsiasi momento all'azienda che fa il trattamento.

L'interessato ha il diritto di sapere se un trattamento dei propri dati personali è in corso e di accedere alle seguenti informazioni:

- finalità del trattamento; categorie dei dati in questione; destinatari o categorie di destinatari a cui i dati sono comunicati; periodo di conservazione dei dati personali previsto oppure, se non è possibile, criteri utilizzati per determinare tale periodo;
- esistenza del diritto di rettificare o cancellare i dati personali o limitare il loro trattamento; diritto di proporre reclamo all'autorità di controllo; tutte le informazioni disponibili sulle fonti dei dati oggetto del trattamento, qualora i dati non siano raccolti presso l'interessato; nel caso di decisioni automatizzate, la logica applicata nei trattamenti automatizzati dei dati.

Il **diritto di rettifica** (Art. 16) sancisce che l'interessato può chiedere di correggere le inesattezze dei dati personali che lo riguardano. Le inesattezze possono riguardare anche l'incompletezza dei dati stessi;

Il **diritto di cancellazione o all'oblio** (Art. 17) significa che il titolare è tenuto a dare corso alla richiesta, senza ingiustificato ritardo quando:

- i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
- l'interessato revoca il consenso su cui si basa il trattamento e non sussiste altro fondamento giuridico per il trattamento;
- l'interessato si oppone al trattamento e non sussiste alcun motivo legittimo prevalente per procedere al trattamento;
- i dati personali sono stati trattati illecitamente;
- per adempiere un obbligo legale;

La prova della legittimità del trattamento è in capo al titolare del trattamento, il quale deve sempre essere in grado di provare l'esistenza di una solida base giuridica per il trattamento dei dati, in virtù del **principio di responsabilizzazione**. Esempio se cambio operatore, il vecchio operatore non è tenuto a cancellare i miei dati in quanto gli servono per poter inviare eventuali bollette.

Il diritto alla cancellazione non è privo di eccezioni, connesse ai casi in cui il trattamento dei dati personali sia necessario per:

- l'esercizio del diritto alla libertà di espressione e di informazione;
- l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare;
- motivi di interesse pubblico nel settore della sanità pubblica;

- per archiviazione nel pubblico interesse, ricerca scientifica, storica o statistica;
- l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria

Il **diritto di limitazione** (Art. 18) indica che gli interessati possono chiedere la limitazione del trattamento quando:

- viene contestata l'esattezza dei dati personali;
- il trattamento è illecito e l'interessato chiede la limitazione dell'utilizzo dei dati personali invece della cancellazione;
- i dati devono essere conservati per la difesa di un diritto in sede giudiziaria;
- è pendente una decisione in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

In caso di revoca della limitazione, il titolare è tenuto a informare l'interessato prima di effettuare tale revoca. Eventuali rettifiche o cancellazioni dei dati personali o limitazioni del trattamento devono essere comunicate dal titolare a ciascuno dei destinatari a cui sono stati trasmessi i dati, a meno che ciò non risulti impossibile o sproporzionato (Art. 19).

Il **diritto alla portabilità dei dati**: gli interessati possono richiedere la portabilità dei dati con dei mezzi automatizzati. Ad esempio se ho dati cartacei posso richiedere la portabilità in digitale. Questo significa che devo avere una opportuna base giuridica per poter fare la portabilità.

Inoltre i dati devono essere portabili tra le varie organizzazioni. Esempio: l'esame del sangue deve essere comprensibile anche in un'altra nazione.

Il **diritto di opposizione**: in determinate condizioni e quando la base giuridica è quella di esecuzione di un diritto privato, posso oppormi. Posso richiedere, motivando, che mi oppongo ad un determinato trattamento. Questo perché esiste un bilanciamento tra i diritti dell'interessato e i diritti legittimi di una organizzazione di business.

Uno degli aspetti importanti di questo diritto è il trattamento automatico delle informazioni. Il GDPR dice che decisioni automatizzate sui dati raccolti o elaborati da un algoritmo, sono vietati. Se ammesse, le decisioni automatizzate devono essere accompagnate da misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, comprendenti almeno il diritto di ottenere l'intervento umano da parte del titolare, di esprimere la propria opinione e di contestare la decisione.

Il GDPR introduce una serie di obblighi che rientrano nel termine di principio di accountability.

Accountability in inglese significa che io registro le attività, quindi io so esattamente che attività faccio, che violazioni ho, avviso delle violazioni. Principio di trasparenza nei trattamenti e rischi. I sistemi andrebbero realizzati adottando la privacy by design e la privacy by default

Convenzione del 2018

In Europa siamo tutti GDPR compliant, quindi finché i miei dati viaggiano in Europa non ci sono problemi. Nel momento in cui ho un trasferimento o trattamento transnazionale dalla comunità Europea a un paese terzo, devo valutare che le garanzie normative del paese terzo siano simili a quelle Europee, se non lo fossero non è consentito il trattamento e il trasferimento. Il Consiglio d'Europa ha realizzato una convenzione dove se tu approvi questa convenzione e il tuo quadro normativo è conforme al GDPR, i dati possono avere valore transnazionale.

Questa convenzione nasce nel 2011 quando il GDPR ancora non c'era, quindi questa convenzione nasce seguendo la direttiva 95. Con il GDPR anche questa convenzione si è aggiornata diventando la 108+.

Molte le novità contenute nella nuova Convenzione: da una parte il rafforzamento degli obblighi del titolare tra cui il principio di accountability, una maggiore trasparenza nei trattamenti, la valutazione preventiva dei rischi del trattamento, i principi di privacy by design e by default, la notifica dei data breach. Dall'altra,

l'ampliamento dei diritti degli interessati, compreso il diritto a non essere soggetto a decisioni automatizzate e a conoscere la logica del trattamento.

Compiti del RPD

Amministratori di Sistema

C'è differenza tra l'amministratore di sistema e il responsabile della protezione dei dati. Sono due figure separate, mai unite. Fondamentalmente l'amministratore di sistema è pagato dall'azienda e non è indipendente quindi non può essere responsabile. Molto spesso l'amministratore di sistema è la persona che affianca il responsabile, il responsabile deve avere conoscenza dell'azienda e chi meglio dell'amministratore di sistema può dargli questa scelta, però in realtà non può fare il responsabile della protezione dei dati e ce lo dice il garante. Un aspetto che però fare l'amministratore di sistema è quello di dare seguito al principio di accountability del GDPR, l'amministratore di sistema gestisce i **log** che non sono altro che sistemi di accountability.

L'amministratore di sistema fondamentalmente monitora i dipendenti, perché sa quando qualcuno effettua l'accesso a un sistema. Qui entra la necessità del login/logout e trattamento dei dati personali, questo perché l'accesso a un sistema è categorizzato come dato personale. Con l'accesso a un sistema posso ricostruire le abitudini di un utente, la pratica aziendale e quindi monitorare il dipendente ed eventualmente escluderlo da eventuali premialità.

Spesso l'amministratore di sistema può essere in outsourcing, ovvero che non è all'interno dell'azienda. Qui entrano in atto una serie di obblighi da parte dell'amministratore in outsourcing. Quando c'è l'outsourcing quindi bisogna anche gestire chi fa il trattamento dei dati personali, chi fa l'accountability ecc.

Un RPD deve anche formare il personale dell'azienda rispetto agli obblighi del GDPR. Questo perché i lavoratori devono essere informati sulle norme e sul trattamento dei dati.

DPIA

La DPIA è il risk assessment sulla privacy. Il Data Protection Impact Assessment (DPIA) è un processo volto a descrivere un trattamento di dati personali, valutarne la necessità e la proporzionalità, nonché gestirne gli eventuali rischi per i diritti e le libertà delle persone fisiche da esso derivanti, effettuando una valutazione del livello del rischio e determinando le misure idonee a mitigarlo.

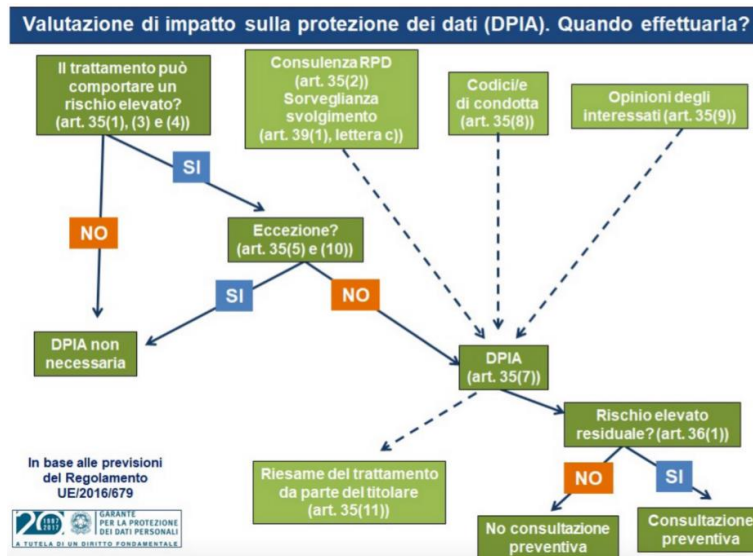
Un processo di DPIA può riguardare una singola operazione di trattamento dei dati. Tuttavia, si potrebbe ricorrere a un singolo DPIA anche nel caso di trattamenti multipli simili tra loro in termini di natura, ambito di applicazione, contesto, finalità e rischi.

L'art. 35 del GDPR stabilisce che è necessario effettuare una DPIA in tutti i casi in cui le operazioni di trattamento presentano rischi elevati per i diritti e le libertà delle persone fisiche in virtù della loro natura, portata o finalità o quando possono procurare un danno economico o sociale importante.

La DPIA deve essere effettuata prima di procedere al trattamento, già dalla fase di progettazione del trattamento stesso e deve essere continuativa. Deve essere continuativa perché in fase di progetto non posso rendermi conto di alcuni rischi che posso individuare solo in fase di esecuzione e quindi prevedere misure opportune in grado di mitigare i rischi.

La valutazione DPIA concorre, insieme ad eventuali altri processi di valutazione e gestione del rischio alla "Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita" come previsto dall'art. 25. Ciò consente di acquisire le necessarie conoscenze sulle misure, garanzie e meccanismi da

prevedere per mitigare il rischio e assicurare la conformità al GDPR, prima che possano essere arrecati danni ai diritti ed alle libertà delle persone fisiche.



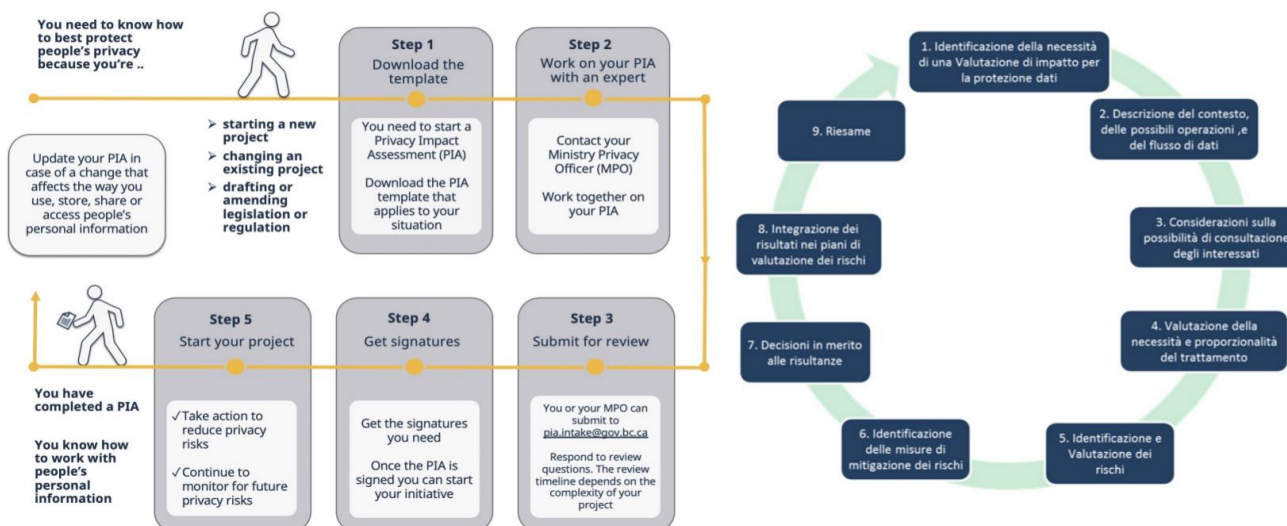
La realizzazione di una DPIA è obbligatoria soltanto qualora il trattamento "possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche" Le linee guida WP24 (organismo di supporto e consulenza europeo) definiscono i casi per cui a DPIA è obbligatoria/necessaria.

Nei casi in cui non è chiaro se sia richiesta una valutazione d'impatto sulla protezione dei dati o meno, si raccomanda di effettuarla comunque, in quanto detta valutazione è uno strumento utile che assiste i titolari del trattamento a rispettare la legge in materia di protezione dei dati. L'Autorità di controllo redige un elenco di trattamenti per cui la DPIA è obbligatoria e lo comunica al Comitato Europeo per la Protezione dei Dati. Una DPIA non è richiesta nei seguenti casi:

- quando il trattamento non è tale da "presentare un rischio elevato
- quando i risultati della valutazione d'impatto sulla protezione dei dati di un trattamento si possono utilizzare per un trattamento analogo
- quando le tipologie di trattamento sono state verificate da un'autorità di controllo prima del maggio 2018 in condizioni specifiche che non sono cambiate;

L'art. 35 al paragrafo 7 definisce il contenuto minimo che deve comunque essere assicurato per la redazione di un DPIA:

- "una descrizione dei trattamenti previsti e delle finalità del trattamento";
- "una valutazione della necessità e proporzionalità dei trattamenti";
- "una valutazione dei rischi per i diritti e le libertà degli interessati";
- "le misure previste per: -"affrontare i rischi"; -"dimostrare la conformità al presente regolamento".



La valutazione del rischio è una funzione $R = f(I, P, V)$, dove R (il rischio) è funzione delle vulnerabilità (V) e degli Impatti (I) e Probabilità (P) delle possibili Minacce che possono insistere sulle vulnerabilità. Un esempio di un software applicativo per la gestione di un processo DPIA è "PIA", scaricabile gratuitamente dal sito di CNIL (Autorità francese per la protezione dei dati).

Il GDPR fa riferimento all'obbligo del titolare (ed eventualmente del responsabile) di tenere conto dei rischi che i trattamenti possono comportare per i diritti e le libertà delle persone fisiche.

- l'art. 24 e 25, collocano l'analisi dei rischi come misura per tener conto per mettere in atto tutte le misure tecniche e organizzative adeguate;
- l'art. 35, che prevede invece una specifica valutazione di impatto quando i trattamenti, considerate le circostanze indicate nella norma, possono presentare rischi elevati per gli interessati.

L'audit e il logging sono quelle fasi di raccolta informazioni e servono per il monitoraggio continuo e servono a ripetere su scala periodica la DIPIA.

Attività di Analisi

Marketing e Profilazione

In generale la profilazione è consentita solo se è su base di legittimo interesse.

- Il direct marketing è generalmente subordinato al consenso dell'interessato quando è effettuato con sistemi automatizzati di chiamata o nell'ambito di comunicazioni elettroniche
- Il consenso non è richiesto quando si utilizza l'indirizzo di posta elettronica, in precedenza fornito dall'interessato nel contesto della vendita di un prodotto o di un servizio, per finalità di vendita diretta di propri prodotti o servizi

Analisi del Sito Web Aziendale

Ha tutta una serie di problematiche, devo raccogliere il consenso, devo gestire i cookie ecc. In realtà questo è l'aspetto più informatico sulla data privacy e quindi io devo valutare un sito per capire se ci sono i cookie e soprattutto come si gestiscono i cookie. Esistono diversi tipi di cookie con differenti funzioni e regole, a seconda che interferiscano o meno con i diritti e le libertà degli utenti. I cookie tecnici sono utilizzati al solo fine di effettuare la trasmissione di una comunicazione su una rete di comunicazione elettronica.

I cookie tecnici possono essere ulteriormente distinti in:

- Cookie funzionali o tecnici sono quelli che consentono al sito di memorizzare informazioni della navigazione effettuata dallo stesso, al fine di essere riutilizzate nelle navigazioni successive, migliorando il servizio e la qualità della navigazione (non è richiesto il consenso).
- Cookie analitici sono utilizzati per raccogliere informazioni, in forma aggregata, al fine di condurre analisi statistiche delle modalità di navigazione del sito.
- Cookie di profilazione sono utilizzati per tracciare le abitudini di navigazione degli utenti con lo scopo di creare profili dei loro gusti e delle loro abitudini, e somministrare contenuti e/o messaggi pubblicitari mirati

Ogni tipologia di cookie ha una diversa base giuridica, in alcuni bisogna chiedere il consenso, in altri non è necessario.

Data Breach

La violazione dei dati personali (**Data Breach**) comporta accidentalmente o in modo illecito la distruzione, la perdita anche temporanea (**disponibilità** delle informazioni), la modifica (**integrità** delle informazioni), la divulgazione non autorizzata o l'accesso (**riservatezza** delle informazioni) di dati personali trasmessi, conservati o comunque trattati. La violazione di integrità e quella di riservatezza sono facilmente identificabili, quella di disponibilità meno.

Non sono obbligato a notificare al garante tutte le violazioni, devo notificare solo le più critiche entro 72 ore dalla violazione altrimenti possono esserci conseguenze importanti. Infatti il garante può commutare delle pene pecuniarie.

Il garante può effettuare verifiche periodiche per mezzo della guardia di finanza. La notifica avviene tramite pec compilando un modulo scaricabile. Il garante richiede che le aziende abbiano un registro delle attività di trattamento; questo registro ha anche un template, il registro è un obbligo di legge previsto dall'articolo 33 del GDPR. Un utente se si accorge di una violazione può fare una notifica al garante tramite una modulistica di reclamo.

Esiste un formulario elaborato dall'ENISA che determina la gravità del data breach considerando tre fattori:

- contesto del trattamento - DPC (natura e volume dei dati violati, campo di attività del titolare, particolari categorie di interessati);
- facilità di identificazione - EI della persona a cui si riferiscono i dati violati (trascurabile, limitata, significativa, massima);
- circostanze della violazione - CB (perdita di riservatezza, integrità, disponibilità, dovuta a un evento accidentale oppure ad un'azione intenzionale).

A questi fattori viene attribuito un valore e il grado di rischio è determinato dalla formula $DPC \times EI + CB$ (rappresentata come bassa, media, alta, molto alta). A determinate soglie scatta la notifica e/o la comunicazione agli interessati. Quando si effettua un controllo da parte della guardia di finanza, la prima cosa richiesta è il registro. Oltre ad essere responsabile del registro, il responsabile del data protection si occupa anche di redigere il piano di protezione dei dati ovvero redigere un piano su quelle che sono le politiche, le tecnologie e le procedure per mettere in piedi la protezione dei dati nell'ottica GDPR.

Il piano può essere redatto all'inizio ma anche revisionato a valle di determinati eventi di violazione, pertanto devono essere garantite per i dati:

- «liceità, correttezza e trasparenza»
- «limitazione della finalità»
- «minimizzazione dei dati»
- «esattezza»
- «limitazione della conservazione»

- «integrità e riservatezza»

Il GDPR parla di misure di sicurezza, ovvero di cosa fare nello specifico per la sicurezza. Tra le misure abbiamo:

- la pseudo-anonimizzazione
- la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico (disaster recovery);
- una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento (auditing, accountability e DPIA continuativa).

La pseudo-anonimizzazione è intesa come un particolare trattamento dei dati personali realizzato in modo tale che i dati stessi non potranno più essere attribuiti direttamente ed automaticamente ad un interessato specifico. Infatti, tali dati potranno essere ricondotti all'interessato cui si riferiscono solo attraverso l'impiego di altre informazioni aggiuntive, che dovranno essere, a tal fine, conservate separatamente e con l'impiego di precauzioni tecniche e organizzative adeguate. In generale le misure di sicurezza possono essere delle misure tecniche/tecnologiche (cybersecurity, autenticazione, autorizzazione ecc.)

Codici di Condotta

I codici di condotta sono regole di condotta o pratiche uniformi elaborate da vari organismi internazionali o anche da singoli Stati, particolarmente diffuse nei rapporti economici internazionali. In genere contengono disposizioni non vincolanti anche se l'autorevolezza dell'organismo da cui promanano fanno sì che siano di larga e diffusa applicazione (art. 40 del GDPR).

Lo stesso Codice in materia di protezione personale presenta come allegati diversi codici di deontologia e buona condotta quali:

- Codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e scientifici.
- Codice di deontologia e di buona condotta per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti.
- Codice di deontologia e di buona condotta per i trattamenti di dati personali effettuati per svolgere investigazioni difensive.
- Codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato a fini di informazione commerciale.

Consenso

Il consenso è la base giuridica che arriva dalla direttiva 95, riutilizzata nella direttiva 58 e riportato nel GDPR. Nel GDPR il consenso è una delle 6 basi giuridiche consentite per definire la liceità del trattamento.

Quando richiede il consenso, il titolare del trattamento deve valutare se questo soddisferà tutti i requisiti per essere valido.

- Se ottenuto nel pieno rispetto del regolamento, il consenso è uno strumento che fornisce all'interessato il controllo sul trattamento dei dati personali che lo riguardano.
- In caso contrario, il controllo diventa illusorio e il consenso non costituirà una base valida per il trattamento, rendendo illecita l'attività di trattamento.

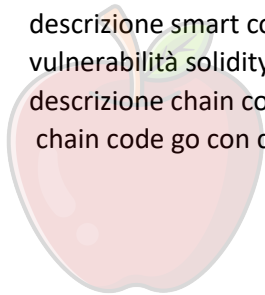
Se il titolare decide di basare il trattamento sul consenso deve assicurarsi che esso presenti le seguenti caratteristiche:

- **Consenso inequivocabile:** può essere sia esplicito che implicito ma deve essere chiaro, preciso e con finalità definite
- **consenso libero:** l'interessato deve essere in grado di operare una scelta effettiva, senza subire intimidazioni o raggiri, né deve subire conseguenze negative a seguito del mancato conferimento del consenso
- **specifico:** relativo alla finalità per la quale è eseguito quel trattamento (granularità del consenso). Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per ogni finalità.
- **informato:** l'interessato sappia quali dati sono trattati, con che modalità e finalità e i diritti che gli sono attribuiti dalla legge. Inoltre, deve essere opportunamente informato sulle conseguenze del suo consenso.
- **verificabile:** l'azienda deve essere in grado di dimostrare che l'interessato lo ha conferito con riferimento a quello specifico trattamento.
- **revocabile:** La revoca deve essere facile così come lo è dare il consenso.

L'ID cookie è di per sé considerato un dato personale ai sensi del GDPR, perché possono essere utilizzati per generare profili dettagliati sui singoli individui, i quali vengono poi venduti alle agenzie di pubblicità online e impiegati per il marketing comportamentale.

5 Esercizi:

- script bitcoin
- descrizione smart contract solidity (possibilità di smart contract con open zeppelin)
- vulnerabilità solidity
- descrizione chain code go
- chain code go con concorrenza, chanel (descrizione)



CosScienze
Associazione