



Lezione 8 – Quadro Normativo ed Etico

Prof. Esposito Christian

Corso di Sicurezza dei Dati



... Sommario

- Norme e Formati della Firma Digitale
- Posta Elettronica Certificata
- Norme sulla Protezione dei Dati e Quadro normative Europeo corrente e futuro
- DPIA e misure di sicurezza
- Standard di CyberSecurity



Norme e Formati della Firma Digitale

::: Introduzione Norme FD



Le modifiche al Codice dell' Amministrazione Digitale (CAD) apportate dal D.Lgs. 179/2016 hanno realizzato il coordinamento della normativa italiana con quella europea definita del Regolamento UE910/2014 eIDAS (electronic IDentification Authentication and Signature).

La definizione di documento informatico è presente all'art. 1 lett. p) del CAD: "il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti".

Il quadro normativo nazionale ed internazionale definisce cosa sia una firma elettronica/digitale e quali caratteristiche debbano avere.

::: Introduzione Norme FD

I vari tipi di firme elettroniche all' art. 1 del Regolamento eIDAS 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.

::: Introduzione Norme FD

I vari tipi di firme elettroniche all' art. 1 del Regolamento eIDAS 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 - “dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare”.

Un tipico esempio di firma semplice è il tratto del dito o di un pennino su un device elettronico, molto usato nel campo delle consegne a domicilio o nei processi interni alle aziende, l'apposizione su un documento informatico della scansione della firma cartacea, il PIN del Bancomat e la combinazione username e password della propria casella di posta elettronica.

::: Introduzione Norme FD

I vari tipi di firme elettroniche all' art. 1 del Regolamento eIDAS 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 avanzata FEA - “una firma elettronica che soddisfi i requisiti di cui all’articolo 26”:
 - è connessa unicamente al firmatario e idonea a identificarlo;
 - è creata mediante dati che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo;
 - è collegata ai dati per identificare ogni successiva modifica.

Può essere quindi utilizzata nella firma di contratti di cui al comma 13) dell’articolo 1350 del c.c., mentre non ha validità nella firma di contratti con maggiori tutele (come le vendite immobiliari o dei diritti immobiliari, di cui al comma 1-12 dello stesso articolo 1350 del c.c.).

::: Introduzione Norme FD

I vari tipi di firme elettroniche all' art. 1 del Regolamento eIDAS 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 avanzata FEA - “una firma elettronica che soddisfi i requisiti di cui all’articolo 26”:



La Firma Grafometrica si ottiene rilevando i dati biometrici di un utente (firmatario) nel momento in cui appone la sua firma su un tablet legando gli stessi in maniera indissolubile al documento elettronico firmato.

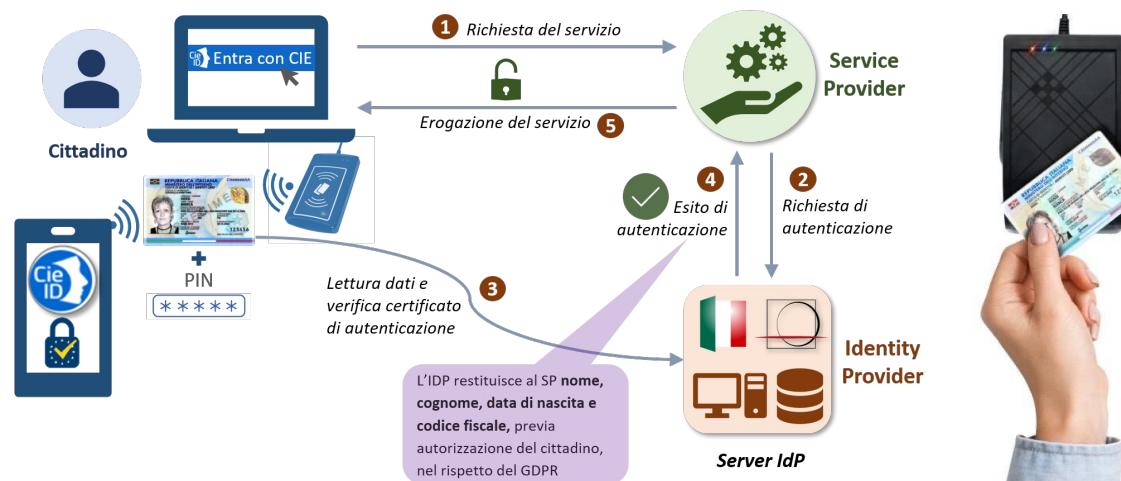
Per firmare, è sufficiente inserire il codice OTP ricevuto via sms, sfruttando così il dispositivo mobile dell’utente per fornire un’autenticazione.



::: Introduzione Norme FD

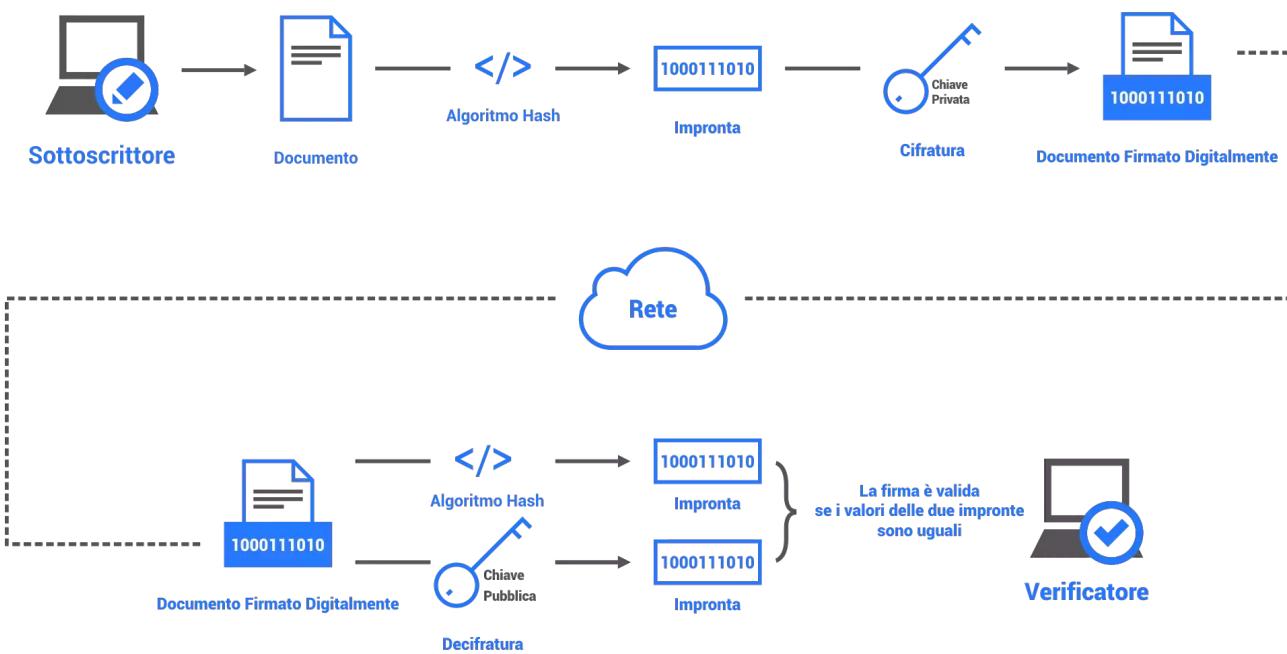
- Firma elettronica qualificata FEQ - art. 1 Regolamento eIDAS “una firma elettronica avanzata creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche”

Questa firma consente di scambiare in rete documenti con piena validità legale. Un esempio di Firma Elettronica Qualificata è una card con chip che contiene alcuni dati anagrafici e il codice fiscale, come la Tessera Sanitaria o la CIE.



::: Introduzione Norme FD

- Firma digitale FD - art. 1, lett. S del CAD: “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”.



::: Introduzione Norme FD

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 <i>ad substantiam</i> 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 <i>ad substantiam</i>	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 <i>ad substantiam</i>	Non neutra, certificato qualificato chiavi asimmetriche e dispositivo sicuro	Smart-card, token USB, MicroSD, Firma remota

::: Introduzione Norme FD

L'efficacia giuridica delle firme elettroniche è pertanto diversa per ognuna di esse partendo dal principio definito di "non discriminazione" sancito dall'art. 25 del Regolamento eIDAS che ne attribuisce valore giuridico:

- Una FEQ ha effetti giuridici equivalenti a quelli di una firma autografa. Una FEQ basata su un certificato qualificato rilasciato in uno Stato membro è riconosciuta quale firma elettronica qualificata in tutti gli altri Stati membri.

L'attuale art. 20 del CAD 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".

::: Introduzione Norme FD

In caso di contenzioso il giudice dovrà valutare, ex art. 116 del c.p.c., 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.

Ai documenti sottoscritti con firma elettronica qualificata o digitale, formati nel rispetto di quanto indicato dal D.P.C.M. 22 febbraio 2013, ai sensi dell'art. 20 del CAD è riconosciuta l'efficacia prevista dall'art. 2702 del c.c. e l'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che questi dia prova contraria.

- Non è il soggetto che produce il documento in giudizio a dover dimostrare che la sottoscrizione non è autentica, ma è il titolare della firma digitale a dover dimostrare l'esistenza di un abuso nell'uso del dispositivo.
- Tra gli obblighi a carico del titolare del certificato di firma vi è anche quello di assicurare la custodia del dispositivo di firma e di utilizzarne personalmente il dispositivo di firma (art. 32 del CAD).

::: Introduzione Norme FD

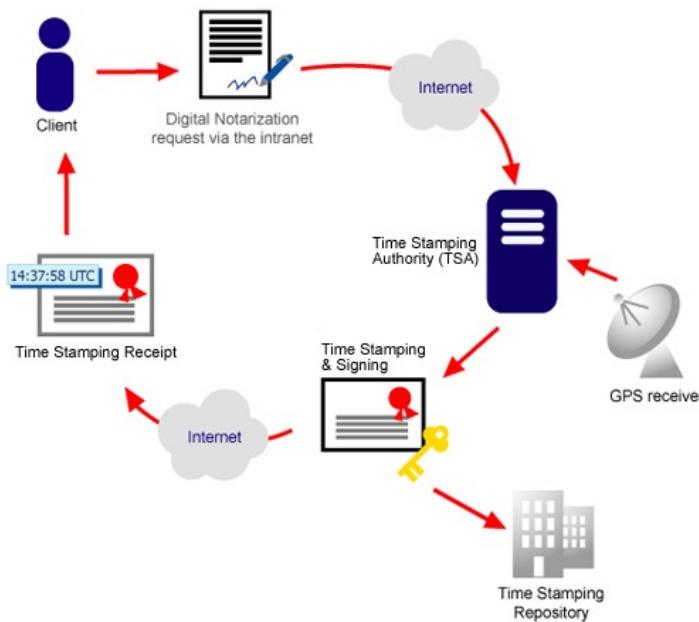
Le sospensioni e le revoche dei certificati qualificati sono giornalmente registrate dai prestatori di servizi fiduciari sulle CRL (Certificate Revocation List) che vengono consultate dai software in sede di verifica della firma digitale proprio con lo scopo di verificare se il certificato è valido o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

- L'art. 36 del CAD, al comma 3, infatti prevede che la revoca o la sospensione del certificato qualificato, qualunque ne sia la causa, ha effetto dal momento della pubblicazione nella lista che lo contiene.

Il momento della pubblicazione deve inoltre essere attestato mediante adeguato riferimento temporale. Pertanto, ai sensi dell'art. 24 del CAD comma 4-bis, 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.

::: Introduzione Norme FD

L'importanza della validazione temporale come strumento per controllare l'efficacia giuridica di una firma elettronica qualificata o digitale è confermata anche dall'art. 3, comma 7, del D.P.C.M. 13 novembre 2014 che ha introdotto 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.

::: Introduzione Norme FD

L'importanza della validazione temporale come strumento per controllare l'efficacia giuridica di una firma elettronica qualificata o digitale è confermata anche dall'art. 3, comma 7, del D.P.C.M. 13 novembre 2014 che ha introdotto 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.

Per attribuire valore giuridico ad un documento informatico sottoscritto con firma elettronica occorre archiviare e conservare insieme ai bit che rappresentano il documento anche le informazioni che caratterizzano il processo di firma in termini di qualità, sicurezza, integrità e immodificabilità.

::: Introduzione Norme FD

Per quanto riguarda la scelta del formato della busta crittografica occorre attenersi alle indicazioni dell'allegato 2 del D.P.C.M. 3 dicembre 2013 sulla conservazione e del D.P.C.M. 13 novembre 2014 in base al quale vanno privilegiati i formati con le seguenti caratteristiche:

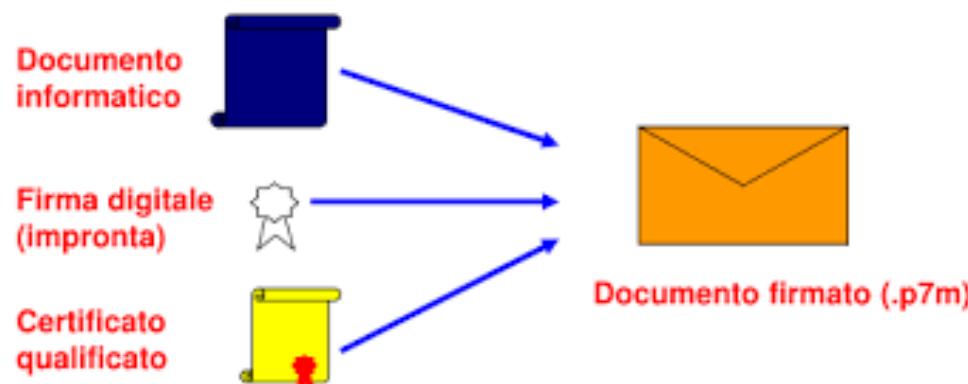
- “aperti” cioè conformi a specifiche pubbliche disponibili a chiunque;
- “non proprietari” cioè formati che sono indipendenti dalle piattaforme tecnologiche utilizzate per la formazione dei documenti;
- “robusti” in grado di recuperare in tutto o in parte il contenuto del file eventualmente corrotto 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.



::: Formati

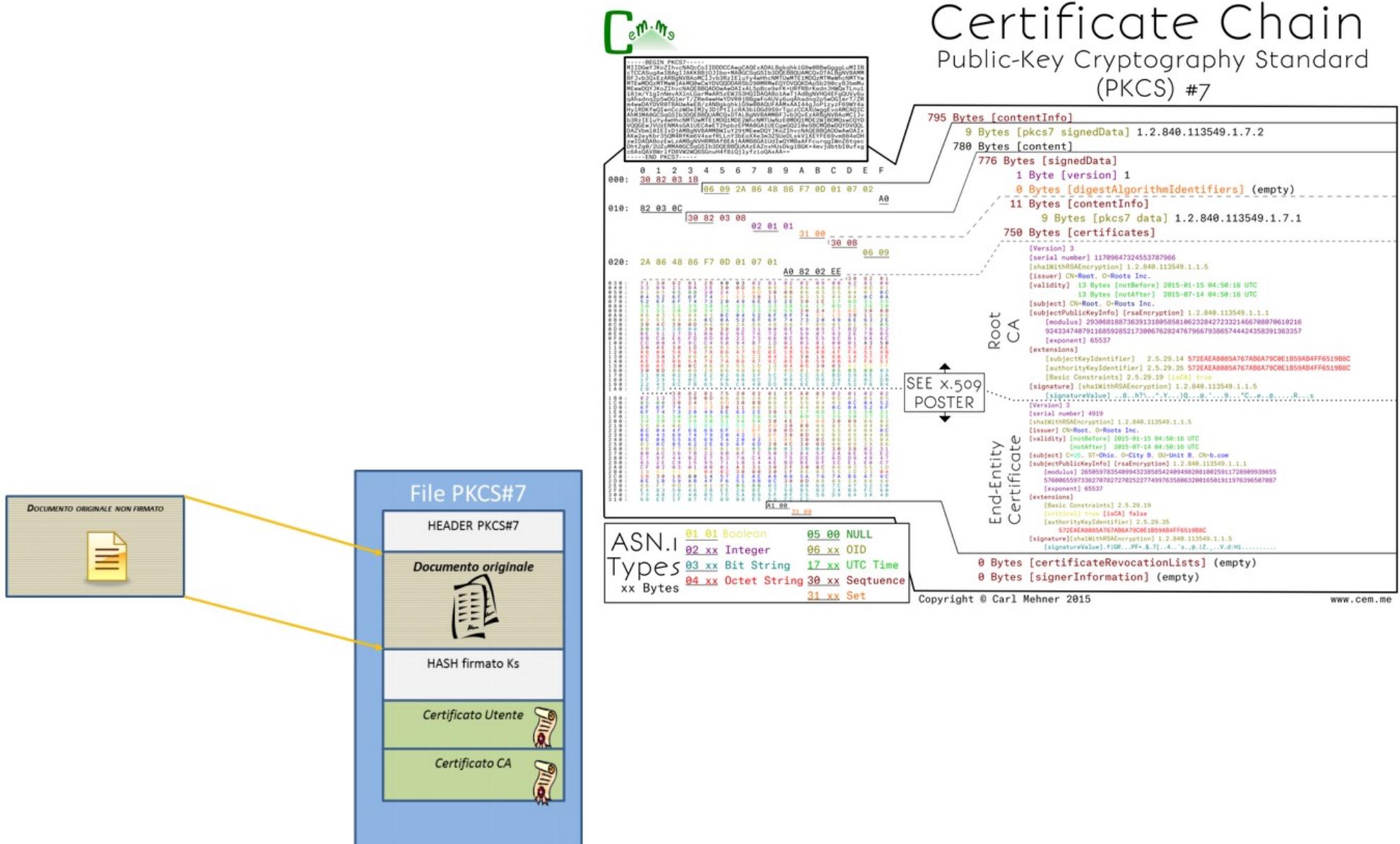
I formati da privilegiare per la conservazione a lungo termine sono i seguenti in relazione alla diversa tipologia documentale:

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

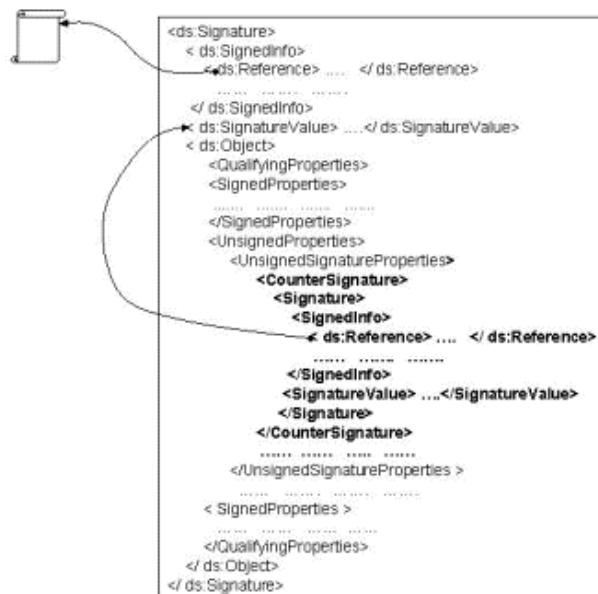
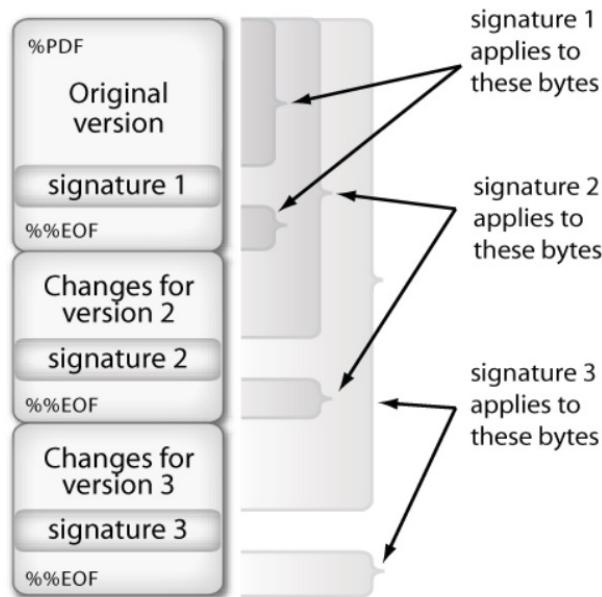
Con l'apposizione di una firma digitale si crea la "busta crittografica" che è un file che racchiude il documento originale, la firma digitale e la chiave di verifica che è contenuta nel certificato del sottoscrittore.

- 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.

... Formati



::: Formati



- 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

Una delle novità della direttiva europea eIDAS e il relativo adeguamento del CAD e delle norme è il sigillo elettronico definito dall'art.3 n. 25 come l'insieme di «dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati in forma elettronica per garantire l'origine e l'integrità di questi ultimi».

Impropriamente un sigillo è visto come una particolare firma che garantisce integrità dei dati e correttezza dell'origine degli stessi, ma non anche quella di identificazione del soggetto che appone il sigillo. Mentre da una firma si può individuare con certezza un soggetto, da un sigillo si può risalire con certezza ad una persona giuridica attraverso la sua denominazione, partita IVA o codice fiscale, ma non alla persona fisica che ha materialmente utilizzato le credenziali per generare tale sigillo.

::: I Sigilli Elettronici

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 legare 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.

::: I Sigilli Elettronici

- 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 di una società.

- L'apposizione di sigilli “sequenziali” può consentire di tracciare le successive modifiche nell'ambito di un ciclo di vita documentale.
- Nella fatturazione elettronica si controlla se il sigillo è già applicato alle ricevute di accettazione.
- Il sigillo può essere utilizzato al posto della firma nei procedimenti di formazione del contrassegno elettronico per le procedure di produzione di copie conformi.
- Il sigillo elettronico qualificato può sostituire la firma in alcune passaggi della conservazione digitale



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.

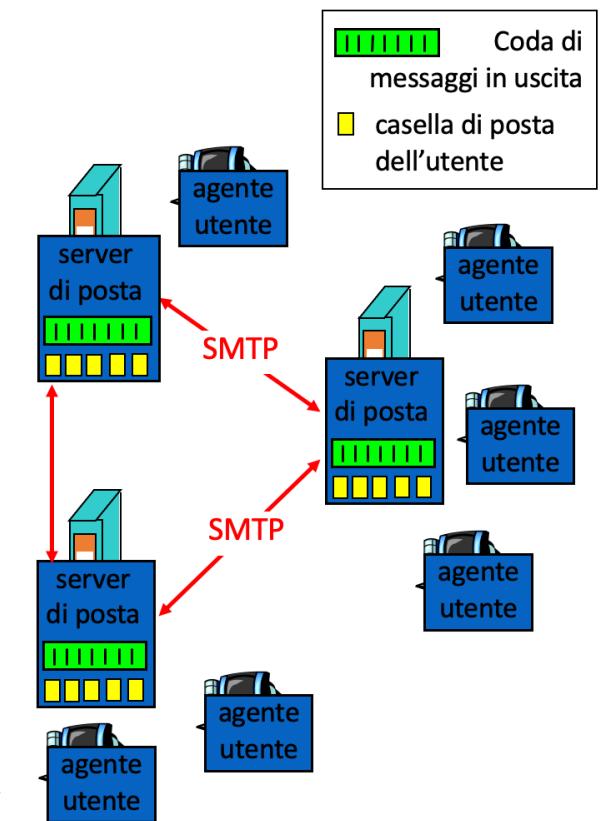
::: La Posta Elettronica

L'implementazione su Internet del servizio di posta elettronica si compone di tre elementi principali:

- Agente utente;
- Server di posta;
- Simple Mail Transfer Protocol (SMTP) [RFC 778].

L'Agente utente, detto anche “mail reader”, rappresenta i programmi per leggere e gestire la posta e le mailboxes, come Eudora, Outlook, ELM, Netscape Messenger.

Possono utilizzare protocolli per la gestione di mailboxes remote (Pop3, IMAP), e i messaggi in uscita o in arrivo sono memorizzati sul server.

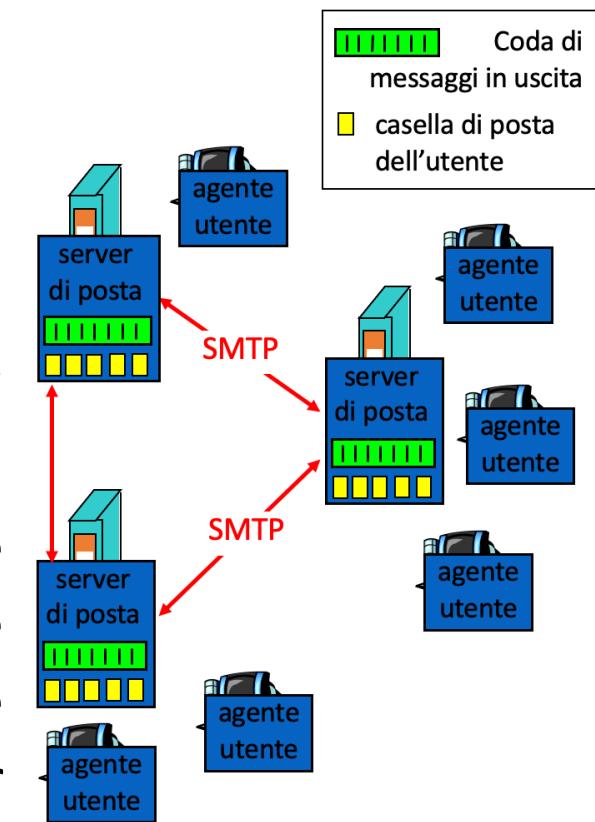


::: La Posta Elettronica

Il server di posta include:

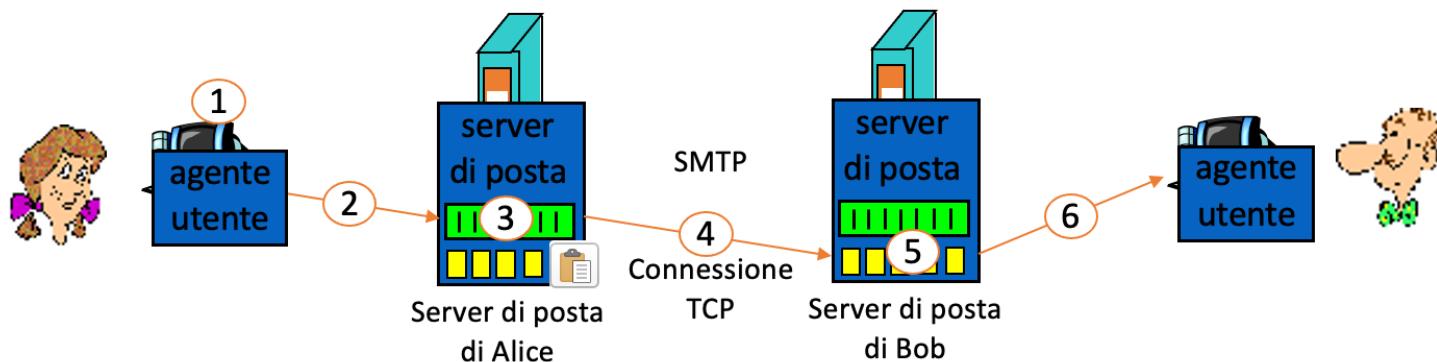
- Casella di posta (mailbox) che contiene i messaggi in arrivo per l'utente;
- Coda di messaggi da trasmettere

Usa il protocollo client-server SMTP tra server di posta per inviare messaggi di posta elettronica, dove il “client” è il server di posta trasmittente mentre il “server” è server di posta ricevente. Tale protocollo usa TCP per trasferire in modo affidabile i messaggi di posta elettronica dal client al server (porta 25).



::: La Posta Elettronica

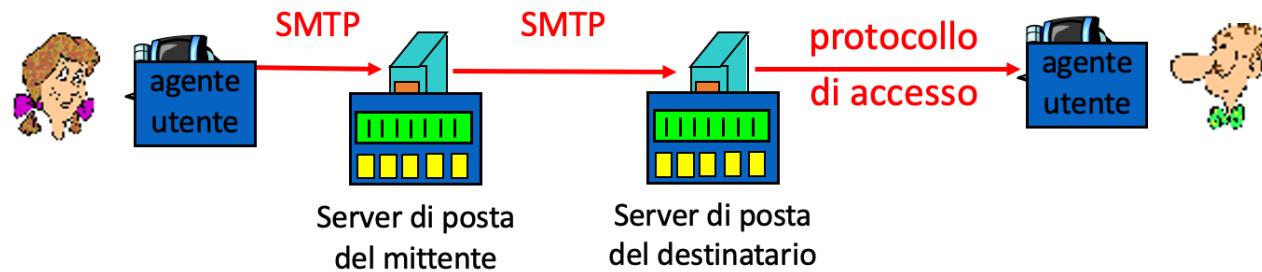
- 1) Alice usa il suo agente utente per comporre il messaggio da inviare a bob@omeschool.edu
- 2) L'agente utente di Alice invia un messaggio nella casella di posta di messaggio al server di posta di Alice, Bob che lo pone nella coda di messaggi
- 3) Il lato client di SMTP apre una connessione TCP con il server di posta di Bob
- 4) Il client SMTP invia il messaggio
- 5) Il server di posta di Bob pone il messaggio nella coda di messaggi
- 6) Bob invoca il suo agente utente



::: La Posta Elettronica

Protocollo di accesso alla posta per ottenere i messaggi dal server

- POP: Post Office Protocol [RFC 1939]
- IMAP: Internet Mail Access Protocol [RFC 1730]



Quando si utilizza il POP3, il client si connette per scaricare i nuovi messaggi e poi si disconnette. Con l'IMAP il client rimane connesso e risponde alle richieste che l'utente fa attraverso l'interfaccia; questo permette di risparmiare tempo se ci sono messaggi di grandi dimensioni. POP3 salva in locale i messaggi, IMAP li lascia sul server e li memorizza temporaneamente nella cache.

::: La Posta Elettronica

Il Multipurpose Internet Mail Extensions (MIME; letteralmente "estensioni multifunzione alla posta di Internet") è uno standard di Internet che estende la definizione del formato dei messaggi di posta elettronica, originariamente definito dall'SMTP, il protocollo di trasmissione delle email. MIME aggiunge il supporto per

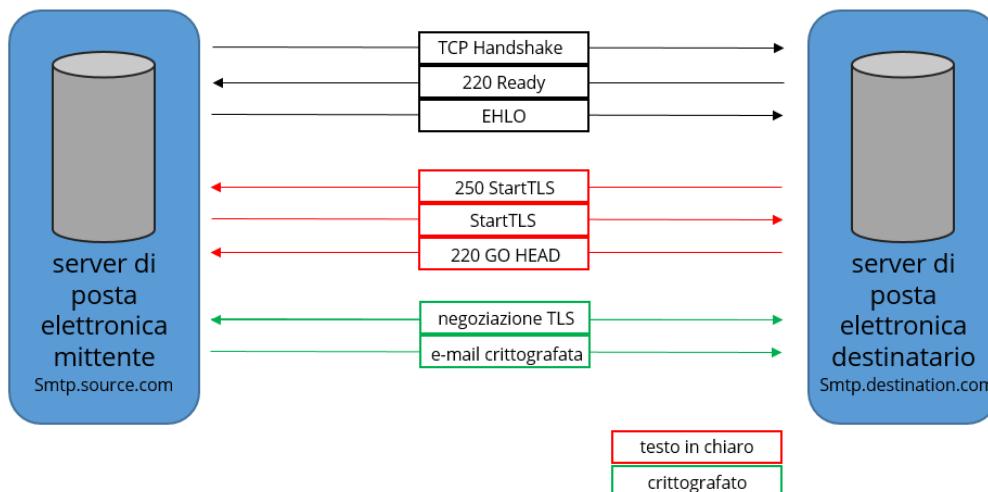
- l'impiego di codifiche di caratteri diversi dall'ASCII,
- l'aggregazione di diversi messaggi tra loro,
- la codifica di messaggi (o loro parti) non testuali.

Queste novità rispetto ad SMTP consentono caratteristiche oggi comuni nell'uso della posta elettronica, come il concetto di allegato, l'invio di file non testuali, la lunghezza arbitraria delle linee di testo e del messaggio stesso, o ancora la firma digitale e la cifratura dei messaggi.

::: La Posta Elettronica - Sicurezza

La posta elettronica è intrinsecamente un metodo di comunicazione insicuro, infatti tutte le interazioni avvengono tramite SMTP, che non utilizza la crittografia o l'autenticazione, rendendo le accessibili da estranei.

- SMTPS (Simple Mail Transfer Protocol Secure) è un metodo per proteggere l'SMTP utilizzando la sicurezza del livello di trasporto come SSL/TLS. Ha lo scopo di fornire l'autenticazione dei partner di comunicazione, nonché l'integrità e la riservatezza dei dati.

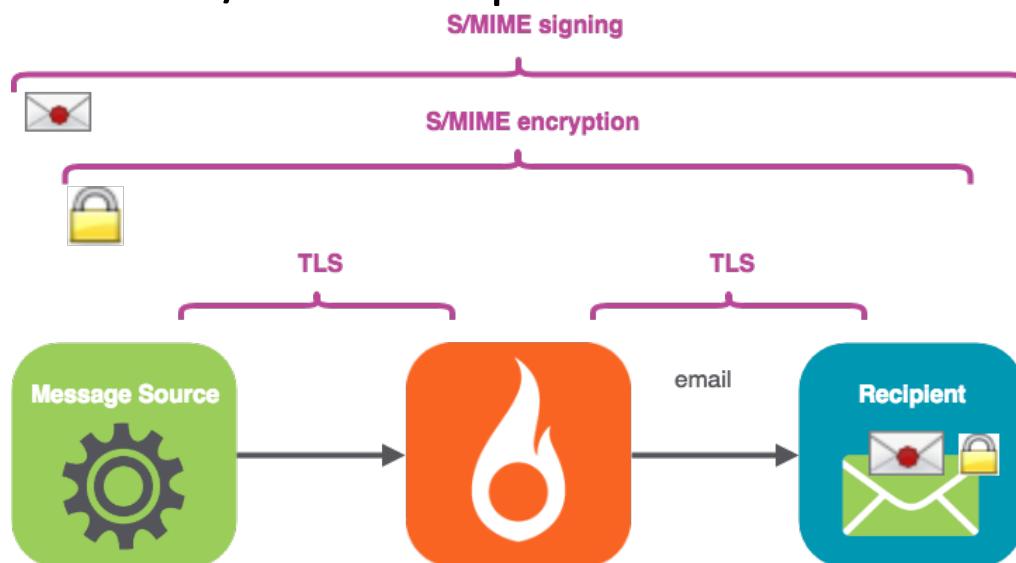


- Con SMTPS viene creato un canale di comunicazione criptato attraverso lo scambio di certificati in modo da garantire l'identità delle parti e la riservatezza dei dati.

::: La Posta Elettronica - Sicurezza

La posta elettronica è intrinsecamente un metodo di comunicazione insicuro, infatti tutte le interazioni avvengono tramite SMTP, che non utilizza la crittografia o l'autenticazione, rendendo le accessibili da estranei.

- S/MIME è uno standard per la crittografia a chiave pubblica e la firma digitale di messaggi di posta elettronica in formato MIME.
- SMTPS realizza la sicurezza a livello di trasporto; al contrario, S/MIME implementa la sicurezza a livello di messaggio.



- Ogni messaggio S/MIME è preceduto da un'intestazione che fornisce al client destinatario le informazioni necessarie per la comprensione e l'elaborazione del contenuto.

::: La Posta Elettronica - Sicurezza

La posta elettronica è intrinsecamente un metodo di comunicazione insicuro, infatti tutte le interazioni avvengono tramite SMTP, che non utilizza la crittografia o l'autenticazione, rendendo le accessibili da estranei.

- SMTPS (Simple Mail Transfer Protocol Secure) è un metodo per proteggere l'SMTP utilizzando la sicurezza del livello di trasporto come SSL/TLS. Ha lo scopo di fornire l'autenticazione dei partner di comunicazione, nonché l'integrità e la riservatezza dei dati.
- S/MIME è uno standard per la crittografia a chiave pubblica e la firma digitale di messaggi di posta elettronica in formato MIME.

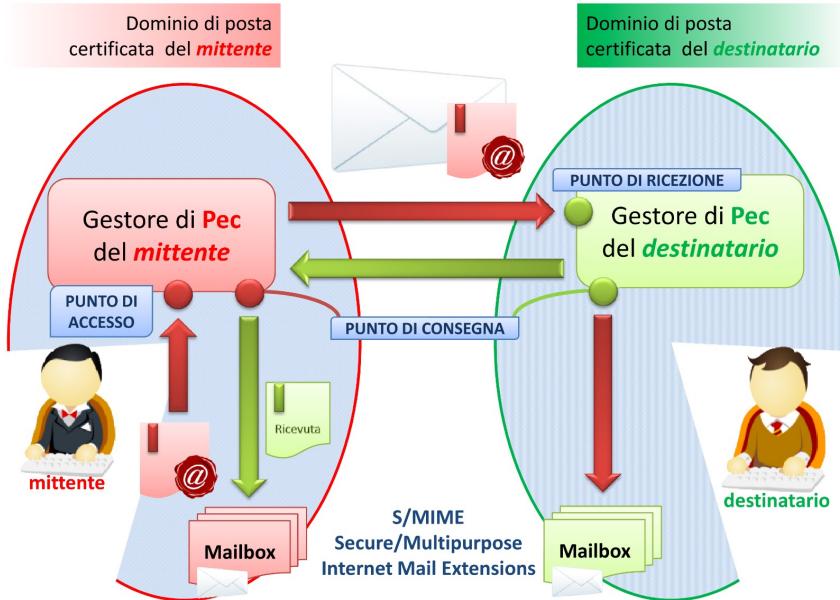
Manca una soluzione per documentare la presa in carico e consegna delle e-mail, così da certificare a livello legale l'avvenuta trasmissione.

::: 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. Rappresenta un'evoluzione in termini di garanzie per la classica posta elettronica che di per sé non ha assolutamente nessun valore legale.

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 gestiscano la posta elettronica “classica”, e la PEC; infatti se ciò accadesse risulterebbe più facile un'eventuale compromissione del servizio PEC.

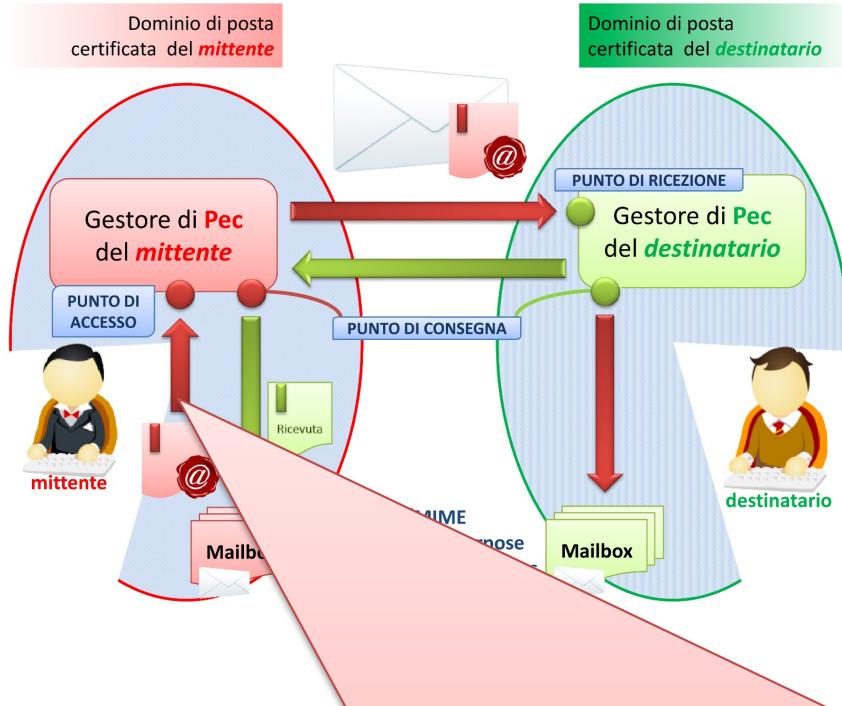
::: Posta Elettronica Certificata



I messaggi di posta certificata vengono spediti tra 2 caselle, e quindi Domini, certificati. Alla trasmissione di un messaggio PEC partecipano diverse entità come in figura.

Quando il mittente possessore di una casella di PEC invia un messaggio ad un altro utente certificato, accede per prima cosa attraverso la verifica delle credenziali di accesso al server di Posta Elettronica Certificata del suo gestore.

::: Posta Elettronica Certificata

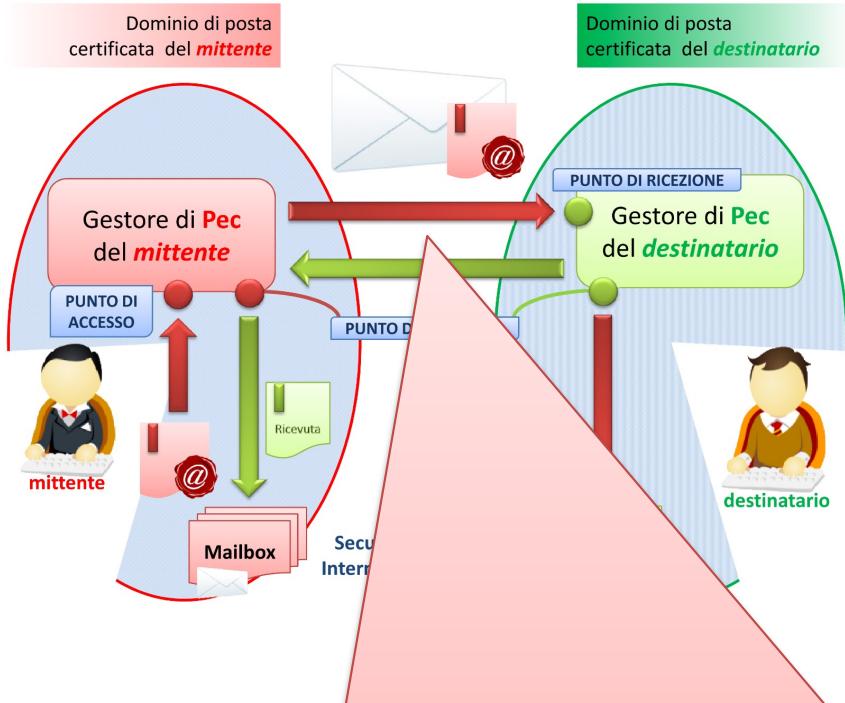


I messaggi di posta certificata vengono spediti tra 2 caselle, e quindi Domini, certificati. Alla trasmissione di un messaggio PEC partecipano diverse entità come in figura.

Quando il mittente possessore di una casella di PEC invia un messaggio ad un altro utente certificato, accede per

Il mittente predisponde il messaggio PEC e lo sottopone al gestore mittente, che ne verifica la correttezza formale del messaggio PEC e, in caso positivo, restituisce al mittente la ricevuta di accettazione come riconoscimento dell'avvenuto invio del messaggio. La ricevuta è firmata digitalmente dal gestore e garantisce l'integrità.

::: Posta Elettronica Certificata

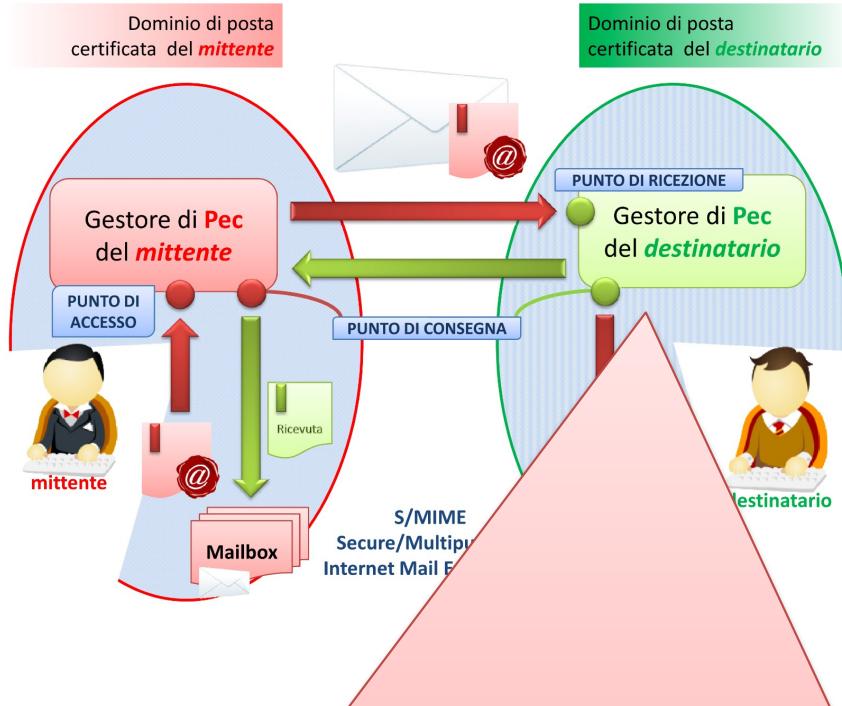


I messaggi di posta certificata vengono spediti tra 2 caselle, e quindi Domini, certificati. Alla trasmissione di un messaggio PEC partecipano diverse entità come in figura.

Quando il mittente possessore di una casella di PEC invia un messaggio ad un altro utente certificato, accede per

Il gestore mittente invia il messaggio al gestore destinatario inserendolo in una busta di trasporto che è il messaggio creato dal server SMTPS utilizzato dal mittente per l'invio, e contiene il messaggio originale inviato dall'utente e i dati di certificazione. La busta è firmata con la chiave del gestore di posta certificata mittente e viene recapitata nella casella di posta certificata del destinatario.

::: Posta Elettronica Certificata

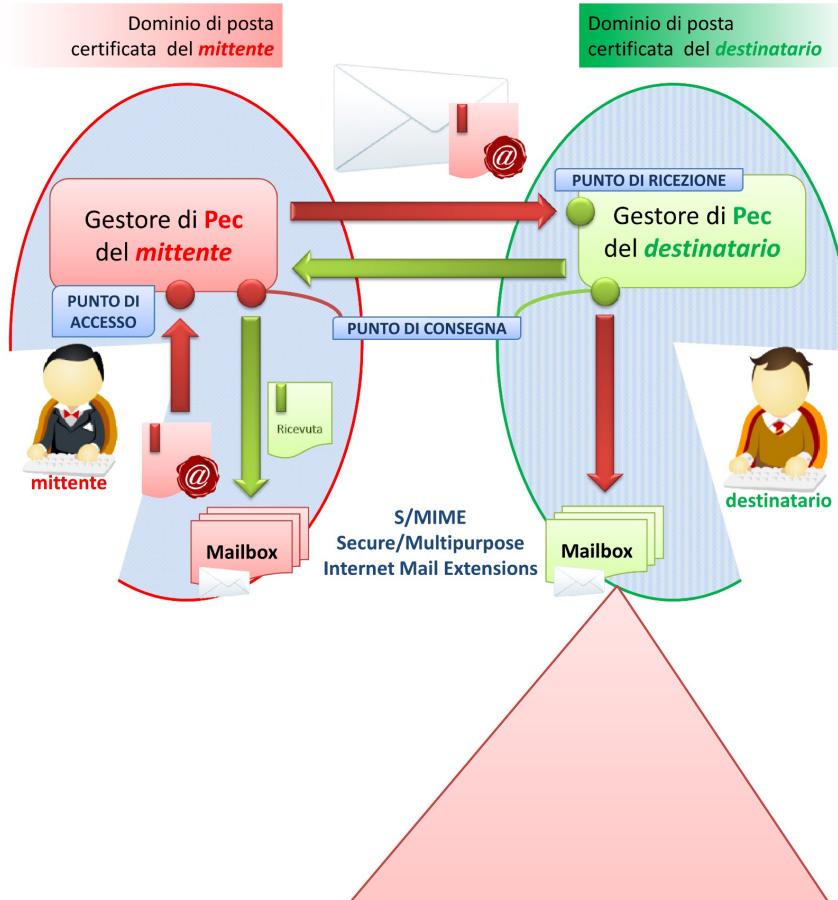


I messaggi di posta certificata vengono spediti tra 2 caselle, e quindi Domini, certificati. Alla trasmissione di un messaggio PEC partecipano diverse entità come in figura.

Quando il mittente possessore di una casella di PEC invia un messaggio ad un altro utente certificato, accede per

Il gestore destinatario, una volta ricevuto il messaggio PEC, consegnerà al gestore mittente una ricevuta di presa in carico che attesta il passaggio di consegne tra i due gestori. Il gestore destinatario verifica in fase di ricezione la correttezza del messaggio e si accerta che non siano presenti virus informatici.

::: Posta Elettronica Certificata

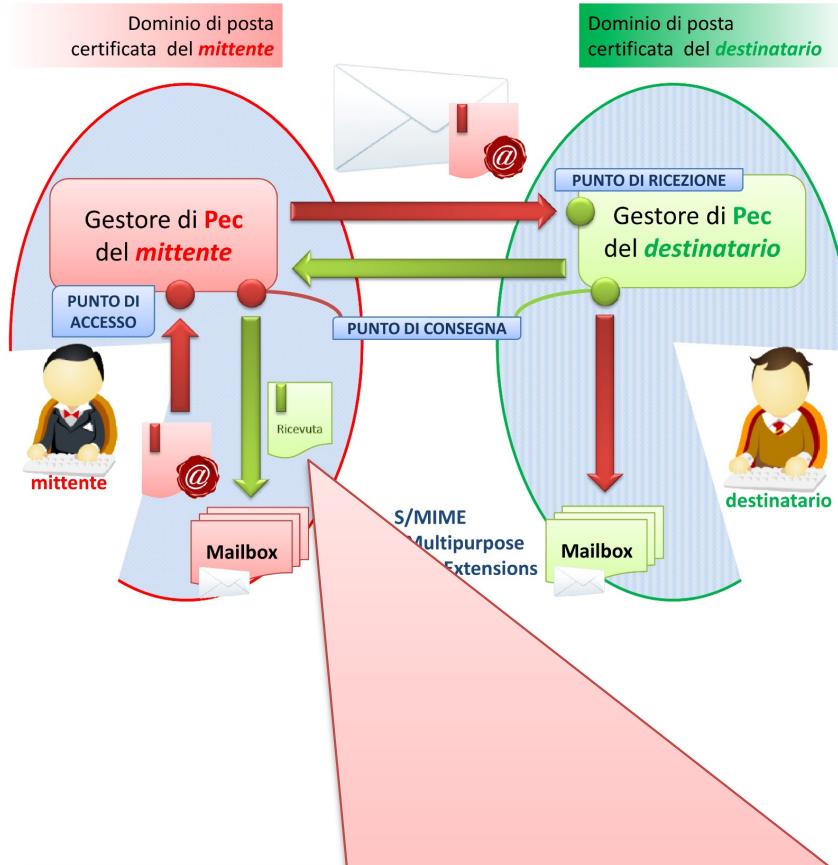


I messaggi di posta certificata vengono spediti tra 2 caselle, e quindi Domini, certificati. Alla trasmissione di un messaggio PEC partecipano diverse entità come in figura.

Quando il mittente possessore di una casella di PEC invia un messaggio ad un altro utente certificato, accede per prima cosa attraverso la verifica delle credenziali di accesso al server di Posta Elettronica Certificata del suo

Nel caso il messaggio superi i suddetti controlli, viene consegnato alla casella di posta del destinatario, che può accedervi e leggerne il contenuto.

::: Posta Elettronica Certificata



I messaggi di posta certificata vengono spediti tra 2 caselle, e quindi Domini, certificati. Alla trasmissione di un messaggio PEC partecipano diverse entità come in figura.

Quando il mittente possessore di una casella di PEC invia un messaggio ad un altro utente certificato, accede per prima cosa attraverso la verifica delle credenziali di accesso al server di

Al mittente perviene una ricevuta di avvenuta consegna, che attesta la disponibilità del messaggio presso il destinatario. La ricevuta è ancora una volta firmata digitalmente e attesta l'integrità del contenuto trasmesso.

::: Posta Elettronica Certificata

È importante sottolineare che la posta elettronica certificata offre la garanzia della consegna del messaggio e non della sua lettura da parte del destinatario. In altre parole, nulla è detto sul fatto che il destinatario abbia letto o meno il messaggio PEC, ma si hanno garanzie sull'avvenuto recapito. Il che, in termini legali, equivale alla raccomandata con ricevuta di ritorno, ma con in più la prova certa del contenuto.

Per la certificazione del messaggio vengono emesse in particolare tre tipi di ricevute in caso di esito positivo per la consegna del messaggio:

- Ricevuta di accettazione, che attesta l'avvenuto invio della mail dal gestore di posta elettronica certificata del mittente.
- Ricevuta di presa in carico, che attesta il passaggio di responsabilità tra due distinti gestori di posta certificata. Questa ricevuta viene scambiata tra i due gestori e non viene percepita dagli utilizzatori.

::: Posta Elettronica Certificata

- 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.

::: Posta Elettronica Certificata

In caso di errori esistono inoltre tre tipi di avvisi rilasciati dal sistema:

- Di non accettazione (per virus o utilizzo di un mittente falso o utilizzo di destinatari in copia nascosta, vietati dalla PEC, o altri problemi).
- Di mancata consegna, che sarà inviata al mittente entro 24 ore.
- Di rilevazione di virus informatici.

Nel caso in cui il messaggio sia inviato contemporaneamente a più destinatari di PEC, il mittente si vedrà recapitare una sola ricevuta di accettazione e tante ricevute di avvenuta consegna, o di non avvenuta consegna, una per ogni destinatario. Se, invece, il messaggio è stato inviato a uno o più destinatari di posta ordinaria (non certificata), oltre a non avere alcun valore legale, non verranno generate le ricevute di avvenuta consegna.

::: Quadro Normativo

Dall'articolo 15, comma 2, della legge 15 marzo 1997, n. 59 il quadro normativo relativo alla Posta Elettronica Certificata è costituito da:

- DPR 11 febbraio 2005, n. 68, “Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3.” (G.U. 28 aprile 2005, n. 97);
- Decreto Ministeriale 2 novembre 2005, “Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata” (G.U. del 14 novembre 2005, n. 265);
- Circolare CNIPA CR/49 24 novembre 2005, “Modalità per la presentazione delle domande di iscrizione all'elenco pubblico dei gestori di posta elettronica certificata” (G.U. 5 dicembre 2005, n. 283);
- Decreto Legislativo 7 marzo 2005, n. 82 (G.U. 16 maggio 2005, n. 93), anche detto “Codice dell'Amministrazione Digitale”.

::: Quadro Normativo

Il Decreto del Presidente della Repubblica del febbraio 2005 stabilisce:

- il documento informatico trasmesso per via telematica si intende spedito dal mittente se inviato al proprio gestore, e si intende consegnato al destinatario se reso disponibile all'indirizzo elettronico da questi dichiarato, nella casella di posta elettronica del destinatario messa a disposizione dal gestore.

Altri contenuti significativi del regolamento riguardano la definizione degli obblighi del gestore: garantire l'interoperabilità dei servizi offerti [art. 5, comma 2]; l'inalterabilità dei documenti trasmessi [art. 11, comma 1]; di tenere traccia delle operazioni svolte, in un apposito log, per una durata di trenta mesi garantendone la riservatezza, la sicurezza, l'integrità e l'inalterabilità [art. 11, comma 2 e 3]; individuare e gestire secondo le regole tecniche gli eventuali messaggi contenenti virus [art. 12]; garantire dei livelli minimi di servizio [art. 13].

::: Quadro Normativo

Il regolamento istituisce l'elenco pubblico dei gestori PEC [art. 14, comma 1], definendo i requisiti che il candidato gestore deve dimostrare di possedere per essere iscritto nello stesso [art 14, commi 2, 3, 4, 5 e 6].



Elenco Pubblico dei Gestori di Posta Elettronica Certificata (PEC) (D.P.R. 11 febbraio 2005, n. 68)

Le seguenti tabelle, che contengono l'elenco dei gestori di posta elettronica certificata (attivi e cessati) accreditati con apposito atto a firma del Direttore Generale dell'Agenzia, sono pubblicate ai sensi dell'art. 18, comma 4 del Decreto 2 novembre 2005 “Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata”.

Denominazione sociale:	Actalis S.p.A.
Sede legale:	Via S. Clemente, 53 – 24036 Ponte San Pietro (BG)
Rappresentante legale:	Cecconi Giorgio
Indirizzo Internet:	http://www.actalis.it/
Data di iscrizione all'elenco:	22/12/2005

Denominazione sociale:	ARUBA PEC S.p.A.
Sede legale:	Via San Clemente n. 53 – 24036 Ponte San Pietro (BG)
Rappresentante legale:	Cecconi Giorgio
Indirizzo Internet:	http://www.pec.it/
Data di iscrizione all'elenco:	12/10/2006

Come previsto dall'art.18 del D.M. 2 novembre 2005, l'AgID pubblica nella pagina https://www.agid.gov.it/sites/default/files/repository_files/elenco_pubblico_gestori_pec.pdf l'elenco dei gestori PEC in formato PDF Advanced Electronic Signature (PAdES).

::: Quadro Normativo

Il regolamento definisce che

- 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'avvento invio e ricezione di un documento informatico [art.48].

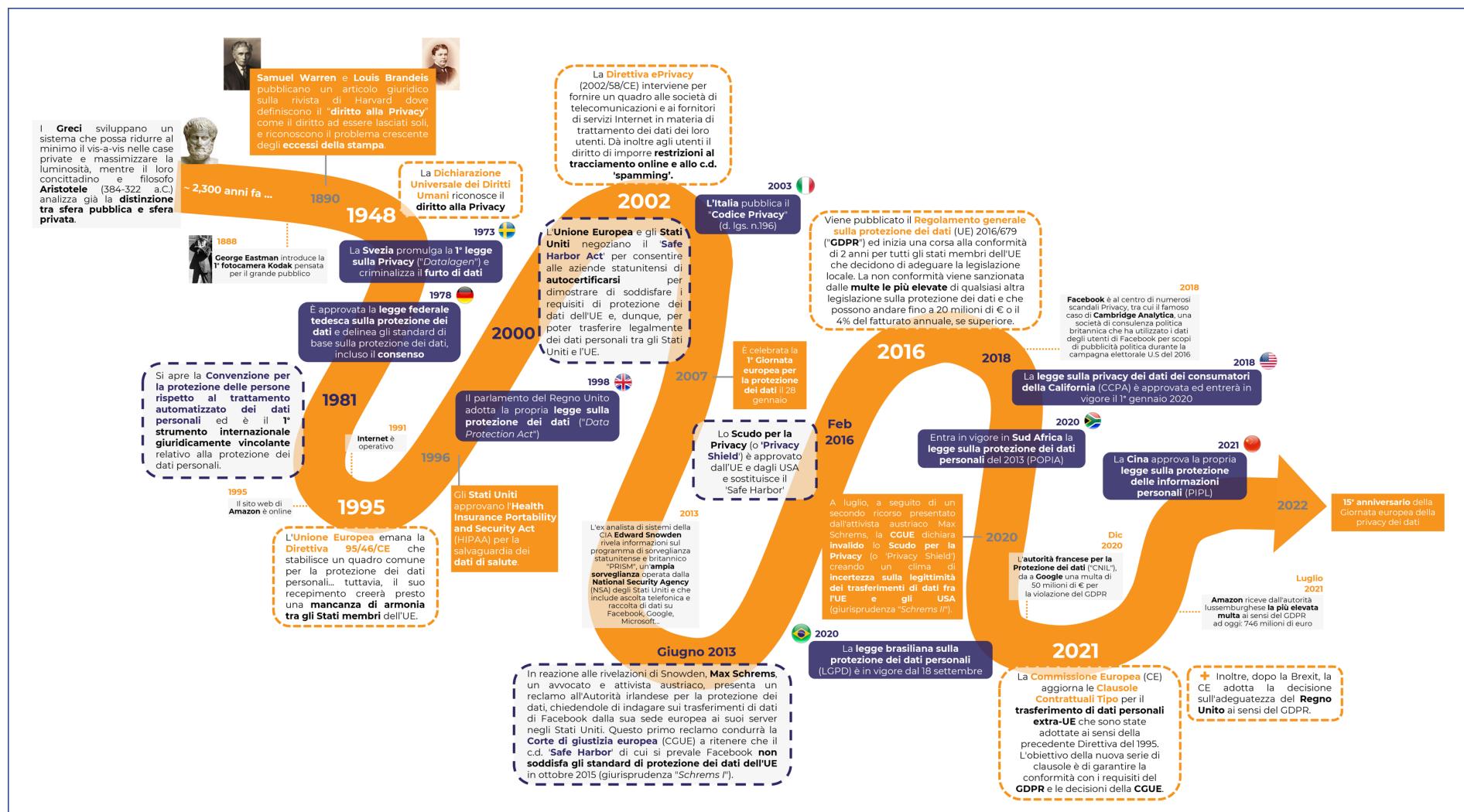
Il valore aggiunto della PEC rispetto ad altri canali di comunicazione		
	Valore aggiunto della PEC	
PEC	✓ certezza consegna ✓ valore legale ✓ certezza casella mittente	E-mail
PEC	✓ velocità e semplicità ✓ valore legale ✓ ubiquità	Fax
PEC	✓ certezza del contenuto ✓ velocità e semplicità ✓ tracciabilità mittente	Raccomandata A/R
PEC	✓ velocità e semplicità ✓ costi ✓ ubiquità	Consegna brevi manu

I possibili impieghi della PEC vanno oltre la sostituzione o integrazione della tradizionale raccomandata.



Norme Protezione dei Dati Personalni

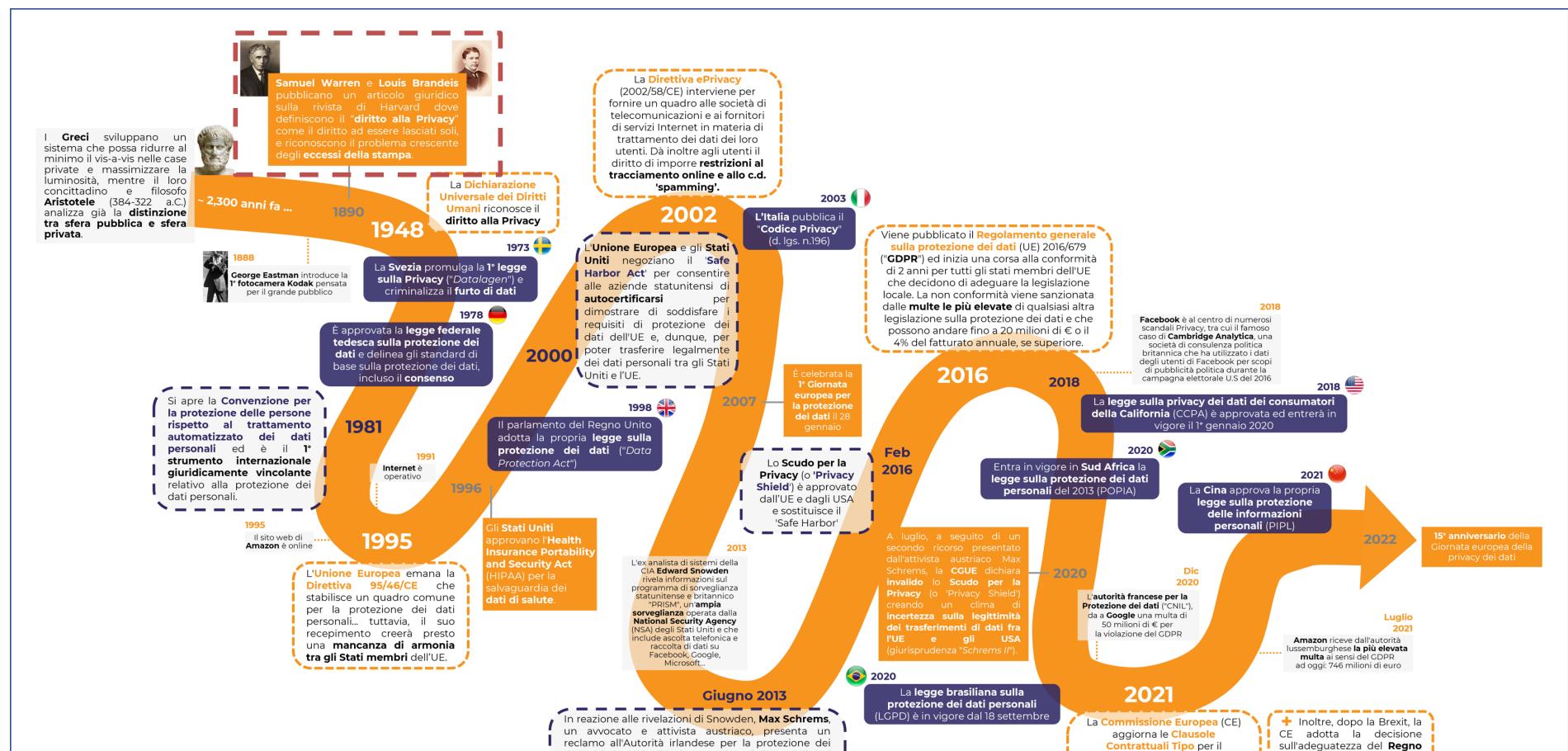
.... Quadro Normativo - Storia



.... Quadro Normativo - Storia

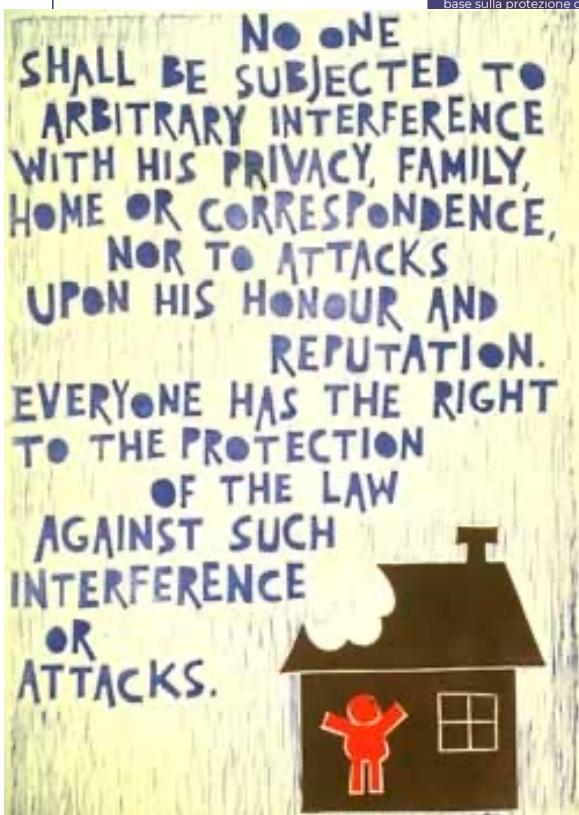


... Quadro Normativo - Storia



Nel 1890, due giuristi statunitensi, Louis Brandeis e Samuel Warren, pubblicarono “The Right of Privacy” sulla Harvard Law Review, prima monografia giuridica a riconoscere “the right to be let alone”, “diritto ad essere lasciato da solo”, esprimendo in queste parole il desiderio di una propria e inviolabile intimità, e riconoscono il problema crescente degli eccessi della stampa.

::: Quadro Normativo - Storia



L'articolo 12 riconosce il diritto alla riservatezza. E' un classico diritto "negativo", nel senso che lo stato (e qualunque altro soggetto) deve astenersi dall'interferire in modo arbitrario o illegale nella vita privata della persona. Alla 'astensione' deve infatti accompagnarsi la 'protezione' del diritto fondamentale.

Il Patto internazionale relativo ai diritti civili e politici (Patto ONU II) contiene l'articolo 17 che riprende integralmente l'articolo 12 della Dichiarazione. È stato adottato dall'Assemblea generale dell'ONU il 16 dicembre 1966. Il Comitato ONU per i diritti umani è l'organo incaricato di verificare che gli Stati parta rispettino i loro obblighi.

.... Quadro Normativo - Storia



::: Quadro Normativo - Storia

Il termine “protezione dei dati” (in tedesco: Datenschutz) venne coniato per il titolo della primissima legge in materia, risalente 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 rimase: il concetto è una definizione succinta per “protezione delle persone fisiche con riguardo al trattamento dei dati personali” (la locuzione usata sia nel titolo della Direttiva UE sulla protezione dei dati del 1995 che nel Regolamento generale dell’UE sulla protezione dei dati del 2016).

::: Quadro Normativo - Storia

La protezione dei dati presenta sia aspetti attinenti alle libertà individuali che aspetti sociali, e si inserisce nella categoria di diritti nota come Persönlichkeitsrechte o anche come Individualrechte

Non tutti gli Stati europei l'hanno inserito nelle rispettive Costituzioni come un diritto sui generis, ma alcuni la identificano come una filiazione diretta del diritto fondamentale o (proto-diritto) al “[rispetto della] persona umana”, o anche dal raffronto per analogia legis di diverse norme.

- La protezione dei dati è finalizzata alla salvaguardia di un equo e ragionevole equilibrio fra gli interessi dei singoli e quelli della comunità [per quanto riguarda il trattamento dei dati personali].

Le prime pronunce di violazione, risalenti agli anni ‘50, furono occasionate da opere cinematografiche e pubblicazioni relative a vicende personali di personaggi noti, che portarono gli interessati ad invocare il diritto alla riservatezza di fronte ai giudici.

::: Quadro Normativo - Storia

In quegli anni gli Stati europei avevano adottato una posizione per cui, allo scopo di raggiungere l'auspicato equilibrio, si devono rispettare i seguenti principi normativi:

- la raccolta e il conseguente uso e diffusione dei dati personali devono essere regolamentati per legge;
- tali leggi dovrebbero essere “leggi omnibus” applicabili, in principio, a tutti gli organismi pubblici e privati che si occupano del trattamento dei dati personali;
- la normativa in questione deve contenere determinate norme di diritto sostanziale e garantire, ai soggetti cui si riferiscono i dati personali, diritti individuali fondamentali;
- l’applicazione di tali leggi dovrebbe essere oggetto di controllo da parte di appositi organismi di vigilanza (generalmente denominati Autorità della protezione dei dati o Data Protection Authority -DPA).

::: Quadro Normativo - Storia

Le leggi varate negli anni '70 in Europa si sono articolate intorno a un “nucleo” di principi e di diritti, sempre più riconosciuti da tutti e simili ai principi di base delle Procedure per la correttezza delle informazioni redatte, circa nello stesso periodo, negli USA (benché queste fossero meno dettagliate e non vincolanti).

I principi base enucleati in queste prime leggi in Europa trovarono un riflesso nei primi strumenti europei (non-vincolanti) in materia ad opera del Consiglio d'Europa:

- 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.

::: Quadro Normativo - Storia

I principi “fondamentali” furono poi riconosciuti in strumenti internazionali globali, ma non ancora vincolanti, quali:

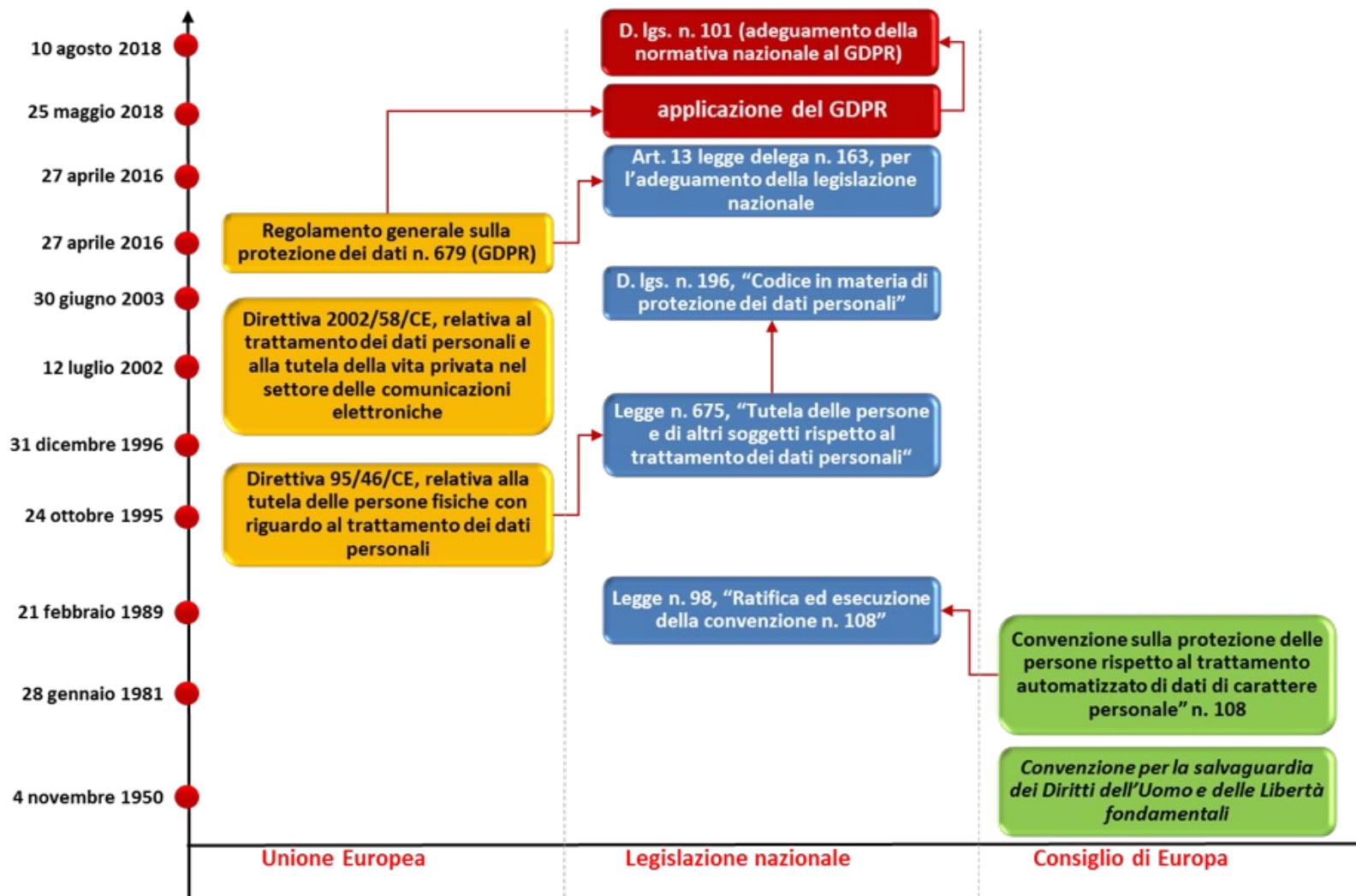
- Le Linee-guida sulla protezione della vita privata e sui flussi transfrontalieri di dati personali dell'OCSE del 1980;
- I Principi guida per la regolamentazione dei file di dati personali computerizzati dell'ONU del 1989, adottati dall'Assemblea Generale dell'ONU (UNGA).

Tutti mirano ad affrontare un problema intrinseco all'impiego dei computer:

- il computer facilita molte e nuove utilizzazioni dei dati, anche di quelli personali, senza che a ciò si accompagni necessariamente l'attenzione ad aspetti di sicurezza o a possibili limitazioni dell'uso.

::: Quadro Normativo - Storia

Evoluzione normativa



.... Quadro Normativo - Storia



::: Quadro Normativo - Storia

La Convenzione del 1981 include definizioni giuridiche più precise dei concetti fondamentali della legislazione sulla protezione dei dati personali: “dati personali”, “titolare del trattamento” e “trattamento”. Si prevede che i dati

- devono essere raccolti e trattati solo in base a specifiche norme che ne autorizzano il trattamento automatizzato,
- devono essere trattati per scopi specifici legittimi e non devono essere destinati a un uso incompatibile con la finalità di trattamento originaria.
- non devono essere conservati oltre il tempo necessario per raggiungere lo scopo prefissato.
- devono essere corretti, pertinenti allo scopo e non eccessivi rispetto alla finalità perseguita.

Contemporaneamente, la Convenzione permetteva agli Stati firmatari l’adozione di eccezioni e restrizioni, al fine di tutelare “la sicurezza dello Stato, la sicurezza pubblica, gli interessi monetari dello Stato o la repressione dei reati” oppure “la persona interessata o i diritti e le libertà di terzi”, a patto che la deroga fosse “prevista dalla legge dello Stato” e “costituisse una misura necessaria [e proporzionata] in una società democratica” per la tutela di tali interessi (Art. 9(2)).

::: Quadro Normativo - Storia

Oltre ad aver conferito valore giuridico ai principi fondamentali della protezione dei dati (con l'aggiunta delle norme speciali sui dati sensibili) e ai diritti dei soggetti interessati, la Convenzione del 1981 confermò anche due importanti requisiti normativi europei:

- applicare le disposizioni adottando norme giuridicamente vincolanti che possono prendere la forma di leggi statutarie, regolamenti o norme amministrative ed essere completate da linee guida o codici non vincolanti;
- un'applicazione di “leggi omnibus”, a (tutte) “le raccolte automatizzate di dati a carattere personale e all’elaborazione automatica degli stessi nel settore pubblico e privato” (Art. 3(1)).

La Convenzione del 1981 non imponeva la creazione di un’Autorità indipendente sulla protezione dei dati personali né affrontava la problematica dei flussi internazionali di dati.

::: Quadro Normativo - Storia

La Convenzione del 1981 si applicava solamente alle “raccolte automatizzate di dati personali e all’elaborazione automatica di tali dati” (Art. 3(1) e anche l’Art. 1). I casellari manuali non venivano disciplinati (sebbene gli Stati firmatari avessero facoltà di estenderne l’applicazione a tali file: Art. 3(2)(c)).

Due di queste mancanze sono state corrette nel Protocollo addizionale relativo alle Autorità di controllo e ai flussi transfrontalieri di dati, adottato nel 2001.

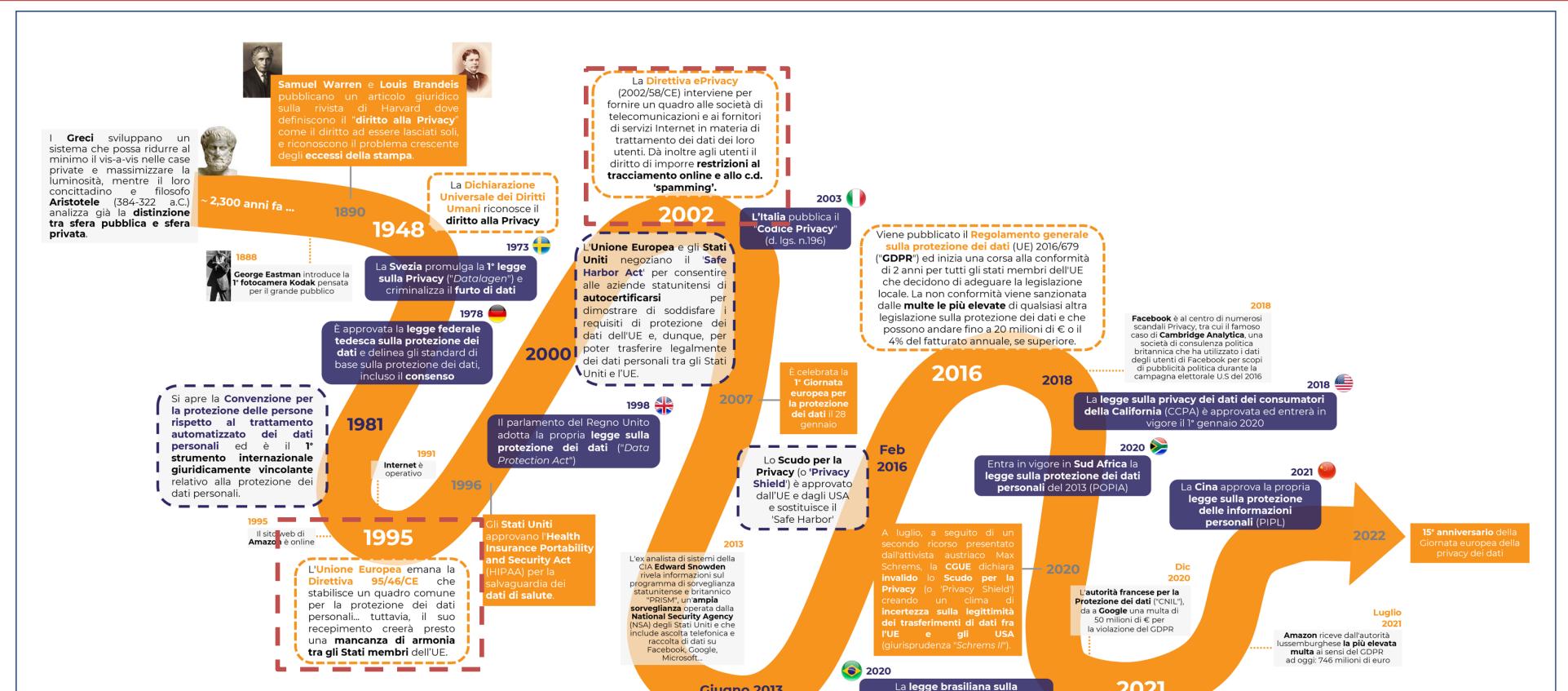
- impone la creazione di DPA indipendenti con poteri di indagine, di intervento e di avvio di azioni legali (Art.1)
- prevede il divieto, in linea di principio, di trasferimento dei dati personali ad un paese che non offre la garanzia di un “livello adeguato di protezione” (Art. 2).

::: Quadro Normativo - Storia

Il Protocollo Addizionale fu adottato soprattutto al fine di avvicinare il regime della Convenzione a quello della Direttiva sulla protezione dei dati dell'UE del 1995. Nel maggio 2018, la Convenzione del 1981 venne ulteriormente “aggiornata”, per allinearla con la più recente legislazione sulla protezione dei dati dell'UE e, più in generale, con gli sviluppi (globali) riguardanti la protezione dei dati.

I problemi relativi alla protezione dei dati sono stati ulteriormente trattati da una serie di organismi, che hanno elaborato molti pareri, raccomandazioni e studi in materia, sempre facendo riferimento alla Convenzione.

.... Quadro Normativo - Storia



Per un certo periodo, la Comunità Europea ritenne che la Convenzione sulla protezione dei dati personali del Consiglio d'Europa del 1981 garantisse, in questo campo, una tutela sufficiente. Alla fine degli anni 90, però, emerse che la Convenzione non avrebbe portato ad una maggiore o più armonizzata protezione dei dati personali nella Comunità:

- solo sette Stati membri l'avevano ratificata, e la legislazione di questi Stati divergeva in maniera considerevole su alcuni aspetti fondamentali.

::: Quadro Normativo - Storia

Il diritto alla protezione dei dati personali è un diritto fondamentale che costituisce un importante obiettivo per l'Unione Europea. Esso è sancito dalla Carta dei diritti fondamentali dell'Unione Europea la quale, all'articolo 8, dispone quanto segue:

1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.
2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso dell'interessato o a un altro fondamento legittimo previsto dalla legge.
3. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica.
4. Il rispetto di tali regole è controllato da un'autorità indipendente.

Tale diritto fondamentale è strettamente connesso al diritto al rispetto della vita privata e della vita familiare sancito all'articolo 7 della Carta.

::: Quadro Normativo - Storia

Il diritto alla protezione dei dati di carattere personale è altresì previsto all'articolo 16, paragrafo 1, del Trattato sul funzionamento dell'Unione europea (TFUE), che ha sostituito a tal proposito l'articolo 286 del Trattato che istituisce la Comunità Europea (CE):

- A decorrere dal 1º gennaio 1999 gli atti comunitari sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati si applicano alle istituzioni e agli organismi istituiti dal presente trattato o sulla base del medesimo.
- Anteriormente alla data di cui al paragrafo 1 il Consiglio, deliberando secondo la procedura di cui all'articolo 251, istituisce un organo di controllo indipendente incaricato di sorvegliare l'applicazione di detti atti alle istituzioni e agli organismi comunitari e adotta, se del caso, tutte le altre pertinenti disposizioni.

Rispetto al diritto derivato, dalla metà degli anni 90 la CE si è dotata di vari strumenti per garantire la tutela dei dati personali.

::: Quadro Normativo - Storia

La frammentazione negli stati membri era inconciliabile con l'obiettivo professato dalla CE di armonizzare tutte le leggi e le norme allo scopo di agevolare l'apertura del mercato interno con la realizzazione della libera circolazione di beni, servizi, capitali e persone. Nel settembre del 1990, la Commissione Europea presentò una serie di proposte finalizzate alla protezione dei dati personali in tutto il territorio della CE:

- una Direttiva generale “relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali” – che dopo un iter legislativo piuttosto lungo ha dato origine alla Direttiva sulla protezione dei dati, Direttiva 95/46/CE);
- un’ulteriore Direttiva di carattere sussidiario “sulla protezione dei dati nel settore delle telecomunicazioni”, Direttiva 97/66/CE, adottata nel dicembre 1997, e sostituita dalla Direttiva 2002/58/CE, la cosiddetta Direttiva e-Privacy.

::: Quadro Normativo - Storia

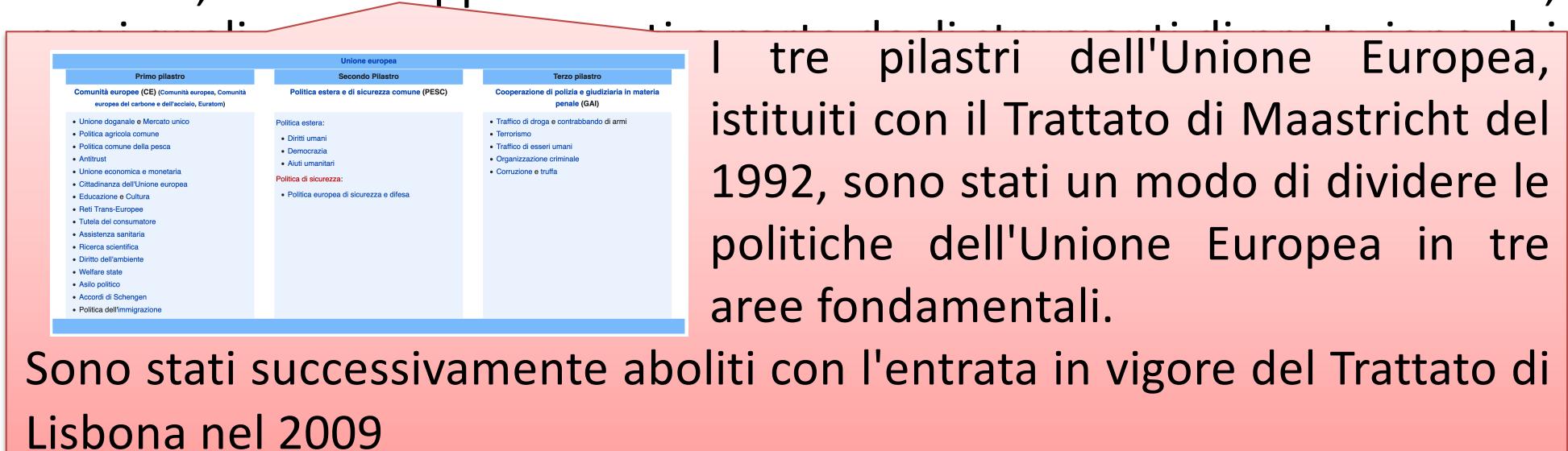
Ogni strumento giuridico dell'UE (in passato CE) è, per sua natura, limitato alle materie di competenza del diritto dell'UE. Alcune materie, soprattutto le attività degli Stati membri nell'ambito della sicurezza nazionale, non rientrano affatto (con poche eccezioni) tra le competenze giuridiche dell'UE, e nessuno strumento normativo dell'UE (o CE) potrà essere di applicazione in questi ambiti.

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. Qualunque cessione o messa a disposizione di dati personali alle forze dell'ordine o ad organismi di sicurezza nazionale era (e nel caso della direttiva e-Privacy, ancora è) disciplinata da tali strumenti, mentre l'ottenimento (ricezione) e l'ulteriore trattamento dei dati divulgati erano regolamentati da altri strumenti, o non affatto subordinati al diritto comunitario (ad es., se tale ottenimento e trattamento fosse operato da organismi di sicurezza nazionale).

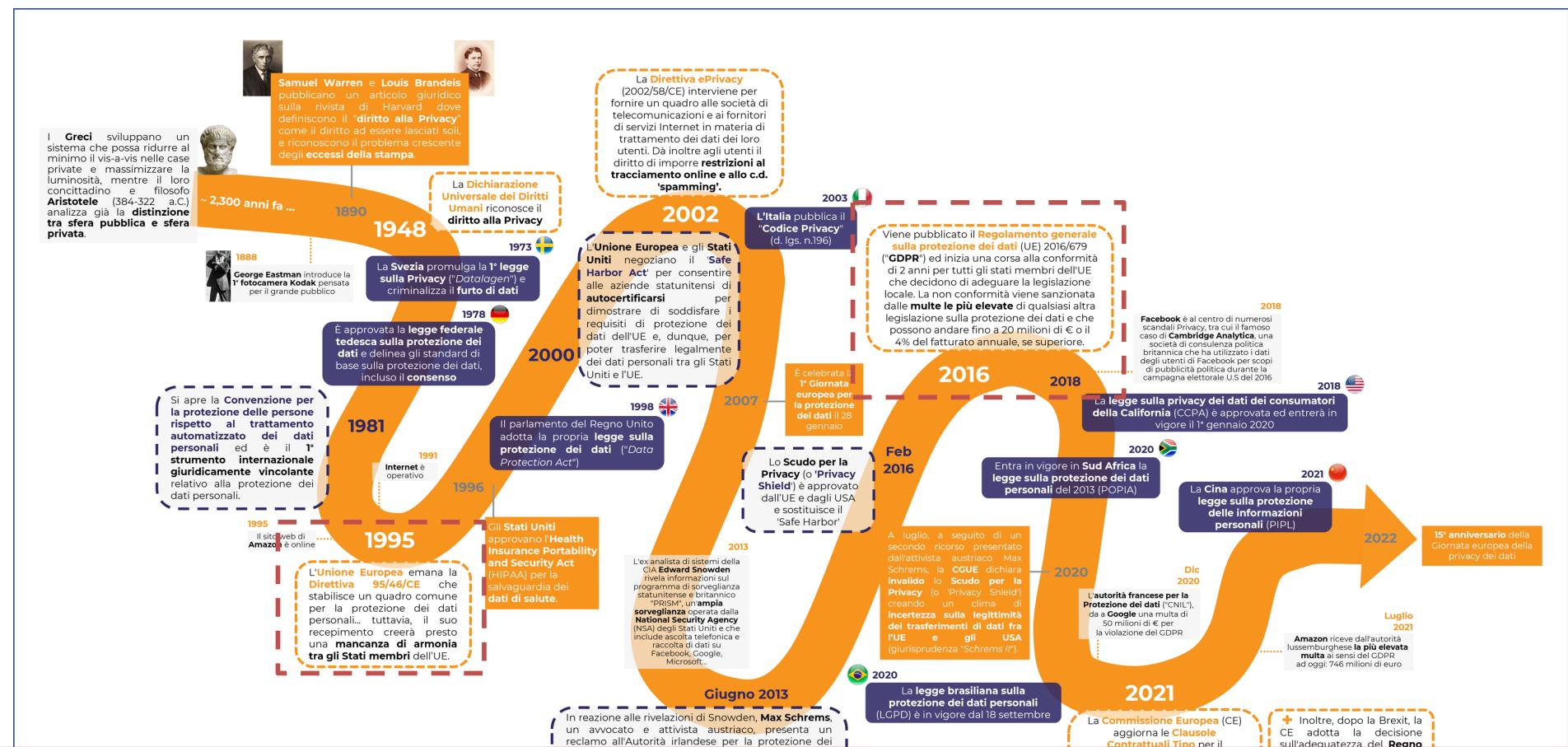
::: Quadro Normativo - Storia

Ogni strumento giuridico dell'UE (in passato CE) è, per sua natura, limitato alle materie di competenza del diritto dell'UE. Alcune materie, soprattutto le attività degli Stati membri nell'ambito della sicurezza nazionale, non rientrano affatto (con poche eccezioni) tra le competenze giuridiche dell'UE, e nessuno strumento normativo dell'UE (o CE) potrà essere di applicazione in questi ambiti.

Le Direttive CE si limitavano a materie nell'ambito del cosiddetto **Primo Pilastro**, e non si applicavano alle attività del **Secondo o Terzo Pilastro**,



... Quadro Normativo - Storia



La necessità di ratifica delle direttive ha generato notevoli divergenze fra gli ordinamenti giuridici degli Stati membri che le hanno recepite. Questo è stato uno dei motivi principali che hanno determinato la scelta di un Regolamento (direttamente applicabile) quale sostituto della Direttiva sulla protezione dei dati del 1995, il GDPR, benché anche un Regolamento possa essere attuato in modi diversi e con diversi aspetti.

::: Direttiva sulla protezione dei dati

La Commissione Europea individuò per la Direttiva sulla protezione dei dati del 1995 due finalità correlate:

- garantire un elevato livello di protezione dei dati, valido per tutto il “Primo Pilastro” della Comunità;
- quale conditio sine qua non per la libera circolazione dei dati personali all’interno della componente principale di questo pilastro, il mercato interno allora emergente.

La Direttiva ha ampliato le definizioni di base della Convenzione del 1981:

- Ha definito quando una persona fisica possa essere “identificabile”, e quando dati inseriti manualmente possano essere considerati sufficientemente “strutturati” da rientrare nell’applicazione della Direttiva.

::: Direttiva sulla protezione dei dati

- Fissa una definizione leggermente modificata di “titolare del trattamento”, ne aggiunge una nuova di “trattamento di dati personali” e definisce concetti quali “responsabile del trattamento”, “terzi” e “destinatario”.
- Aggiunge, inoltre, una definizione di “consenso della persona interessata” e le condizioni che devono essere riunite perché un consenso al trattamento sia considerato valido: “manifestazione di volontà libera, specifica e informata”, e, in un certo modo, espressa (Art. 2(h)).

La Direttiva riprendeva ampiamente i principi della Convenzione del 1981, ma con alcuni chiarimenti, fra cui lo scopo per il quale i dati personali devono essere trattati, non solo “specificato” e “legittimo” (Art. 5(b) della Convenzione), ma anche “esplicito” (Art. 6(1)(b)), nonché con riguardo ai “trattamenti ulteriori per scopi storici, statistici o scientifici” (Art. 6(1)(c) e (e)).

::: Direttiva sulla protezione dei dati

Una grande novità della Direttiva del 1995 fu l'individuazione di una serie di principi “relativi alla legittimazione del trattamento dei dati” Art. 7 :

1. la persona interessata ha manifestato il proprio consenso inequivocabile;
2. il trattamento è necessario all'esecuzione del contratto concluso con la persona interessata o all'esecuzione di misure precontrattuali prese su richiesta di tale persona (ad es., per una verifica di solvibilità);
3. il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il responsabile del trattamento; oppure
4. il trattamento è necessario nell'interesse vitale della persona interessata;
5. il trattamento è necessario per lo svolgimento di un compito di interesse pubblico o nell'esercizio di pubblici poteri di cui è investito il responsabile del trattamento o il terzo cui vengono comunicati i dati;
6. il trattamento è necessario per il perseguimento dell'interesse legittimo del responsabile del trattamento oppure del o dei terzi cui vengono comunicati i dati, a condizione che non prevalgano l'interesse o i diritti e le libertà fondamentali della persona interessata.

La direttiva aveva una visione proprietaria del dato stesso, e se ne favoriva un'applicazione formalistica (tramite le informative e il consenso). Il dato era dell'interessato e quindi non poteva essere usato senza consenso, che era lo snodo fondamentale per l'utilizzo ampio del dato stesso.

::: Direttiva sulla protezione dei dati

La Convenzione del 1981 prevedeva semplicemente che si dovessero prendere “idonee misure di sicurezza” per proteggere i dati personali contro “la distruzione accidentale o non autorizzata o la perdita accidentale, nonché contro l’accesso, la modifica o la diffusione non autorizzati” (Art. 7).

La Direttiva ha ampiamente approfondito questi aspetti imponendo un dovere di riservatezza a chiunque sia coinvolto nel trattamento dei dati personali (Art. 16), e inoltre sancendo che il titolare del trattamento debba adottare “misure tecniche ed organizzative appropriate al fine di garantire la protezione dei dati personali dalla distruzione accidentale o illecita, dalla perdita accidentale o dall'alterazione, dalla diffusione o dall'accesso non autorizzati, segnatamente quando il trattamento comporta trasmissioni di dati all'interno di una rete, o da qualsiasi altra forma illecita di trattamento di dati personali” (Art. 17(1)).

::: Direttiva sulla protezione dei dati

La Direttiva del 1995 elenca anche le principali “categorie particolari di dati” – che comunemente si definiscono come “dati sensibili” – in gran parte corrispondenti a quelle già fissate dalla Convenzione del 1981.

La Convenzione del 1981 non chiedeva agli Stati firmatari di adottare il divieto di esportazione dei dati personali dal proprio territorio a quello di uno Stato che non garantisse tutele assimilabili, disciplinando soltanto i flussi di dati personali fra i firmatari della Convenzione. L'introduzione di questo divieto è stata un'altra importante novità della Direttiva del 1995.

La Direttiva prevede che i dati personali che rientrano nel suo ambito applicativo possano essere trasferiti verso un paese terzo solo nel caso in cui questi garantisca un livello di protezione “adeguato” ai sensi della Direttiva (Art. 25(1)); e che la Commissione Europea abbia facoltà di constatare e decidere l'adeguatezza del livello di protezione dei dati di un determinato paese terzo (Art. 25(2)).

::: Direttiva sulla protezione dei dati

Un'altra novità introdotta dalla Direttiva è stato il riferimento a codici di condotta quali mezzi per “contribuire, in funzione delle specificità settoriali, alla corretta applicazione delle disposizioni nazionali di attuazione della presente direttiva, adottate dagli Stati membri” (art. 27(1)).

- Nella pratica, solo un numero molto limitato di questi codici è arrivato all'approvazione o anche solo alla fase di presentazione per l'approvazione.

La Commissione Europea ha incentivato anche la creazione di sistemi di certificazione, con il marchio di certificazione European Privacy Seal (EuroPriSe), per la valutazione di prodotti e di servizi richiedenti l'utilizzo di dati personali che, se in conformità con la Direttiva attribuisce un marchio di certificazione che attesta tale conformità.

::: Direttiva sulla protezione dei dati

Un'altra novità di rilievo della Direttiva del 1995, rispetto alla Convenzione del 1981, è rappresentata dalla richiesta che tutti gli Stati membri nominino “autorità di controllo” (Garanti) – comunemente chiamate Autorità per la protezione dei dati o DPA – che dovevano disporre, in particolare, di ampi poteri investigativi, di intervento e di indirizzo (Art. 28(3), primo e secondo capoverso), ed essere “pienamente indipendenti nell'esercizio delle funzioni loro attribuite” (Art. 28(1), secondo punto).

Si prevede l'obbligo che le autorità vengano consultate dallo Stato membro al momento dell'elaborazione delle misure regolamentari o amministrative relative alla protezione dei dati (Art. 28(2)) e che dispongano del potere “di promuovere azioni giudiziarie” in caso di violazione delle disposizioni nazionali di attuazione della Direttiva (Art. 28(3), terzo capoverso).

Le DPA sono i principali difensori dei diritti sulla protezione dei dati negli stati membri, con la definizione di un'autorità superiore a livello UE denominata Garante europeo della protezione dei dati (GEPD).

::: Direttiva sulla protezione dei dati

Per ottenere una generale trasparenza e un pieno rispetto della legislazione, la Direttiva del 1995 stabiliva un articolato sistema di notificazione delle operazioni di trattamento dei dati personali (Art. 18; si veda l'Art. 19 per i dettagli dei contenuti delle notificazioni), sancendo che gli elementi di tale notificazione fossero inseriti in un registro consultabile da chiunque (Art. 21(2)).

La Direttiva del 1995 stabiliva che i trattamenti che “potenzialmente presentano rischi specifici per i diritti e le libertà delle persone” (“trattamenti rischiosi”) fossero messi in atto previo un “controllo preliminare”(Art. 20). Gli Stati membri potevano stabilire quali tipologie di trattamenti dovessero essere oggetto di questa disposizione, e come e da chi questo controllo dovesse essere effettuato.

::: Direttiva sulla protezione dei dati

La direttiva si occupava anche di regolamentare il trasferimento dei dati personali al di fuori dello Spazio Economico Europeo (SEE), vietandolo se lo Stato di destinazione avesse avuto un livello di protezione non adeguato alle norme europee.

In tal modo rovescia l'approccio della Convenzione 108, per la quale ogni trasferimento verso paesi terzi è lecito a meno che non vi siano problemi, adottando l'approccio opposto in base al quale nessun trasferimento è ammesso a meno che il paese terzo non garantisca una protezione adeguata.

La direttiva non si applicava alle questioni riguardanti la cooperazione a livello di pubblica sicurezza e giustizia penale. Altra esenzione riguardava i trattamenti di dati personali effettuati da privati per fini esclusivamente personali (art. 3 par. 2):

- Gli impianti di videosorveglianza finalizzati esclusivamente alla sicurezza individuale.

::: Direttiva sulla protezione dei dati

La Convenzione del 1981 sanciva che gli Stati firmatari si impegnavano a “stabilire sanzioni e strumenti di ricorso appropriati” per le violazioni delle disposizioni di diritto interno a protezione dei dati personali, senza peraltro chiarire cosa dovesse essere considerato “appropriato” in tal senso.

La Direttiva del 1995 stabilisce che chiunque debba disporre di un ricorso giurisdizionale in caso di violazione (presunta) dei propri diritti (Art. 22). Inoltre, chiunque subisca un danno cagionato da un trattamento illecito o da qualsiasi altro atto incompatibile con le disposizioni della Direttiva ha il diritto di ottenere il risarcimento del pregiudizio dal titolare del trattamento (Art. 23).

La Direttiva del 1995 stabiliva la creazione di due organismi a livello UE denominati in riferimento agli articoli che ne stabilivano la creazione:

::: Direttiva sulla protezione dei dati

- “Gruppo di lavoro Articolo 29” (WP29) composto da rappresentanti delle Autorità per la protezione dei dati degli Stati membri, dal Garante europeo della protezione dei dati (GEPD) e da un rappresentante della Commissione Europea, con il compito di contribuire ad un’applicazione più armonizzata della Direttiva in particolare attraverso l’adozione di raccomandazioni e pareri (d’iniziativa) nonché di emanare pareri sui progetti di codici di condotta presentati a livello Ue;
- “Comitato Articolo 31” composto da rappresentanti del Governo degli Stati membri, ma presieduto da un rappresentante della Commissione, cui si faceva obbligo di presentare un parere su tutte le misure da intraprendere ai sensi della Direttiva.

Il WP29 ha elaborato numerosi pareri e documenti di lavoro su un ampio ventaglio di problematiche in materia di applicazione della Direttiva sulla protezione dei dati del 1995.

::: Direttiva sulla protezione dei dati

Gli Stati membri dovevano recepire la direttiva nel proprio diritto interno entro la fine del 1998. Purtroppo sussistevano delle problematiche:

- Sussistevano 27 normative nazionali sulla protezione dei dati, che bisognava armonizzare in un unico regolamento unificato;
- Bisognava migliorare le regole sul trasferimento dei dati aziendali al di fuori dell’Unione Europea;
- Si doveva migliorare il controllo dell’utente sui dati identificativi personali.

Sebbene gli obiettivi e i principi alla base della Direttiva 95/46/CE rimanessero validi, si erano rese necessarie revisioni per far fronte alle sfide degli sviluppi tecnologici e della globalizzazione nel 2010. Si rendeva necessario un regime di responsabilità “cumulativa”, in base al quale ciascun attore può essere ritenuto responsabile alla luce del suo ruolo nel trattamento.

::: GDPR

Il Regolamento 2016/679 UE è direttamente applicabile in tutti gli Stati membri dell’Unione europea, tuttavia, l’Italia ha dovuto adottare il D.Lgs. 101/2018 per adeguare le norme contenute nel D.Lgs. 196/2003 alle nuove regole del GDPR. L’art. 5 è dedicato ai principi applicabili al trattamento di dati personali:

- Principio di liceità: i dati personali sono trattati in rispetto delle disposizioni di legge ed autorizzati per una base giuridica (art. 6);
- Principio di correttezza: i dati personali sono trattati in buona fede;
- Principio di trasparenza: sussiste il diritto dell’interessato al controllo delle proprie informazioni;
- Principio di pertinenza: la trattazione è assolutamente necessaria per il perseguimento della finalità autorizzata;
- Principio di necessità: i dati personali sono limitati a quanto necessario rispetto alle finalità per le quali sono trattati;

::: GDPR

- Principio di sicurezza: la sicurezza è una garanzia per i diritti dell'interessato e un obbligo stringente per coloro che effettuano il trattamento;
- Principio di responsabilizzazione: il titolare del trattamento deve rispettare e applicare i principi del regolamento e deve essere in grado di dimostrarlo.

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. Tra le basi giuridiche del trattamento, infatti, l'art.6 GDPR comprende sì il consenso dell'interessato, ma accanto ad altre numerose ipotesi:

- La necessità di dare esecuzione a un contratto di cui l'interessato è parte o a misure precontrattuali adottate su richiesta dello stesso;

::: GDPR

- 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 perseguimento di un interesse legittimo del titolare del trattamento o di terzi, come la trasmissione di dati personali all'interno di uno stesso gruppo imprenditoriale a fini amministrativi interni (es. gestione del personale), la prevenzione delle frodi o l'attività di marketing diretto.

EDPB ha osservato che se il titolare del trattamento sceglie il consenso quale propria base giuridica, non si può basare successivamente il trattamento su una diversa base giuridica.

.... GDPR

Il “consenso” nel GDPR è solo in parte quello della Direttiva 95/46:

- Oltre ad essere “manifestazione di volontà libera, specifica, informata e inequivocabile”, il consenso deve essere manifestato attraverso una “dichiarazione o azione positiva inequivocabile”.
- All’art. 7 paragrafo 1 del GDPR troviamo in maniera chiara l’obbligo per il Titolare di dimostrare il consenso fornito dall’interessato.

Come specificano gli artt. 13 e 14 paragrafi 1, lettera c), nelle informative da rendere agli interessati devono essere chiaramente indicate sia le finalità del trattamento che la sua base giuridica, perché i suoi diritti sono diversi a seconda della base giuridica scelta:

- Il diritto alla revoca del consenso (art. 7, paragrafo 3) non si ha negli altri casi di una diversa base giuridica di legittimazione;
- il diritto a ottenere la portabilità dei dati si ha solo se il trattamento è basato sul contratto o sul consenso (art. 20);
- il diritto di opposizione dell’art. 21 non sussiste se la legittimità del trattamento è basata sul consenso, proprio perché in questo caso prevale il diritto alla revoca.

.... GDPR

Diversi sono gli attori del trattamento dei dati personali (Art. 4) :

- Il **titolare** (Data Controller) è 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 (Art. 26). I contitolari determineranno in un accordo specifico le rispettive responsabilità per il rispetto degli obblighi previsti dal regolamento.
- Il responsabile del trattamento (Data Processor), 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. Sebbene il titolare sia tenuto a esercitare sempre un controllo sul trattamento, 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).

::: GDPR

- La maggiore responsabilizzazione del titolare e del responsabile del trattamento, unita alla crescente complessità e ai rischi per i diritti e le libertà delle persone fisiche, ha indotto a introdurre il **responsabile per la protezione dei dati** (DPO), 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.

Il DPO 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 (Art. 37, p. 6).

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

- se il trattamento è svolto da un'autorità o da un organismo pubblico;
- per monitoraggio regolare e sistematico degli interessati su larga scala;
- 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.

... GDPR

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

- 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 del DPO, il GDPR stabilisce alcune garanzie:

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

... GDPR

Per quanto attiene, diversamente, allo svolgimento dei trattamenti per conto del titolare o del responsabile del trattamento, questi ultimi possono affidare specifici compiti e funzioni a figure interne alla loro organizzazione, che operano sotto la loro responsabilità. A tal fine, il GDPR impone di individuare quei soggetti all'interno dell'organizzazione – c.d. autorizzati – che hanno il compito di trattare tali dati, e di fornire agli stessi specifiche istruzioni, specificando che gli stessi agiscono sotto la diretta autorità del titolare o del responsabile (Art. 29).

Sulla scorta di questa previsione, il legislatore italiano ha ritenuto opportuno introdurre, con l'Art. 2-quaterdecies, D.Lgs. 196/2003, 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.

... GDPR

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

- L'art. 4, par. 9, del GDPR, 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 è assicurata dal riconoscimento di una serie di diritti, elencati analiticamente agli Artt. 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).

.... GDPR

Prodromico all'esercizio di tutti gli altri diritti, il **diritto di accesso** ai propri dati personali è riconosciuto all'interessato dall'Art. 15. Il titolare del trattamento dovrà fornire all'interessato una copia dei dati personali oggetto di trattamento, in forma intelligibile.

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.

.... GDPR

Il **diritto di rettifica** (Art. 16) sancisce che l'interessato può chiedere di correggere le inesattezze dei propri dati personali. Le rettifiche dovranno avvenire senza ingiustificato ritardo, a meno che la richiesta non sia correlata a questioni giuridicamente rilevanti, legittimando la richiesta di prove delle presunte inesattezze.

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;

::: GDPR

- per adempiere un obbligo legale;
- i dati sono raccolti relativamente a servizi per minori, ai sensi dell'Art. 8.

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**.

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 o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri;
- motivi di interesse pubblico nel settore della sanità pubblica;
- per pubblico interesse, ricerca scientifica, storica o statistica;
- l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

::: GDPR

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).

.... GDPR

L'interessato può chiedere al titolare di fornire le informazioni riguardanti tali destinatari e il titolare è tenuto a fornirgliele. A titolo di esempio, un titolare del trattamento può limitare il trattamento dei dati personali trasferendo temporaneamente i dati selezionati verso un altro sistema di trattamento, renderli inaccessibili agli utenti o rimuoverli temporaneamente.

L'Art. 20 specifica che gli interessati possono esercitare il **diritto alla portabilità** dei dati trattati con mezzi automatizzati e sulla base del consenso o per l'esecuzione di un contratto. Questo significa che tale diritto non si applica qualora il trattamento dei dati personali si basi su un fondamento giuridico diverso dal consenso o contratto. Gli interessati hanno il diritto di ottenere la trasmissione diretta dei loro dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile.

Il titolare del trattamento deve sviluppare formati interoperabili che consentano la portabilità dei dati, ma il GDPR non ne impone uno.

.... GDPR

Il **diritto di opposizione** (Art. 21) è riconosciuto agli interessati che si trovano in particolari condizioni, quando la base giuridica del trattamento è l'esecuzione da parte del titolare di un compito svolto nel pubblico interesse o il legittimo interesse del titolare stesso, compresa la profilazione fondata su tali basi giuridiche.

Nell'esercizio del diritto di opposizione occorre valutare il bilanciamento tra i diritti di protezione dei dati dell'interessato e i motivi legittimi (che devono essere “cogenti”, come specificato dall'art. 21 del GDPR) per i quali il titolare intenderebbe continuare a trattare tali dati. L'onere della prova spetta, dunque, al titolare, il quale dovrà dimostrare l'esistenza di motivi cogenti per continuare il trattamento.

- Una volta accolta un'opposizione, il titolare non può più trattare i dati dell'opponente. Resteranno valide, tuttavia, tutte le operazioni svolte prima dell'opposizione.

... GDPR

Le **decisioni automatizzate**, adottate sulla base di dati personali, possono produrre effetti giuridici o incidere significativamente sulle vite delle persone fisiche. L'Art. 22, par. 1, le vieta, a meno che esse:

- siano necessarie per la conclusione o l'esecuzione di un contratto tra l'interessato e il titolare del trattamento;
- siano autorizzate dal diritto, purché i diritti, le libertà e i legittimi interessi dell'interessato siano adeguatamente garantiti;
- si basino sul consenso esplicito dell'interessato.

Tra i trattamenti automatizzati rientra la profilazione, cioè quella forma di valutazione automatizzata del rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato”.

Se ammesse, le decisioni automatizzate devono essere accompagnate da misure appropriate per tutelare l'interessato: ottenere l'intervento umano del titolare, esprimere la propria opinione e contestare la decisione.

::: Direttiva sulla protezione dei dati Telco

Direttiva 95/46/CE relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati

accoppiata

Direttiva 97/66/CE sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni

::: Direttiva sulla protezione dei dati Telco

L'Articolo 1(2) afferma che le disposizioni di questa direttiva sono finalizzate a “precisare ed integrare” la Direttiva Privacy del 1995:

- la delega agli Stati membri per la definizione di modalità di trattamento dei dati del tabulato (entro la scadenza del periodo per le contestazioni)
- il diritto del chiamante all'anonimato (gratuito) e del chiamato a respingere in automatico chiamate anonime (ossia senza ricevere lo squillo al terminale telefonico).

Il recepimento di questa Direttiva subì ritardi dovuti in parte al fatto che, nel 1999, la Commissione decise di intraprendere una revisione generale del quadro di regolamentazione delle comunicazioni elettroniche alla luce delle nuove tecnologie e prassi aziendali in via di definizione. Uno dei risultati della revisione fu la proposta, nel 2000, di sostituzione della Direttiva sulla protezione dei dati nelle telecomunicazioni con una nuova Direttiva riguardante la protezione dei dati nel settore delle comunicazioni elettroniche.

::: Direttiva sulla protezione dei dati Telco

Direttiva 95/46/CE relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati

accoppiata

Direttiva 97/66/CE sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni

sostituita

Direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche

::: Direttiva e-Privacy

La Direttiva 2002/58/CE, abitualmente definita “Direttiva e-Privacy”, è ancora in vigore, anche se la Direttiva sulla protezione dei dati del 1995 è stata sostituita dal GDPR.

L’European Data Protection Board (EDPB), che ha sostituito il WP29, ha adottato un’opinione che chiarisce il rapporto tra Direttiva e-Privacy e il GDPR, e la loro sovrapposizione è emersa, d’altra parte, in disparati casi posti all’attenzione della Corte Europea di giustizia.

- Nelle materie specificamente disciplinate dalla Direttiva e-Privacy, quest’ultima si applica in luogo del GDPR, perché contiene norme più specifiche per il trattamento di dati personali nel contesto specifico delle comunicazioni elettroniche.

Il WP29, nel Parere del 2011, ha tratto che la Direttiva e-Privacy si applica ai fornitori di servizi di comunicazione elettronica, e non in relazione a fornitori di servizi della società dell’informazione.

::: Direttiva e-Privacy

Alla luce del parere espresso dal WP29, il trattamento di qualsiasi dato, compresi quelli disciplinati in modo più specifico dalla Direttiva e-Privacy (come i dati relativi al traffico), svolto da soggetti diversi dai fornitori di servizi di comunicazione elettronica è disciplinato dal GDPR anziché dalle direttive e-Privacy, nonostante quest'ultima rechi disposizioni speciali riguardo ai dati in questione.

- Lex specialis derogat legi generali

Le definizioni di termini più tecnici e relativi alle comunicazioni elettroniche della Direttiva quadro per le Reti ed i Servizi di Comunicazione elettronica si applicano anche ai termini tecnici fondamentali della Direttiva e-Privacy. Fra questi termini figura quello di “abbonato” (a un servizio di comunicazione elettronica). Inoltre, l’Art.2 della 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”.

::: Direttiva e-Privacy

La Direttiva e-Privacy prevede il consenso dell’utente o dell’abbonato:

- Art. 5.3: ai fini della memorizzazione o della raccolta di informazioni dal terminale dell’utente o dell’abbonato;
- Artt. 6 e 9: ai fini del riutilizzo di dati relativi al traffico e all’ubicazione per la prestazione di servizi a valore aggiunto o per la commercializzazione di servizi di comunicazione elettronica;
- Art. 12: ai fini della creazione di elenchi di abbonati;
- Art. 13: ai fini delle comunicazioni indesiderate.

L’Articolo 4(1) sancisce che i fornitori di servizi di comunicazione elettronica devono prendere “appropriate misure tecniche e organizzative per salvaguardare la sicurezza dei propri servizi”, aggiungendo che, “se necessario”, tale tutela va assicurata “congiuntamente con il fornitore della rete pubblica di comunicazione”. Inoltre, il livello di sicurezza deve essere “adeguato al rischio esistente”.

::: Direttiva e-Privacy

Il consenso è indicato come obbligatorio nella Direttiva 2002/58, e nel subentro del GDPR si ha che il consenso viene considerato come un “prerequisito” o una “precondizione” per la legittimità dei trattamenti stessi oggetto della direttiva.

- In tutti i casi in cui un trattamento si basa sul contratto ma i dati trattati richiedono, per la loro natura o per la minore età degli interessati, un consenso specifico, questo si configura non come base di legittimità del trattamento ma come precondizione necessaria.

Una precondizione che non incide sulla base di legittimità del trattamento ove questa sia una delle altre cinque previste dall'art. 6 e in particolare quando consista nell'adempimento di un contratto o di modalità precontrattuali.

::: Direttiva e-Privacy

Sia la Direttiva e-Privacy (Art. 4) sia il GDPR (Artt. 32-34) prevedono un obbligo di garantire la sicurezza oltre all'obbligo di notificare le violazioni dei dati personali all'autorità nazionale competente e all'autorità di controllo [cioè all'autorità di protezione dati], rispettivamente.

L'art. 4, paragrafo 1-bis, prevede inoltre che "Le autorità nazionali competenti sono legittimate a verificare le misure adottate dai fornitori di servizi di comunicazione elettronica accessibili al pubblico e a emanare raccomandazioni sulle migliori prassi in materia di sicurezza che tali misure dovrebbero conseguire". Le "autorità nazionali competenti" non sono necessariamente le autorità nazionali di protezione dei dati.

- L'Autorità per le Garanzie nelle Comunicazioni (AGCOM) è un'Autorità indipendente, istituita dalla legge 249 del 1997 per la regolamentazione e vigilanza nei settori delle comunicazioni elettroniche, dell'audiovisivo, dell'editoria, delle poste e più recentemente delle piattaforme online.

::: Direttiva e-Privacy

In base all'Art. 4, paragrafo 2, della direttiva e-Privacy, nel caso in cui esista un particolare rischio di violazione della sicurezza della rete, il fornitore di un servizio di comunicazione elettronica accessibile al pubblico ha l'obbligo di informarne gli abbonati indicando, qualora il rischio sia al di fuori del campo di applicazione delle misure che devono essere prese dal fornitore di servizio, tutti i possibili rimedi, compresi i relativi costi presumibili.

- L'obbligo di "notificare il rischio" va distinto da quello di "notifica delle violazioni dei dati" introdotto solo nel 2009, mentre l'Art. 4, paragrafo 2, impone di notificare il rischio di una eventuale violazione.

Non occorre informare di una violazione dei dati gli abbonati e altre persone interessate se il fornitore è in grado di dimostrare alla "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.

::: Direttiva e-Privacy

La Direttiva e-Privacy fissa una norma generale di riservatezza delle comunicazioni e una serie di disposizioni specifiche e condizioni per determinati dati o trattamenti.

- La Direttiva e-Privacy prevede il requisito del consenso (per esempio ai fini dell'accesso a informazioni contenute su dispositivi dell'utente (Art. 5.3) oppure per l'invio di messaggi indesiderati di commercializzazione (Art. 13))
- Inoltre, elenca una serie di specifiche basi giuridiche e specifiche finalità di trattamento (per esempio in rapporto al trattamento di dati relativi al traffico (Art. 6)).
- Chiunque sia soggetto a tali disposizioni (chiunque, effettivamente, per quanto riguarda gli Artt. 5(3) e 13, e invece solo i fornitori di servizi di comunicazione elettronica per quanto riguarda l'Art. 6) non può fare riferimento ad altri fondamenti di liceità del trattamento fissati nel GDPR.

::: Direttiva e-Privacy

L'Art. 5, paragrafo 1 mette in risalto la fondamentale importanza della riservatezza delle comunicazioni sancendo che gli Stati membri devono:

- 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 si vieta l'ascolto, la captazione, la memorizzazione e altre forme di intercettazione delle comunicazioni, e dei relativi dati sul traffico, ad opera di persone diverse dagli utenti, senza il loro consenso, eccetto quando sia autorizzato legalmente.

Al paragrafo 3 viene enunciato che gli Stati membri assicurano che:

- l'archiviazione di informazioni oppure l'accesso a informazioni già archiviate nell'apparecchiatura terminale di un abbonato o di un utente sia consentito unicamente a condizione che l'abbonato o l'utente in questione abbia espresso preliminarmente il proprio consenso, dopo essere stato informato in modo chiaro e completo, a norma della Direttiva 95/46/CE, tra l'altro sugli scopi del trattamento.

::: Direttiva e-Privacy

L'Art. 5, paragrafo 1 mette in risalto la fondamentale importanza della riservatezza delle comunicazioni sancendo che gli Stati membri devono:

- assicurare, mediante disposizioni di legge nazionali, la riservatezza delle

Questa frase si riferisce, in un linguaggio tecnico, a quelle operazioni che permettono al visitatore di un sito web di essere riconosciuto dal sito stesso e tracciato nel suo utilizzo del sito, o anche di più siti. Lo strumento più importante a tale scopo è rappresentato dai cosiddetti "cookie".

Al paragrafo 3 viene precisato che gli Stati membri assicurano che:

- **l'archiviazione di informazioni oppure l'accesso a informazioni già archiviate nell'apparecchiatura terminale di un abbonato o di un utente** sia consentito unicamente a condizione che l'abbonato o l'utente in questione abbia espresso preliminarmente il proprio consenso, dopo essere stato informato in modo chiaro e completo, a norma della Direttiva 95/46/CE, tra l'altro sugli scopi del trattamento.

::: Direttiva e-Privacy

Al periodo successivo la Direttiva chiarisce quanto segue:

- Ciò non impedisce l'eventuale memorizzazione tecnica o l'accesso al solo fine di effettuare o facilitare la trasmissione di una comunicazione su una rete di comunicazione elettronica, o nella misura strettamente necessaria a fornire un servizio della società dell'informazione esplicitamente richiesto dall'abbonato o dall'utente.

Lo scopo e il significato della disposizione di cui all'Articolo 5, paragrafo 3, sono delucidati in un linguaggio più semplice nei Considerando (24) e (25) della Direttiva e-Privacy, che chiariscono che la norma ha un'applicazione ben più ampia dei “cookie”.

La Direttiva e-Privacy tratta “cookie” e strumenti di tracciatura allo stesso modo, senza distinzione. Si è favorito in Internet una cultura del “prendere o lasciare” per la quale gli utenti del web sono obbligati a cliccare “Acconsento” (all'inserimento di “cookie” di solito non meglio specificati) per avere accesso ad un sito.

::: Direttiva e-Privacy

L'Art. 6 della Direttiva e-Privacy impone severe limitazioni e restrizioni al trattamento dei dati sul traffico e dei dati relativi all'ubicazione da parte dei fornitori di servizi di comunicazione elettronica. In linea di principio, i dati sul traffico possono essere elaborati e immagazzinati solo da un fornitore di servizi di comunicazione elettronica per la trasmissione di una comunicazione elettronica, la fatturazione all'abbonato della comunicazione o l'interconnessione di pagamenti (Art. 6(1) e (2)).

- Questi trattamenti non necessitano del consenso da parte dell'abbonato o dell'utente del servizio in quanto necessari ai fini della prestazione del servizio.
- Quando non più necessari a tali fini, questi dati devono essere “cancellati o resi anonimi” (Art. 6(1)).

I dati sul traffico possono essere utilizzati per il marketing di servizi di comunicazioni elettroniche o per la fornitura di servizi a valore aggiunto, ma solo con il consenso dell'abbonato o dell'utente.

::: Direttiva e-Privacy

La Direttiva e-Privacy prevede inoltre che il fornitore di servizi debba informare l'abbonato o l'utente dei servizi sul tipo di traffico dei dati oggetto del trattamento e sulla durata di tale trattamento; per il trattamento che si basa sul consenso, l'informativa deve essere fornita prima dell'ottenimento del consenso (Art. 6(4)).

Infine, la Direttiva e-Privacy stabilisce che il trattamento dei dati del traffico da parte di un fornitore di servizi di comunicazione elettronica debba essere limitato ad una serie di servizi sussidiari relativi alla fornitura del servizio, da parte di persone che agiscono sotto l'autorità del fornitore o sono al suo servizio, e ristretto sulla base della “necessità di accesso”.

La Direttiva e-Privacy è ancora più cogente nei riguardi del trattamento di dati che indicano la posizione geografica dell'apparecchiatura terminale dell'utente (ed esempio, un cellulare) e che non sono trattati allo scopo di permettere una comunicazione elettronica o inviare una fatturazione per tale comunicazione.

::: Direttiva e-Privacy

Questi dati possono essere oggetto di trattamento solo quando vengono resi anonimi, oppure, con il consenso degli utenti o degli abbonati a tali servizi (Art. 9(1), primo enunciato). L'utente e l'abbonato devono continuare ad avere la possibilità di negare, in ogni momento, il consenso, e/o disconnettersi dal tracciamento dell'ubicazione, “mediante una funzione semplice e gratuita” (Art. 9(2)). Ancora una volta, il trattamento di tali dati è riservato alle persone che agiscono sotto l'autorità del fornitore del servizio (Art. 9(3)).

Gli abbonati hanno il diritto di ricevere fatture non dettagliate (Art. 7(1)), e gli Stati membri devono anche applicare modalità alternative che tutelino maggiormente la vita privata in relazione a fatture dettagliate (Art. 7(2)).

La Direttiva incorpora disposizioni per cui gli abbonati devono essere informati di ogni intenzione di includere i loro dati in un elenco abbonati; devono inoltre godere del diritto a non essere inclusi in tali elenchi senza onere alcuno e senza obblighi di motivazione (Art. 12(1) e (2)).

::: Direttiva e-Privacy

La Direttiva del 1995 già garantisce il diritto incondizionato di opporsi all'uso di qualsiasi dato personale a scopo di marketing diretto (Art. 14(b)). La Direttiva e-Privacy aggiunge una norma di consenso previo all'utilizzo di dispositivi automatici di chiamata e fax con tale scopo (Art. 13(1)).

La disciplina dei cookie era già normata dalla Direttiva e-Privacy, ma risultava poco efficace. Data la varietà di cookie disponibili, l'utente deve poter esprimere un consenso esplicito sulla pluralità di cookie che un sito impiega.

La modifica principale introdotta dalla Direttiva del 2009 ha riguardato il regime relativo all'utilizzo di queste tecnologie.

::: Direttiva e-Privacy - Modifica

Direttiva 95/46/CE relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati

accoppiata

Direttiva 97/66/CE sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni

sostituita

Direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche

emendata

Direttiva 2009/136/CE recante modifica della direttiva 2002/22/CE

::: Modifica Direttiva e-Privacy

Da un sistema basato sull'informazione preventiva dell'utente o dell'abbonato e sulla possibilità per questi di esercitare un "diritto di opposizione" all'installazione di cookie (ecc.), si è passati al sistema attualmente vigente in base all'Art. 5, paragrafo 3, per cui l'installazione dei cookie è consentita solo se l'abbonato o l'utente sono stati informati preventivamente e hanno dato il proprio consenso esplicito e positivo conformemente ai requisiti di validità del consenso di cui alla direttiva "madre" del 1995.

- Per consenso si intende quanto definito dal GDPR: l'utilizzo di caselle pre-spuntate ai fini del consenso all'uso di cookie ecc. non sarà più conforme ai requisiti fissati in merito dalla direttiva e-Privacy.

::: Convenzione del 2018

Benché la Convenzione del Consiglio d'Europa del 1981 sia stata (ampiamente) armonizzata con la Direttiva sulla protezione dei dati personali CE del 1995, grazie all'aggiunta di norme sui flussi transfrontalieri di dati e alla creazione di autorità indipendenti sulla protezione dei dati figuranti nel Protocollo addizionale adottato nel 2001, si trattava di un testo che, come la Direttiva, risultava ormai superato.

- I lavori di “ammodernamento” della Convenzione cominciarono nel 2011, e la “Convenzione aggiornata”, denominata Convenzione 108+ venne adottata il 18 maggio 2018 e aperta alla firma il 10 ottobre 2018 e firmata dall’Italia nel Marzo 2019.

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.

::: Convenzione del 2018

Il Protocollo rafforza i compiti delle autorità di protezione dati e del Comitato della Convenzione, chiamato a svolgere un ruolo specifico nel processo di valutazione dell'effettivo rispetto dei principi della Convenzione, che deve essere assicurato dai Paesi che intendono aderire ad essa, nonché dei Paesi che, pur essendo già parti, saranno comunque sottoposti ad una verifica riguardo l'osservanza della Convenzione.

Le nuove norme avvicinano il regime della Convenzione al GDPR. Per l'adeguatezza del regime di protezione dei dati di un paese terzo, il fatto di aver aderito alla Convenzione 108+ è un elemento fondamentale.

- I principi fondamentali del GDPR non saranno più vincolanti solo in virtù dell'applicazione territoriale del Regolamento.
- Per chi già sottoposto agli obblighi del GDPR ad una prima valutazione pare non risultino differenze sostanziali rilevanti,
- Per i titolari in Paesi firmatari extra UE i richiamati principi sono applicabili anche al di fuori dei casi già coperti dal GDPR.

::: Convenzione del 2018

Una conseguenza interessante è la facilitazione del trasferimento internazionale dei dati, che non potrà essere limitato salvo reali e seri rischi, in quanto i firmatari della Convenzione assicurano una protezione adeguata agli individui e ai loro dati.

È importante sottolineare gli effetti del protocollo di modifica anche nell'ambito di ricerca e sviluppo di sistemi di AI, tutti i progetti basati sull'intelligenza artificiale devono rispettare i contenuti della Convenzione, in particolare attuando valutazioni d'impatto sulle possibili conseguenze che il loro perfezionamento potrebbe avere sui diritti fondamentali, minimizzando i rischi e “vigilando” sugli algoritmi.

::: Regolamento e-Privacy

La Direttiva 2002/58/CE, o Direttiva e-Privacy, riguarda il trattamento dei dati personali e la tutela della vita privata, con l'obiettivo di garantire la riservatezza in tutte le comunicazioni elettroniche (come messaggi di testo, e-mail, messaggi social etc.).

- La Direttiva e-Privacy è *lex specialis* rispetto alla *lex generalis* di cui al GDPR (*lex specialis derogat lex generalis*). Il GDPR non disciplina in modo specifico l'ambito digitale. E' applicabile ovviamente ai siti internet ma non contiene specifiche disposizione per questo contesto.

Il GDPR non impone alcun obbligo supplementare a quelli indicati dalla Direttiva e-Privacy. La natura speciale della Direttiva e-Privacy comporta la prevalenza delle sue specifiche previsioni sulle misure più generali dettate dal GDPR, nel caso in cui esse non siano compatibili tra loro.

Un nuovo Regolamento e-Privacy, non ancora entrato in vigore, andrà a sostituire la Direttiva 2002/58/CE c.d. Direttiva e-Privacy, così come è successo con il GDPR nei confronti della Direttiva 95/46.

::: Regolamento e-Privacy

La Direttiva e-Privacy del 2002 è divenuta obsoleta considerando l'evoluzione dei sistemi comunicativi attuali. L'oggetto di disciplina del nuovo regolamento sarà il marketing, l'e-Commerce, il call center, la pubblicità online, oltre che gli operatori Over-The-Top al fine di una evoluzione normativa più adeguata a garantire il diritto alla protezione delle comunicazioni elettroniche.

Il futuro Regolamento e-Privacy avrà il compito di innalzare il livello di protezione offerta dalla Direttiva e-Privacy attualmente in vigore, integrandosi di fatto con i contenuti normativi del GDPR al fine di fornire garanzie aggiuntive per tutti i tipi di comunicazioni elettroniche.

- Il Regolamento e-Privacy non deve abbassare il livello di protezione offerto dall'attuale Direttiva e-Privacy.
- Il Regolamento e-Privacy dovrebbe garantire la protezione di tutti i tipi di comunicazioni elettroniche, in modo tecnologicamente neutrale.[†]
- Dovrebbe essere incoraggiato l'uso di dati di comunicazione elettronica realmente anonimi.

::: Regolamento e-Privacy

Uno degli obiettivi è semplificare le regole dei cookie e di razionalizzare il metodo di raccolta del consenso per renderlo più “user friendly”.

- i siti web non dovranno più mostrare i pop up per il consenso ai cookie, in antitesi al rinomato Provvedimento n. 229 del 2008 del Garante italiano emanato sulla scorta della Direttiva e-Privacy.
- Gli utenti dovranno avere sotto controllo ogni informazione o dato conservato sui loro device, senza dover necessariamente cliccare su di un banner ogni volta che visitano un sito web.
- Tale semplificazione verrà prevista tramite la possibilità per gli utenti di “settare” le impostazioni per il consenso/rifiuto ai cookie direttamente dalle impostazioni dei loro browser.

Un ulteriore elemento innovativo è il consenso online, che si applicherà anche “mutatis mutandis” alle persone giuridiche. La Proposta ha previsto:

- il consenso dovrà essere specifico, esplicito e sempre dimostrabile, e di rinnovare periodicamente il consenso.

::: Regolamento e-Privacy

Il Regolamento ePrivacy esclude l'interesse legittimo come base per il rilascio di cookie. Il consenso sarà quindi la base per poter rilasciare cookie di profilazione. Riguardo al consenso, il regolamento prevede chiaramente che il consenso possa essere espresso mediante software, mediante il proprio device cliccando su un'opzione o selezionandola con un contrassegno (“flag”).

- Le recenti Linee Guida sui cookie del Garante italiano affermano la sostanziale illiceità dei c.d. “cookie walls”, ovvero i cookie che impongono all’utente di accettare cookie di profilazione per visionare il sito.
- Il Regolamento ePrivacy esprime una opinione diversa al riguardo: si permette di condizionare alla prestazione del consenso ai cookie l’accesso al sito. Ciò però non deve privare l’utente “di una facoltà di scelta effettiva”, ovvero l’utente può scegliere tra:
 - un servizio che include il consenso all’uso dei cookie per finalità aggiuntive; oppure
 - un’offerta equivalente che non comporta il consenso dell’utente all’uso dei suoi dati per finalità aggiuntive.

::: Regolamento e-Privacy

Il Regolamento attribuisce dignità normativa sia alla segretezza delle comunicazioni elettroniche sia al divieto di ogni tipo di interferenza. L'articolo 6 stabilisce quando è consentito il trattamento dei dati di comunicazione elettronica da parte dei fornitori di reti e servizi, definendo quattro ipotesi di liceità, fondamentalmente per esigenze di natura tecnica e di sicurezza. Peraltro, viene anche stabilito che il trattamento di tali dati è consentito solo per la durata necessaria allo scopo o agli scopi specificati qualora non sia possibile utilizzare informazioni rese anonime.

Tale protezione si estende anche ai metadati, di cui il regolamento introduce la definizione all'art. 4 come segue:

- per “metadati di comunicazione elettronica” si intendono i dati utilizzati per rintracciare e identificare la fonte e la destinazione di una comunicazione, i dati sull’ubicazione del dispositivo generati nel contesto della fornitura di servizi di comunicazione elettronica, nonché la data, l’ora, la durata e il tipo di comunicazione

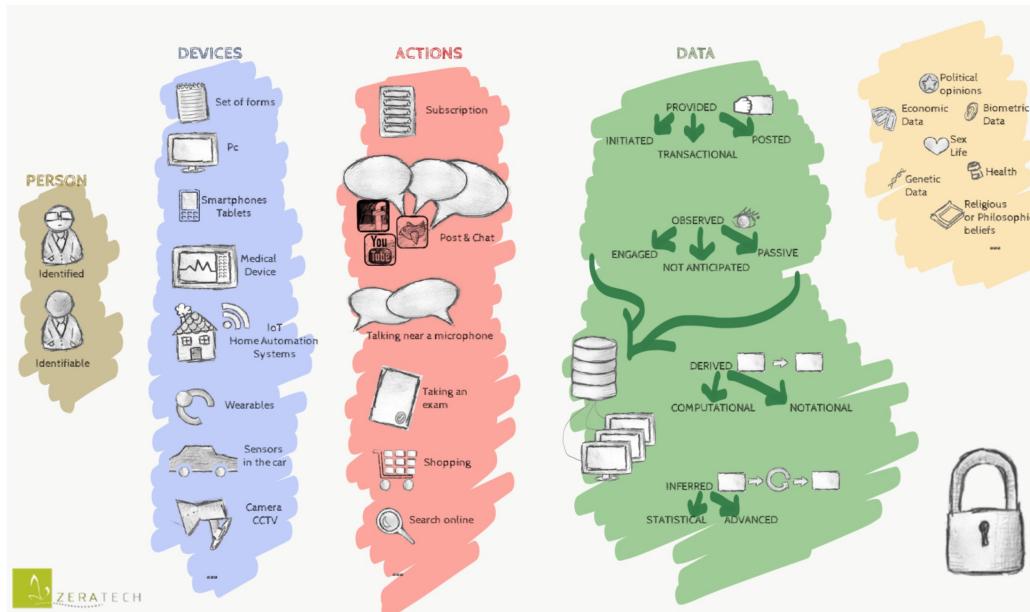
::: Regolamento e-Privacy

Il trattamento dei metadati delle comunicazioni elettroniche da parte dei fornitori di reti e servizi di comunicazione elettronica è consentito unicamente in sei ipotesi previste dalla norma (6b) e precisamente per esigenze tecniche, fatturazione, individuazione o cessazione dell'uso fraudolento o abusivo dei servizi, consenso dell'interessato, tutela degli interessi vitali di una persona fisica, e per i dati sull'ubicazione per fini di ricerca scientifica o storica o a fini statistici.



Dettagli su Data Privacy

::: Dati PersonalI



Il GDPR definisce come dati personali “qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»)” (Art.4 – 1). Sono “dati personali” anche quelli raccolti automaticamente o risultanti da rielaborazioni successive.

La ricerca e l'innovazione richiedono, per loro natura, l'accesso a vasti quantitativi di informazioni che, qualora riguardino persone fisiche, si qualificano come dati personali. Il bilanciare dell'avanzamento tecnologico con il rispetto per la privacy non ha sempre prodotto i risultati auspicati. Recentemente, si è assistito all'emergere di un'innovativa applicazione: i dati sintetici, che riuscirebbe a contemperare da un lato le esigenze di tutela della privacy degli interessati, dall'altro rappresenta un sostegno all'innovazione, superando gli “ostacoli” del passato.

::: Dati Personal

I dati sintetici sono dati artificiali generati da dati originali e da un modello che viene addestrato a riprodurre le caratteristiche e la struttura dei dati originali”; e “ciò significa che i dati sintetici e i dati originali dovrebbero fornire risultati molto simili quando vengono sottoposti alla stessa analisi statistica”.

I dati sintetici, se correttamente generati, non solo riflettono fedelmente la distribuzione, le tendenze e i pattern dei dati originali, ma lo fanno in maniera tale da annullare qualsiasi rischio di ricondurre le informazioni a singoli individui. Questo processo non necessita della conservazione di dati "primari" legati a persone specifiche e permette di generare dati utili per analisi statistiche e di machine learning.

Al dato sintetico – se ottenuto in maniera da impedire o da non consentire più l'identificazione dell'interessato (utilizzando la formulazione contenuta nel Considerando 26 del GDPR) – non dovremmo riconoscere garanzie in materia di protezione dei dati personali.

::: Dati Personal

Un altro aspetto significativo dei dati sintetici è la loro capacità di mitigare i bias presenti nei dati originali. Difatti, attraverso tecniche di generazione controllata, è possibile produrre set di dati equilibrati e rappresentativi, contribuendo a ridurre le disparità e migliorare l'equità dei sistemi di intelligenza artificiale. Questo aspetto è di fondamentale importanza al fine di garantire che le tecnologie emergenti siano inclusive e non perpetuino discriminazioni preesistenti.

I dati non personali non sono soggetti alle stesse restrizioni sul trattamento dei dati personali, ad esempio non è necessario il consenso dell'interessato per il loro trattamento. Questo è stato ulteriormente normato alla luce dell'entrata in scena del FFD (Free-Flow-Data), il Regolamento UE 2018/1807 sulla libera circolazione dei dati non personali.

::: Dati Personal

L'obiettivo primario del Regolamento 1807 o FFD è la costruzione del Digital Single Market, l'equivalente digitale del Mercato Unico Europeo, al fine di consentire la libera circolazione dei dati non personali.

- In coordinamento con il Regolamento UE 2016/679 o GDPR, da una parte e con la Direttiva UE 2016/1148 o NIS riguardante la sicurezza delle reti e dei sistemi informativi, dall'altra, FFD definisce lo spazio comune europeo dei dati, garantendo altresì che i requisiti di sicurezza relativi all'archiviazione dei dati di persone fisiche e/o giuridiche vengano applicati uniformemente in tutti gli stati membri.

Sussistono quattro principali ostacoli alla libera circolazione dei dati non personali:

1. la mancanza di fiducia fra gli stati membri sussistendo diversi standard di sicurezza applicati ai rischi legati al trattamento di tali dati, il che comporta difficoltà nel trasferimento da un paese all'altro;

::: Dati Personal

2. la presenza di obblighi di localizzazione dei dati previsti dalle diverse legislazioni degli stati membri, che impone di effettuare il trattamento di dati nel territorio di un determinato stato membro, o che ostacoli il trattamento in un diverso stato membro;
3. le cosiddette pratiche di vendor lock-in nei settori privati, ovverosia ostacoli al libero trasferimento dei dati da un fornitore di servizi ad un altro, o il ri-trasferimento verso i propri sistemi informatici;
4. in generale, la mancanza di uniformità legislativa e di principi condivisi causano sfiducia, costi elevati e applicazione di misure di sicurezza non uniformi.

FFD ha vietato gli obblighi di localizzazione dei dati, con la sola eccezione dei casi in cui ciò sia necessario per giustificati motivi di sicurezza pubblica (ovvero la sicurezza interna ed esterna di uno stato membro), nel rispetto del principio di proporzionalità. Il concetto di **libera trasferibilità** richiama fortemente il concetto di portabilità ed il relativo diritto degli interessati di cui all'art. 20, GDPR.

::: Dati Personal

I dati non personali possono essere catalogati secondo la loro provenienza e precisamente:

- quelli che, ab origine, non si riferiscono ad un soggetto identificato o identificabile;
- quelli che, sebbene nati come dati personali, sono stati sottoposti ad anonimizzazione, pur essendo sempre necessario valutare di volta in volta se i dati siano stati adeguatamente anonimizzati e non sia più possibile risalire al soggetto cui appartengono.

Il problema sorge nel momento in cui non risulta possibile scindere con certezza i dati personali da quelli non personali. Quale disciplina applicare nel caso di insieme di dati composti?

Il dubbio è risolto al comma 2 dell'art. 1, Regolamento FFD: lo stesso si applicherà solamente “alla parte dell'insieme contenente i dati non personali”. Nel caso in cui le due tipologie di dati siano indissolubilmente legate tra loro, il Regolamento FFD non pregiudica l'applicazione del GDPR.

::: Analisi del Sito Web Aziendale

I cookie sono delle informazioni contenute in piccoli file di testo che i siti visitati dagli utenti inviano ai loro dispositivi, dove vengono memorizzati per essere poi ritrasmessi agli stessi siti nelle visite successive. Di solito, queste piccole stringhe di testo vengono memorizzate nel browser degli utenti con lo scopo di essere poi ritrasmesse al sito nel corso delle successive visite. L'utente può ricevere sul suo terminale anche cookie di siti o di web server diversi (c.d. cookie di "terze parti") perché sul sito web visitato sono presenti elementi che risiedono su server diversi da quello sul quale si trova la pagina richiesta.

I cookie possono avere finalità molto differenti dalle quali derivano diversi effetti e criticità nell'utilizzo degli stessi. Sono usati per eseguire autenticazioni informatiche, monitoraggio di sessioni e memorizzazioni di informazioni specifiche riguardanti gli utenti che accedono ai server.

::: Analisi del Sito Web Aziendale

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, o nella misura strettamente necessaria al fornitore di un servizio della società dell'informazione, esplicitamente richiesto dall'abbonato o dall'utente, a erogare tale servizio.

I cookie tecnici posso essere ulteriormente distinti in:

- I Cookie di navigazione sono quelli che consentono al sito di funzionare correttamente, permettendo la navigazione e la fornitura di servizi richiesti dall'utente. Sono temporanei e cancellati al termine della loro durata. Senza tali cookie alcune operazioni sarebbero meno sicure o più complesse e, in alcuni casi, non potrebbero proprio essere compiute.

::: Analisi del Sito Web Aziendale

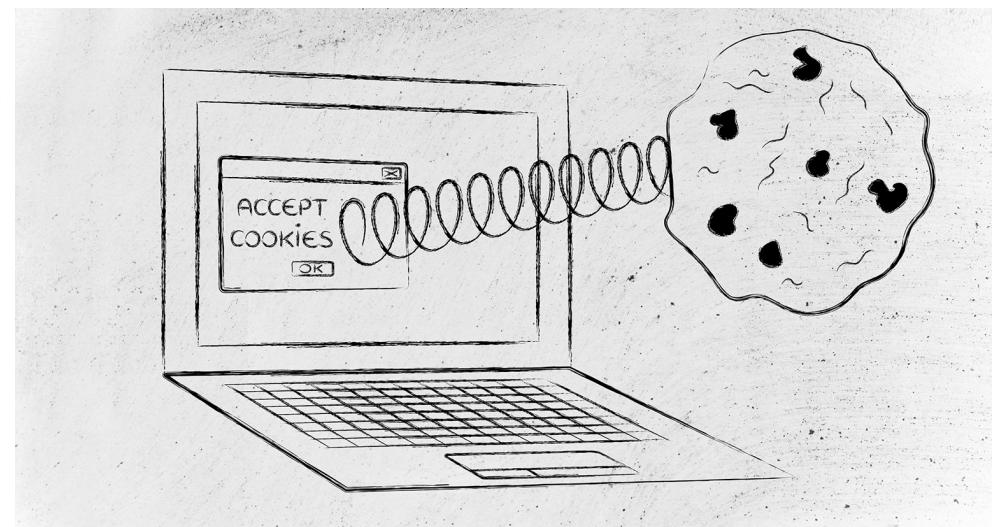
- I Cookie funzionali o tecnici sono quelli che consentono al sito di memorizzare informazioni della navigazione effettuata dallo stesso, al fine di essere riutilizzate nelle navigazioni successive, migliorando il servizio e la qualità della navigazione.
- I Cookie analitici sono utilizzati per raccogliere informazioni, in forma aggregata, al fine di condurre analisi statistiche delle modalità di navigazione del sito. Sono dati anonimi, di solito utilizzati per migliorare le funzionalità del sito tramite la raccolta dei dati dell'utenza che lo utilizza, e possono essere assimilati ai cookie funzionali solo se utilizzati al fine di un'ottimizzazione del sito da parte del gestore dello stesso.
- I 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. I cookie possono essere installati dal gestore del sito che l'utente sta visitando, o editore, e si parla in tali casi di cookie di prima parte. Quando è un soggetto proprietario di un sito diverso che installa cookie per il tramite del sito editore si è di fronte, invece, a cookie di terze parti.

::: Analisi del Sito Web Aziendale

Questa classificazione dei cookie permette di comprendere quando è necessario richiedere il consenso dell'utente.

Strictly necessary cookies	Senza questi cookie la trasmissione di una comunicazione su rete elettronica non sarebbe possibile. Questi sono collegati a un servizio espressamente richiesto dal visitatore, es. quelli del carrello virtuale nei siti di e-commerce	NON è necessario il consenso
Performance cookies	Questi cookie raccolgono informazioni sull'uso del sito da parte dei visitatori, in maniera anonima e senza profilazione (es. Google Analytics, advertising e pay per click).	Se trattano dati in forma anonima e aggregata NON è necessario il consenso.
Functionality cookies	Servono a ricordare le scelte dell'utente e automatizzano alcune procedure (come il login) oppure personalizzano l'accesso e la navigazione del sito (es. lingua dell'utente)	NON è necessario il consenso
Targeting o advertising cookies	Cookie pubblicitari che consentono la profilazione degli utenti al fine di fornire pubblicità mirata, legati spesso a siti di terze parti, che raccolgono informazioni relative alla navigazione degli utenti.	Necessario il consenso

La Commissione europea e l'Autorità Garante per la protezione dei dati personali hanno, infatti, individuato quattro categorie di cookie in base alle quali modulare la prestazione del consenso.



::: Analisi del Sito Web Aziendale

- Il primo accesso alla home page o a qualunque altra pagina di un sito web deve essere sempre preceduto da un banner, se si utilizzano cookie di profilazione (di prima e/o di terza parte). Nel caso in cui si utilizzino solo cookie tecnici è sufficiente la sola informativa estesa, che fornisca informazioni circa l'utilizzo e le finalità dei cookie presenti sul sito.

Il banner deve comparire in primo piano e presentare dei colori e dei caratteri tali da rendere percettibile la discontinuità nella fruizione dei contenuti della pagina web che si sta visitando, senza impedire le interazioni con la pagina stessa.

Esso conterrà le seguenti indicazioni:

- che utilizza cookie di profilazione per inviare messaggi pubblicitari in linea con le preferenze manifestate dall'utente nell'ambito della navigazione in rete;

::: Analisi del Sito Web Aziendale

- che il sito consente anche l'invio di cookie di “terze parti”;
- il link all'informativa estesa, con indicazioni sull'uso dei cookie tecnici e analitici, dando la possibilità di scegliere quali autorizzare;
- l'indicazione che alla pagina dell'informativa estesa (linkabile da ogni pagina del sito e posta in calce ad essa) è possibile negare il consenso all'installazione di qualunque cookie;
- l'indicazione che costituisce accettazione dei cookie la prosecuzione della navigazione mediante accesso ad altra area del sito, la selezione di un elemento dello stesso (ad esempio di un'immagine o di un link), l'eventuale chiusura del banner facendo click sulla “X” o lo scorrimento della pagina (scroll).

La prestazione del consenso è registrata e conservata dall'editore mediante l'utilizzo di un cookie tecnico. Ciò permetterà di non riproporre l'informativa breve alla seconda visita del sito, benché l'utente possa in qualunque momento modificare o negare il consenso sull'utilizzo dei cookie.

::: Analisi del Sito Web Aziendale

Non esiste una soluzione tecnologica di semplice applicazione che dia la certezza dell'avvenuta prestazione del consenso da parte dell'utente. Per questo si suggerisce al titolare /gestore del sito di:

- prevedere un sistema di risposta all'utente, il quale in caso di lamentela dovrà al più presto ricevere un riscontro su come esercitare il proprio consenso/diniego selettivo o come cancellare i cookie dal proprio browser, prevedendo all'occorrenza apposite pagine informative;
- predisporre una sorta di certificazione del processo di acquisizione e conservazione del cookie tecnico del consenso.

L'informativa estesa o cookie policy (accessibile da ogni pagina del sito, sia dagli utenti registrati che da quelli non registrati) contiene tutti gli elementi di cui all'art. 13 del GDPR. Inoltre, devono essere presenti:

- una spiegazione generale di cosa sono i cookie e della gestione degli stessi tramite le impostazioni dei browser;
- la descrizione delle categorie di cookie tecnici suddivisi per finalità;

::: Analisi del Sito Web Aziendale

- la spiegazione di come viene prestato il consenso (scroll, tasto “ok” o “X”, link);
- la descrizione dei cookie di profilazione di prima parte, con il relativo modulo di consenso;
- le informazioni relative alla profilazione sia degli utenti registrati che non;
- la descrizione delle finalità dei cookie di terza parte.

All’interno di tale informativa deve essere inserito anche il link aggiornato alle informative e ai moduli di consenso delle terze parti con cui l’editore ha stipulato accordi per l’installazione di cookie tramite il proprio sito.

Nello spazio dell’informativa estesa deve essere richiamata la possibilità per l’utente (art. 122, c. 2, D.Lgs. 196/2003) di manifestare le proprie opzioni in merito all’uso dei cookie da parte del sito anche attraverso le impostazioni del browser, indicando almeno la procedura da seguire per configurare tali impostazioni.

::: Analisi del Sito Web Aziendale

Se l'utente non interagisce con i moduli del consenso ed esce dall'informativa stessa, chiudendola o proseguendo la navigazione del sito, di fatto presta il consenso per tutti i cookie, a condizione, però, che nell'informativa estesa sia stata inserita questa indicazione in maniera esplicita e trasparente.

::: Il Consenso ai Cookie

In base al GDPR, è responsabilità legale dei proprietari e degli operatori dei siti web assicurarsi che i dati personali vengano raccolti e trattati in modo legale. Anche i siti web al di fuori dell'UE sono tenuti a rispettare il GDPR se raccolgono dati da utenti che si trovano nell'UE.

Nonostante i cookie siano menzionati una sola volta nel GDPR, il consenso ai cookie è comunque un pilastro della conformità per i siti web con utenti situati nell'UE. Ciò è dovuto al fatto che uno dei modi più comuni per raccogliere e condividere i dati personali online è rappresentato dai cookie dei siti internet. Il GDPR stabilisce regole specifiche per l'utilizzo dei cookie.

In virtù del GDPR, il consenso ai cookie è il fondamento giuridico più frequentemente utilizzato dai siti web per poter trattare i dati personali e utilizzare i cookie.

::: Il Consenso ai Cookie

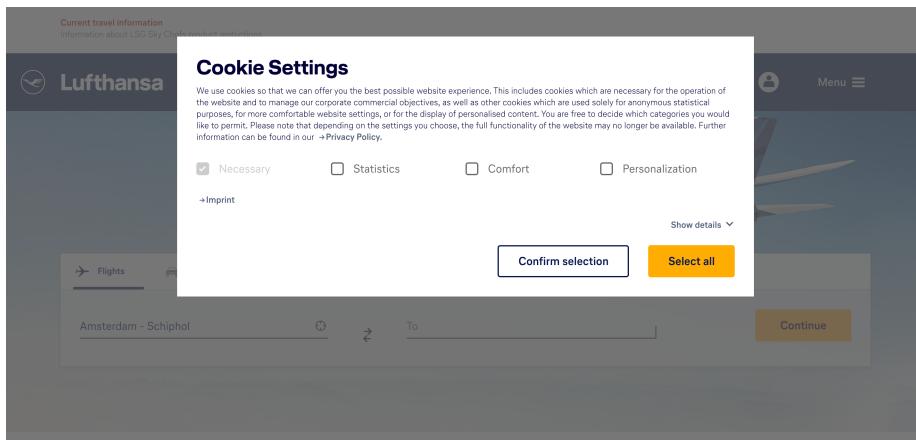
Il GDPR prescrive che un sito web sia autorizzato a raccogliere i dati personali degli utenti solo dopo che questi abbiano espresso il loro consenso esplicito alle relative specifiche finalità di utilizzo.

Secondo il GDPR, i siti web devono soddisfare i seguenti requisiti per il consenso ai cookie:

- Il consenso preventivo ed esplicito deve essere ottenuto prima di qualsiasi attivazione dei cookie (ad eccezione dei cookie necessari, inseriti nella whitelist).
- I consensi devono essere specifici, ovvero l'utente deve poter attivare alcuni cookie, lasciandone al contempo disattivati altri: non deve quindi trovarsi costretto ad acconsentire a tutti o a nessuno.
- Il consenso deve essere prestato liberamente, cioè non deve essere forzato, e poter essere revocati con la stessa facilità con cui vengono forniti.

::: Il Consenso ai Cookie

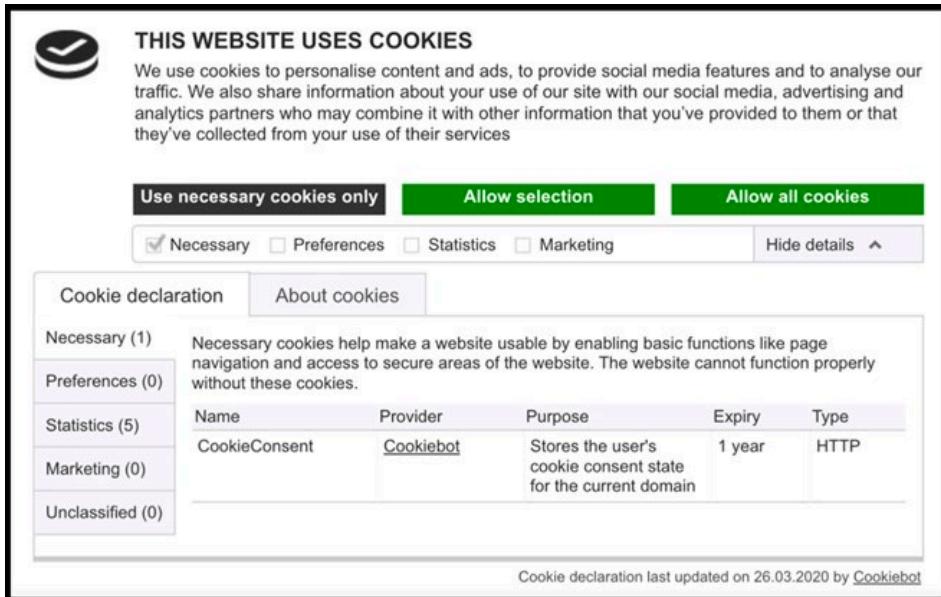
- I consensi devono essere custoditi in sicurezza, come documentazione legale.
- Il consenso deve essere rinnovato annualmente. Tuttavia, alcune direttive nazionali sulla protezione dei dati raccomandano un rinnovo più frequente, ad esempio ogni sei mesi.



La conformità al GDPR per quanto riguarda i cookie viene in genere raggiunta grazie ai cookie banner, i quali permettono agli utenti di selezionare e accettare l'attivazione di determinati cookie piuttosto che altri.

Le linee guida del Comitato europeo per la protezione dei dati (EDPB) del mese di maggio 2020 affermano che il cookie banner di un sito non può presentare caselle preselezionate, e la prosecuzione dello scorrimento o della navigazione da parte degli utenti non possono essere considerati come un consenso valido per il trattamento dei dati personali.

::: Il Consenso ai Cookie



Sussistono soluzioni per testare la conformità al GDPR come su <https://www.cookiebot.com/it/>.

Affinché un sito web sia autorizzato ad attivare i cookie e trattare i dati personali, gli utenti devono manifestare il loro consenso con un'azione chiara e affermativa.

Cookiebot Cos'è il CCPA? Cos'è il GDPR? Prezzi Assistenza Funzioni Rivenditori Accedi Provalo gratuitamente →

COOKIEBOT TI AIUTA A RENDERE CONFORME L'USO DEI COOKIE E DEL TRACCIAMENTO ONLINE

Il mio sito è conforme?

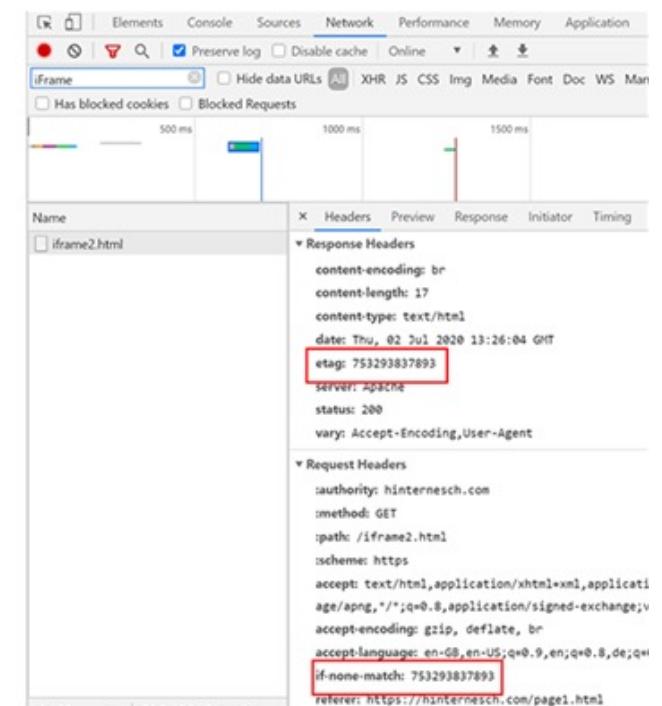
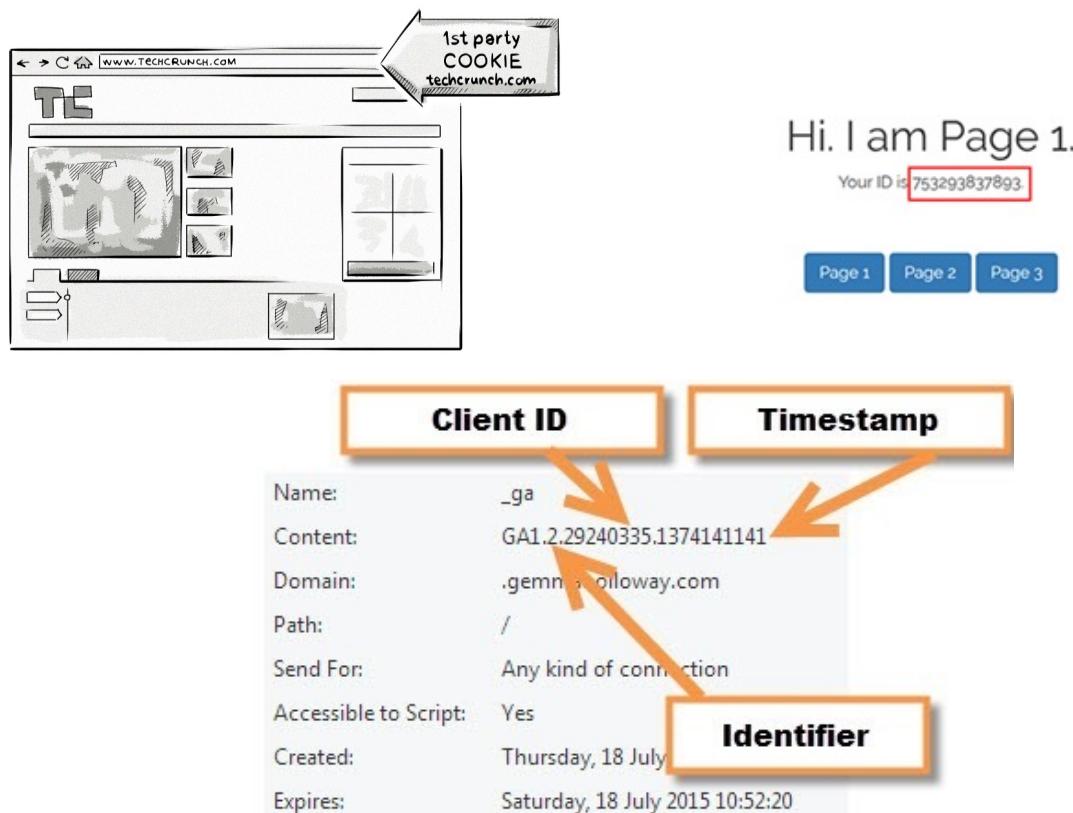
Il Regolamento Generale sulla Protezione dei Dati (GDPR) si applica a tutti i siti web con utenti dell'UE. Verifica se l'uso dei cookie e del monitoraggio online da parte del tuo sito è conforme al GDPR e alla Direttiva ePrivacy (ePR). Scopri quali dati vengono raccolti dal tuo sito e con quali terze parti sono condivisi - utile anche per la conformità al California Consumer Privacy Act (CCPA).

Indirizzo del tuo sito web VERIFICA IL MIO SITO

I cookie contengono spesso un identificatore (noto come "ID cookie") che permette di ricordare ciascun singolo utente e le sue preferenze. Tali ID cookie spesso seguono gli utenti attraverso Internet.

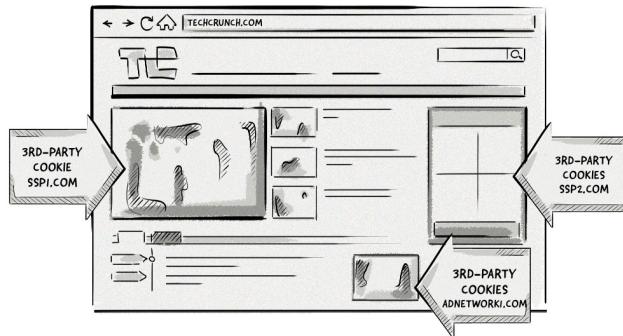
::: Il Consenso ai Cookie

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.



::: Il Consenso ai Cookie

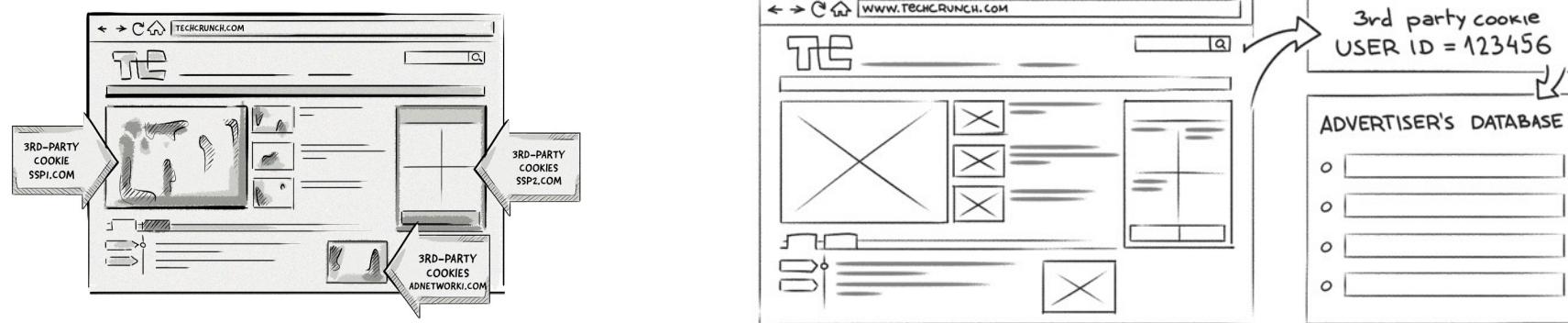
L'ID cookie è di per sé considerato un dato personale ai sensi del GDPR, perché possono essere utilizzati per generare profili dettagliati sui singoli individui, i quali vengono poi venduti alle agenzie di pubblicità online e impiegati per il marketing comportamentale.



Una pagina web contiene banner e annunci pubblicitari che sono attivati al caricamento della pagina e a cui sono passate varie informazioni.

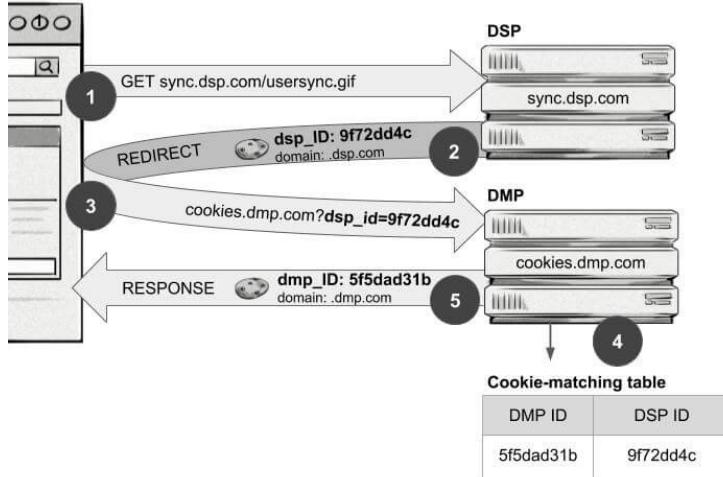
::: Il Consenso ai Cookie

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.



I cookie sono specifici del dominio, il che significa che quelli creati da un tracker di terze parti non possono essere letti da un altro. Per gli inserzionisti, questo limita la quantità di informazioni che possono raccogliere su un utente. La soluzione è quella di mappare gli ID utente da un sistema all'altro. Questo processo è noto come sincronizzazione dei cookie – **Cookie syncing**.

::: Il Consenso ai Cookie

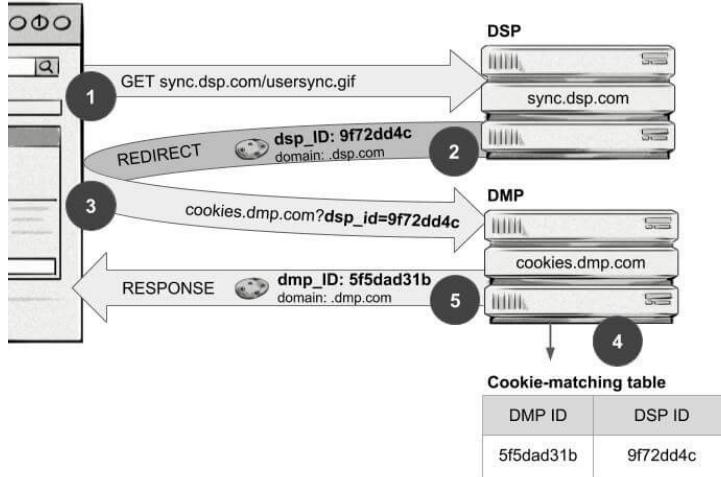


La sincronizzazione dei cookie funziona quando due diversi sistemi pubblicitari mappano gli ID univoci dell'altro e successivamente condividono le informazioni che entrambi hanno raccolto sullo stesso utente.

Ogni volta che un utente visita un sito Web che contiene annunci, il browser invia una richiesta a una piattaforma di tecnologia pubblicitaria (ad esempio un demand-side platform (DSP)).

- Il DSP crea quindi un ID utente univoco, se non ne esiste già uno, e memorizza tale ID in un cookie.
- All'interno di questa richiesta, il DSP richiama anche un pixel URL fornito da una piattaforma tecnologica pubblicitaria diversa (ad es. un data management platform (DMP)). Il DSP include il suo ID utente, come parametro nella chiamata dell'URL.

::: Il Consenso ai Cookie



La sincronizzazione dei cookie funziona quando due diversi sistemi pubblicitari mappano gli ID univoci dell'altro e successivamente condividono le informazioni che entrambi hanno raccolto sullo stesso utente.

- Il server del DMP legge l'ID utente creato dal DSP e legge il cookie nel proprio dominio per vedere se ha già un ID per questo particolare utente. Se non esiste, crea un proprio ID utente.
- Memorizza il mapping del proprio ID e di quello del DSP in una tabella di corrispondenza dei cookie. La DMP può restituire il proprio in modo che la sincronizzazione sia bidirezionale.

Questo processo di creazione dell'ID si verifica per quasi tutti gli annunci e il processo di sincronizzazione dei cookie avviene su molte piattaforme tecnologiche pubblicitarie diverse.

::: Le Informative Privacy

Il titolare del trattamento adotta le misure appropriate per fornire all'interessato tutte le informazioni relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare per quelle informazioni destinate ai minori.

Il rispetto degli obblighi di trasparenza prevede due tipi diverse di misure.

- Da un lato, si è prevista la responsabilizzazione del titolare (e del responsabile), a cui è demandata la predisposizione di misure adeguate ad assicurare fra gli altri il principio di trasparenza.
- Dall'altro, si sanziona l'inosservanza degli obblighi informativi.

Quando i dati personali sono ottenuti, il titolare del trattamento ha l'obbligo di fornire le informazioni di cui all'art. 13, par. 1 e 2:

- l'identità e i dati di contatto del titolare del trattamento o del suo rappresentante, ovvero la persona fisica o giuridica che è designata dal titolare del trattamento o dal responsabile del trattamento che non sono stabiliti nell'Unione e li rappresenta per quanto riguarda gli obblighi rispettivi a norma del GDPR;

::: Le Informative Privacy

- i dati di contatto dell'eventuale responsabile della protezione dei dati, in quanto punto di contatto anche rispetto agli interessati;
- la finalità e la base giuridica del trattamento. Se il trattamento è necessario per il perseguimento del legittimo interesse del titolare o di terzi, questi deve essere specificato;
- gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
- ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'indicazione delle condizioni che legittimano il trasferimento;
- il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- 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 dei dati;
- qualora il trattamento sia basato sul consenso espresso dall'interessato, 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 (in Italia il Garante per la protezione dei dati personali);

::: Le Informative Privacy

- 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;
- l'esistenza di un processo decisionale automatizzato, e informazioni significative sulla logica utilizzata, nonché conseguenze previste.

Il titolare del trattamento può evitare di fornire l'informativa qualora l'interessato disponga già delle informazioni, risulta impossibile o implicherebbe uno sforzo sproporzionato.

Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui sono stati raccolti, deve fornire all'interessato le seguenti ulteriori informazioni:

- indicazione della nuova finalità, e diritti dell'interessato;
- periodo di conservazione dei dati personali o, quando non è possibile i criteri utilizzati per determinare tale periodo;
- eventuale processo decisionale basato unicamente su trattamento automatizzato, logica utilizzata e conseguenze per l'interessato;

::: Le Informative Privacy

Nel caso di dati raccolti presso un soggetto diverso dall'interessato (art. 14), il contenuto dell'informativa aggiunge a quella fornita ai sensi dell'art. 13:

- origine dei dati personali, precisando se gli stessi provengano eventualmente da fonti accessibili al pubblico;
- categorie di dati personali trattati.
- Il titolare fornisce le informazioni previste all'art. 14, par. 1 e 2:
- entro un termine ragionevole dall'ottenimento dei dati personali, ma al più tardi entro un mese, in considerazione delle specifiche circostanze in cui i dati personali sono trattati;
- nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, al più tardi al momento della prima comunicazione dall'interessato;
- nel caso sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati personali;
- i dati personali debbano rimanere riservati conformemente a un obbligo di segreto professionale disciplinato dal diritto dell'Unione o degli Stati membri, compreso un obbligo di segretezza previsto per legge.

::: Data Breach



Violazioni di dati personali
(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.

Una violazione dei dati personali può avvenire anche per fatti che sono indipendenti dalla volontà di un soggetto.

Occorre valutare le condizioni oggettive con cui si verifica una violazione e non la provenienza dei comportamenti che l'hanno cagionata.

::: Data Breach

Il titolare del trattamento non è obbligato a notificare all'Autorità Garante ogni violazione dei dati personali, a meno che sia probabile che tale violazione presenti un rischio per i diritti e le libertà delle persone fisiche.

In caso di notifica, questa andrà effettuata senza ingiustificato ritardo e, qualora possibile, entro 72 ore dal momento in cui il titolare del trattamento ne è venuto a conoscenza. A tale riguardo, il responsabile del trattamento deve informare il titolare delle violazioni di cui è venuto a conoscenza, senza ingiustificato ritardo.

- Il termine di 72 ore non è tassativo, il titolare può notificare al Garante l'avvenuta violazione anche oltre tale termine, purché giustifichi i motivi del ritardo.

::... Data Breach

La notifica al Garante deve contenere almeno:

1. la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
2. il nome e dei dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
3. le probabili conseguenze della violazione dei dati personali;
4. le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

::: Data Breach

La notifica può avvenire anche per fasi successive qualora non sia possibile farlo contestualmente, purché, ancora una volta, senza ingiustificato ritardo

A prescindere dalla notifica al Garante o dalla comunicazione all'interessato, il titolare deve sempre documentare, nel c.d. Registro delle violazioni, qualsiasi violazione dei dati personali, comprese le circostanze in cui si sono manifestate, le sue conseguenze e i provvedimenti adottati per porvi rimedio.



Il Registro consente all'autorità di controllo di verificare il rispetto dell'art. 33 del GDPR.

::: Data Breach

Il Garante può prescrivere misure correttive nel caso sia rilevata una violazione delle disposizioni del Regolamento stesso, anche per quanto riguarda l'adeguatezza delle misure di sicurezza tecniche e organizzative applicate ai dati oggetto di violazione. Sono previste sanzioni pecuniarie fino a 10 milioni di euro o, nel caso di imprese, fino al 2% del fatturato totale annuo mondiale.



Il reclamo consente all'interessato di rivolgersi al Garante per la protezione dei dati personali per lamentare una violazione della disciplina in materia di protezione dei dati personali (art. 77 del Regolamento (UE) 2016/679 e artt. da 140-bis a 143 del Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento) e di richiedere una verifica dell'Autorità.



Il reclamo e l'eventuale procura dovranno essere compilati per usando il modulo su <https://www.garanteprivacy.it/modulistica-e-servizi-online/reclamo>.

::: Data Breach

Se una violazione possa presentare un rischio elevato, il titolare del trattamento è tenuto a comunicarla agli interessati, senza giustificato ritardo. Tale comunicazione deve descrive con un linguaggio semplice e chiaro la natura della violazione indicando:

- i dati di contatto del RPD o altri soggetti da cui ottenere ulteriori informazioni;
- la descrizione delle probabili conseguenze della violazione;
- le misure per porvi rimedio e attenuarne i possibili effetti negativi.

La comunicazione all'interessato non è richiesta nei seguenti casi:

- il titolare del trattamento aveva adottato misure tecniche ed organizzative adeguate per proteggere i dati personali oggetto della violazione (es. pseudonimizzazione o cifratura);
- il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato;
- detta comunicazione richiederebbe sforzi sproporzionati.

::: Data Breach



Sul sito del Garante è disponibile un modulo per la notifica di violazioni: <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9128501>.

Al fine di valutare la gravità della violazione e quindi il grado di rischio, Il WP29 (ora EDPB) suggerisce di prendere in considerazione:

- le caratteristiche particolari del titolare e degli interessati;
- il numero delle persone fisiche coinvolte;
- il tipo di violazione;
- la natura della violazione;
- il carattere sensibile e il volume dei dati personali violati;
- la facilità di identificazione delle persone fisiche interessate.



Maggiori dettagli su <https://www.aepd.es/sites/default/files/2019-09/Guide-on-personal-data-breach.pdf>.

::: Data Breach

Per calcolare il rischio, le Linee Guida propongono una formula elaborata 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 (trascutabile, 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 x EI + CB (rappresentata come bassa, media, alta, molto alta). A determinate soglie scatta la notifica e/o la comunicazione agli interessati.

::: Misure di Sicurezza

Un primo riferimento alle misure di sicurezza è contenuto nell'art. 22 del GDPR, il quale dispone che il titolare del trattamento adotti misure tecniche e organizzative idonee al fine di assicurare, ed essere poi in grado di dimostrare, che il trattamento è realizzato in modo conforme alla disciplina dettata dal Regolamento stesso.

L'art. 32 del GDPR si occupa nello specifico della sicurezza del trattamento dei dati personali: il titolare e il responsabile del trattamento dovranno predisporre ed attuare delle misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio, tenendo debitamente conto dell'attuale stato dell'arte (della tecnologica disponibile, dei sistemi informatici, ecc), dei costi di attuazione, della natura dei dati e dei meccanismi adottati, del campo di applicazione, del contesto e delle finalità del trattamento dei dati, oltre che del rischio per i diritti e le libertà delle persone fisiche che può essere più o meno probabile e più o meno alto a seconda di ciascun diverso contesto.

::: Misure di Sicurezza

Alcune delle misure che il titolare o il responsabile del trattamento dei dati potranno concretamente adottare sono, come stabilito dall'art. 32, paragrafo 1:

- la pseudo-anonimizzazione e la cifratura dei dati personali;
- 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;
- una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

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.

::: Misure di Sicurezza

- La finalità ultima è difatti quella di garantire che i dati personali non possano essere attribuiti ad una persona fisica identificata o identificabile.

Un'altra misura che potrà essere adottata è quella della cifratura dei dati, da realizzare attraverso l'utilizzo di appositi algoritmi. Consentono in una prima fase di "occultare" i dati per poi renderli disponibili in un secondo momento (solitamente attraverso un processo di autenticazione).

- Si tratta quindi di un meccanismo che permette di proteggere i dati conservati attraverso modalità che, nella maggior parte dei casi, non sono superabili o aggirabili da malintenzionati.



::: Misure di Sicurezza

- La finalità ultima è difatti quella di garantire che i dati personali non possano essere attribuiti ad una persona fisica identificata o identificabile.

Un'altra misura che potrà essere adottata è quella della cifratura dei dati, da realizzare attraverso l'utilizzo di appositi algoritmi. Consentono in una prima fase di "occultare" i dati per poi renderli disponibili in un secondo momento (solitamente attraverso un processo di autenticazione).

- Si tratta quindi di un meccanismo che permette di proteggere i dati conservati attraverso modalità che, nella maggior parte dei casi, non sono superabili o aggirabili da malintenzionati.



Dati in chiaro

Nome	Genere	Età	Colore preferito
Giulia Bianchi	Donna	23	Rosso
Michele Verdi	Uomo	35	Giallo
Antonio Rossi	Uomo	58	Blu

FONTE: @Ros_Imperiali

::: Misure di Sicurezza

- La finalità ultima è difatti quella di garantire che i dati personali non possano essere attribuiti ad una persona fisica identificata o identifiable.

Un'altra misura che potrà essere adottata è quella della cifratura dei dati, da realizzare attraverso l'utilizzo di appositi algoritmi. Consentono in una prima fase di "occultare" i dati per poi renderli disponibili in un secondo momento (solitamente attraverso un processo di autenticazione).

- Si tratta quindi di un meccanismo che permette di proteggere i dati conservati attraverso modalità che, nella maggior parte dei casi, non sono superabili o aggirabili da malintenzionati.



Dati pseudonimizzati

Identificativo	Genere	Età	Colore preferito
FQZ32A	Donna	23	Rosso
B473F3	Uomo	35	Giallo
009JHE	Uomo	58	Blu

Codice	Nome
FQZ32A	Giulia Bianchi
B473F3	Michele Verdi
009JHE	Antonio Rossi

::: Misure di Sicurezza

- La finalità ultima è difatti quella di garantire che i dati personali non possano essere attribuiti ad una persona fisica identificata o identificabile.

Un'altra misura che potrà essere adottata è quella della cifratura dei dati, da realizzare attraverso l'utilizzo di appositi algoritmi. Consentono in una prima fase di "occultare" i dati per poi renderli disponibili in un secondo momento (solitamente attraverso un processo di autenticazione).

- Si tratta quindi di un meccanismo che permette di proteggere i dati conservati attraverso modalità che, nella maggior parte dei casi, non sono superabili o aggirabili da malintenzionati.



Dati anonimizzati

Genere	Età	Colore preferito
Donna	23	Rosso
Uomo	35	Giallo
Uomo	58	Blu

::: Misure di Sicurezza

- La finalità ultima è difatti quella di garantire che i dati personali non possano essere attribuiti ad una persona fisica identificata o identificabile.

Un'altra misura che potrà essere adottata è quella della cifratura dei dati, da realizzare attraverso l'utilizzo di appositi algoritmi. Consentono in una prima fase di "occultare" i dati per poi renderli disponibili in un secondo momento (solitamente attraverso un processo di autenticazione).

- Si tratta quindi di un meccanismo che permette di proteggere i dati conservati attraverso modalità che, nella maggior parte dei casi, non sono superabili o aggirabili da malintenzionati.



::: Misure di Sicurezza

- La finalità ultima è difatti quella di garantire che i dati personali non possano essere attribuiti ad una persona fisica identificata o identifiable.

Un'altra misura che potrà essere adottata è quella della cifratura dei dati, da realizzare attraverso l'utilizzo di appositi algoritmi. Consentono in una prima fase di "occultare" i dati per poi renderli disponibili in un secondo momento (solitamente attraverso un processo di autenticazione).

- Si tratta quindi di un meccanismo che permette di proteggere i dati conservati attraverso modalità che, nella maggior parte dei casi, non sono superabili o aggirabili da malintenzionati.



::: Misure di Sicurezza

La norma fa poi riferimento al concetto di resilienza dei sistemi e dei servizi informatici che trattano i dati personali, ovvero alla capacità intrinseca di un sistema di adattarsi alle condizioni d'uso e di resistere all'usura al fine di assicurare sempre la disponibilità dei servizi che vengono forniti e la adeguata protezione dei dati che vengono trattati con tali sistemi.

La norma attribuisce rilievo anche al disaster recovery, che consiste nella capacità di reagire in modo efficace e tempestivo ad eventuali criticità dovute ad incidenti fisici o tecnici, allo scopo di ripristinare la disponibilità e l'accesso dei dati personali oggetto di trattamento.

- sarà quindi importante per i titolari predisporre un programma specifico attraverso cui analizzare innanzitutto i rischi che potrebbero andare a colpire il sistema informatico; prevedere poi le adeguate misure da adottare per minimizzarli; ed infine predisporre un piano di emergenza che permetta di attuare un sistema alternativo di elaborazione dei dati da utilizzare in attesa della completa riattivazione.

::: Misure di Sicurezza

Una valutazione di quale misura di sicurezza adottare sarà rimessa direttamente al titolare e al responsabile del trattamento, che dovranno compierla caso per caso in relazione ai rischi specificamente individuati, come stabilito del resto dallo stesso art. 32 del GDPR. Infine, è opportuno richiamare l'attenzione anche sulla possibilità dell'utilizzo di specifici codici di condotta o meccanismi di certificazione che consentano di documentare l'idoneità delle misure di sicurezza adottate.



::: Misure di Sicurezza

Per scendere nel concreto, con riferimento alle principali vulnerabilità evidenziate nei provvedimenti dei Garanti europei, emergono le seguenti misure di sicurezza.

- **Gestione degli accessi**

È una misura non di natura esclusivamente informatica, ma in primo luogo di tipo organizzativo. Una corretta gestione degli accessi permette di limitare l'accesso a determinati dati (tra cui ovviamente anche dati personali) unicamente agli utenti che ne hanno necessità per lo svolgimento delle proprie mansioni lavorative. Precisiamo che la gestione degli accessi non distingue tra categorie di persone che accedono ad un dato, e si applica tanto ad utenti interni ad un'organizzazione (come, ad esempio, dipendenti e consulenti) quanto ad utenti esterni (fornitori, clienti o semplici visitatori).

::: Misure di Sicurezza

- Autenticazione degli utenti

Con riferimento agli utenti interni all'organizzazione, l'autenticazione presuppone che ciascun utente sia dotato di un proprio account individuale. In tal modo è possibile verificare univocamente l'identità del soggetto, così riconducendo a lui con certezza le azioni compiute all'interno del sistema, facilitando il rispetto del principio di accountability. La connessione fra autenticazione e accountability è stata sottolineata dal Garante italiano, per il quale “la condivisione delle credenziali impedisce di attribuire le azioni compiute in un sistema informatico a un determinato incaricato, con pregiudizio anche per il titolare, privato della possibilità di controllare l'operato di figure tecniche così rilevanti” (provvedimento 4/4/2019). In conseguenza “l'avvenuta condivisione delle credenziali di autenticazione tra più soggetti legittimati alla gestione della piattaforma rappresenta una violazione dell'obbligo di predisposizione, da parte del responsabile del trattamento, di misure tecniche e organizzative adeguate”.

::: Misure di Sicurezza

In caso di accesso dall'esterno, occorre che l'utente sia autenticato in modo corretto. Un'errata o mancata configurazione di un'applicazione permetterebbe a terzi non autorizzati di prendere conoscenza di dati riservati. L'accesso di terzi non autorizzati a dati personali contenuti in aree clienti riservate costituisce una violazione grave della sicurezza.

I meccanismi di autenticazione possono essere vari, e devono comunque essere oggetto di specifiche politiche di generazione, utilizzo, custodia, aggiornamento e distruzione. Ad esempio, occorre impartire precise istruzioni agli autorizzati al trattamento affinché adottino le necessarie cautele per assicurare la segretezza delle loro credenziali e la sicurezza dei dispositivi necessari per l'autenticazione. Occorre prevedere delle procedure per la sostituzione degli incaricati nel caso di prolungata assenza o impedimento, al fine di assicurare la disponibilità di un particolare trattamento di dati.

::: Misure di Sicurezza

- Autorizzazione degli utenti

L'assegnazione di account individuali o l'autenticazione di un utente costituisce solo una prima misura di sicurezza, che deve essere naturalmente seguita dall'individuazione delle categorie di dati accessibili dagli account rilevanti, e, dunque, dalle autorizzazioni assegnate. La necessità di prevedere autorizzazioni specifiche emerge implicitamente dall'articolo 29 GDPR, ai sensi del quale chi agisce sotto l'autorità del titolare o del responsabile non può trattare dati personali se non è istruito in tal senso. Tale misura di sicurezza consente di restringere l'accesso ai soli dati essenziali per i quali viene effettuato l'accesso, ed è importante quanto l'autenticazione, in quanto quest'ultima sarebbe inutile se tutti gli utenti fossero autorizzati ad accedere a tutti i dati, circostanza che costituisce una violazione dell'art. 32 del GDPR. In maniera similare, secondo il Garante italiano, la mancata implementazione di sistemi di autorizzazione integra la violazione dell'articolo 5(1)(f) del GDPR.

::: Misure di Sicurezza

A livello informatico, l'autorizzazione all'accesso a dati viene di regola impostata sulla base dell'appartenenza di un utente ad un determinato gruppo, ma altre tecniche possono essere implementate, come ad esempio la restrizione di accesso al di fuori di determinati orari. I profili di autorizzazione devono definire in dettaglio tutte le azioni consentite. Le definizioni dei profili devono essere verificate periodicamente, e comunque almeno una volta l'anno.

- **Aggiornamento degli applicativi**

L'utilizzo di applicazioni non aggiornate o obsolete costituisce senza ombra di dubbio una violazione delle misure di sicurezza. Alla scoperta di vulnerabilità di una applicazione segue il rilascio di aggiornamenti. Il mancato aggiornamento rende il sistema vulnerabile, non solo perché esiste la vulnerabilità dell'applicativo, ma soprattutto perché tale vulnerabilità diventa di dominio pubblico e quindi sfruttabile da un gran numero di malintenzionati.

::: Misure di Sicurezza

Il continuo aggiornamento delle applicazioni costituisce una misura di sicurezza idonea a correggere vulnerabilità di volta in volta rese note al pubblico e corrette dagli sviluppatori. In aggiunta alla regolare installazione di patch e aggiornamenti, può essere opportuno implementare una procedura di tipo organizzativo che permetta di verificare il regolare e corretto svolgimento di tali operazioni.

- **Conservazione e condivisione dei dati**

Un'altra categoria di vulnerabilità riguarda la conservazione e la condivisione dei dati. Nonostante esista una grandissima varietà di misure di sicurezza implementabili per proteggere i dati espressamente citate dall'articolo 32(1)(a) del GDPR, per motivi pratici o tecnici non sempre è possibile implementarle o garantire il massimo livello di sicurezza possibile. Non dimentichiamo che la tecnica di protezione dei dati dovrebbe essere adeguata al trattamento dei dati che viene effettuato.

::: Misure di Sicurezza

- **La protezione dei dati trattati attivamente**

I dati trattati attivamente da un’azienda non possono essere né pseudonimizzati né cifrati (essendo necessario utilizzarli), ma devono spesso essere disponibili “in chiaro”. In tali casi le misure di sicurezza sono per lo più relative all’accesso ai dati. Per questo motivo la maggior parte delle decisioni delle autorità si focalizzano sulla sicurezza dei dati in trasmissione o archiviazione.

- **La protezione dei dati trasmessi a terzi**

Il dato che viene trasmesso a terzi può essere intercettato, il dato condiviso può subire una violazione di confidenzialità. Il Garante (provvedimento del 23 gennaio 2020) ha stabilito che “il mancato utilizzo di strumenti di crittografia per il trasporto dei dati si pone in contrasto con l’articolo 32 del GDPR”. L’utilizzo di protocolli di cifratura, come il protocollo TLS e la cifratura end-to-end delle email costituisce, quindi, una misura di sicurezza adeguata ai sensi dell’articolo 32 del GDPR.

::: Misure di Sicurezza

- **La protezione dei dati archiviati**

Quando un dato, a seguito del trattamento attivo, deve essere conservato, deve essere adeguatamente protetto. La prima misura di sicurezza può essere certamente l'implementazione e il rispetto di una data retention policy, poiché eliminando i dati non più necessari da un sistema è si riduce il rischio di violazioni. Ma anche i dati personali archiviati e non attivamente utilizzati dovrebbero essere cifrati.

- **Protezione di dati e sistemi**

I dati e i sistemi elettronici devono essere protetti da accessi non consentiti. Si impone, quindi, l'utilizzo di software di contrasto ai virus e ai malware informatici, i quali devono essere aggiornati periodicamente. Ovviamente devono essere aggiornati periodicamente anche i sistemi operativi e gli applicativi utilizzati per il trattamento dei dati. I soggetti autorizzati devono essere formati al fine di minimizzare il rischio di un utilizzo improprio degli strumenti elettronici.

::: Misure di Sicurezza

- **Procedure di continuità operativa**

I dati e i sistemi sono protetti da incidenti o violazione dei dati tramite un sistema di backup dei dati giornaliero, e una conseguente procedura di ripristino degli stessi potenzialmente da effettuarsi in tempo reale rispetto al momento della conoscenza dell'incidente, o comunque nel termine massimo di 12 ore.

- **Impostazione dei log dei sistemi**

La conservazione e l'analisi dei messaggi di log costituisce una misura di sicurezza essenziale in quanto non solo permette al titolare di essere sempre a conoscenza degli eventi che si verificano nei propri sistemi (ad esempio, accessi o operazioni compiute dagli utenti), ma soprattutto di essere sempre in grado di dimostrare l'adeguatezza delle misure di sicurezza implementate.

::: Misure di Sicurezza

Conseguentemente, la registrazione e la conservazione dei log è espressamente richiesta in diversi provvedimenti settoriali emanati dalle autorità di controllo. In assenza di log non è possibile individuare vulnerabilità, né per quanto riguarda il titolare, né per quanto riguarda le autorità di controllo. Inoltre, in assenza di log, non è possibile analizzare ex post le modalità di un attacco e, soprattutto, le conseguenze con riguardo ai dati personali conservati.

- **Misure di Auditing**

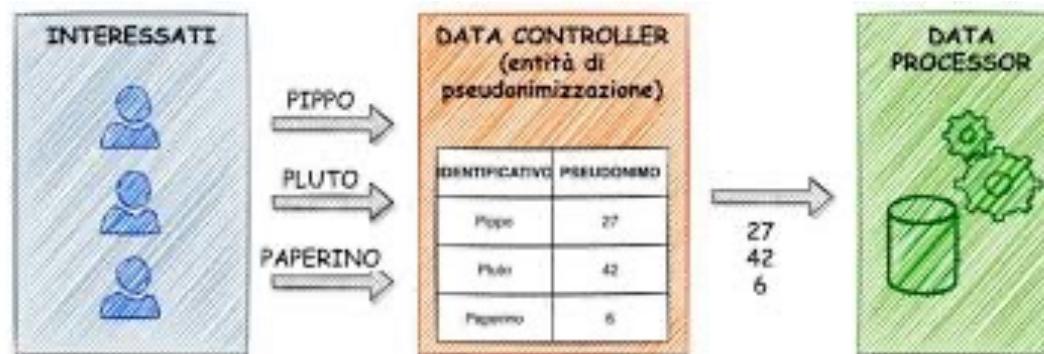
- Vulnerability scan

Strumento imprescindibile per le organizzazioni complesse o per quelle che hanno server accessibili da Internet e che, dunque, espongono dati al pubblico. Secondo l'ICO e il Garante italiano i vulnerability scan dovrebbero essere effettuati regolarmente, e comunque a seguito di cambiamenti importanti.

- Penetration test

::... (Pseudo)-Anonimizzazione

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 si può definire come pseudonimizzazione il processo di de-associazione dell'identità di un interessato dai dati personali. Il processo può essere eseguito sostituendo uno o più identificativi personali, che possono consentire l'identificazione di un soggetto, con pseudonimi.

::... (Pseudo)-Anonimizzazione

Partendo dall'Art. 4 n. 1) GDPR, “[...] si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all’ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale”.

All’articolo 4 comma 5 il GDPR definisce la pseudo-anonimizzazione come “il trattamento dei dati personali [deve avvenire] in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l’utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile”.

::: (Pseudo)-Anonimizzazione

Due standard ISO (ISO/TS 25237:2017 e ISO/IEC 20889:2017) definiscono la pseudo-anonimizzazione come “un particolare tipo di anonimizzazione” in cui si rimuove l’associazione con l’interessato e si aggiunge una associazione tra un set di informazioni con uno o più pseudonimi. Proprio in ottica GDPR, la pseudo-anonimizzazione serve a nascondere le informazioni che identificherebbero direttamente la persona fisica (interessato) mediante un set di pseudonimi.

La giusta pseudo-anonimizzazione deve poter assolvere a due dettami:

- gli pseudonimi non dovrebbero consentire una facile re-identificazione da parte di figure non autorizzate,
- non deve essere banale per un non autorizzato riprodurre gli pseudonimi.

Con il termine “non autorizzato” si intende una figura terza che non sia il data controller (o il titolare) o uno dei data processor (responsabile).

::: (Pseudo)-Anonimizzazione

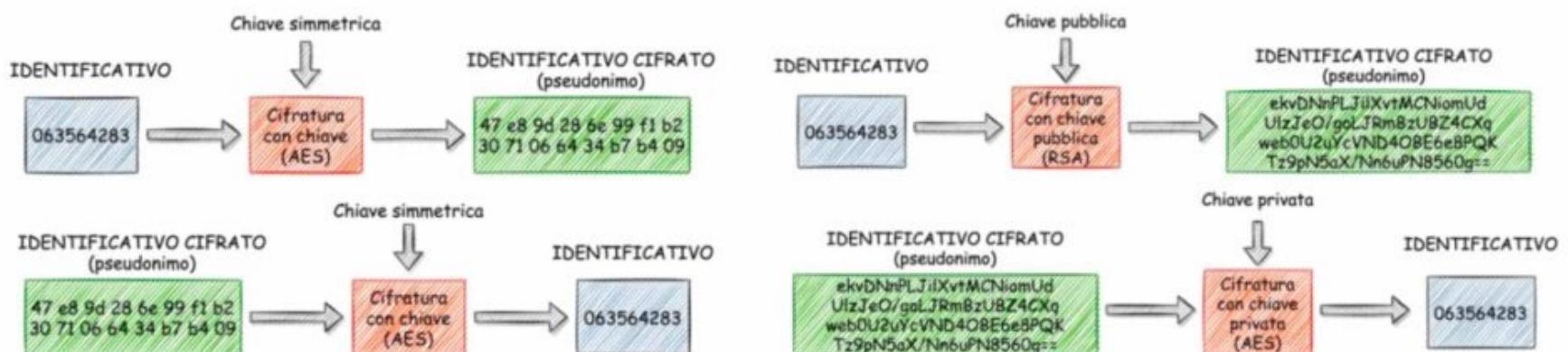
Un'altra misura che potrà essere adottata (citata nel paragrafo 1 dell'Art. 32 GDPR) è quella della cifratura dei dati, da realizzare attraverso l'utilizzo di appositi algoritmi. Consentono in una prima fase di "occultare" i dati per poi renderli disponibili in un secondo momento (solitamente attraverso un processo di autenticazione).

- Si tratta quindi di un meccanismo che permette di proteggere i dati conservati attraverso modalità che, nella maggior parte dei casi, non sono superabili o aggirabili da malintenzionati.
- La crittografia viene confusa spesso come un metodo di anonimizzazione mentre essa risulta in realtà essere uno strumento di pseudo-anonimizzazione. Le chiavi segrete utilizzate per la decrittazione sono da considerarsi come le suddette "informazioni aggiuntive", che possono rendere leggibili i dati personali e, di conseguenza, l'identificazione. Nemmeno l'eliminazione della chiave di crittografia dei dati crittografati sarebbe una soluzione adatta in ogni caso a rendere i dati anonimi.

::: (Pseudo)-Anonimizzazione

La cifratura può essere impiegata anche per la creazione di pseudonimi mediante hashing: l'identificativo originario è cifrato creando così lo pseudonimo o con chiavi simmetriche o asimmetriche (chiave pubblica e privata).

L'hashing è un metodo algoritmico (anche crittografico) che trasforma record di dati e caratteri di qualsiasi lunghezza in una sequenza di bit (o una stringa), detta digest, strettamente correlata con i dati in ingresso, tali che non è possibile risalire ai dati originari.



::... (Pseudo)-Anonimizzazione

L'**anonimizzazione** è un processo mediante il quale dati personali vengono modificati in modo irreversibile così che il titolare del trattamento, da solo o in collaborazione con altre parti, non possa più identificare direttamente o indirettamente l'interessato.

- Il GDPR prevede che i dati anonimizzati non siano considerati dati personali, in quanto non consentono l'identificazione dell'interessato. Pertanto, i dati anonimizzati non sono soggetti alle stesse restrizioni sul trattamento dei dati personali, ad esempio non è necessario il consenso dell'interessato per il loro trattamento.

L'anonymizzazione deve essere distinta dalla pseudo-anonymizzazione: la differenza fondamentale è la mancanza/presenza della “reversibilità” delle due operazioni, ciò che separa una tecnica che rientra nel GDPR da un'altra che ne è estranea.

::: (Pseudo)-Anonimizzazione

- Considerando (26) “[...] I dati personali sottoposti a pseudo-anonimizzazione, i quali potrebbero essere attribuiti a una persona fisica mediante l'utilizzo di ulteriori informazioni, dovrebbero essere considerati informazioni su una persona fisica identificabile. Per stabilire l'identificabilità di una persona è opportuno considerare tutti i mezzi, come l'individuazione, di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica direttamente o indirettamente. Per accettare la ragionevole probabilità di utilizzo dei mezzi per identificare la persona fisica, si dovrebbe prendere in considerazione l'insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici. [...]”.
- Per il Considerando (28) “l'applicazione della pseudo-anonimizzazione ai dati personali può ridurre i rischi per gli interessati e aiutare i titolari del trattamento e i responsabili del trattamento a rispettare i loro obblighi di protezione dei dati. L'introduzione esplicita della «pseudo-anonimizzazione» nel presente regolamento non è quindi intesa a precludere altre misure di protezione dei dati”.

::: (Pseudo)-Anonimizzazione

- Infine, per il Considerando (29) “al fine di creare incentivi per l’applicazione della pseudonimizzazione nel trattamento dei dati personali, dovrebbero essere possibili misure di pseudonimizzazione con possibilità di analisi generale all’interno dello stesso titolare del trattamento, qualora il titolare del trattamento abbia adottato le misure tecniche e organizzative necessarie ad assicurare, per il trattamento interessato, l’attuazione del presente regolamento, e che le informazioni aggiuntive per l’attribuzione dei dati personali a un interessato specifico siano conservate separatamente. Il titolare del trattamento che effettua il trattamento dei dati personali dovrebbe indicare le persone autorizzate all’interno dello stesso titolare del trattamento”.

Un dato pseudo-anonimizzato può correre il rischio di essere ricostruito, mentre uno anonimo non è “ricostruibile” e non è pertanto possibile re-identificare l’identità dell’utente. Ecco perché nel Considerando 75 si parla del rischio di “decifratura non autorizzata della pseudo-anonimizzazione”; e generalmente questa procedura si attua attraverso un principio di “disaccoppiamento” tra le informazioni personali di identificazione.

::: (Pseudo)-Anonimizzazione

Sebbene l'anonimizzazione al 100% sia l'obiettivo più desiderabile dal punto di vista della protezione dei dati personali, in alcuni casi non è possibile e bisogna tenere conto di un rischio residuo di nuova identificazione. Esiste il rischio che alcuni processi di anonimizzazione divengano reversibili in futuro, e, a seconda del contesto o della natura dei dati, i rischi di re-identificazione non possono essere sempre sufficientemente mitigati.

Così, un solido processo di anonimizzazione mira a ridurre il rischio di re-identificazione al di sotto di una certa soglia. Tale soglia dipenderà da diversi fattori come i controlli di mitigazione esistenti, l'impatto sulla privacy delle persone in caso di nuova identificazione, oppure le motivazioni e la capacità di un hacker di re-identificare i dati.

Il rischio è connaturato ed ineliminabile, tant'è che l'art. 15 del Codice Privacy in vigore fino al 2018 prevedeva che i danni cagionati per effetto del trattamento fossero da risarcirsi ai sensi all'art. 2050 del Codice Civile:

::... (Pseudo)-Anonimizzazione

- “Responsabilità per l’esercizio di attività pericolose” – Art 2050: “Chiunque cagiona danno ad altri nello svolgimento di un’attività pericolosa, per sua natura o per la natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee a evitare il danno”.

Dal 2018 l’art. 15 del Codice Privacy è abrogato, ma si ritiene che la responsabilità ex 2050 codice civile possa, insieme alla responsabilità aquiliana ex 2043, ancora riconoscersi come conseguenza della mancata osservanza degli obblighi imposti dal GDPR e dalla normativa ad esso correlata. L’art. 82 del GDPR al paragrafo 2 recita: “Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento. (...)”. E al paragrafo 3 si specifica: “Il titolare del trattamento (...) del trattamento è esonerato dalla responsabilità, a norma del paragrafo 2 se dimostra che l’evento dannoso non gli è in alcun modo imputabile”.

::... (Pseudo)-Anonimizzazione

Il GDPR prevede inoltre sanzioni patrimoniali amministrative con massimali dissuasivi (fino a 4 milioni o 10% del fatturato globale annuo) per chi semplicemente non osserva i dettami della normativa, ossia a prescindere dal prodursi di un danno per uno o più interessati. Sussistono però due indicazioni di principio:

- Se si devono trattare dati personali, è meglio farlo il meno possibile, lo stretto necessario al perseguimento di un legittimo scopo.
- Se possibile, è meglio non trattarli affatto.

Il primo consiglio sostanzia il cosiddetto principio di minimizzazione del trattamento, che può essere declinato in vari modi: in termini quantitativi, qualitativi e temporali. Tra questi, un ruolo decisivo possono giocarlo le tecniche di pseudonimizzazione che intervengono rendendo momentaneamente indisponibile il dato personale, minimizzando così il trattamento e di conseguenza il rischio intrinseco.

::... (Pseudo)-Anonimizzazione

Il GDPR prevede inoltre sanzioni patrimoniali amministrative con massimali dissuasivi (fino a 4 milioni o 10% del fatturato globale annuo) per chi semplicemente non osserva i dettami della normativa, ossia a prescindere dal prodursi di un danno per uno o più interessati. Sussistono però due indicazioni di principio:

- Se si devono trattare dati personali, è meglio farlo il meno possibile, lo stretto necessario al perseguitamento di un legittimo scopo.
- Se possibile, è meglio non trattarli affatto.

Il secondo precetto realizza a pieno il principio in base al quale evitando – laddove possibile – di trattare dati personali si rifugge dalle responsabilità di privacy. Il titolare può raggiungere questo traguardo astenendosi ab origine dall’acquisire uno o più insiemi di dati personali o anonimizzando quelli in suo legittimo possesso.

::... (Pseudo)-Anonimizzazione

L'anonimizzazione è un trattamento di dati personali, per cui bisogna trovare una delle condizioni di liceità elencate all'art. 6 del GDPR (diversamente, se i dati sono di natura particolare occorrerà una condizione tra quelle elencate all'art. 9, se i dati sono relativi a condanne penali o reati occorrerà una condizione tra quelle elencate all'art. 10).

- Limitando l'attenzione ai dati personali comuni, la base giuridica sarà il legittimo interesse del titolare (o del responsabile) ogniqualvolta l'operazione sarà frutto di una sua scelta intesa a mantenere il possesso delle informazioni irreversibilmente de-identificate per finalità lecite: può essere il caso dell'uso per fini statistici o storici, così come lo scopo di monitorare o migliorare i servizi offerti tramite analisi dei dati accuratamente anonimizzati.
- Può accadere che l'anonimizzazione sia imposta per legge oppure in adempimento di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri o – ancora – in esecuzione di una specifica disposizione contrattuale. Più raramente si ricorrerà al consenso.

::: 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).

In ambito comunitario, il Codice di condotta è stato utilizzato per codificare alcune disposizioni relative all'esercizio delle funzioni dei commissari europei. Questi ultimi sono nominati a titolo individuale e devono esercitare le loro funzioni in piena indipendenza. Proprio per garantire la massima indipendenza e trasparenza dell'attività istituzionale la Commissione europea ha adottato, il 17 aprile 1999, una serie di Codici di condotta che stabiliscono le regole di comportamento e di organizzazione della stessa Commissione.

::: Codici di Condotta

I codici di condotta sono stati previsti in Italia per la prima volta nel campo della protezione dei dati personali all'art. 31, comma 1, lett. h) della legge 675/96 in sede di recepimento dell'art. 27, paragrafo 3, della direttiva 95/46/CE. Con il D.lgs. n. 196/2003 hanno assunto tutt'altra rilevanza diventando oggetto di una disposizione autonoma e cioè dell'art. 12, mentre nella precedente legge rientravano semplicemente nell'elencazione dei compiti del Garante.

Indubbiamente la maggiore rilevanza di tali codici è dovuta storicamente al d.lgs. n. 467/2001 che all'art. 20 li ha introdotti allo scopo di disciplinare il trattamento dei dati personali in determinati settori quali Internet, il marketing, il campo previdenziale, i sistemi informativi adottando un modello già sperimentato per il passato in altri campi, come quello giornalistico.

::: Codici di Condotta

L'intento era di pubblicare questi codici di autodisciplina sulla Gazzetta Ufficiale. Difatti questi codici devono essere elaborati direttamente dalle parti interessate, che potranno così difendersi dal pericolo dell'uso improprio delle informazioni.

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.

Nel Regolamento Europeo n. 679/2016 continua l'incoraggiamento all'utilizzo dei codici di condotta, ma ovviamente adesso in un'ottica comunitaria.

::: Codici di Condotta

Il Regolamento GDPR all'art. 40 sancisce che gli Stati membri, le autorità di controllo, il Comitato europeo per la protezione dei dati e la Commissione incoraggiano l'elaborazione di codici di condotta destinati a contribuire alla corretta applicazione del Regolamento, in funzione delle specificità settoriali e delle esigenze specifiche delle micro, piccole e medie imprese.

Le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o responsabili del trattamento possono, quindi, elaborare i codici di condotta, modificarli o prorogarli, allo scopo di precisare l'applicazione delle disposizioni del Regolamento.

Le associazioni e gli altri organismi previsti dal Regolamento che intendono elaborare un codice di condotta o modificare o prorogare un codice esistente sottopongono il progetto di codice all'autorità di controllo, che ne esprime un parere sulla conformità al GDPR e lo approva, se ritiene che offra garanzie sufficientemente adeguate. In questo caso l'autorità di controllo registra e pubblica il codice.

::: Codici di Condotta

Qualora il progetto di codice di condotta si riferisca alle attività di trattamento in vari Stati membri, prima di approvare il progetto, la modifica o la proroga, l'autorità di controllo che è competente ai sensi dell'articolo 55 del GDPR lo sottopone, tramite la procedura di coerenza, al comitato, il quale formula un parere sulla conformità al regolamento del progetto di codice, della modifica o della proroga o, nel caso di cui al paragrafo 3 dell'art. 40 del GDPR, sulla previsione di adeguate garanzie.

Qualora il parere confermi che il progetto di codice di condotta, la modifica o la proroga è conforme al regolamento o, nel caso di cui al paragrafo 3, fornisce adeguate garanzie, il comitato trasmette il suo parere alla Commissione, che può decidere che il codice di condotta, la modifica o la proroga approvati sottoposti hanno validità generale all'interno dell'Unione, secondo l'art. 93, paragrafo 2.

::: Codici di Condotta

La Commissione provvede a dare un'adeguata pubblicità dei codici approvati per i quali è stata decisa la validità generale ai sensi del paragrafo 9 dell'art. 40 del GDPR. Il comitato raccoglie in un registro tutti i codici di condotta, le modifiche e le proroghe approvati e li rende pubblici mediante mezzi appropriati.

Sicuramente i codici di condotta assumono un ruolo molto importante. Best practice, codici di condotta e certificazioni possono essere utilizzati come elementi di prova anche dai titolari o responsabili del trattamento non soggetti all'applicazione del Regolamento.

Orientamenti per la messa in atto di opportune misure per quanto riguarda l'individuazione del rischio connesso al trattamento, la sua, e l'individuazione di migliori prassi per attenuare il rischio, sono forniti mediante codici di condotta.

::: Codici di Condotta

The screenshot shows the homepage of the Garante per la Protezione dei Dati Personal (GPDp) website. At the top, there is a blue header bar with the GPDp logo and the text 'GARANTE PER LA PROTEZIONE DEI DATI PERSONALI'. Below the header, there is a navigation menu with links to 'Home', 'L'Autorità', 'Provvedimenti e normativa', 'Attività e documenti', 'Stampa e comunicazione', 'Attività internazionali', and language selection ('Scegli la lingua: IT EN'). There are also two main sections: 'Diritti' (with 'Come tutelare i tuoi dati') and 'Doveri' (with 'Come trattare correttamente i dati'). Below the menu, a breadcrumb navigation shows 'Provvedimenti e normativa > Codici di condotta >'. A search bar with placeholder 'inserisci chiave di ricerca', search buttons ('cerca', 'testo', 'docweb'), and an advanced search link ('ricerca avanzata') are visible. On the left, a sidebar titled 'CODICI DI CONDOTTA' lists a single item: '- Codice di condotta per il trattamento dei dati personali in materia di informazioni commerciali'. To the right, there is a thumbnail image labeled 'IL TESTO DEL REGOLAMENTO' featuring the European Union flag.

L'insieme dei codici di condotta approvati sono disponibili su
<https://www.garanteprivacy.it/codici-di-condotta>.

AssoSoftware ha introdotto un Codice di Condotta (<https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10077212>), per garantire la privacy by design nei software gestionali che automatizza i processi interni delle aziende, dalla gestione delle vendite e delle fatturazioni, alla gestione del magazzino, dei clienti e dei dati contabili, fino ai processi complessi delle amministrazioni pubbliche come le gare e le commesse.



DPIA

::: Introduzione DPIA

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. Il DPIA va inquadrato come uno strumento essenziale e fondamentale per tutti i titolari e responsabili del trattamento al fine di dar corso al nuovo approccio alla protezione dei dati personali richiamato dal regolamento europeo e fortemente basato sul principio della accountability.

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.

::: Introduzione DPIA

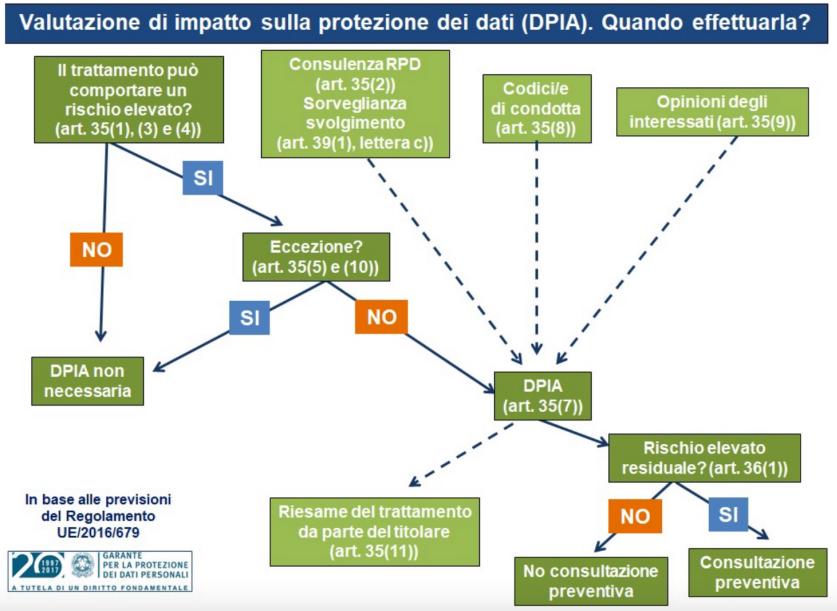
L'art. 35 del GDPR stabilisce che è necessario effettuare una DPIA in tutti i casi in cui le operazioni di trattamento presentano rischi elevati per i diritti e le libertà delle persone fisiche in virtù della loro natura, portata o finalità o quando possono procurare un danno economico o sociale importante.

La DPIA deve essere effettuata prima di procedere al trattamento, già dalla fase di progettazione del trattamento stesso anche se alcune delle operazioni di trattamento non sono ancora note, in coerenza con i principi di privacy by design e by default per determinare se il trattamento deve prevedere misure opportune in grado di mitigare i rischi.

L'aggiornamento della valutazione d'impatto sulla protezione dei dati nel corso dell'intero ciclo di vita del progetto garantirà che la protezione dei dati e della vita privata sia presa in considerazione e favorisca la creazione di soluzioni che promuovono la conformità.

::: Introduzione DPIA

La valutazione DPIA concorre, insieme ad eventuali altri processi di valutazione e gestione del rischio (es. Gestione del rischio in ambito Information Security Management System (ISMS), o ISO/IEC 27001) 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.



Ecco uno schema interessante (fonte Garante Privacy Italiano) che chiarisce il processo di valutazione della obbligatorietà di un processo DPIA e tutti gli elementi che ne concorrono.

::: Introduzione DPIA

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" (articolo 35, paragrafo 1, 3 e 4). Le linee guida WP248 (<http://www.interlex.it/2testi/autorit/wp248dpia.pdf>) 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.

The screenshot shows the GPD website's homepage. At the top, there is a navigation bar with links for 'Home', 'Diritti' (Rights), 'Come tutelare i tuoi dati', 'Doveri' (Duties), 'Come trattare correttamente i dati', and language selection ('Language: IT EN'). Below the navigation is a search bar with options for 'text' or 'docweb' and a link to 'advanced search'. A main content area displays a document titled 'Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679 - 11 ottobre 2018 [9058979]'. This document is presented as a 'CARD' with fields for 'Doc-Web:', 'Date:', and 'Type:'. At the bottom of the page, there is a footer with the 'RGPD' logo and the text 'REGOLAMENTO (UE) 2016/679 GARANTE PER LA PROTEZIONE DEI DATI PERSONALI'.

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: <https://www.garanteprivacy.it/en/home/docweb/-/docweb-display/docweb/9058979>.

::: Introduzione DPIA

Una DPIA non è richiesta nei seguenti casi:

- quando il trattamento non è tale da "presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (articolo 35, paragrafo 1);
- quando i risultati della valutazione d'impatto sulla protezione dei dati di un trattamento si possono utilizzare per un trattamento analogo (articolo 35, paragrafo 11);
- quando le tipologie di trattamento sono state verificate da un'autorità di controllo prima del maggio 2018 in condizioni specifiche che non sono cambiate;
- qualora un trattamento, effettuato a norma dell'articolo 6, paragrafo 1, lettere c) o e), trovi una base giuridica nel diritto dell'Unione o nel diritto dello Stato membro, tale diritto disciplini il trattamento specifico o sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nel contesto dell'adozione di tale base giuridica (articolo 35, paragrafo 10), a meno che uno Stato membro non abbia dichiarato che è necessario effettuare tale valutazione prima di procedere alle attività di trattamento;
- qualora il trattamento sia incluso nell'elenco facoltativo (stabilito dall'autorità di controllo) delle tipologie di trattamento per le quali non è richiesta alcuna valutazione d'impatto sulla protezione dei dati (articolo 35, paragrafo 5).

::: Introduzione DPIA

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".

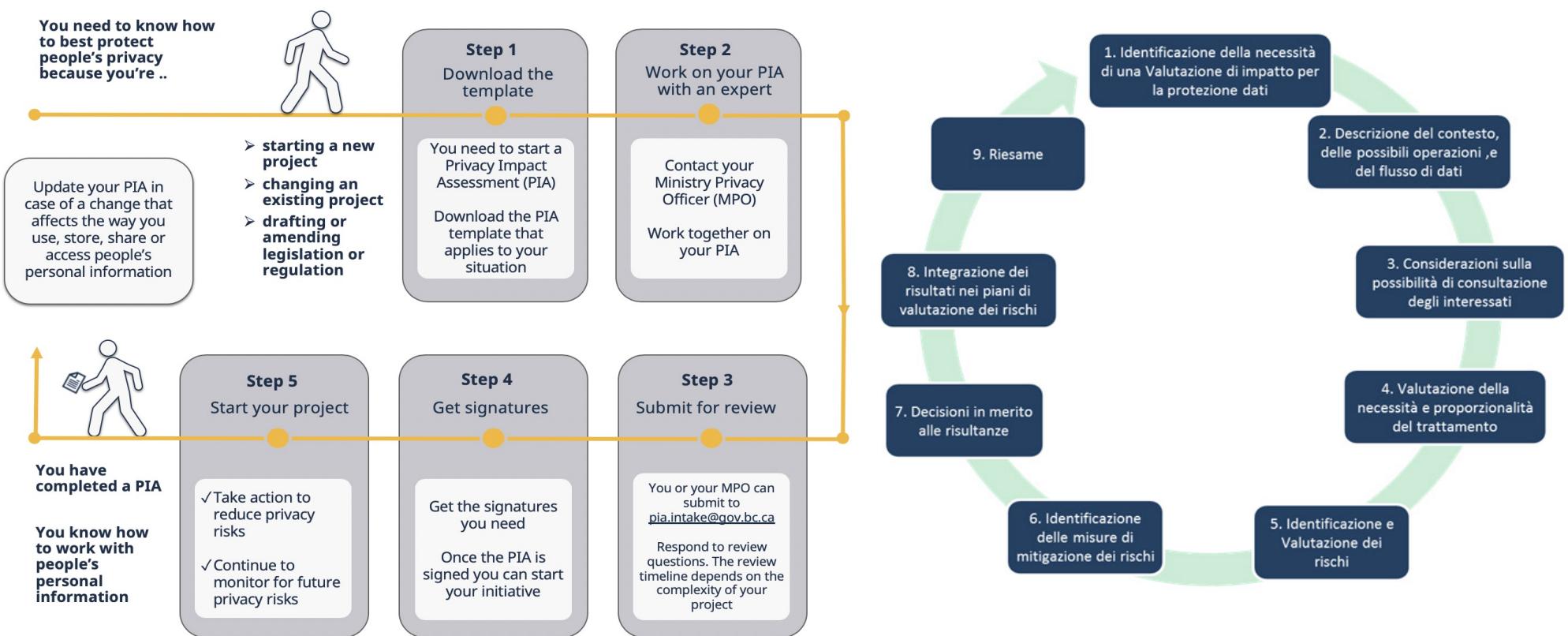
Partendo dai punti offerti dal paragrafo 7 ed integrandoli con i suggerimenti offerti dalle line guida WP248 uno schema di massima per la realizzazione di una DPIA conforme alle prescrizioni del GDPR deve includere i seguenti punti:

1. la descrizione sistematica del trattamento e delle finalità;
2. la descrizione della natura, del contesto e degli scopi del trattamento;

::: Introduzione DPIA

3. i dati personali trattati, i destinatari e il periodo per il quale sono conservati;
4. una descrizione funzionale dell'operazione di trattamento;
5. la descrizione dell'asset model su cui si basano i dati personali (es. Siti, hardware, software, reti, organizzazione, ecc.);
6. la valutazione della necessità e la proporzionalità del trattamento;
7. la descrizione delle misure previste per conformarsi al regolamento;
8. la descrizione del modo in cui sono gestiti i rischi per i diritti e le libertà degli interessati;
9. la descrizione dell'origine, della natura, della particolarità e della gravità dei rischi;
10. la determinazione delle misure previste per il trattamento di tali rischi;
11. la descrizione del modo in cui sono coinvolte le parti interessate;
12. il parere del DPO;
13. le opinioni eventualmente raccolte dagli interessati o dei loro rappresentanti.

::: Introduzione DPIA



:::... DPIA e Analisi dei Rischi

Uno degli aspetti più rilevanti nella realizzazione di un'analisi dei rischi è fissare fin da subito una metodologia definita, condivisa e ripetibile in grado di accompagnare l'azienda in un processo ricorsivo da ripetersi con cadenza puntuale o al cambiare del contesto di riferimento.

- Un'analisi dei rischi non è tanto il valore assoluto dei suoi risultati, in termini spesso “qualitativi”, ma è il confronto dei risultati rispetto alla precedente “elaborazione” che deve far comprendere all'azienda il trend di miglioramento in corso.
- L'analisi del rischio è quindi un processo per identificare e valutare il danno causabile da minacce e vulnerabilità in combinazione su uno o più Asset aziendali ben precisi.

Gli obiettivi principali dell'analisi del rischio sono identificare e quantificare l'impatto, e permettere di individuare il bilanciamento ottimale tra l'impatto e il costo delle misure di sicurezza necessarie a ridurlo.

::: DPIA e Analisi dei Rischi

Tale analisi mira a valutare una funzione che vede la possibilità di subire perdite al seguito del verificarsi di un evento dannoso rappresentabile con la seguente 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.

Si sostanzia nelle risposte alle seguenti domande:

- Quali sono i miei asset da proteggere e qual' è il loro valore? (i dati e i trattamenti)
- Cosa potrebbe accadere? (qual è la minaccia e su quale vulnerabilità può insistere?).
- Quale danno potrebbe causare (qual è l'impatto sui diritti dell'interessato?)
- Quanto spesso può accadere? (qual è la frequenza di accadimento?)

Risulta quindi chiaro che uno dei primi elementi da identificare in una analisi dei rischi è il dominio degli asset su cui intervenire e il loro valore.

:::... DPIA e Analisi dei Rischi

La DPIA ha come obiettivo minimizzare la probabilità e impatti che possibili violazioni dei dati personali potrebbe comportare agli individui (distruzione, perdita, modifica, divulgazione non autorizzata o accesso non autorizzato ai dati personali - art. 32 GDPR). Per ciò che riguarda invece il valore alla base delle analisi dei rischi in ambito GDPR deve essere chiaro che non si tratta del valore che l'informazione ha per l'azienda ma bensì al valore che il trattamento, e le relative informazioni in esso contenute, hanno per l'interessato.

Per via della complessità di un processo DPIA e relativa fase di analisi dei rischi sarebbe bene, quando possibile, affidarsi a strumenti applicativi specializzati in grado di gestire tutte le fasi del processo e in grado di riproporre la sua applicabilità nel tempo.

- 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).

:::... DPIA e Analisi dei Rischi

The screenshot shows a news article from the CNIL website. The header includes links for Publications, Glossary, FR, EN, and Cookies Management. The main title is "CNIL.". Below it is a subtitle: "To protect personal data, support innovation, preserve individual liberties". The article title is "The open source PIA software helps to carry out data protection impact assesment". It was published on "25 June 2019". The text describes the PIA software's purpose: "The PIA software aims to help data controllers build and demonstrate compliance to the GDPR. The tools is available in French and in English. It facilitates carrying out a data protection impact assessment, which will become mandatory for some processing operations as of 25 May 2018. This tool also intends to ease the use of the DPA guidance published by the CNIL". There are also icons for accessibility (AA) and a printer.

Il software è disponibile su <https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment>.

Può offrire un focus sugli elementi principali di cui si compone la procedura di DPIA. Può quindi costituire un utile supporto metodologico e di orientamento allo svolgimento di una DPIA, ma non va inteso come schema predefinito per ogni valutazione d'impatto che va integrata in ragione delle tipologie di trattamento esaminate. Può servire inoltre per comprendere meglio quali possono essere i requisiti di base di un applicativo DPIA adeguato alla propria realtà aziendale.

::: DPIA e Analisi dei Rischi

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 in 2 norme diverse:

- 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.

Anche dalla lettura della WP248 emerge che ogni trattamento deve essere analizzato dal titolare per verificare se i relativi rischi siano o no elevati.

Ne consegue che anche l'analisi implicitamente prevista dall'art.24 è finalizzata all'accertamento del livello di rischio perché solo a valle di questa il titolare può decidere se il rischio per i cittadini sia elevato o meno. Come sottolinea il WP248, prima di porre in essere un qualunque trattamento, è sempre necessaria l'analisi dei rischi che possono derivarne.

:::... DPIA e Analisi dei Rischi

La differenza tra le misure di sicurezza da adottare per via di quanto previsto dagli art. 24 e 25 e quelle che devono essere adottate per via di quanto previsto dall' art. 35 emerge solo a valle della analisi preventiva dei trattamenti, ed è sulla base di questa che il titolare dovrà decidere in concreto quali misure adottare. Quanto espresso quindi dagli art.24 e 25 può essere riconducibile al concetto di Privacy by default, applicabile quindi a tutti i trattamenti a prescindere dalla loro potenziale criticità.

Ne deriva che è sempre necessaria un'analisi dei rischi di "base" in grado di garantire una sicurezza minima e una conformità sulle modalità di trattamento su tutti i trattamenti in essere. A tal fine quindi, qualora l'azienda sia dotata di un ISMS (Information Security Management System o sistema di gestione della sicurezza delle informazioni) e abbia effettuato un'analisi dei rischi (es. per la ISO27001) tale analisi può essere utilizzata come base per valutare la conformità requisiti espressi dagli art.24 e 25 ed integrata con eventuali ulteriori criteri se necessario (estensione degli asset nel dominio dell'analisi dei rischi, ulteriori dimensioni di analisi per la Data Protection, estensione delle minacce e vulnerabilità, ecc.)

::: Standard per DPIA

Ogni processo di valutazione, essendo un insieme di attività tese al raggiungimento di un obiettivo, ha i suoi rischi. Chi si occupa di valutazione dei rischi sa bene che al fine di ridurre il più possibile il margine di errore o di interpretazione soggettiva degli scenari, è essenziale l'utilizzo di riferimenti standard, possibilmente approvati e ufficiali, anche per esigenze di rappresentazione di garanzia e affidabilità nell'esecuzione di tali delicati processi.

La famiglia di norme ISO/IEC 27000 si occupa dei sistemi di gestione per la sicurezza delle informazioni, e quindi anche degli aspetti connessi al risk assessment in ambito information security; invece la famiglia di norme ISO/IEC 29100, nata nel 2011, ha ristretto l'ambito di applicazione alla privacy (in un quadro generale più ampio della data protection regolamentata nel GDPR), e alle Personally Identifiable Information (PII) ossia le informazioni riferite a persone.

::: Standard per DPIA

La norma ISO/IEC 29134 “Information technology — Security techniques — Guidelines for privacy impact assessment”, pubblicata nel 2011 e aggiornata nel 2017, è probabilmente la norma più utilizzata, attualmente, come riferimento per la definizione, preparazione, esecuzione e predisposizione delle valutazioni di impatto privacy. Ha come obiettivo quello di fornire utili linee guida per lo svolgimento della valutazione di impatto sulla protezione dei dati, ed è indicato nelle indicazioni fornite dal Gruppo di Lavoro ex art. 29 in tema di Data Protection Impact Assessment (DPIA) all'interno del documento WP248 17/IT.

Lo standard ISO 29134 considera la DPIA come un processo che deve iniziare prima dell'effettuazione del trattamento dei dati personali, quando vi è ancora la possibilità di indirizzare il trattamento stesso (in un'ottica di “privacy by design”). Poiché le previsioni dell'art. 35 del GDPR, relativo alla DPIA, possono essere ricondotte, in qualche modo, ai requisiti della ISO/IEC 29134, molti software o tool si sono ispirati a questa norma.

::: Standard per DPIA

Non tutte le fattispecie della valutazione di impatto privacy del GDPR possono essere ricondotte ai requisiti della norma ISO/IEC 29134; ad esempio, quest'ultima non considera la valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità; né traccia specifiche indicazioni per valutare i rischi per i diritti e le libertà degli interessati, come previsto dall'art. 35 del GDPR.

La norma ISO/IEC 29134 dedica i paragrafi fondamentali, il 5, il 6 e il 7, rispettivamente a:

- preparazione delle basi per il Privacy Impact Assessment;
- linee guida sulla conduzione del processo di valutazione di impatto;
- risultanze e report del privacy impact assessment.

La ISO/IEC 29134: 2017 è una norma facoltativa che può essere utilizzata, associata alle linee guida WP248 art.29, per strutturare al meglio un processo DPIA e le relative responsabilità all'interno dell'organizzazione.

La norma fornisce inoltre spunti interessanti per la strutturazione dei report finali. All'interno dell'allegato B troviamo anche alcuni esempi di minacce che possono essere prese in considerazione durante la DPIA.

::: Standard per DPIA

La norma ISO/IEC è molto orientata ai rischi tecnici e/o comunque legati a minacce e vulnerabilità tecniche senza prendere in considerazione, al contempo, i rischi derivanti da possibili vulnerabilità non-tecniche.

Nel 2019, la norma ISO/IEC 27701:2019 – Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines ha ulteriormente esteso i controlli per realizzare, nell'ambito di un Sistema di Gestione per la Sicurezza delle informazioni (ISMS o, in italiano, SGSI) un PIMS – Personal Information Management System), un Sistema di Gestione per i dati personali.

Esistono anche importanti documenti di riferimento italiani:

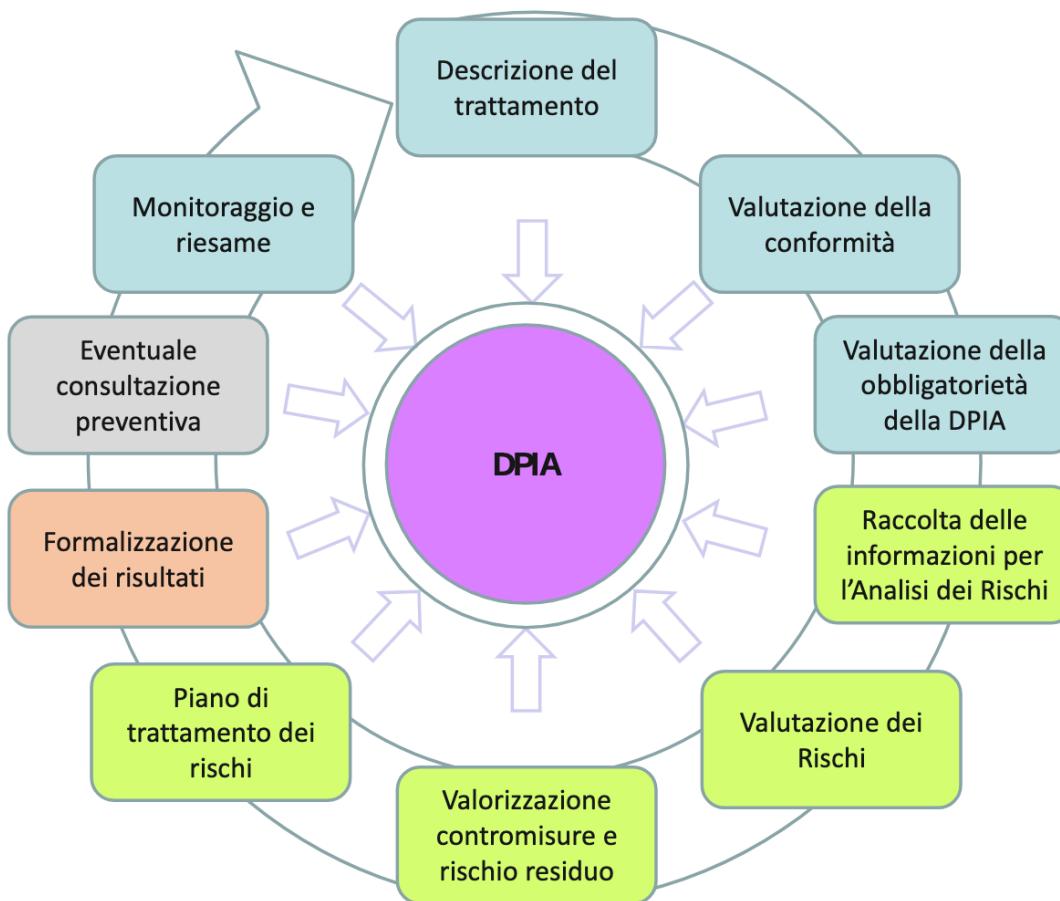
- La UNI/PdR 43.1:2018 – Linee guida per la gestione dei dati personali in ambito ICT secondo il Regolamento UE 679/2016 (GDPR) – Gestione e monitoraggio dei dati personali in ambito ICT;
- Il Framework Nazionale per la Cybersecurity e la Data Protection;
- Le Misure minime di sicurezza ICT per le pubbliche amministrazioni emanate dall'AgID (Agenzia per l'Italia digitale);
- Schema di valutazione per la conformità al GDPR ISDP10003:2018.

::: Standard per DPIA

Ulteriori spunti per una corretta definizione di un processo ed una metodologia di analisi dei rischi possono essere ricavati dalla ISO/UNI 31000:2010 che è una norma internazionale che fornisce principi e linee guida generali sulla gestione del rischio e dal “Handbook on Security of Personal Data Processing” pubblicato da ENISA (agenzia dell’Unione europea per la sicurezza delle reti e dell’informazione - centro di competenze in materia di sicurezza informatica in Europa) che fornisce spunti interessanti per la definizione degli elementi atti a quantificare i rischi in relazione alle conseguenze per l’interessato.

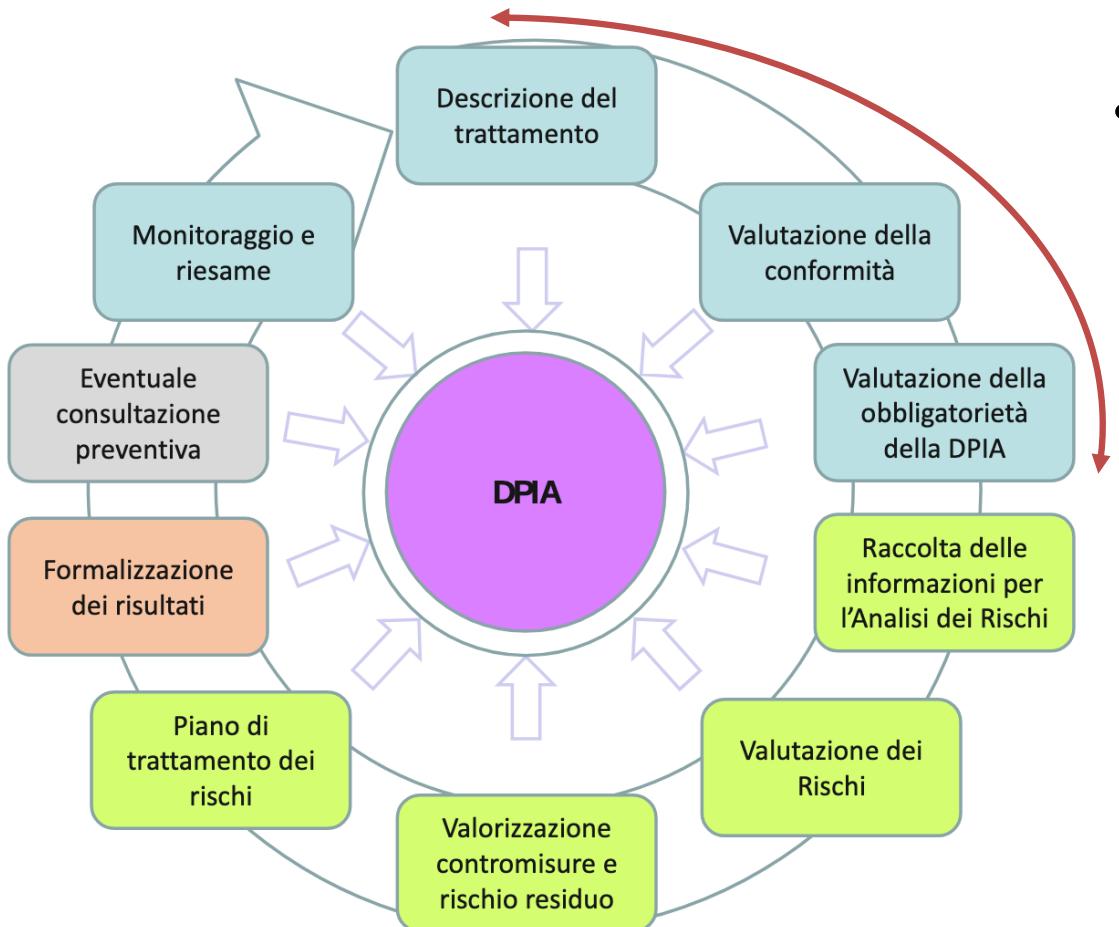
::: Il Processo DPIA

Un processo DPIA normalmente si compone di 5 fasi principali:



::: Il Processo DPIA

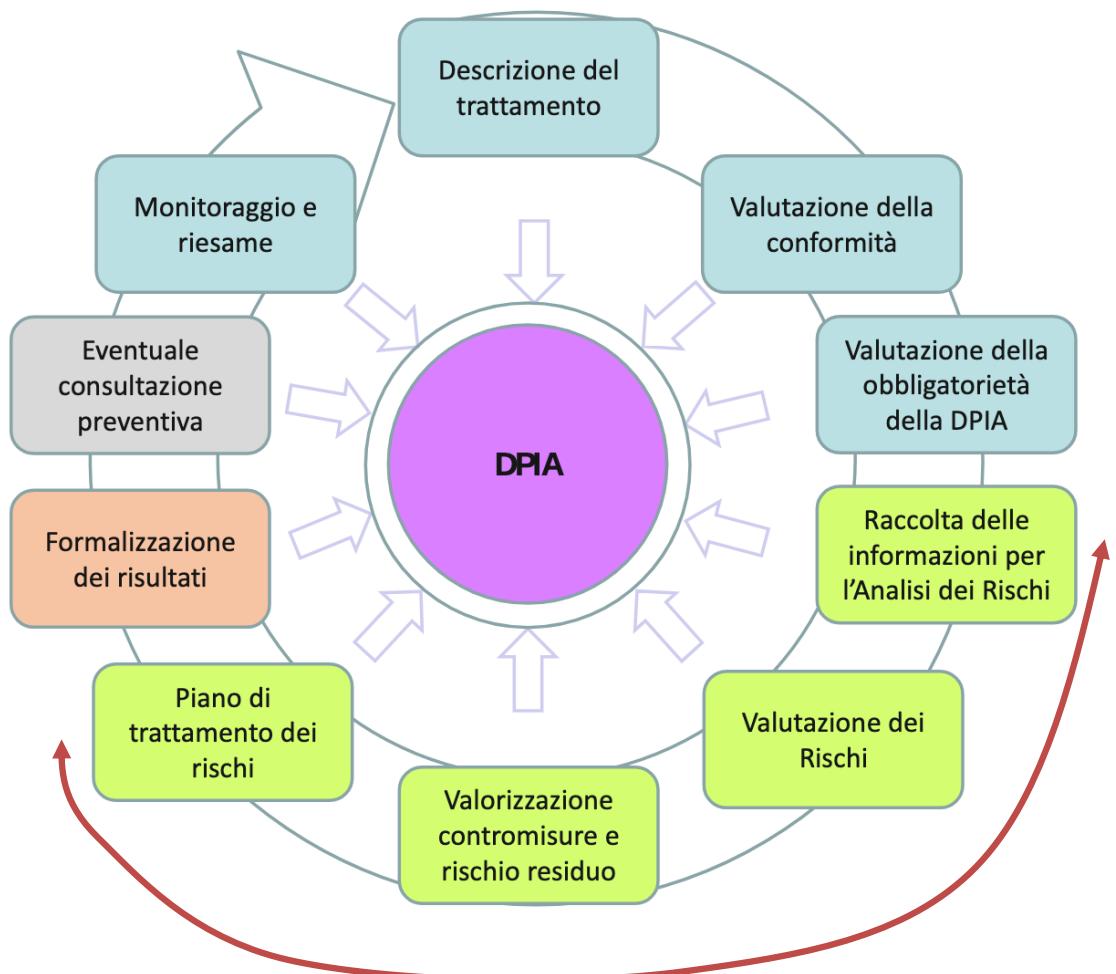
Un processo DPIA normalmente si compone di 5 fasi principali:



- Valutazione **preliminare:** raccogliere tutte le informazioni necessarie a valutare prima di tutto se il trattamento è conforme al regolamento GDPR e in seconda battuta comprendere se quel trattamento deve essere sottoposto ad una valutazione DPIA.

::: Il Processo DPIA

Un processo DPIA normalmente si compone di 5 fasi principali:



- Esecuzione DPIA: una volta determinata la necessità di procedere ad una attività di DPIA si rende necessario procedere alla raccolta delle informazioni necessarie allo sviluppo successivo delle attività di analisi dei rischi e produzione del piano dei trattamenti.

::: Il Processo DPIA

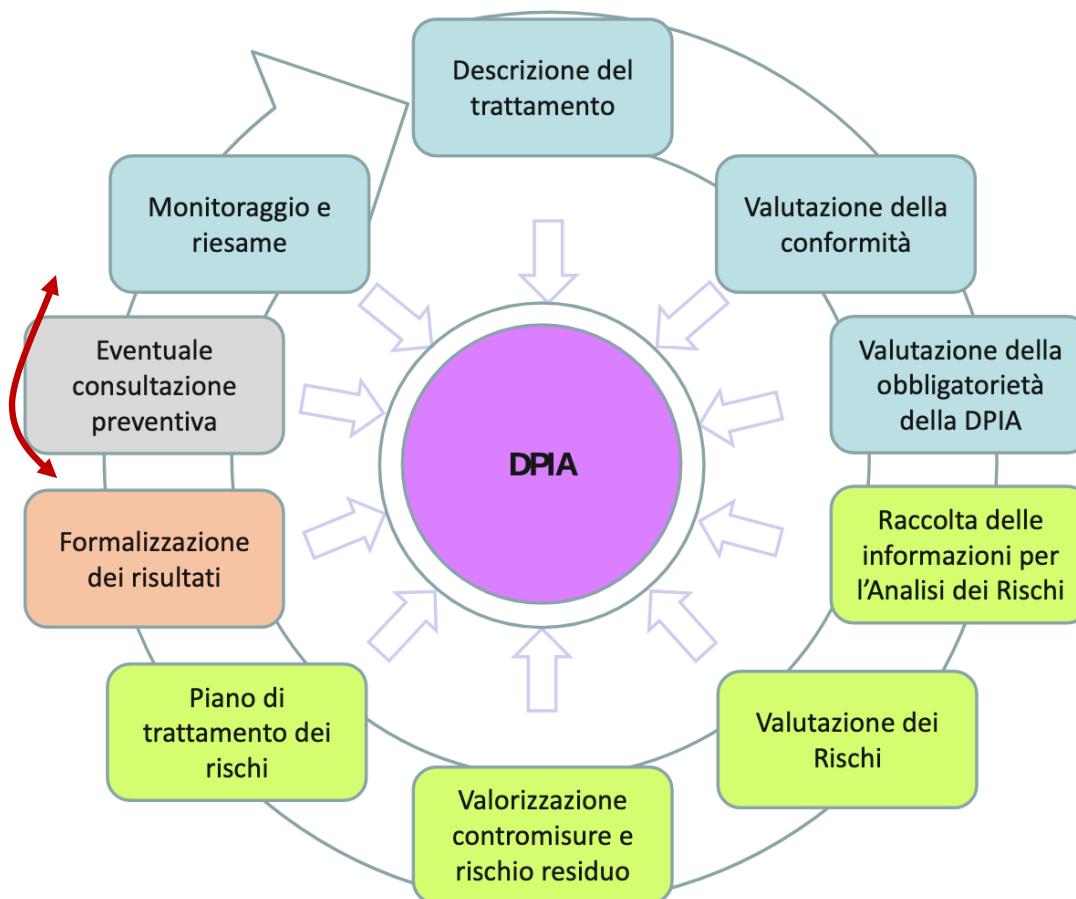
Un processo DPIA normalmente si compone di 5 fasi principali:



- Formalizzazione dei risultati: valutare se le misure individuate sono idonee a mitigare i rischi ad un livello accettabile, stimando in tal senso un rischio residuo, nonché documentare i risultati di tutte le attività svolte durante la DPIA ed i razionali che determinano la scelta se procedere o meno alla Consultazione Preventiva.

::: Il Processo DPIA

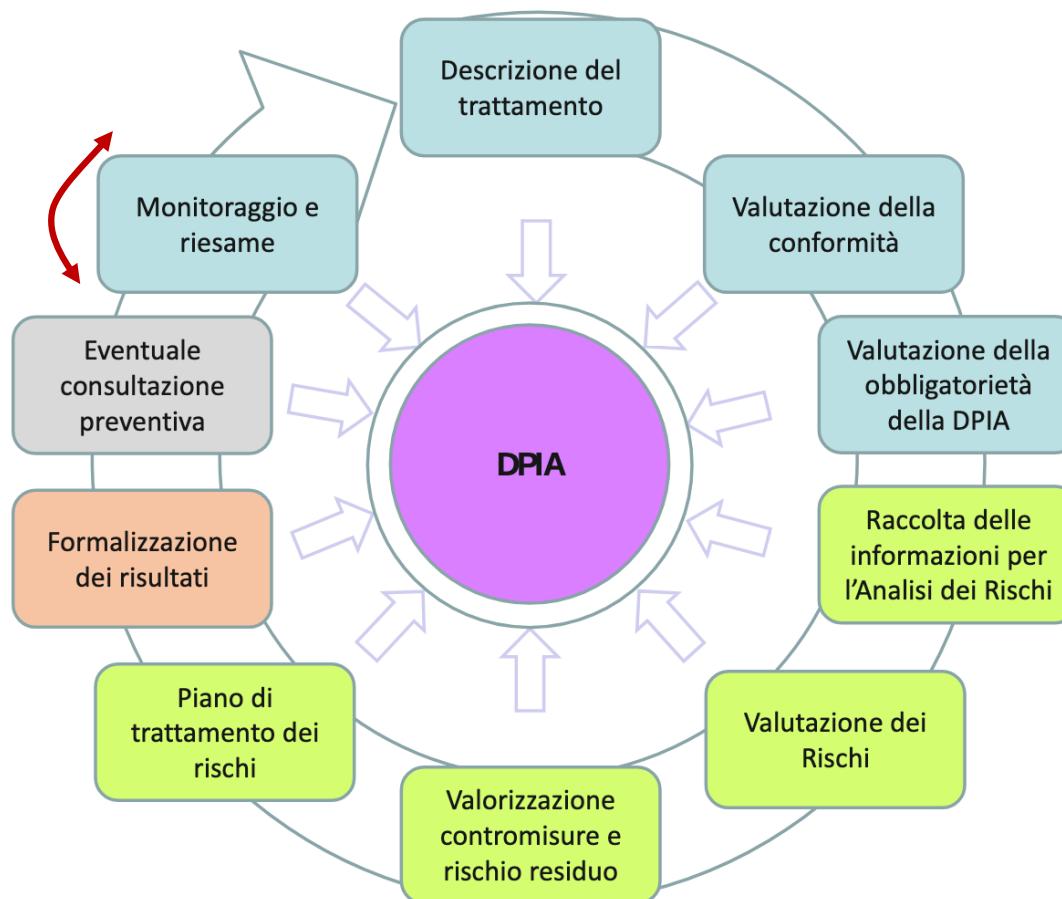
Un processo DPIA normalmente si compone di 5 fasi principali:



- Eventuale Consultazione Preventiva: consultare l'Autorità di Controllo qualora non sia stato possibile ridurre il rischio residuo a un livello accettabile. L'attività include il recepimento dell'eventuale risposta e l'attuazione degli eventuali interventi necessari per aderire al parere fornito dall'Autorità.

::: Il Processo DPIA

Un processo DPIA normalmente si compone di 5 fasi principali:



- Monitoraggio e Riesame: il processo DPIA è riconducibile al ciclo di Denim, dove le attività una volta terminate devono prevedere un monitoraggio dei risultati raggiunti e un conseguente riesame costante al fine di garantire nel tempo la mitigazione dei rischi e la conformità al Regolamento Europeo anche a fronte di fisiologici cambiamenti a cui sono soggetti tutti i trattamenti.

::: Risk Assessment

Il "Risk Assessment" o "Analisi del Rischio" è una metodologia volta alla determinazione del rischio associato a determinati pericoli o sorgenti di rischio. La terminologia di riferimento è la seguente:

- Rischio: si intende la pericolosità di un evento ed è determinato dal prodotto tra P (probabilità dell'evento) e G (gravità);
- Probabilità (P): si intende la probabilità che l'evento indesiderato si possa verificare tenendo conto delle misure precauzionali già in essere al momento della valutazione. In genere viene distinta in 3-4 classi.
- Gravità (G): la severità delle conseguenze dell'evento indesiderato. In genere viene distinta in 3-4 classi.
- Pericolo, sorgente di rischio: entità/evento che provoca danni.

L'attività di Risk Assessment si sviluppa sulla base dei seguenti step metodologici:

- Step 1: Definizione del valore di criticità dei trattamenti
- Step 2: Identificazione trattamenti critici.

::: Risk Assessment

La definizione del valore di criticità dei trattamenti è effettuata partendo dalla mappatura dei trattamenti dei dati personali effettuati e tracciati all'interno del "Registro delle attività di Trattamento" aziendale.

Per ognuno dei trattamenti mappati, il titolare procede con la valorizzazione qualitativa (SI; NO) di un certo numero variabili utili per la definizione del livello di criticità dei trattamenti.

Allegato 1 - Variabili oggetto di valutazione e relativi pesi

#	Variable	Peso della variable per la determinazione del livello di criticità del trattamento
1	Dati che rivelano l'origine razziale o etnica	3
2	Dati che rivelano le opinioni politiche	3
3	Dati che rivelano le convinzioni religiose o filosofiche	3
4	Dati che rivelano l'appartenenza sindacale	3
5	Dati genetici	3
6	Dati biometrici	3
7	Dati relativi alla salute (Appartenenza a categoria protetta o info su permessi per malattia o info su permessi per Maternità senza visibilità del referto medico)	2
8	Dati relativi alla salute (con evidenza del referto medico e/o informazioni su particolari disabilità)	3
9	Dati relativi alla vita sessuale o all'orientamento sessuale di una persona	3
10	Profilazione e/o marketing su minori	3
11	Tutte le altre variabili non comprese nelle precedenti	2

Esso sono classificate in varie categorie, corrispondenti ai principali determinanti che contribuiscono all'esposizione al rischio di ciascun trattamento.

::: Risk Assessment

La definizione del valore di criticità dei trattamenti è effettuata partendo dalla mappatura dei trattamenti dei dati personali effettuati e tracciati all'interno del "Registro delle attività di Trattamento" aziendale.

Per ognuno dei trattamenti mappati, il titolare procede con la valorizzazione qualitativa (SI; NO) di un certo numero variabili utili per la definizione del livello di criticità dei trattamenti.

Esso sono classificate in varie categorie, corrispondenti ai principali determinanti che contribuiscono all'esposizione al rischio di ciascun trattamento.

A ognuna delle variabili è associato un peso, espressione del livello di criticità associato alla variabile stessa sulla base di una scala nota a priori.

Livelli di criticità delle variabili		
Livello di criticità	Peso delle variabili	Descrizione
ALTO	3	Variabile che può determinare un alto livello di criticità in termini di accessi non autorizzati, di modifica / cancellazione / furto / e diffusione di dati personali, determinando un alto impatto sui diritti e sulle libertà delle persone fisiche
MEDIO	2	Variabile che può determinare un medio livello di criticità in termini di accessi non autorizzati, di modifica / cancellazione / furto / e diffusione di dati personali, determinando un medio impatto sui diritti e sulle libertà delle persone fisiche
BASSO	1	Variabile che può determinare un basso livello di criticità in termini di accessi non autorizzati, di modifica / cancellazione / furto / e diffusione di dati personali, determinando un basso impatto sui diritti e sulle libertà delle persone fisiche

Il valore di criticità del trattamento è ottenuto come somma del peso delle variabili valorizzate con "SI".

::: Risk Assessment

La DPIA inizia con la valutazione del Rischio Inerente, attraverso il quale viene identificato il rischio del trattamento, senza considerare gli eventuali presidi di controllo posti in essere per la sua mitigazione, combinando, sulla base di metriche predefinite, le seguenti due dimensioni:

- Impatto, o il possibile effetto che la diffusione dei dati potrebbe avere;
- Probabilità di accadimento, o la frequenza con cui il trattamento è effettuato.

Il Titolare valuta qualitativamente l'impatto e la probabilità connessi a ciascun trattamento sulla base di specifiche scale di valutazione. I valori di Impatto e Probabilità sono tradotti quantitativamente su una scala dove 1 corrisponde al valore minimo (es. Impatto Trascurabile; Probabilità rara) e 4 al valore massimo (es. Impatto Massimo; Evento probabile).

Il Rischio Inerente è calcolato quantitativamente come il prodotto tra i valori di Impatto e Probabilità associati a ciascun trattamento in un range da 1 a 16.

.... Risk Assessment

Allegato 2 - Criteri di valutazione dell'Impatto

Criteri di valutazione dell'Impatto		
Valutazione	Scala	Descrizione
MASSIMO	4	Informazioni che, se divulgate, potrebbero avere delle conseguenze quasi irreversibili per l'interessato: elevati problemi finanziari, problemi fisici e psicologici di lungo termine (es. dettagli giudiziari, dati relativi alla salute etc.).
SIGNIFICATIVO	3	Informazioni che, se divulgate, potrebbero avere significative conseguenze per l'interessato: peggioramento stato di salute, perdita del lavoro, rischio di essere inserito in black list (es. morosità esattoriale etc.).
LIMITATO	2	Informazioni che, se divulgate, potrebbero causare all'interessato problemi di carattere personale: danno economico, stress, impossibilità di accedere a determinati servizi/prodotti, lieve danno fisico (es. dettagli note spese, CV, retribuzione, benefit sociali).
TRASCURABILE	1	Informazioni quasi pubbliche che, nel caso fossero divulgate a persone non autorizzate, non creerebbero nessuna problematica all'interessato (es. dati pubblici, numero di telefono fisso privato presente negli elenchi telefonici).

Allegato 3 - Criteri di valutazione della Probabilità di accadimento

Criteri di valutazione della Probabilità di accadimento		
Valutazione	Scala	Descrizione
EVENTO PROBABILE	4	Il trattamento avviene con frequenza giornaliera (almeno una volta al giorno).
EVENTO POSSIBILE	3	Il trattamento avviene con frequenza settimanale (almeno una volta a settimana).
EVENTO IMPROBABILE	2	Il trattamento avviene con frequenza mensile/ trimestrale (almeno una volta al mese o a trimestre).
EVENTO RARO	1	Il trattamento avviene con frequenza semestrale/ annuale (almeno una volta a semestre/anno).

In seguito all'identificazione della tipologia di trattamento, il titolare effettua la valutazione dei controlli per i trattamenti in funzione della tipologia identificata:

- Tipologia di trattamento cartaceo: valutazione dei seguenti 4 controlli, definiti sulla base delle best-practice di Risk Management ISO 31001:
 - chiara identificazione di ruoli e responsabilità del controllo;
 - periodico svolgimento delle attività di controllo;
 - formale definizione dei controlli/ norme comportamentali in policy/procedure aziendali;
 - presenza di misure di sicurezza fisiche per la gestione del cartaceo (es. presenza armadi/distruggi documenti).

.... Risk Assessment

Allegato 2 - Criteri di valutazione dell'Impatto

Criteri di valutazione dell'Impatto		
Valutazione	Scala	Descrizione
MASSIMO	4	Informazioni che, se divulgate, potrebbero avere delle conseguenze quasi irreversibili per l'interessato: elevati problemi finanziari, problemi fisici e psicologici di lungo termine (es. dettagli giudiziari, dati relativi alla salute etc.).
SIGNIFICATIVO	3	Informazioni che, se divulgate, potrebbero avere significative conseguenze per l'interessato: peggioramento stato di salute, perdita del lavoro, rischio di essere inserito in black list (es. morosità esattoriale etc.).
LIMITATO	2	Informazioni che, se divulgate, potrebbero causare all'interessato problemi di carattere personale: danno economico, stress, impossibilità di accedere a determinati servizi/prodotti, lieve danno fisico (es. dettagli note spese, CV, retribuzione, benefit sociali).
TRASCURABILE	1	Informazioni quasi pubbliche che, nel caso fossero divulgate a persone non autorizzate, non creerebbero nessuna problematica all'interessato (es. dati pubblici, numero di telefono fisso privato presente negli elenchi telefonici).

Allegato 3 - Criteri di valutazione della Probabilità di accadimento

Criteri di valutazione della Probabilità di accadimento		
Valutazione	Scala	Descrizione
EVENTO PROBABILE	4	Il trattamento avviene con frequenza giornaliera (almeno una volta al giorno).
EVENTO POSSIBILE	3	Il trattamento avviene con frequenza settimanale (almeno una volta a settimana).
EVENTO IMPROBABILE	2	Il trattamento avviene con frequenza mensile/ trimestrale (almeno una volta al mese o a trimestre).
EVENTO RARO	1	Il trattamento avviene con frequenza semestrale/ annuale (almeno una volta a semestre/anno).

- Tipologia di trattamento elettronico: valutazione di 14 controlli, coincidenti con i domini dello standard ISO/IEC 27001/2013, associati a specifici obiettivi in materia di Sicurezza delle Informazioni:
 - politiche per la sicurezza delle informazioni;
 - organizzazione della sicurezza delle informazioni;
 - sicurezza delle risorse umane;
 - gestione degli asset, controllo degli accessi,crittografia;

.... Risk Assessment

Allegato 2 - Criteri di valutazione dell'Impatto

Criteri di valutazione dell'Impatto		
Valutazione	Scala	Descrizione
MASSIMO	4	Informazioni che, se divulgate, potrebbero avere delle conseguenze quasi irreversibili per l'interessato: elevati problemi finanziari, problemi fisici e psicologici di lungo termine (es. dettagli giudiziari, dati relativi alla salute etc.).
SIGNIFICATIVO	3	Informazioni che, se divulgate, potrebbero avere significative conseguenze per l'interessato: peggioramento stato di salute, perdita del lavoro, rischio di essere inserito in black list (es. morosità esattoriale etc.).
LIMITATO	2	Informazioni che, se divulgate, potrebbero causare all'interessato problemi di carattere personale: danno economico, stress, impossibilità di accedere a determinati servizi/prodotti, lieve danno fisico (es. dettagli note spese, CV, retribuzione, benefit sociali).
TRASCURABILE	1	Informazioni quasi pubbliche che, nel caso fossero divulgate a persone non autorizzate, non creerebbero nessuna problematica all'interessato (es. dati pubblici, numero di telefono fisso privato presente negli elenchi telefonici).

Allegato 3 - Criteri di valutazione della Probabilità di accadimento

Criteri di valutazione della Probabilità di accadimento		
Valutazione	Scala	Descrizione
EVENTO PROBABILE	4	Il trattamento avviene con frequenza giornaliera (almeno una volta al giorno).
EVENTO POSSIBILE	3	Il trattamento avviene con frequenza settimanale (almeno una volta a settimana).
EVENTO IMPROBABILE	2	Il trattamento avviene con frequenza mensile/ trimestrale (almeno una volta al mese o a trimestre).
EVENTO RARO	1	Il trattamento avviene con frequenza semestrale/ annuale (almeno una volta a semestre/anno).

- sicurezza fisica e ambientale e delle attività operative;
- sicurezza delle comunicazioni;
- acquisizione, sviluppo e manutenzione dei sistemi;
- relazioni con i fornitori;
- gestione degli incidenti relative alla sicurezza delle informazioni;
- disaster recovery – business continuity;
- compliance.

... Risk Assessment

Allegato 2 - Criteri di valutazione dell'Impatto

Criteri di valutazione dell'Impatto		
Valutazione	Scala	Descrizione
MASSIMO	4	Informazioni che, se divulgate, potrebbero avere delle conseguenze quasi irreversibili per l'interessato: elevati problemi finanziari, problemi fisici e psicologici di lungo termine (es. dettagli giudiziari, dati relativi alla salute etc.).
SIGNIFICATIVO	3	Informazioni che, se divulgate, potrebbero avere significative conseguenze per l'interessato: peggioramento stato di salute, perdita del lavoro, rischio di essere inserito in black list (es. morosità esattoriale etc.).
LIMITATO	2	Informazioni che, se divulgate, potrebbero causare all'interessato problemi di carattere personale: danno economico, stress, impossibilità di accedere a determinati servizi/prodotti, lieve danno fisico (es. dettagli note spese, CV, retribuzione, benefit sociali).
TRASCURABILE	1	Informazioni quasi pubbliche che, nel caso fossero divulgate a persone non autorizzate, non creerebbero nessuna problematica all'interessato (es. dati pubblici, numero di telefono fisso privato presente negli elenchi telefonici).

Allegato 3 - Criteri di valutazione della Probabilità di accadimento

Criteri di valutazione della Probabilità di accadimento		
Valutazione	Scala	Descrizione
EVENTO PROBABILE	4	Il trattamento avviene con frequenza giornaliera (almeno una volta al giorno).
EVENTO POSSIBILE	3	Il trattamento avviene con frequenza settimanale (almeno una volta a settimana).
EVENTO IMPROBABILE	2	Il trattamento avviene con frequenza mensile/ trimestrale (almeno una volta al mese o a trimestre).
EVENTO RARO	1	Il trattamento avviene con frequenza semestrale/ annuale (almeno una volta a semestre/anno).

- Tipologia di trattamento Cartaceo/Elettronico: valutazione sia dei controlli per i trattamenti cartacei, che dei controlli definiti per i trattamenti elettronici, per un totale di 18 controlli.

Ogni controllo è valutato quantitativamente su una scala a tre livelli:

- 0: Controllo nullo/assente;
- 0,5: Controllo parzialmente soddisfatto;
- 1: Controllo totalmente soddisfatto.

::: Risk Assessment

Ai fini del calcolo del Livello di Controllo, distintamente per le due tipologie di controlli (per trattamenti elettronici/Per trattamenti cartacei) è associato un peso uniforme. La valutazione del controllo per ogni trattamento è ottenuta come somma ponderata della valutazione associata a ciascun controllo per il relativo peso. Ai fini della definizione del livello di Rischio Residuo, per i Trattamenti effettuati in modalità Cartaceo/Elettronico è considerata la minore tra le valutazioni del controllo associate.

Il valore del Rischio Residuo per ciascun trattamento è definito a partire dal valore di Rischio Inerente e in considerazione del valore del controllo mediante l'applicazione del seguente algoritmo di calcolo:

Valore Rischio Residuo = Valore Rischio Inerente * (1 – Valutazione Controllo)

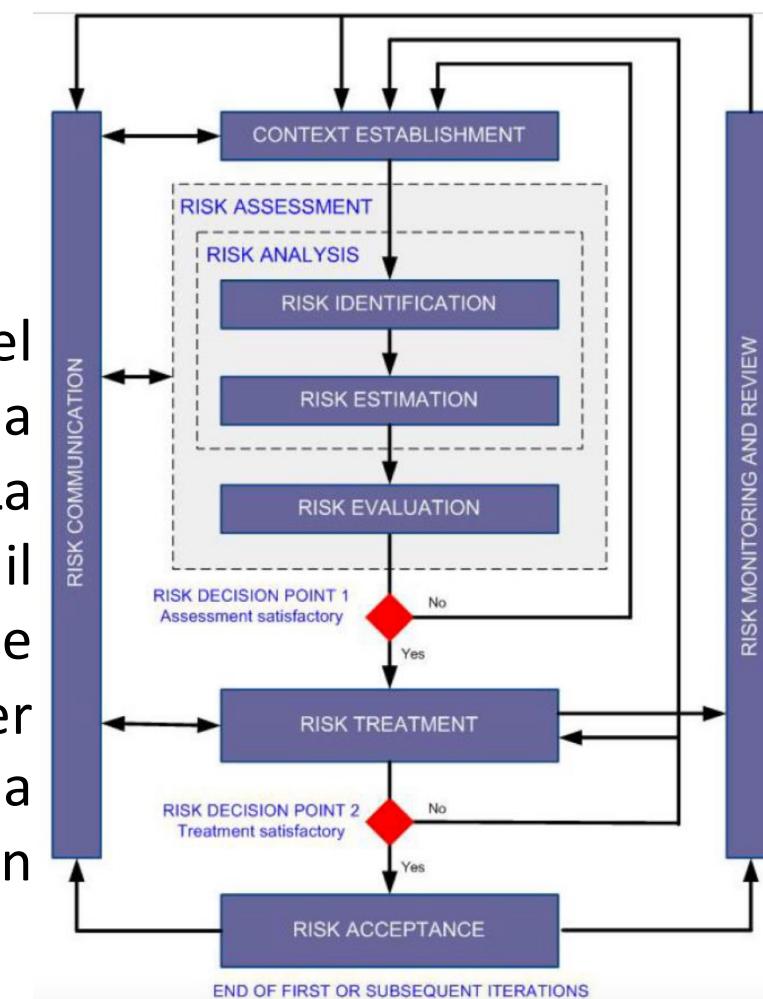
... Risk Assessment

Allegato 5 – Scala di valutazione del livello di Rischio Residuo

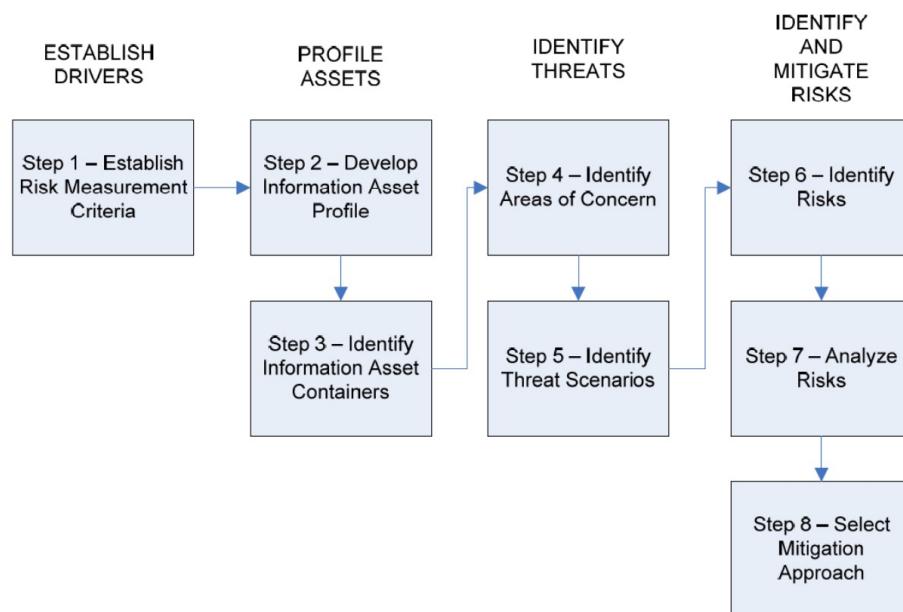
		Intervallo Numerico Rischio	
Livello Rischio Residuo		Da	a
Trascurabile	Trascurabile	0	2
	Molto - Basso	2	4
Basso	Basso	4	6
	Medio - Basso	6	8
Medio	Medio	8	10
	Medio - Alto	10	12
Alto	Alto	12	14
	Molto - Alto	14	16

ISO/IEC 27005 è lo standard di analisi del rischio per aiutare le organizzazioni a proteggere le risorse di informazioni. La ISO/IEC 27001 è lo standard che definisce il sistema di gestione della sicurezza delle informazioni (ISMS). È stato progettato per fornire requisiti per l'implementazione della sicurezza delle informazioni basata su un approccio di gestione del rischio.

Il valore ottenuto è successivamente ricondotto a una scala qualitativa ad 8 valori.



::: Risk Assessment

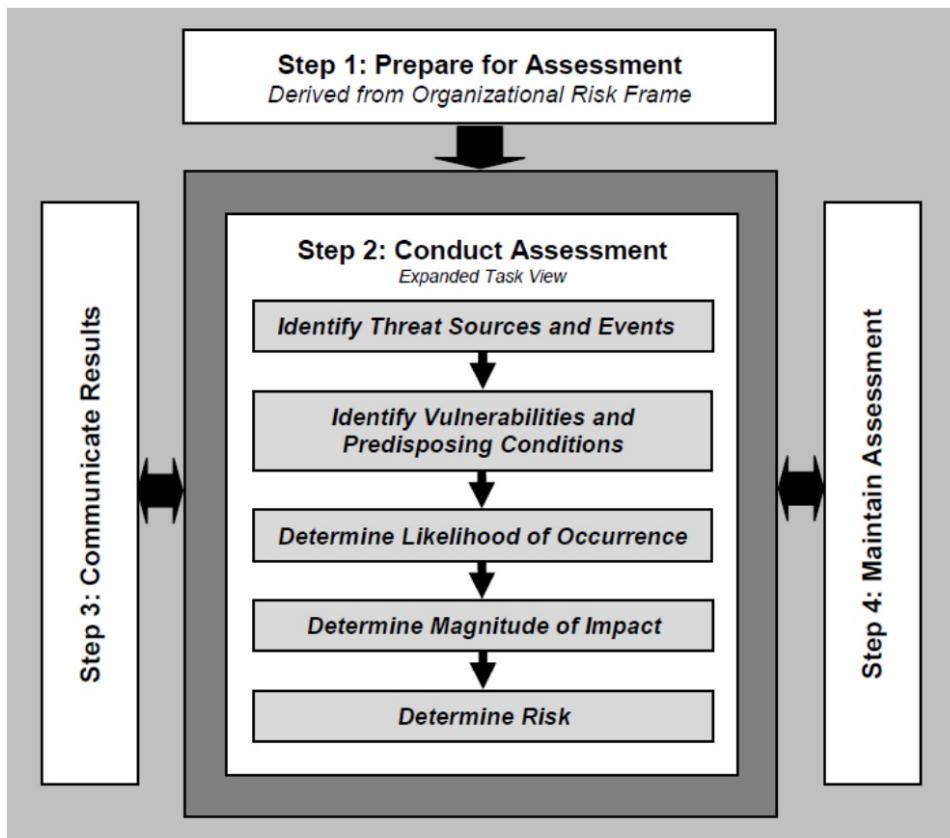


Octave Allegro è la nuova generazione della metodologia OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) per l'identificazione e la valutazione dei rischi per la sicurezza delle informazioni.

Il processo di valutazione del rischio OCTAVE è ottimizzato per fornire risultati efficienti con risorse limitate. È più adatto per organizzazioni di piccole o medie dimensioni.

Questa metodologia si concentra principalmente sulle risorse informative, come vengono utilizzate, dove vengono archiviate, trasportate ed elaborate e come sono esposte a minacce, vulnerabilità e interruzioni.

::: Risk Assessment



NIST 800-30 è uno standard sviluppato dal National Institute of Standards and Technology, negli USA, e fornisce una guida nella conduzione di analisi dei rischi, in particolare per i sistemi IT, identificando fattori di rischio specifici, monitoraggio continuo e identificazione dei cambiamenti del livello di rischio.

::: Audit

La verifica dell'adeguatezza alle norme è essenziale. L'audit sulla data protection è la valutazione e revisione dei processi aziendali per valutarne l'efficienza o il rendimento, la conformità rispetto alle politiche e alle procedure stabilite, e alle norme in materia di protezione dei dati personali, e il raggiungimento degli obiettivi dichiarati, eseguito da un esperto indipendente (auditor). Il termine audit è inglese, e viene tradotto in italiano con diversi termini: revisione, controllo, verifica.

In base alla norma italiana UNI EN ISO 19011:2012 (Linee guida per gli audit dei sistemi di gestione) l'audit è un processo sistematico, indipendente e documentato per ottenere evidenze e valutarle con obiettività, al fine di stabilire in quale misura i criteri individuati precedentemente sono stati soddisfatti. L'audit, quindi, richiede che siano rispettate scrupolosamente una serie di regole.

::: Audit

Alla base dell'attività di audit vi è una corretta valutazione del rischio. La gestione del rischio (risk management) è quel processo attraverso il quale si stima il rischio relativo ad una attività e si sviluppano le strategie per fronteggiarlo. In sostanza si tratta di individuare le possibili minacce e il correlato rischio, e quindi i danni che possono derivarne.

Sostanzialmente l'audit consiste in un'intervista al titolare del trattamento, finalizzata a conoscere in che modo i dati sono trattati, e nella verifica dei trattamenti.

Uno dei primi compiti dell'auditor è quello di comprendere, e quindi descrivere, l'azienda come sistema, in particolare redigendo un organigramma dei soggetti che svolgono compiti in materia di protezione dei dati personali.

::: Accountability

Il termine accountability è mutuato dal mondo anglosassone e indica, in generale, l'obbligo di introdurre meccanismi di responsabilizzazione e controllo al fine di garantire un efficiente utilizzo delle risorse e la produzione di risultati, sia all'interno dell'azienda sia nei confronti degli "interessati" esterni all'azienda (cc.dd. stakeholder).

- Il **principio di accountability** prescrive in capo al titolare e al responsabile l'adozione di misure giuridiche, organizzative, tecniche, anche attraverso l'elaborazione di specifici modelli organizzativi (come quelli già approntati sulla base del D.Lgs. 231/2001).
- Il principio di accountability mira a minimizzare i rischi per i diritti e le libertà fondamentali. L'obbligo per il titolare del trattamento è permanente, necessita di revisioni periodiche che tengano conto di nuovi rischi o della presenza di misure più efficaci.
- Il GDPR ha rovesciato la prospettiva della disciplina della protezione dei dati personali in quanto tutto è prevalentemente incentrato sui doveri e sulla responsabilizzazione del titolare del trattamento (o responsabile).

::: Accountability

Il titolare ha certo maggiore discrezionalità nel decidere come conformarsi alle disposizioni, ma deve essere in grado di dimostrarlo (compliance). Nessuno è escluso dall'obbligo di responsabilità, accanto al titolare anche il responsabile, il DPO e il personale incaricato devono conformare la loro attività alle prescrizioni.

L'accountability va ricercata in tutto il GDPR, procedendo in una duplice direzione:

- tutelare l'interessato con procedure trasparenti, mediante informative ai dipendenti e ai clienti, convenzioni di contitolarità con i partner e accordi con i responsabili del trattamento (fornitori e/o consulenti),
- definire i ruoli dei soggetti del trattamento dei dati, predisponendo i mansionari per dipendenti autorizzati al trattamento dei dati, indicando i designati e nominando, laddove sia necessario o comunque opportuno, il RPD.

::: Accountability

In sintesi, le principali obbligazioni di compliance previste nel GDPR sono:

- Tenuta dei registri delle attività di trattamento, mediante i quali effettuare, tra l’altro, la mappatura dei trattamenti (art. 30);
- Analisi dei rischi;
- La c.d. privacy by design e by default;
- La predisposizione di idonee misure di sicurezza (art. 32);
- la valutazione d’impatto sulla protezione dei dati – DPIA – (art. 35);
- la consultazione preventiva dell’autorità di controllo (art. 36), qualora la valutazione d’impatto all’art. 35 GDPR, mostri che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dallo stesso titolare per attenuarlo;
- la nomina di un DPO (artt. 37, 38 e 39);
- la notifica e la comunicazione di un “data breach” (artt. 33 e 34).

::: Privacy by Design e by Default

PRINCIPIO DI ACCOUNTABILITY

PRIVACY BY DESIGN

Obbligo di predisporre una struttura organizzativa, misure tecniche e procedure appropriate per conformarsi al regolamento.

PRIVACY BY DEFAULT

Devono essere adottati meccanismi tali che assicurino l'utilizzo e la raccolta dei soli dati necessari per una specifica finalità e la non conservazione dei dati oltre il tempo necessario al raggiungimento di tale scopo.

Il Regolamento GDPR introduce il principio di accountability e da ciò derivano altri due principi importanti: **privacy by design** e **privacy by default**.

Le azioni volte alla protezione dei dati sarebbero vanificate se non si intervenisse nel punto più prossimo al verificarsi di un rischio. Quando si progetta un trattamento e nel corso dello stesso, il titolare predispone adeguate misure tecniche/ organizzative (es. la pseudonimizzazione), affin-

Privacy by design e by default

art. 25 GDPR – Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita



- occorre prevedere le giuste misure di sicurezza per la tutela dei dati dal momento in cui nasce il progetto fino alla conclusione del ciclo di vita della raccolta stessa.



- il titolare del trattamento deve adottare misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, **solo i dati personali necessari per ogni specifica finalità** del trattamento.



- prevenire la raccolta di dati non necessari alle finalità perseguite dal titolare del trattamento.
- Garantire che i **dati personali non siano accessibili a un numero indefinito di persone** e che gli interessati sappiano sempre per quali finalità vengono raccolti i propri dati.

ché siano attuati i principi di protezione dei dati (ad es. la minimizzazione), oltre alle garanzie di tutela dei diritti degli interessati.

::: Privacy by Design e by Default

Le misure di sicurezza tecniche e organizzative adeguate che il titolare e il responsabile vorranno adottare deve essere scelte in relazione a diversi fattori:

- lo stato dell'arte e dei costi di attuazione di una misura;
- la natura, l'ambito di applicazione, il contesto e le finalità della soluzione in fase di progettazione che include il trattamento di dati personali;
- tutti i rischi di violazione delle disposizioni o delle garanzie per i diritti delle persone interessate, incluse le diverse probabilità e gravità dei rischi.

Impedire per impostazione predefinita che i dati personali non necessari alla specifica finalità del trattamento siano trattati per l'erogazione di un determinato servizio, ad esempio, costituisce un esempio di come approntare misure tecniche e organizzative adeguate (c.d. privacy by default).

::: Privacy by Design e by Default

L'approccio da seguire è quello della neutralità tecnologica e dunque metodologico, sulla scorta dei seguenti principi:

- proattività e non reattività – prevenire non correggere, cioè i problemi vanno valutati nella fase di progettazione, e l'applicativo deve prevenire il verificarsi dei rischi;
- privacy come impostazione di default (ad es., non deve essere obbligatorio compilare il campo di un form il cui conferimento è facoltativo);
- privacy incorporata nella progettazione (ad esempio, l'utilizzo di tecniche di pseudonimizzazione o minimizzazione dei dati);
- massima funzionalità, in modo da rispettare tutte le esigenze;
- sicurezza fino alla fine – piena protezione del ciclo di vita;
- visibilità e trasparenza di tutte le fasi operative per verificare la tutela dei dati;
- centralità dell'utente, quindi rispetto dei suoi diritti, tempestive e chiare risposte alle sue richieste di accesso.

::: Registro delle Attività di Trattamento

b) Consente l'archiviazione in maniera ordinata, organizzata e verificabile da terzi delle informazioni relative all'adozione delle misure tecniche ed organizzative adeguate ed efficaci finalizzate ad attuare il principio di accountability.

La tenuta dei registri in forma scritta (anche in formato elettronico), da parte del titolare e del responsabile del trattamento, permette di dimostrare la legittimità del trattamento e assolvere all'onere della prova, tutte le volte in cui debba essere valutata la responsabilità del titolare e/o del responsabile (art. 30, c.3, del GDPR). Infatti, su richiesta dell'autorità di controllo, tale Registro deve essere messo a sua disposizione (art. 30, c.4, del GDPR).

I titolari e i responsabili del trattamento sono tenuti a redigere il Registro delle attività di trattamento In particolare, ricorre l'obbligo di tenuta del Registro per:

- imprese o organizzazioni con almeno 250 dipendenti;

::: Registro delle Attività di Trattamento

- qualunque titolare o responsabile (in imprese o organizzazioni con meno di 250 dipendenti) che effettui trattamenti che possano presentare un rischio – anche non elevato – per i diritti e le libertà dell'interessato;
- qualunque titolare o responsabile (in imprese o organizzazioni con meno di 250 dipendenti) che effettui trattamenti non occasionali;
- qualunque titolare o responsabile (in imprese o organizzazioni con meno di 250 dipendenti) di trattamenti di particolari dati di cui all'art. 9, paragrafo 1 del GDPR, o di dati personali relativi a condanne penali e a reati di cui all'art. 10.

Alla luce di quanto detto sopra, sono tenuti all'obbligo di redazione del Registro, ad esempio:

- esercizi commerciali, esercizi pubblici o artigiani con almeno un dipendente (bar, ristoranti, officine, negozi, piccola distribuzione, ecc.) e/o che trattino dati sanitari dei clienti (es. parrucchieri, estetisti, ottici, odontotecnici, tatuatori ecc.);
- liberi professionisti con almeno un dipendente e/o che trattino dati sanitari e/o dati relativi a condanne penali o reati (es. commercialisti, notai, avvocati, osteopati, fisioterapisti, farmacisti, medici in generale);

::: Registro delle Attività di Trattamento

- associazioni, fondazioni e comitati ove trattino “categorie particolari di dati” e/o dati relativi a condanne penali o reati (ad es. organizzazioni di tendenza; associazioni a tutela di soggetti c.d. “vulnerabili” quali ad esempio malati, persone con disabilità, ex detenuti ecc.; associazioni che perseguono finalità di prevenzione e contrasto delle discriminazioni di genere, razziali, basate sull’orientamento sessuale, politico o religioso ecc.; associazioni sportive con riferimento ai dati sanitari trattati; partiti e movimenti politici; sindacati; associazioni e movimenti a carattere religioso);
- i condomini ove trattino “categorie particolari di dati” (es. delibere per interventi di superamento e all’abbattimento delle barriere architettoniche ai sensi della L. n. 13/1989; richieste di risarcimento danni comprensive di spese mediche relativi a sinistri avvenuti all’interno dei locali condominiali).

::: Registro delle Attività di Trattamento

Il GDPR non prevede né un termine entro il quale aggiornare il Registro né un obbligo espresso di aggiornamento dello stesso. Tuttavia, sulla base del principio di accountability, il titolare è tenuto a garantire la conformità dei trattamenti al GDPR nonché essere in grado di dimostrarlo. Pertanto, spetterà al titolare approntare tutte le misure per garantire un costante aggiornamento del Registro.

- Nulla toglie che possano essere riportate nel Registro informazioni ulteriori che il titolare o il responsabile ritengano utili (ad es. le modalità di raccolta del consenso, le eventuali valutazioni di impatto effettuate, l'indicazione di eventuali “referenti interni” individuati dal titolare in merito ad alcune tipologie di trattamento ecc.).



È possibile scaricare il modello di “registro semplificato” per PMI:
<https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9048342>.

::: Piano di Protezione Dati

Il Piano di Protezione Dati (PPD) individua le politiche, gli obiettivi strategici e gli standard di sicurezza per garantire la tutela dei diritti e delle libertà fondamentali delle persone fisiche rispetto alle attività di trattamento dei dati personali, definendo il quadro delle misure di sicurezza informatiche/logiche, logistiche/fisiche, organizzative e procedurali da adottare e da applicare per ridurre/eliminare il rischio di violazione dei dati derivante dal trattamento. In tale quadro, il documento disciplina, secondo i principi della norma UNI ISO 31000, il processo di gestione del rischio di violazione dei dati personali all'interno di una determinata azienda, mediante trattamento di tutti i dati personali effettuato per mezzo di strumenti di elaborazione elettronici, e di altra natura (ed esempio: Cartacei, Audio, Visivi e Audiovisivi, ecc..).

Il PPD, in attuazione del GDPR e della normativa nazionale, è funzionale alla protezione dei diritti e delle libertà fondamentali delle persone fisiche, e la sicurezza del trattamento dei dati personali, programmando e pianificando gli interventi affinché i dati personali siano:

::: Piano di Protezione Dati

- A. trattati in modo lecito, corretto e trasparente nei confronti dell'interessato (**«liceità, correttezza e trasparenza»**),
- B. raccolti per precise finalità, esplicite e legittime, e successivamente trattati; un ulteriore trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o statistici non è, conformemente all'art. 89, par 1, incompatibile con le finalità iniziali (**«limitazione della finalità»**);
- C. adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (**«minimizzazione dei dati»**);
- D. esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati (**«esattezza»**);
- E. conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati (**«limitazione della conservazione»**);
- F. trattati garantendo un'adeguata sicurezza, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali (**«integrità e riservatezza»**).



Consenso

::: Introduzione al Consenso

Il concetto di consenso di cui alla direttiva sulla protezione dei dati (direttiva 95/46/CE) e alla direttiva relativa alla vita privata e alle comunicazioni elettroniche (direttiva 2002/58/CE) si è evoluto con il regolamento (UE) 2016/679 ("regolamento generale sulla protezione dei dati"), fornendo ulteriori chiarimenti e specifiche sui requisiti per ottenere e dimostrare un consenso valido.

Il consenso rimane una delle sei basi legittime per trattare i dati personali (art. 6 GDPR). Prima di avviare attività che implicano il trattamento di dati personali, il titolare deve sempre valutare con attenzione la base legittima per il trattamento.

Di norma il consenso può costituire la base legittima appropriata solo se all'interessato vengono offerti il controllo e l'effettiva possibilità di scegliere se accettare i termini proposti o rifiutarli senza subire pregiudizio.

::: Introduzione al Consenso

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.

L'invito ad accettare il trattamento dei dati dovrebbe essere soggetto a criteri rigorosi, poiché sono in gioco i diritti fondamentali dell'interessato e il titolare del trattamento intende svolgere un trattamento che senza il consenso sarebbe illecito.

::: Introduzione al Consenso

L'ottenimento del consenso non fa venir meno né diminuisce in alcun modo l'obbligo del titolare del trattamento di rispettare i principi applicabili al trattamento sanciti nel GDPR, in particolare all'art. 5, per quanto concerne la correttezza, la necessità e la proporzionalità, nonché la qualità dei dati.

Il fatto che il trattamento dei dati personali si basi sul consenso dell'interessato non legittima la raccolta di dati non necessari a una finalità specifica di trattamento, che sarebbe fondamentalmente iniqua.

Non sono imposti obblighi supplementari in relazione al trattamento nel quadro della fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione. Il consenso rappresenta condizione preliminare per la liceità del trattamento.

::: Introduzione al Consenso

L'articolo 4, punto 11, del GDPR definisce il consenso dell'interessato come: “qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento”.

La nozione di consenso rimane sostanzialmente simile a quella della direttiva 95/46/CE, ma fornisce ulteriori indicazioni su come il titolare del trattamento deve agire per rispettare gli elementi principali del requisito del consenso.

L'inclusione, nel regolamento, di disposizioni e considerando specifici sulla revoca del consenso conferma che quest'ultimo dovrebbe essere una decisione reversibile e che l'interessato mantiene un certo grado di controllo.

::: Introduzione al Consenso

Il consenso è un prerequisito del regolamento ePrivacy. Quest'ultimo, infatti, nel disciplinare le comunicazioni elettroniche, compreso i cookie, fa riferimento alla definizione di consenso contenuta nella normativa generale, che oggi è il regolamento europeo. Di conseguenza nell'applicare la ePrivacy occorre sempre fare riferimento al consenso di cui al GDPR. Ad esempio, nella gestione dei cookie occorre che il consenso sia specifico, cioè separato per finalità.

::: Caratteristiche del Consenso

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

1. Consenso inequivocabile (unambiguous nella versione inglese) vuol dire che non è necessario che sia esplicito ma può anche essere implicito (ma non tacito), purché, nel momento in cui sia desunto dalle circostanze, non sussista alcun dubbio che col proprio comportamento l'interessato abbia voluto comunicare il proprio consenso (es. l'inerzia non può costituire manifestazione di consenso, come anche i form precompilati e caselle già presunte). Cioè deve prevedere una chiara azione positiva (come spuntare una casella od inserire la mail in un campo dove è specificata la finalità per la quale sarà usato il dato).

Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste. Se il consenso è richiesto attraverso mezzi elettronici, la richiesta deve essere chiara, concisa e non interferire immotivatamente con il servizio per il quale il consenso è espresso”.

::: Caratteristiche del Consenso

2. Il consenso deve, invece, essere **esplicito** (art. 9 GDPR) nel caso di trattamento di dati sensibili o nel caso di processi decisionali automatizzati (es. profilazione). Il consenso esplicito si può avere con una dichiarazione scritta e firmata dall'interessato o tramite l'invio di un'email, oppure raccogliendo il consenso in due passaggi: inviare un'email all'interessato, che poi dovrà confermare la prima azione di consenso.
3. Il consenso deve essere dato **liberamente**, il ché significa che 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. L'articolo 7 del GDPR chiarisce che “nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto”.

::: Caratteristiche del Consenso

Non è libero il consenso a ulteriori trattamenti dei dati personali che l'interessato debba prestare quale condizione per conseguire una prestazione richiesta (provvedimento del Garante del 31 gennaio 2008).

- Sussiste il rischio che molti dei consensi ottenuti dai servizi online possano essere ritenuti invalidi: una app mobile per il fotoritocco chiede il consenso per accedere alla geolocalizzazione e i dati vengono utilizzati a fini di pubblicità comportamentale. Ma né la geolocalizzazione, né la pubblicità sono necessari per la fornitura del servizio (fotoritocco), per cui subordinare l'uso della App a tale consenso rende il consenso non libero e quindi illecito.

Un altro problema riguarda il consenso dei dipendenti. Se il datore di lavoro richiede il consenso all'utilizzo del dato e vi è un pregiudizio reale o potenziale per il cliente non consenziente, il consenso non può ritenersi valido perché non libero. Dato lo squilibrio di potere tra datore e dipendente, quest'ultimo può dare un consenso valido solo in circostanze eccezionali. Quindi, il consenso non può costituire la base giuridica del trattamento in caso di evidente squilibrio tra le parti. In tal caso sarebbe preferibile trattare i dati su base giuridica differente.

::: Caratteristiche del Consenso

4. Il consenso deve essere **specifico**, cioè 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 (Considerando 32 GDPR).

Nel caso di titolari congiunti ogni titolare deve acquisire il consenso relativamente alle proprie finalità.

- Un caso classico riguarda i cookie, dove il consenso deve essere specifico, non può essere unico per tutti i cookie se questi hanno finalità differenti.

5. Il consenso deve essere **informato**, occorre cioè che 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.

L'informazione si ha attraverso l'apposita informativa, che diventa una vera e propria condizione di legittimità del trattamento.

::: Caratteristiche del Consenso

6. Consenso **verificabile** non vuol dire che il consenso deve essere documentato per iscritto, ma che l'azienda deve essere in grado di dimostrare che l'interessato lo ha conferito con riferimento a quello specifico trattamento. L'azienda dovrà dimostrare anche a quale informativa l'utente ha acconsentito, distinguendo tra le varie versioni.

Il WP29 suggerisce di utilizzare un registro nel quale siano conservate le informazioni relative alla sessione in cui è stato espresso il consenso, unitamente alla documentazione del flusso di lavoro del consenso, e una copia delle informazioni presentate all'interessato in quel momento.

7. Il consenso deve essere **revocabile** in qualsiasi momento. La revoca deve essere facile così come lo è dare il consenso. Non vi è alcun obbligo di motivare la revoca, a seguito della quale il trattamento deve interrompersi, a meno che non sussista una differente base giuridica.

Per revocare il consenso, quindi, il titolare dovrebbe predisporre una procedura analoga a quella offerta per concedere il consenso, oppure effettuare una comunicazione.

::: Caratteristiche del Consenso

Con la revoca si innesca il diritto di cancellazione. Ovviamente vi sono motivi legittimi in base ai quali un'azienda ha necessità di conservare alcuni dati dell'utente anche dopo la revoca del consenso, come ad esempio mantenere un registro delle transazioni per motivi fiscali. In ogni caso l'azienda può avvertire l'interessato che a seguito della revoca del consenso, vi sarà la cancellazione dei dati e la conseguente impossibilità di fornire ulteriori servizi.

Occorre tenere presente che il consenso non dura per sempre.

- Quando si raccolgono dati personali occorre informare l'interessato della durata della conservazione (e quindi trattamento) del dato, scaduta la quale il dato va o anonimizzato oppure cancellato.

Data la durata limitata del consenso, in alcuni casi potrebbe essere preferibile una base giuridica diversa dal consenso, come ad esempio i legittimi interessi del titolare del trattamento.

Il consenso dei minori è valido a partire dai 16 anni di età. Prima dei 16 anni occorre raccogliere il consenso dei genitori o di chi ne fa le veci.



Oltre il GDPR

::: Nuovi Strumenti Normativi

GDPR

95/46 EC

REGULATION (EU) No XXX/2016
OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
on the protection of individuals with regard to the processing of personal data and on
the free movement of such data (General Data Protection Regulation)

DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 24 October 1995

on the protection of individuals with regard to the processing of personal data and on the free
movement of such data

Article 2 – Definitions

(a) '**Personal Data**' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

eIDAS

REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT
AND OF THE COUNCIL
of 23 July 2014

on electronic identification and trust services for electronic
transactions in the internal market and repealing Directive 1999/93/EC

Article 3 – Definitions

(13) '**Trust Service**' means an electronic service normally
provided for remuneration which consists of:
(a) the creation, verification, and validation of
electronic signatures, electronic seals or electronic
time stamps, electronic registered delivery services
and certificates related to those services, or
(b) the creation, verification and validation of
certificates for website authentication; or
(c) the preservation of electronic signatures, seals
or certificates related to those services;

NIS

Directive of the European Parliament and of the Council concerning measures
to ensure a high common level of network and
information security across the Union

Article 3 – Definitions

(11d) '**Digital Service**' means a service within the meaning of
point (b) of Article 1 of Directive 2015/1535 which is of a type
listed in Annex III.

Note:

Annex III. Online Marketplace; Online Search Engine; Cloud Computing service

Directive 2015/1535 Article 1

(1b) 'service' means any Information Society service, that is to say, any service
normally provided for remuneration, at a distance, by electronic means and at the
individual request of a recipient of services.

2018

::: Network and Information Security

La direttiva 2016/1148 sulla sicurezza delle reti e delle informazioni (NIS) mirava a raggiungere un livello comune elevato di sicurezza informatica in tutta l'UE. Sebbene abbia aumentato le capacità di cybersicurezza degli Stati membri, la sua attuazione si è rivelata difficile, con conseguente frammentazione a diversi livelli nel mercato interno.

Con il Decreto Legislativo 18 maggio 2018, n.65, l'Italia ha dato attuazione alla Direttiva NIS e si applica a

- gli Operatori di Servizi Essenziali (OSE) - i soggetti, pubblici o privati, che forniscono servizi essenziali per la società e l'economia nei settori sanitario, dell'energia, dei trasporti, bancario, delle infrastrutture dei mercati finanziari, della fornitura e distribuzione di acqua potabile e delle infrastrutture digitali;
- Fornitori di Servizi Digitali (FSD) - le persone giuridiche, né "piccole" o "micro", che forniscono servizi di e-commerce, cloud computing o motori di ricerca, con stabilimento principale, sede sociale o rappresentante designato sul territorio nazionale.

::: Network and Information Security

Tanto gli OSE che gli FSD:

- sono chiamati ad adottare misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi e a prevenire e minimizzare l'impatto degli incidenti a carico della sicurezza delle reti e dei sistemi informativi, al fine di assicurare la continuità del servizio;
- hanno l'obbligo di notificare, senza ingiustificato ritardo, gli incidenti che hanno un impatto rilevante al Computer Security Incident Response Team (CSIRT).

**Un incidente a carico di un FSD è rilevante
se si verifica almeno una delle seguenti condizioni**

Indisponibilità del servizio fornito per oltre 5.000.000 di ore utente

Perdita di integrità, autenticità o riservatezza dei dati per oltre 100.000 utenti dell'UE

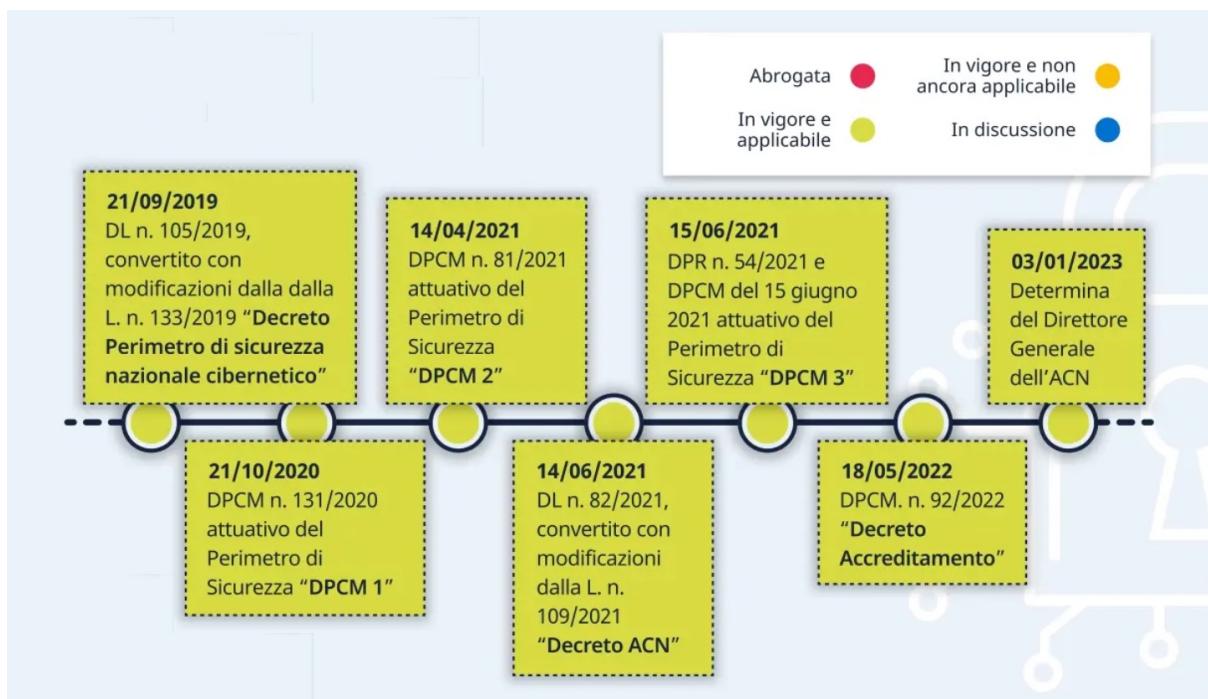
Rischio per la sicurezza e/o l'incolumità pubblica, o in termini di perdite di vite umane

Danni materiali superiori a 1.000.000 di EUR per almeno un utente nell'UE

I soggetti giuridici non identificati come OSE e che non sono FSD possono inoltrare al CSIRT notifiche volontarie degli incidenti che abbiano un impatto rilevante.

::: Perimetro Cibernetico

Il Perimetro di Sicurezza Nazionale Cibernetica è stato istituito con Decreto Legge 105/2019 convertito con Legge 133/2019) al fine di assicurare un “livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti pubblici e privati che rivestono un’importanza strategica nel panorama nazionale”. Il Decreto Perimetro si affianca quindi al Decreto NIS, per rafforzare e complementare il quadro di sicurezza informativa nazionale.



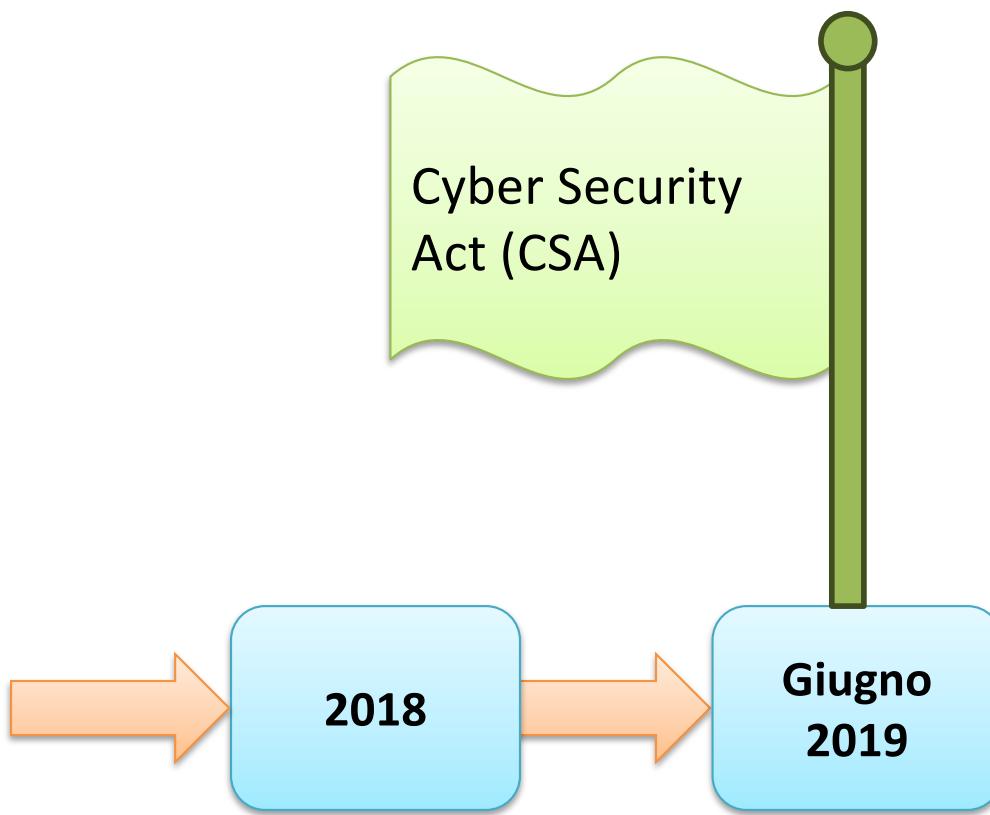
Generalmente, i soggetti che rientrano nel NIS ricadono anche all’interno del Perimetro di Sicurezza. Il Perimetro di Sicurezza, al contrario, ha un ambito di applicazione più ampio e include anche operatori che potrebbero non ricadere nel NIS.

::: Perimetro Cibernetico

Il Decreto Perimetro individua gli obblighi a cui sono soggetti chi è compreso nell'ambito del Perimetro imponendo loro:

- la predisposizione e l'aggiornamento, almeno annuale, di elenchi dei beni ICT “strategici” dal cui malfunzionamento, interruzione o utilizzo improprio possa derivare un pregiudizio per la sicurezza nazionale;
- l’obbligo di notificare gli incidenti di sicurezza aventi impatto sui beni ICT (secondo i criteri e le modalità definiti dal DPCM 2) al CSIRT;
- l’obbligo di implementare adeguate misure di sicurezza (come meglio dettagliate dal DPCM 2);
- l’obbligo di comunicare l’intenzione di acquisire beni, sistemi e servizi ICT destinati ad essere impiegati sui loro asset strategici a enti appositamente istituiti (Centri di Valutazione (“CV”) e al Centro di Valutazione e Certificazione Nazionale (“CVCN”) per consentire i necessari controlli di sicurezza e affidabilità (come specificato dai decreti attuativi DPCM 3).

::: Nuovi Strumenti Normativi



::: CyberSecurity Act

Il CyberSecurity Act (CSA) dell'UE è entrato in vigore il 27 giugno 2019, rafforzando il mandato dell'Agenzia europea per la sicurezza informatica (ENISA) e lanciando il quadro europeo di certificazione della sicurezza informatica per prodotti, processi e servizi digitali ICT.

La certificazione è volontaria, ma è in valutazione l'obbligatorietà di questa certificazione per specifiche categorie di prodotti e servizi.

- Si basa su Common Criteria, sulla Common Methodology for Information Technology Security Evaluation e sugli standard corrispondenti, rispettivamente, ISO/IEC 15408 e ISO/IEC 18045.
- Il CSA pone l'accento sulla categorizzazione di prodotti e servizi in base ai casi d'uso e alle capacità computazionali.
- Secondo l'art. 52, vengono specificati tre possibili livelli di certificazione: livello base, sostanziale o elevato. Il livello è commisurato al rischio associato al previsto uso del prodotto, servizio o processo, in termini di probabilità e impatto di un incidente.

::: CyberSecurity Act

Il Cybersecurity Act definisce 3 livelli differenti di certificazione:

1. Livello base - è sufficiente svolgere un riesame della documentazione tecnica, una valutazione delle possibili attività sostitutive equivalenti e si può ricorrere all'autocertificazione.
2. Livello sostanziale – si prevede una valutazione di sicurezza effettuata per ridurre al minimo i rischi di cyber-attacchi commessi da soggetti che dispongono di risorse e abilità limitate. Sarà necessario valutare che non ci siano vulnerabilità pubblicamente note, e successivamente, ci siano tutte le necessarie funzionalità di sicurezza.
3. Livello elevato - la valutazione di sicurezza viene effettuata per ridurre al minimo il rischio di cyber-attacchi commessi da soggetti che dispongono di risorse e abilità specifiche e significative. Le valutazioni di sicurezza richiedono che non esistano vulnerabilità pubblicamente note, si attuino regolarmente le funzioni avanzate di sicurezza e si garantisca la resistenza agli attacchi di soggetti qualificati (mediante specifici test di penetrazione).

::: CyberSecurity Act

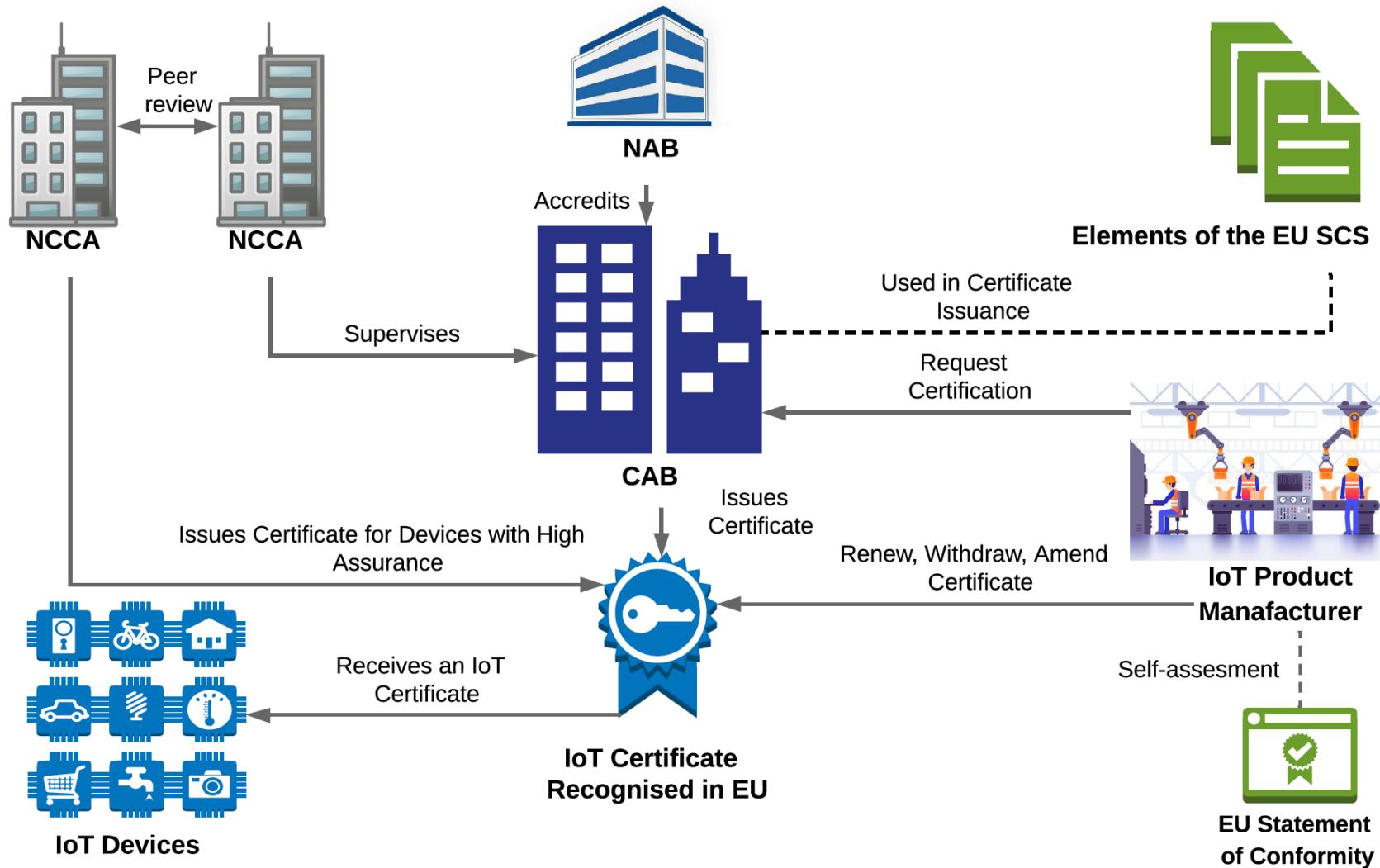
L'infrastruttura di certificazione si compone dei seguenti elementi:

- Un Organismo di Valutazione della Conformità (CAB) è responsabile dell'esecuzione della procedura di valutazione ed è una terza parte indipendente, visto che non è né il produttore nè il fornitore del prodotto/servizio/processo da valutare.
- Un Organismo Nazionale di Accreditamento (NAB) è responsabile dell'accreditamento dei CAB se soddisfano le specifiche dei requisiti.
- Gli schemi di certificazione di sicurezza (SCS) dovrebbero abilitare la funzionalità di autovalutazione per il livello di garanzia Base in cui il produttore/fornitore stesso è responsabile della valutazione dell'obiettivo.
- In caso di autovalutazione da parte dei produttori, è obbligatorio che rilascino e presentino una dichiarazione di conformità UE all'ENISA e all'Autorità nazionale di certificazione della sicurezza informatica (NCCA).

::: CyberSecurity Act

- Una NCCA è un ente di fondamentale importanza in quanto è responsabile della supervisione di molti aspetti dell'intero processo di certificazione.
 - Dovrebbe fornire ai NAB competenze e informazioni.
 - Dovrebbe convalidare i CAB che soddisfano i requisiti stabiliti nello schema e autorizzarli a effettuare valutazioni e certificazioni.
 - Tutti i reclami da parte di persone giuridiche riguardanti i certificati emessi devono essere indirizzati e gestiti dall'NCCA.
 - L'NCCA dovrebbe collaborare con altre autorità nazionali o NCCA, condividendo informazioni sulla potenziale non conformità dei prodotti o sui problemi con i requisiti del SCS o della legge sulla sicurezza informatica dell'UE.
 - La richiesta di emissione del certificato viene inoltrata all'NCCA dal CAB laddove un SCS UE richiede un livello di garanzia Alto.

::: CyberSecurity Act



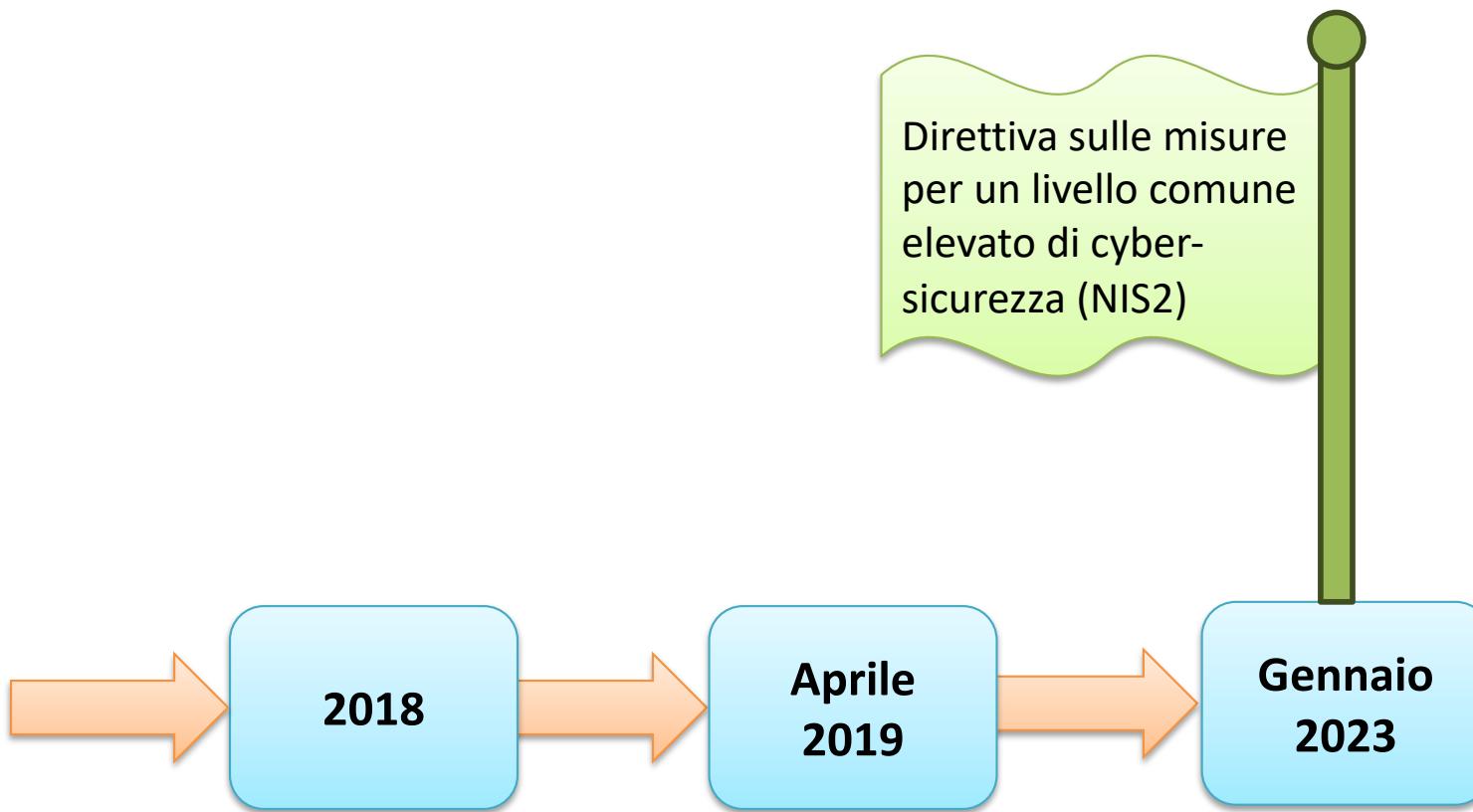
::: Network and Information Security



Gli obiettivi fondamentali della strategia nazionale di cybersicurezza da perseguire sono stati definiti da ACN come risposta alle minacce, agli incidenti e alle crisi cyber nazionali, attraverso sistemi di monitoraggio, rilevamento, analisi e attivazione di processi che coinvolgano l'intero ecosistema di cybersicurezza nazionale.

Il quadro strategico nazionale cybersecurity comprende la protezione degli asset strategici nazionali, attraverso un approccio sistematico orientato alla gestione e mitigazione del rischio, formato sia da un quadro normativo che da misure, strumenti e controlli.

::: Nuovi Strumenti Normativi



::: Network and Information Security 2

Il 16 gennaio 2023, la Direttiva (UE) 2022/2555 (nota come NIS2) è entrata in vigore migliorando lo stato di sicurezza informatica esistente in tutta l'UE in diversi modi:

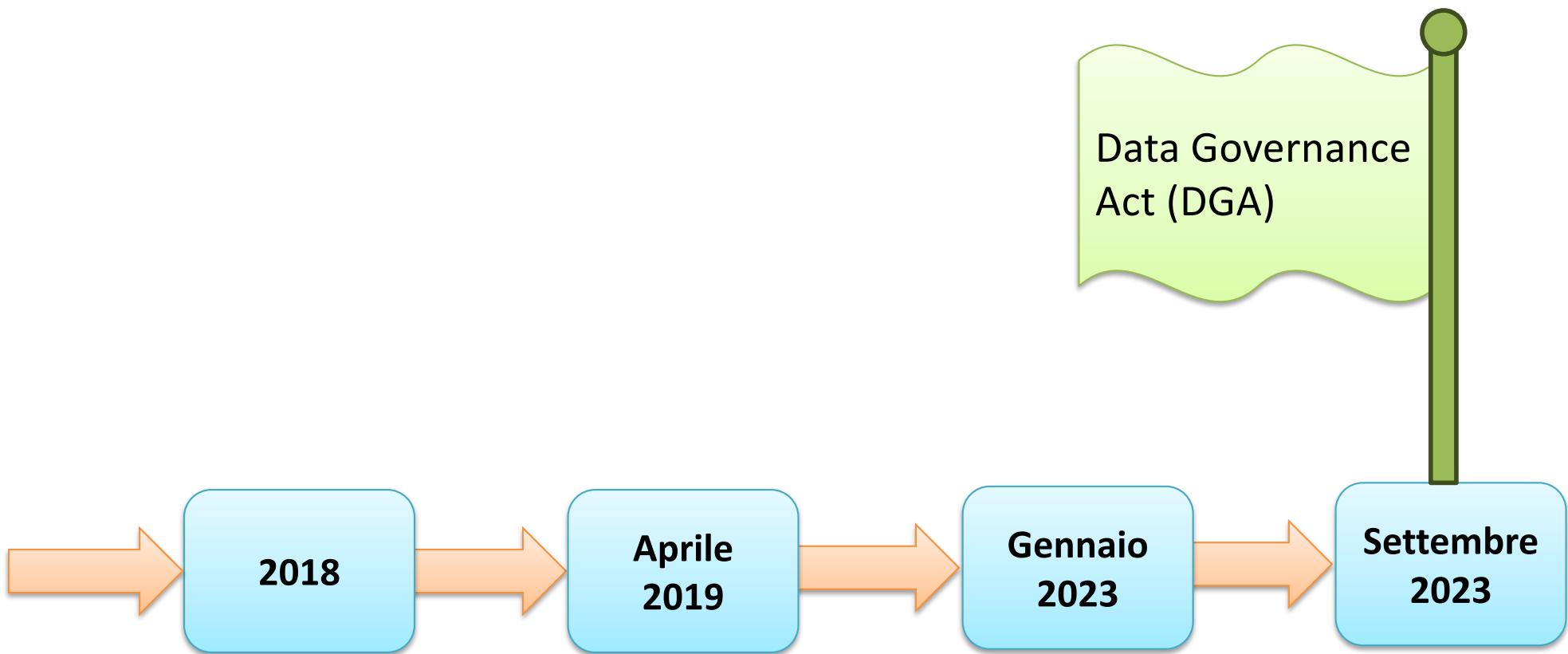
- creazione della struttura di gestione delle crisi informatiche (CyCLONe);
- aumentare il livello di armonizzazione per quanto riguarda i requisiti di sicurezza e gli obblighi di segnalazione;
- incoraggiare gli Stati membri a introdurre nuovi interessi quali la catena di approvvigionamento, la gestione delle vulnerabilità, l'internet centrale e l'igiene informatica;
- apportare nuove idee come le revisioni tra pari per migliorare la collaborazione e la condivisione delle conoscenze tra gli Stati membri;
- coprire una quota più ampia dell'economia e della società includendo più settori, il che significa che più entità sono obbligate ad adottare misure per aumentare il proprio livello di sicurezza informatica.

::: Network and Information Security 2

Oltre a definire i settori di attività da disciplinare, la NIS2 prevede l’elenco dei requisiti minimi che i soggetti coinvolti sono chiamati a garantire:

- analizzare e valutare i rischi di sicurezza dei sistemi informativi con operazioni di vulnerability assessment, penetration test ecc.;
- gestire gli incidenti di sicurezza informatici con un piano e un’attività di monitoraggio continuo e incident response;
- dotarsi di un piano di continuità di business e gestione delle crisi;
- testare regolarmente la sicurezza dell’infrastruttura IT e l’efficacia delle misure di gestione del rischio adottate;
- assicurare la sicurezza delle supply chain, controllando che i propri fornitori dispongano di adeguati requisiti in termini di sicurezza.

::: Nuovi Strumenti Normativi



::: Data Governance Act

Il Data Governance Act (DGA) approvato nell'aprile 2022 dal Parlamento Europeo, è il primo tassello nella strategia di creazione di uno spazio europeo di condivisione dei dati nei settori strategici. Gli obiettivi sono:

1. mettere a disposizione dei dati del settore pubblico per il riutilizzo, nel caso in cui tali dati siano oggetto di diritti di terzi;
2. condividere dati tra imprese, dietro un compenso in qualsiasi forma;
3. prestare il consenso all'utilizzo dei dati personali, con l'ausilio di un "intermediario", per aiutare i singoli individui a esercitare i propri diritti a norma del regolamento generale sulla protezione dei dati;
4. prestare il consenso ai dati per scopi altruistici.

Il DGA va ad integrare quanto già previsto dalla Direttiva UE 2019/1024 ritenuta non sufficiente a disciplinare le attuali necessità, essendo profondamente mutati i contesti tecnologici e sociali, ed essendo intervenute ulteriori normative di settore che richiedono un'armonizzazione legislativa generale.

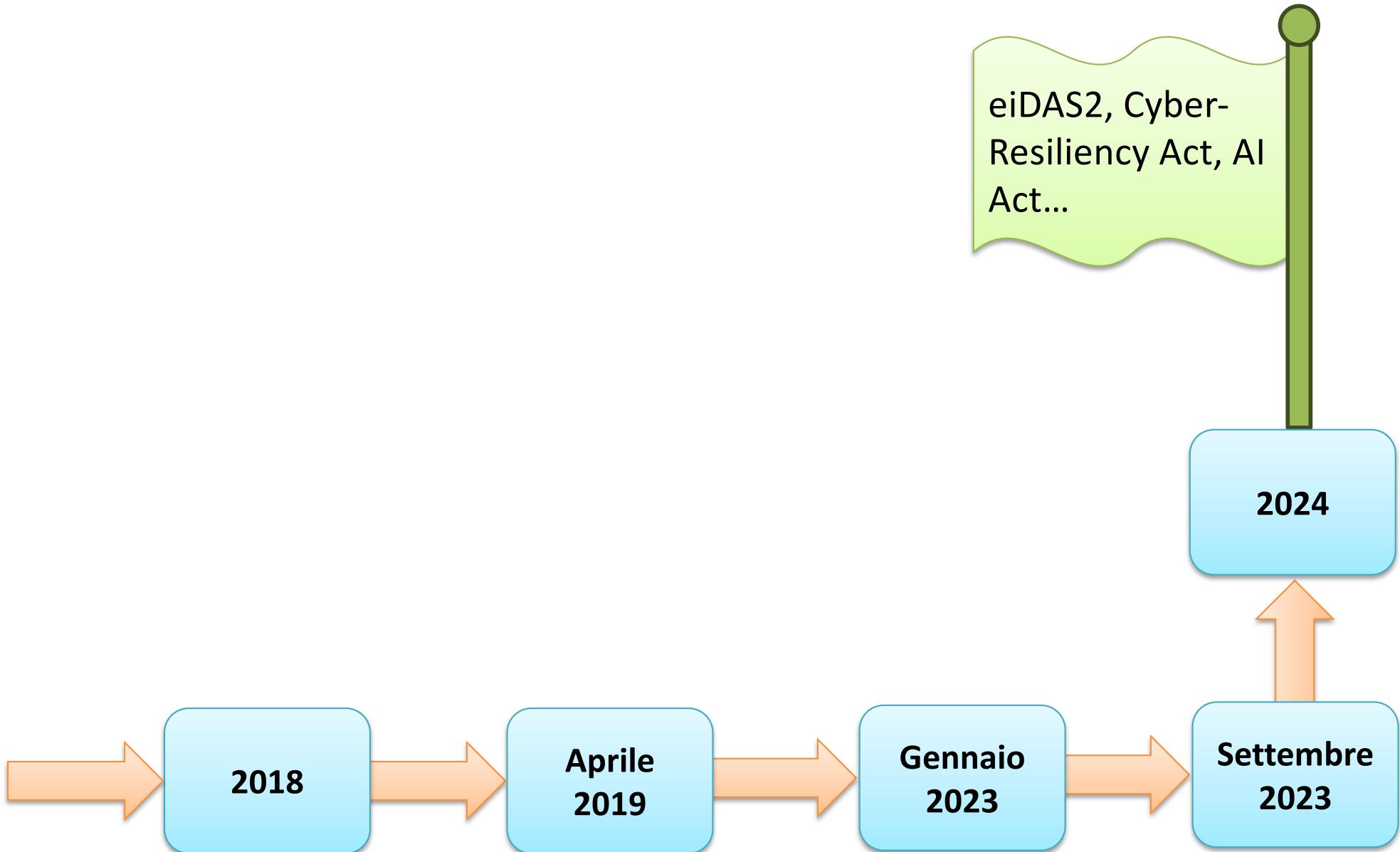
::: Data Governance Act

Oggetto del DGA non sono esclusivamente i dati personali (cui, invece, fa riferimento il GDPR) ma tutti i dati ritenuti particolarmente “sensibili” per differenti motivazioni.

L'UE intende promuovere lo sviluppo di sistemi affidabili di condivisione dei dati secondo adeguati e flessibili meccanismi di riutilizzo dei dataset pubblici a beneficio della società, nel rispetto dei classici principi “FAIR” (secondo cui i dati devono essere “reperibili”, “accessibili”, “interoperabili”, “riutilizzabili”). Il razionale è quello del “Data Altruism”, che si focalizza sulla messa a disposizione volontaria dei dati per il bene comune da parte di aziende o persone fisiche. Il requisito fondamentale per l'utilizzo di tali dati è la finalità di interesse generale.

- nell'ambito dell'attuazione del DGA, occorrerà rispettare le norme del GDPR. Nel caso in cui la manifestazione altruistica di volontà concerna dati di natura personale, occorrerà che il relativo consenso sia espresso nel rispetto dei requisiti agli artt. 7 e 8 del GDPR.

::: Nuovi Strumenti Normativi



::: Cyber Resiliency Act

Il Cyber Resilience Act dell'UE, la cui attuazione è prevista per il 2024, apporta cambiamenti significativi al panorama dei prodotti digitali in Europa. Questo quadro normativo impone rigorosi requisiti di sicurezza informatica per quasi tutti i prodotti con componenti digitali, dallo sviluppo alla gestione della fine del ciclo di vita. La CRA è progettata per funzionare in modo complementare con il quadro di sicurezza informatica dell'UE che coinvolge NIS2 e CSA.

- L'obiettivo è proteggere i consumatori e il mondo del business da prodotti operanti nel mondo digitale grazie a connessioni digitali che presentino inadeguate caratteristiche relative alla sicurezza.
- Al centro del CRA non stanno tanto le regole relative all'uso dei dati digitali, quanto le reti di trasmissione stesse e le modalità tecniche con le quali i dati sono scambiati.
- Bisogna garantire che i prodotti hardware e software siano immessi sul mercato con meno vulnerabilità, e i produttori prendano sul serio la sicurezza durante tutto il ciclo di vita di un prodotto.

::: eiDAS 2

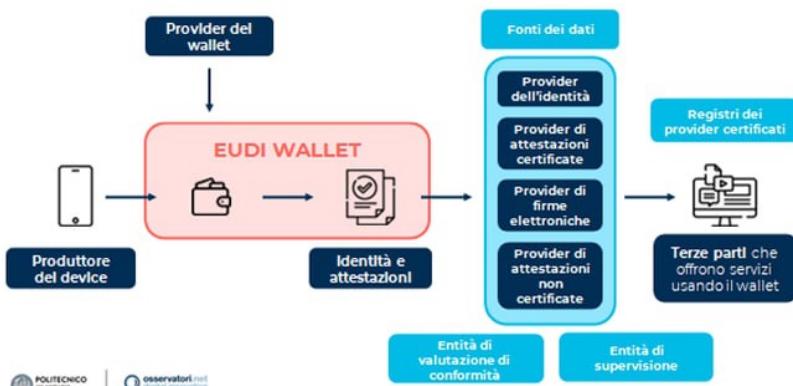
È in discussione la modifica del Regolamento n. 910/2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche:

- La novità è il cosiddetto E-Wallet, un sistema di identità che consenta di firmare documenti digitali attraverso firme elettroniche qualificate, oltre che di richiedere, memorizzare, condividere, in modo sicuro, trasparente e tracciabile per l'utente, i propri dati personali di identificazione, nonché l'attestazione elettronica degli attributi per l'autenticazione richiesti da servizi pubblici e privati online.
- Ciò sarebbe possibile collegando l'E-Wallet e un nucleo centrale dell'identità personale (PID), mentre l'attestazione elettronica degli attributi personali (EEA), dovrebbe essere realizzata da Prestatori di servizi fiduciari (Trust Service Provider), di natura pubblica o privata.
- Un aspetto importante è ciò che si potrà attestare con l'E-Wallet: dai semplici dati anagrafici ai documenti personali, fino a includere titoli di studio e licenze professionali, oltre che documenti giuridici comprovanti l'attivazione di regimi di tutela, rappresentanza o delega.

::: eiDAS 2



Lo European Digital Identity Wallet (o EUDI) sarà il prossimo passo per l'identità digitale in Italia e in Europa. Nella prospettiva degli utenti finali, l'obiettivo è la creazione di un'app che permetta all'utente di avere il pieno controllo dei propri dati.

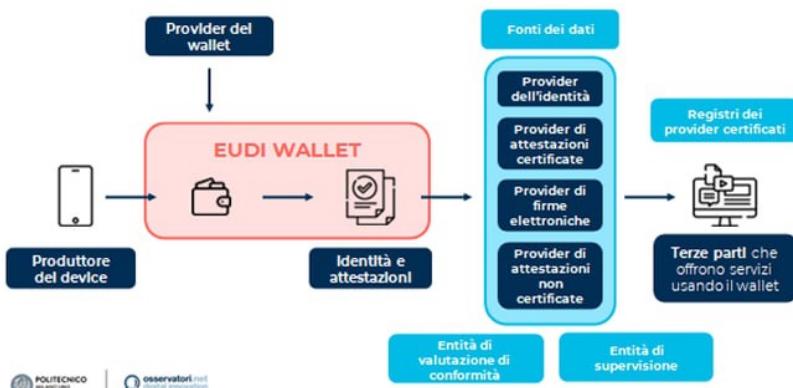


Oltre a ruoli più tradizionali, come il provider dell'identità, assimilabile per esempio ai dieci Identity Provider coinvolti nel sistema SPID, si introducono nuove figure.

::: eiDAS 2

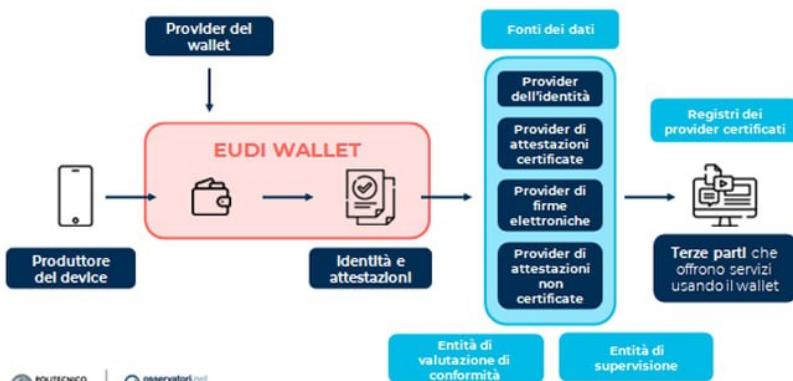
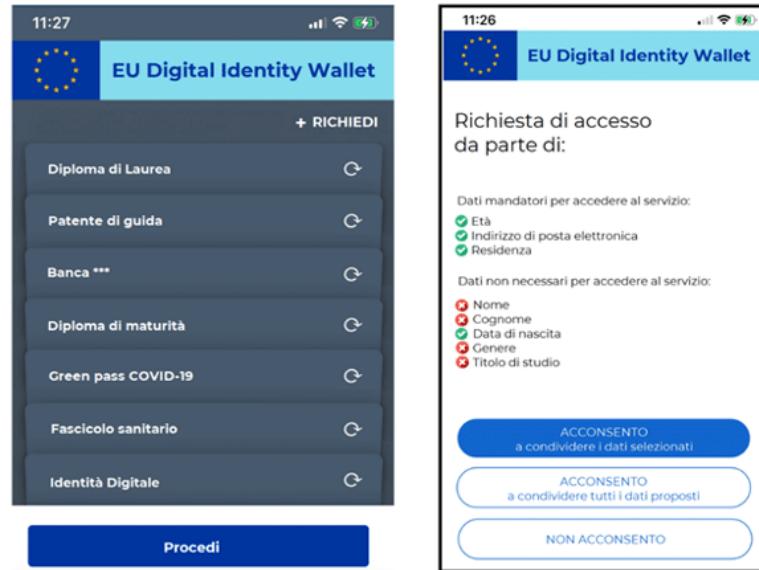


Lo European Digital Identity Wallet (o EUDI) sarà il prossimo passo per l'identità digitale in Italia e in Europa. Nella prospettiva degli utenti finali, l'obiettivo è la creazione di un'app che permetta all'utente di avere il pieno controllo dei propri dati.



Tra i ruoli più interessanti c'è sicuramente il Provider del wallet, che si occuperà di fornire il supporto tecnologico per la distribuzione del sistema e per l'aggregazione di diversi certificati.

::: eiDAS 2



Lo European Digital Identity Wallet (o EUDI) sarà il prossimo passo per l'identità digitale in Italia e in Europa. Nella prospettiva degli utenti finali, l'obiettivo è la creazione di un'app che permetta all'utente di avere il pieno controllo dei propri dati.

Un ulteriore ruolo chiave è il Provider delle attestazioni (certificate e non), che emette certificati che comprovino alcuni attributi dell'utente. Questi potranno essere di natura certificata, come il possesso di un titolo di studio, ma anche non certificata, includendo potenzialmente qualsiasi badge o card, come la tessera dei trasporti o le carte fedeltà.

::: DSA & DMA

I servizi digitali comprendono un'ampia categoria di servizi online, dai semplici siti web ai servizi di infrastruttura internet e alle piattaforme online. Le regole specificate nella Digital Services Act (DSA) riguardano principalmente gli intermediari e le piattaforme online. Ad esempio, mercati online, social network, piattaforme di condivisione di contenuti, app store e piattaforme di viaggi e alloggi online.

Il Digital Markets Act (DMA) include norme che regolano le piattaforme online gatekeeper, ovvero quelle digitali con un ruolo sistematico nel mercato interno che funzionano come strozzature tra imprese e consumatori per importanti servizi digitali. Alcuni di questi servizi sono disciplinati anche dalla Digital Services Act, ma per ragioni diverse e con diversi tipi di disposizioni.

::: DSA & DMA

Sebbene i vantaggi della trasformazione digitale siano numerosi, vi sono anche dei problemi. Una delle preoccupazioni principali è il commercio e lo scambio di beni, servizi e contenuti illegali online. I servizi online vengono inoltre utilizzati in modo improprio da sistemi algoritmici manipolatori per amplificare la diffusione della disinformazione e per altri scopi dannosi. Nonostante una serie di interventi mirati, ci sono ancora lacune significative e oneri giuridici da colmare. Ad esempio, alcune grandi piattaforme controllano importanti ecosistemi nell'economia digitale. Sono emersi come gatekeepers dei mercati digitali, con il potere di agire come regolatori privati. Queste regole a volte si traducono in condizioni ingiuste per le imprese che utilizzano queste piattaforme e in una minore scelta per i consumatori.

Pertanto, l'Unione Europea ha adottato un quadro giuridico moderno che garantisce la sicurezza degli utenti online, stabilisce una governance con la protezione dei diritti fondamentali in prima linea e mantiene un ambiente di piattaforma online equo e aperto.

Con il DMA, si vuole contrastare gli abusi di posizione dominante prima che si verifichi la violazione.

::: DSA & DMA

Le società che ospitano dati altrui non sono responsabili del contenuto a meno che non sappiano effettivamente che è illegale, e una volta ottenuta tale conoscenza non agiscono per rimuoverlo. Il DSA introduce un'ampia serie di nuovi obblighi sulle piattaforme:

- obblighi di trasparenza (art.i 15, 26, 27, 30, 40)
- meccanismo di segnalazione e azione per la presenza di informazioni specifiche che possano costituire contenuti illegali; se le informazioni costituiscono contenuti illegali, vi saranno delle restrizioni che dovranno essere chiaramente e specificatamente motive;
- obbligo di informare l'utente della decisione di attuare moderazione del contenuto, motivando e permettendo la contestazione (art. 17);
- obbligo di fornire l'opzione di non ricevere suggerimenti basati sulla profilazione (art. 27);
- obbligo di chiarezza e rispetto dei diritti fondamentali nei termini di servizio (art. 14)
- obbligo di presenza di un quadro completo di gestione del rischio e relativo audit indipendente.

::: DSA & DMA

Per gatekeeper, si indica chi ha il potere di far filtrare o meno una informazione e, nel business, indica le società che hanno il controllo di un determinato settore di mercato. Nel mercato digitale, le società gatekeeper sono le LoPs – Large Online Platforms, che hanno il controllo per motivi quantitativi e qualitativi.

- Tra i motivi quantitativi: copertura delle quote di mercato, numero di utenti della piattaforma, tempo di utilizzo per utente della piattaforma, ricavi annuali.
- Tra i motivi qualitativi: capacità di porsi come intermediario tra la concorrenza e gli utenti, capacità di gestire i dati degli utenti a scopi analitici anche per competere su altri mercati.

I gatekeeper del mercato digitale sono i fornitori di servizi di piattaforma di base: social network, browser, motori di ricerca, servizi di messaggistica o social media.

Il Digital Markets Act individua i gatekeeper su tre parametri misurabili e verificabili:

- introiti annuali uguali o superiori a 7,5 miliardi di euro negli ultimi 3 anni o valore totale delle azioni di mercato di almeno 7,5 miliardi nell'ultimo anno e fornitura di servizi di piattaforma ad almeno tre Stati dell'UE;
- la registrazione di almeno 10.000 utenti europei attivi durante l'ultimo anno e più di 45 milioni di utenti europei finali attivi al mese;
- una posizione durevole e stabile sul mercato, se i due precedenti criteri sussistono contemporaneamente da almeno tre anni.

::: DSA & DMA

La DMA stabilisce da un lato un elenco di comportamenti che dovrebbero essere vietati (blacklist art. 5), dall'altro, gli obblighi che le piattaforme identificate come gatekeepers dovrebbero rispettare (whitelist art. 6) e case by case assessment, ovvero valutazioni da applicare caso per caso alle grandi piattaforme. Le azioni generali della lista nera sono:

- il leveraging, cioè lo sfruttamento della propria posizione dominante per monopolizzare nuovi mercati, attraverso l'imposizione di commissioni elevate o la limitazione forzata dell'accesso a servizi e prodotti online;
- il self preferencing, cioè il favorire arbitrariamente i propri prodotti sulla piattaforma a discapito di quelli proposti da altre società;
- il rifiuto di accesso ai dati dell'utenza a terze parti terze, previa autorizzazione dell'utente stesso;
- l'obbligo di termini e condizioni che bloccano l'accesso a determinate funzionalità;
- le pratiche di vincolo (tying) e aggregazione (bundling), come la vendita o l'offerta congiunta e ingiustificata di beni/servizi diversi;

::: DSA & DMA

- l'imposizione di termini e condizioni poco chiare, come raccolta ingiustificata dei dati degli utenti finali;
- la limitazione o il rifiuto della portabilità dei dati o del riuso dei dati, per scoraggiare o impedire all'utente l'abbandono della piattaforma;
- il rifiuto immotivato di soluzioni di interoperabilità per rendere più difficile cambiare piattaforma;
- la combinazione di dati personali dell'utente, ricavati dai servizi di piattaforma, con altri dati personali ricavati da altri servizi, anche di terze parti, senza espressa autorizzazione dell'utente stesso.

Tra gli obblighi previsti per le aziende nella whitelist:

- permettere agli utenti di disinstallare qualsiasi app preinstallata;
- astenersi dal garantire posizionamento e trattamento più favorevole ai prodotti che appartengono alla stessa impresa rispetto a quelli altrui;
- fornire a inserzionisti ed editori i dati necessari per verificare e monitorare dati indipendenti dell'offerta di spazio pubblicitario;

::: DSA & DMA

- fornire a titolo gratuito agli utenti commerciali, o a terzi autorizzati da un utente commerciale, un accesso efficace, continuo e in tempo reale a dati aggregati e non aggregati forniti o generati nel contesto dell'uso dei pertinenti servizi di piattaforma di base (ovviamente solo previo consenso dell'utente).

Tecnicamente, il DMA è uno strumento normativo ex ante: regola e definisce condotte e obblighi per le imprese prima che avvenga l'abuso. Al contrario, la normativa antitrust agisce ex post: ovvero, sanziona dopo che la violazione anticoncorrenziale è stata già messa in atto.

Le norme antitrust vigenti, infatti, hanno il limite della durata delle indagini, durante cui non è arginato l'effetto lesivo dell'eventuale abuso sulla concorrenza. Inoltre, risultano inefficaci se il danno alla concorrenza non è causato tanto dal comportamento specifico della piattaforma in questione quanto dalle caratteristiche intrinseche del mercato digitale.

::: Artificial Intelligence Act

La questione se il GDPR protegga adeguatamente i dati personali nel contesto dell'AI è ancora oggetto di dibattito. Il cosiddetto "AI Act" identifica i sistemi di AI ad alto rischio, quando incidono sensibilmente sui diritti fondamentali, e pone sulla loro progettazione specifiche esigenze:

- gli sviluppatori eseguano una valutazione dei rischi, adottino misure di sicurezza a protezione dei dati e forniscano una documentazione adeguata agli utenti;
- tutti i modelli di IA devono prevedere la sorveglianza e l'intervento umano, la robustezza tecnica e la sicurezza, la tutela della privacy e la data governance, la trasparenza, il benessere sociale e ambientale, la diversità, la non discriminazione e la correttezza.
- alcuni utilizzi dell'AI che potrebbero minacciare i diritti fondamentali sono esplicitamente vietati.

Questi requisiti hanno implicazioni significative per la conformità al GDPR dei sistemi di AI ad alto rischio che trattano dati personali.

::: EU vs USA



La differenza più significativa è la mancanza nella legislazione statunitense di una legge completa sulla privacy per tutti i tipi di dati e contesti.

Invece, la legge americana adotta un approccio più frammentato con varie normative che disciplinano diversi settori e tipologie di dati, tra cui:

- Health Insurance Portability and Accountability Act (HIPAA) – Questa legge federale protegge i dati sanitari sensibili specificando come gli operatori sanitari devono proteggere tali dati da frodi e furti. La legge stabilisce inoltre limiti al modo in cui le organizzazioni possono utilizzare o divulgare informazioni sanitarie protette.
- Il Gramm-Leach-Bliley Act (GLBA) – Si applica alle istituzioni finanziarie e stabilisce responsabilità e standard per proteggere la riservatezza e la sicurezza dei dati personali non pubblici dei consumatori. La Federal Trade Commission (FTC) ha annunciato importanti modifiche alla GLBA nel 2022, descrivendo nel dettaglio le misure di sicurezza dei dati più prescrittive.

::: EU vs USA

- Federal Information Security Management Act (FISMA): questa legge federale impone alle agenzie federali di sviluppare, documentare e implementare un programma che garantisca la sicurezza delle informazioni. FISMA 2022 è un aggiornamento con un approccio strategico per garantire che i sistemi IT federali possano prepararsi e rispondere meglio alle minacce per informazioni e sistemi informativi federali da accesso, utilizzo e divulgazione non autorizzati.

La mancanza di un vero approccio sistematico incentrato sulla privacy nelle diverse normative americane rende necessario aggiornarle in linea con i diritti fondamentali che le persone ora si aspettano riguardo al modo in cui i loro dati vengono utilizzati, condivisi o divulgati.

Negli ultimi anni sono emerse leggi statali che tentano di fornire una maggiore protezione dei dati personali agli individui in tali giurisdizioni e una maggiore trasparenza sul modo in cui i dati vengono condivisi. La legge statunitense più paragonabile al GDPR è il California Consumer Privacy Act (CCPA), che si applica ai consumatori residenti in California.

::: EU vs USA

Il CCPA è entrato in vigore nel gennaio 2020, ma il California Privacy Rights Act (CPRA) modifica la legislazione sulla privacy per espandere i diritti di opt-out e introdurre altre modifiche che lo allineano ancora di più al GDPR. Il CPRA è entrato in vigore nel gennaio 2023. È interessante notare che dall'approvazione del CCPA, altri 11 stati degli Stati Uniti hanno firmato una legge completa sulla privacy dei dati.

Esistono importanti differenze culturali che non possono essere ignorate quando si valutano le diverse leggi sulla privacy dei dati tra UE e Stati Uniti. Un esempio dei diversi approcci è il modo in cui la Carta dei diritti fondamentali dell'UE stabilisce che la protezione dei dati è un diritto fondamentale. Questa mentalità attenta alla privacy deriva probabilmente da una storia di utilizzo delle informazioni personali per scopi nefasti che risale ai tempi del nazionalsocialismo e del comunismo.

::: EU vs USA

Al contrario, gli Stati Uniti hanno tradizionalmente adottato un approccio più passivo che favorisce le aziende che raccolgono e utilizzano dati personali. L'utilizzo dei dati personali per scopi commerciali supera l'importanza della riservatezza dei dati. Gli ultimi anni hanno visto la mentalità spostarsi in qualche modo verso una migliore protezione degli individui poiché le violazioni dei dati continuano a causare il caos, ma le differenze culturali sottostanti richiederanno più tempo per dissolversi e portare gli Stati Uniti in un più completo allineamento con la mentalità e le leggi dell'UE.

Un importante cambiamento normativo è stato annunciato nel marzo 2022 con il Trans-Atlantic Data Privacy Framework (TADPF) per sostituire Privacy Shield UE-USA, invalidato dalla Corte di Giustizia Europea nel 2020. Il TADPF introduce garanzie che limitano l'accesso ai dati da parte delle autorità di intelligence statunitensi a quanto necessario e proporzionato per proteggere la sicurezza nazionale.

::: EU vs USA

Con TADPF, è richiesto alle aziende statunitensi di certificare la loro adesione al nuovo Protocollo e di impegnarsi a rispettare una serie dettagliata di obblighi in materia di protezione dei dati personali, di sicurezza dei sistemi e di condivisione dei dati con terze parti.

- tutte le società che operano quali titolari del trattamento soggetti all'ambito di applicazione del GDPR hanno l'opportunità di rivedere i loro processi interni riprendendo i flussi di trasferimenti di dati personali verso gli U.S.A. sospesi a seguito della sentenza della Corte di giustizia del luglio 2020.
- i titolari del trattamento rivedano le basi giuridiche del trasferimento di dati, adeguando la documentazione informativa nei confronti degli interessati e la documentazione a supporto degli accordi con i fornitori ("Data Transfer Agreement"), con particolare attenzione alle clausole contrattuali tipo, alle norme vincolanti d'impresa ed all'analisi del rischio.

::: EU vs USA

Il nuovo California Privacy Rights Act mira ad integrare la precedente versione della normativa sulla protezione dei dati dei consumatori con previsioni che appaiono prestate dal Regolamento europeo:

- ambito di applicazione: la normativa è volta a tutelare i soli residenti in California ed è rivolta a specifiche aziende;
- base giuridica: la normativa parte dal presupposto che le aziende utilizzino le informazioni personali dei consumatori, ma non si riferisce alle modalità e basi mediante le quali tali dati siano raccolti;
- misure: benché vi siano continui riferimenti ad obblighi e doveri non vi sono (ancora) precise indicazioni circa le modalità dell'utilizzo dei dati dei consumatori;
- ruoli: non sono disciplinati i ruoli aziendali in un'ottica di attribuzione delle responsabilità. Manca una figura che sia internamente incaricata della verifica dell'adeguamento alle previsioni in materia di protezione delle informazioni personali dei consumatori, come l'europeo DPO;

::: EU vs USA

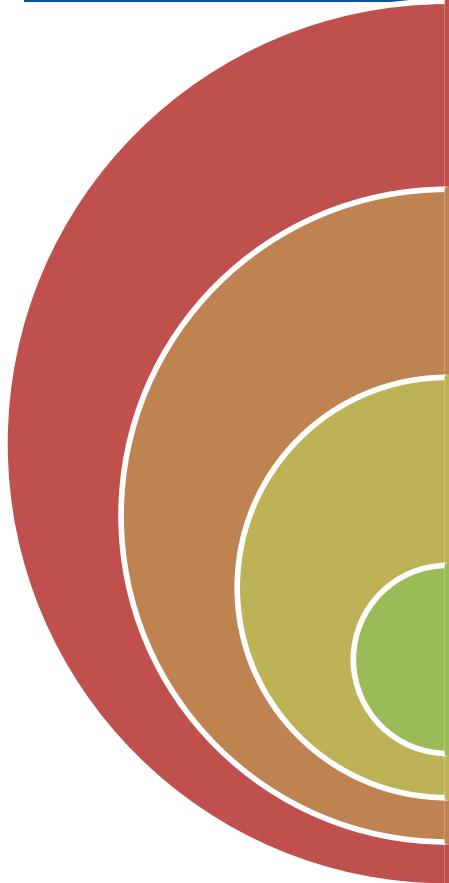
- trasferimenti: manca una specifica disciplina del trasferimento delle informazioni personali, soprattutto alla luce del fatto che molte aziende che si trovino fuori dallo Stato della California o degli Stati Uniti possano effettivamente avere interessi economici in California e rivolgersi ad utenti californiani, senza contare i terzi providers o contractors, che sono agganciati alla normativa e che potrebbero essere situati in Stati o Paesi terzi.

Mentre CCPA e CPRA disciplinano il “nocciolo” dell’utilizzo dei dati, focalizzandosi in una già in atto divulgazione, vendita e condivisione, nonché sui diritti dei consumatori, il GDPR fornisce le istruzioni, dal progetto alla successiva conservazione dei dati personali per le persone giuridiche che li trattino.

::: EU vs China



Entrata in vigore a novembre 2021 in Cina, la Personal Information Protection Law (PIPL) punta a regolamentare la protezione dei dati. La PIPL appare modellata sul GDPR, ma gli oneri sono molti e alcuni piuttosto stringenti.

	Cyber Security Law	<ul style="list-style-type: none">• 1 Giugno 2017• Descrive i principi che chi usa reti e ICT deve soddisfare
	Cybersecurity Classified Protection Scheme	<ul style="list-style-type: none">• 1 Dicembre 2019• Traduce i requisiti del CSL in controlli tecnici ed organizzativi dettagliati
	Data Security Law	<ul style="list-style-type: none">• 1 Settembre 2021• Regola l'elaborazione e sicurezza dei dati e i diritti delle persone e organizzazioni
	Personal Information Protection Law	<ul style="list-style-type: none">• 1 Novembre 2021• Disciplina i dati personali e la loro elaborazione e i diritti delle persone

::: EU vs China



Entrata in vigore a novembre 2021 in Cina, la Personal Information Protection Law (PIPL) punta a regolamentare la protezione dei dati. La PIPL appare modellata sul GDPR, ma gli oneri sono molti e alcuni piuttosto stringenti.

CSL: coloro che gestiscono, mantengono e utilizzano la rete in Cina, nonché la supervisione e la gestione della sicurezza della rete, sono soggetti a questa legge: devono mettere in sicurezza la rete per proteggerla da interferenze, sabotaggio o accesso non autorizzato, e per proteggere i dati di rete da perdite, furti o manomissioni.

È richiesto che gli operatori di infrastrutture ICT chiave conservino tutti i dati personali raccolti e generati durante il loro funzionamento in Cina. Esiste una disposizione simile (articolo 40) nella PIPL: per infrastrutture ICT chiave, gli operatori e gli incaricati al trattamento dei dati personali conserveranno i dati raccolti e generati in Cina fino a quando la quantità di dati raggiungerà un determinato importo (non specificato).

::: EU vs China



Entrata in vigore a novembre 2021 in Cina, la Personal Information Protection Law (PIPL) punta a regolamentare la protezione dei dati. La PIPL appare modellata sul GDPR, ma gli oneri sono molti e alcuni piuttosto stringenti.

Sebbene il CSL tocchi la sicurezza dei dati, rimane generale e non si concentra su un quadro per la governance della sicurezza dei dati. In risposta, la DSL introduce anche sovereignty security e stabilisce un sistema di sicurezza dei dati fondamentale e categorizzato che si applica potenzialmente a tutte le attività di trattamento, indipendentemente dal fatto che siano online o offline.

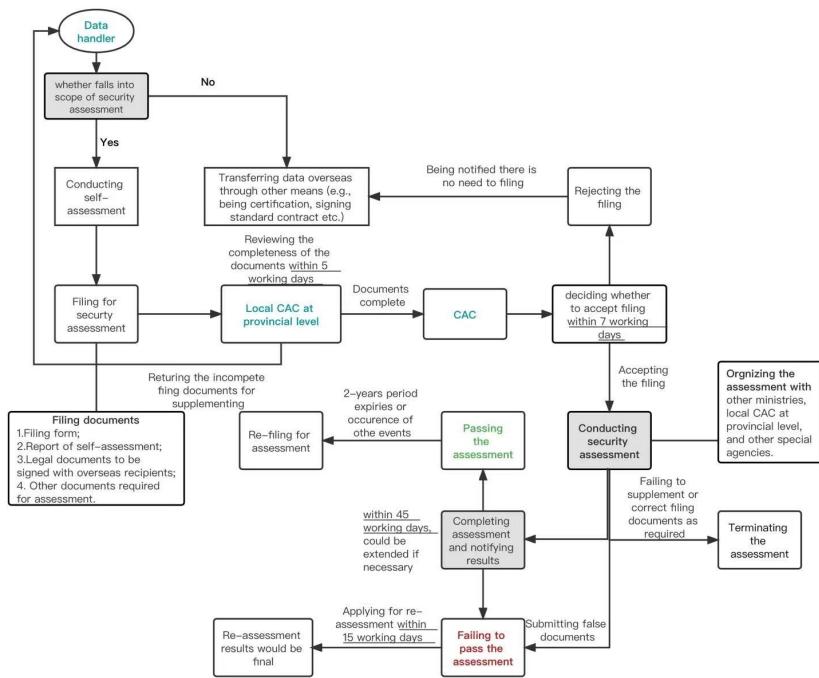
A differenza dei requisiti incentrati sulla sicurezza previsti dal CSL e dal DSL, il PIPL si concentra sulla privacy. La DSL si applica anche alle informazioni personali, secondo l'art. 53, ma la PIPL ha norme e regolamenti più specifici su tematiche privacy.

... EU vs China



Entrata in vigore a novembre 2021 in Cina, la Personal Information Protection Law (PIPL) punta a regolamentare la protezione dei dati. La PIPL appare modellata sul GDPR, ma gli oneri sono molti e alcuni piuttosto stringenti.

PIPL si applica anche alle attività di trattamento al di fuori della Cina secondo il paragrafo 2 dell'articolo 3. La DSL può applicarsi anche al



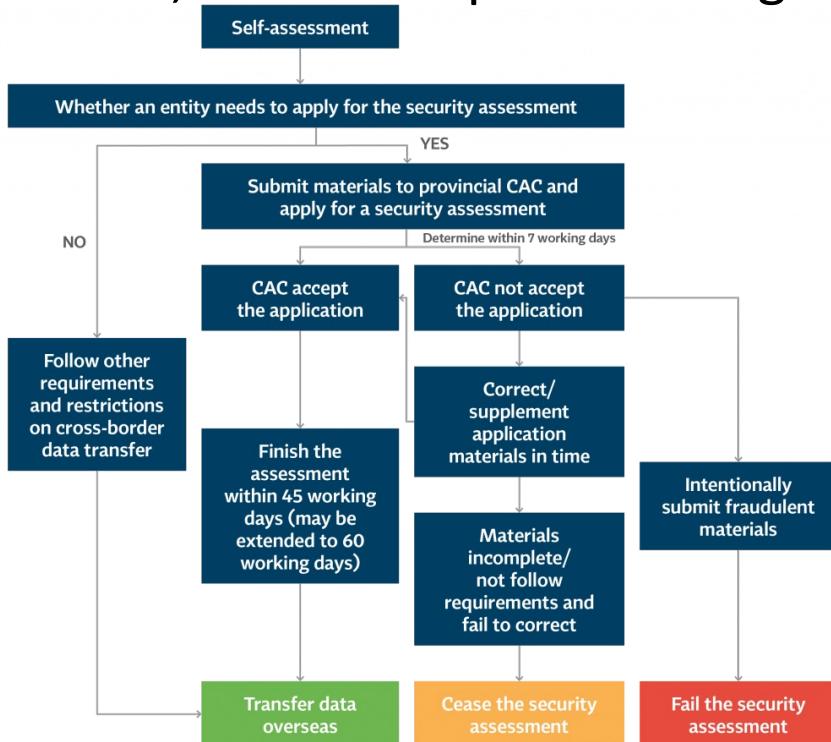
PIPL definisce un preciso processo autorizzativo per i trasferimenti fuori la Cina:

::: EU vs China



Entrata in vigore a novembre 2021 in Cina, la Personal Information Protection Law (PIPL) punta a regolamentare la protezione dei dati. La PIPL appare modellata sul GDPR, ma gli oneri sono molti e alcuni piuttosto stringenti.

PIPL definisce un preciso processo autorizzativo per i trasferimenti fuori la Cina, che si compone dei seguenti passi:



- (i) fornire determinate informazioni specifiche sui trasferimenti e ottenere un consenso separato (art. 39),
- (ii) adottare le misure necessarie per garantire che i destinatari esteri possano fornire lo stesso livello di protezione richiesto dal PIPL (art. 38),
- (iii) effettuare una valutazione d'impatto sulla protezione dei dati personali (art. 55).

::: EU vs China

Il Capitolo I della PIPL individua i principi che devono essere rispettati nel trattare i dati personali, la maggior parte dei quali assomiglia ai principi dettati dall'articolo 5 del GDPR:

- il trattamento deve rispettare i principi di trasparenza, liceità, buona fede, necessità e minimizzazione.

La PIPL fa una distinzione tra gli ultimi due principi:

- il principio di necessità è generalmente applicabile a tutte le attività di trattamento, mentre il principio di minimizzazione si applica specificamente alla raccolta di dati personali.

Il principio di trasparenza comporta la necessità di informare gli interessati sulle modalità di trattamento dei dati personali, con modalità concise, facilmente accessibili, facili da capire e in un linguaggio chiaro e semplice: bisogna rendere disponibile sul proprio sito web o sulle applicazioni un'informativa privacy, in un formato chiaro e leggibile.

::: EU vs China

Prima della PIPL, la normativa cinese basava la liceità principalmente sul consenso, pertanto, se non diversamente previsto dalle leggi. La PIPL prevede, invece, come il GDPR, diverse basi giuridiche :

- consenso;
- conclusione o esecuzione di un contratto;
- adempimento di obblighi stabiliti dalla legge;
- risposta ad un'emergenza sanitaria pubblica o per proteggere, in caso di emergenza, la vita, la salute o la proprietà di una persona fisica;
- cronaca, opinione pubblica nel pubblico interesse;
- trattamento di informazioni rese pubbliche dagli stessi interessati;
- altre circostanze previste da leggi e regolamenti.

A differenza del GDPR, non è previsto il legittimo interesse come base giuridica per il trattamento. La normativa cinese richiede in alcuni casi un consenso separato, secondo condizioni specifiche.

::: EU vs China

La PIPL dispone che nel trattare i dati personali sia garantita la qualità delle informazioni, predisponendo le misure adeguate a garantire che tutti i dati personali siano accurati, completi e aggiornati.

- L'art. 9 della PIPL prevede che i titolari siano responsabili delle attività di trattamento e debbano garantirne la sicurezza.
- Ogni azienda deve effettuare una valutazione delle misure di sicurezza, e la loro adeguatezza ed efficacia per garantire la sicurezza, considerando la quantità di dati trattate, i metodi e la frequenza delle attività di trattamento, se sono coinvolte dati personali sensibili.
- È opportuno predisporre meccanismi per la conformità alla normativa, formalizzando policy, procedure, sistemi per la conservazione dei log e implementando attività di formazione.

Sussiste la necessità di nominare un Personal Information Officer, simile al Data Protection Officer prevista dal GDPR, anche se la PIPL non prevede specifiche caratteristiche e competenze per ricoprire questo ruolo.

::: EU vs China

Il PIPL offre maggiore discrezionalità al governo e agli enti amministrativi per quanto riguarda la protezione dei dati e la promozione degli interessi di sicurezza nazionale, prevedendo che possano ostacolare il trasferimento dei dati al di fuori della Cina.

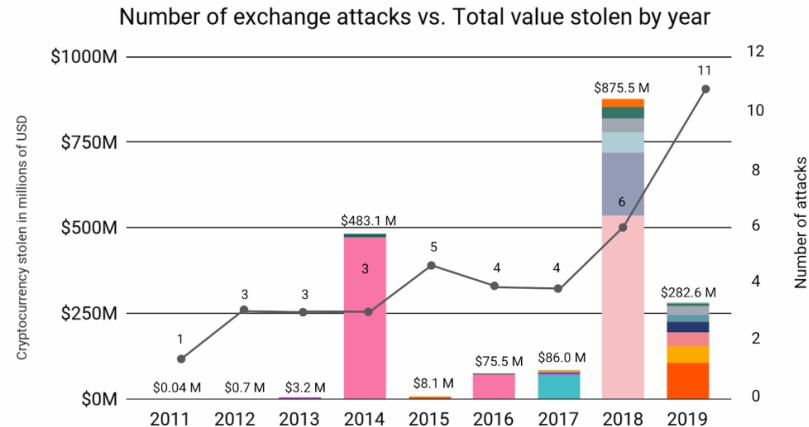
Rispetto al GDPR, il PIPL prevede prescrizioni molto più stringenti e difficili da ottenere:

- Le 72 ore concesse dal regolamento europeo per la notifica di violazione, sono azzerate da quello cinese che impone la notifica immediata;
- Il regolamento cinese, a differenza di quello europeo, persegue anche le persone fisiche che ricoprono ruoli di vertice in organizzazioni responsabili delle violazioni.



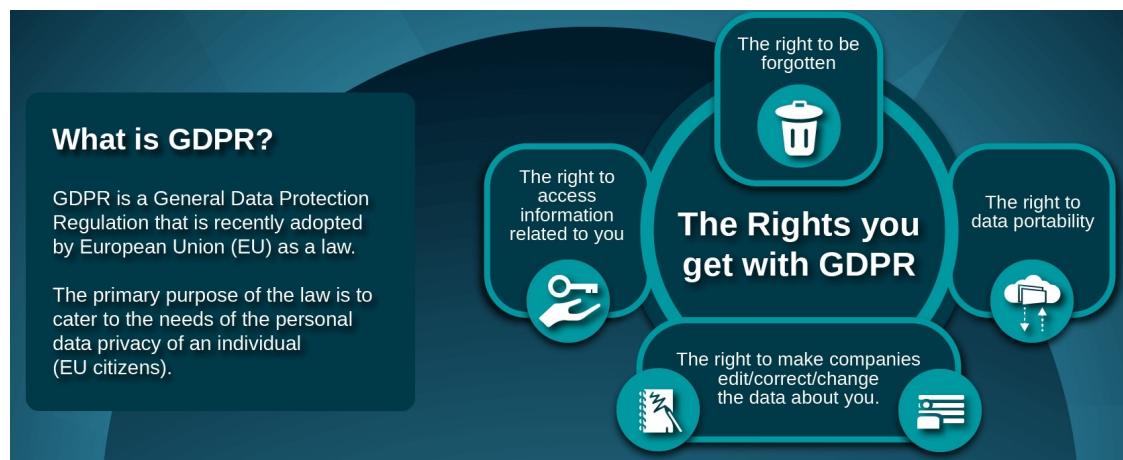
Blockchain e GDPR

::: Blockchain vs GDPR (1/9)



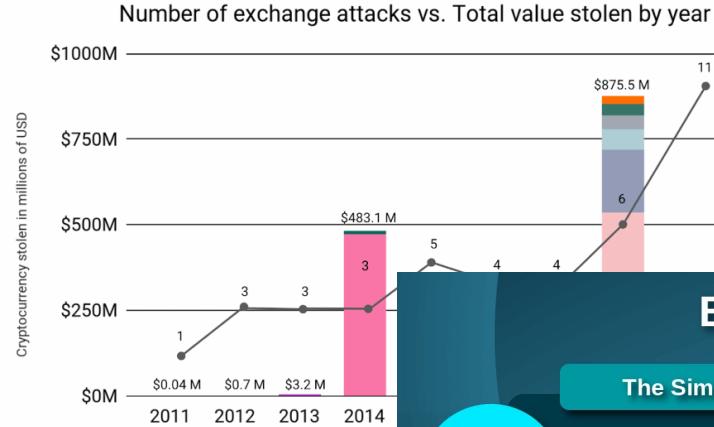
Per quanto la blockchain dia forti garanzie di sicurezza, non sono più isolati gli episodi di hackeraggio ai danni degli Exchange Coin-to-Coin (scambio di criptovalute).

Ad eccezione di un hardware wallet, violabili mediante un accesso fisico, le chiavi private per accedere ai wallet possono essere soggette ad attacchi, soprattutto phishing, alla stregua delle altre password.

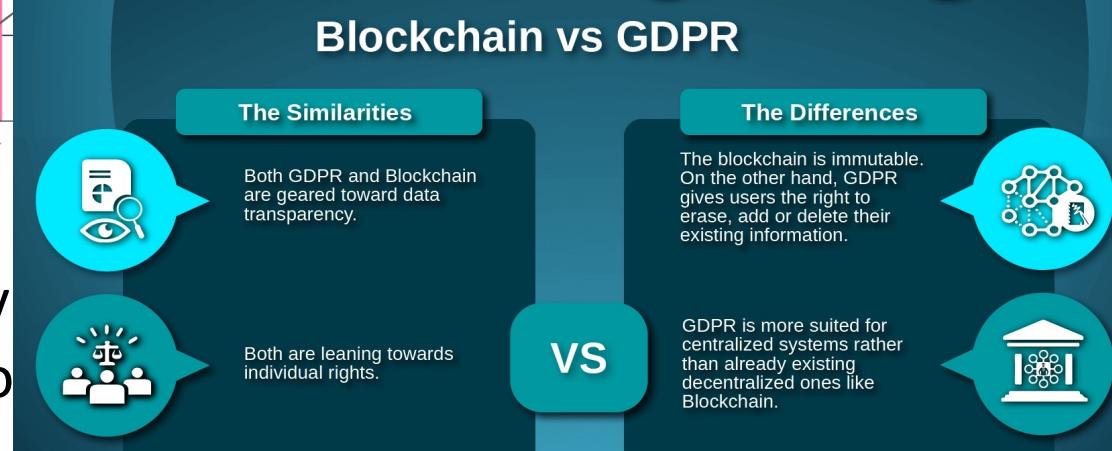


Il Regolamento Generale sulla Protezione dei Dati (GDPR) è un regolamento dell'Unione europea in materia di trattamento dei dati personali e di privacy.

::: Blockchain vs GDPR (1/9)



Ad eccezione fisico, le chiavi ad attacchi, so



Per quanto la blockchain dia forti garanzie di sicurezza, non sono più isolati gli episodi di hackeraggio ai danni degli Exchange Coin-to-Coin (e neanche solo).

te un accesso essere soggetto password.

Nel contesto della privacy e del GDPR, le blockchain presentano varie sfide: Come garantire i diritti del titolare dei dati immessi nella catena, fino al diritto di cancellazione se i dati sono immutabili? Chi risponde del trattamento dei dati in una rete di registri replicati? Il trattamento dei dati è tecnicamente solo quello che si conclude con la chiusura del primo blocco o è continuo?

::: Blockchain vs GDPR (2/9)

Circa l'adeguamento della blockchain al Regolamento UE 2016/679 o GDPR, lo scoglio apparentemente insormontabile è garantire i diritti dell'interessato, disciplinati al capo III, negli artt. 12 – 23.

- la peculiarità intrinseca della blockchain della non modificabilità e cancellazione di garantire l'integrità dei dati e aumentare la fiducia nella rete risulta essere in forte contrasto con requisiti legali come il “diritto di rettifica” e il “diritto all'oblio” sanciti nell'artt. 16 e 17.

Soluzioni al diritto di oblio potrebbero essere:

- la crittografia dei dati personali e la successiva eliminazione delle corrispettive chiavi, lasciando su blockchain solo i dati indecifribili;
- mediante l'uso dei cosiddetti modelli di memoria “fuori catena”: registrare su blockchain solo un “collegamento”, lasciando il dato vero e proprio al di fuori del libro mastro;
- garantire il diritto all'oblio mediante una corretta anonimizzazione.

::: Blockchain vs GDPR (2/9)

Circa l'adeguamento della blockchain al Regolamento UE 2016/679 o GDPR, lo scoglio apparentemente insormontabile è garantire i diritti dell'interessato, disciplinati al capo III, negli artt. 12 – 23.

- la peculiarità intrinseca della blockchain della non modificabilità e cancellazione dei dati nella rete

*Anche il **diritto di accesso** – articolo 15, GDPR – va ridimensionato a causa delle caratteristiche della blockchain, poiché appare complicato poter consultare i dati registrati su blockchain quando questi sono cifrati.*

Soluzioni al di

- la crittografia dei dati personali e la successiva eliminazione delle corrispettive chiavi, lasciando su blockchain solo i dati indecifrabili;
- mediante l'uso dei cosiddetti modelli di memoria "fuori catena": registrare su blockchain solo un "collegamento", lasciando il dato vero e proprio al di fuori del libro mastro;
- garantire il diritto all'oblio mediante una corretta anonimizzazione.

::: Blockchain vs GDPR (3/9)

È in corso un dibattito sul fatto che

- i dati archiviati in una blockchain, come chiavi pubbliche e dati transazionali, si qualifichino come dati personali ai fini del GDPR;
- se i dati personali che sono stati crittografati o sottoposti a hash si qualificano ancora come dati personali.

::: Blockchain vs GDPR (3/9)

È in corso un dibattito sul fatto che

- i dati archiviati in una blockchain, come chiavi pubbliche e dati transazionali, si qualifichino come dati personali ai fini del GDPR;
- se i dati personali che sono stati crittografati o sottoposti a hash si qualificano ancora come dati personali.

Secondo il Considerando n. 26, il GDPR è applicabile ai dati pseudonimizzati, ma non alle informazioni anonime.

- Anche se non idonei a permettere l'identificabilità, i dati pseudonimizzati in blockchain, tramite la funzione di hash, sono comunque da ritenere dati personali, con il conseguente obbligo di applicarvi le regole del GDPR.
- Anche le chiavi pubbliche fanno parte dei dati personali perché non garantiscono l'irreversibilità dell'identificazione. La pseudonimia non assicura la totale schermatura della propria identità poiché sarebbe sempre possibile risalirvi grazie alla chiave pubblica e all'insieme di tracce che ogni soggetto lascia sul web.

::: Blockchain vs GDPR (3/9)

È in corso un dibattito sul fatto che

- i dati archiviati in una blockchain, come chiavi pubbliche e dati transazionali, si qualifichino come dati personali ai fini del GDPR;
- se i dati personali che sono stati crittografati o sottoposti a hash si qualificano ancora come dati personali.

Le blockchain sono un particolare tipo di database di sola aggiunta che crescono continuamente man mano che vengono aggiunti nuovi dati, che vengono replicati su molti computer diversi. Ciò pone problemi circa la minimizzazione dei dati e limitazione delle finalità.

- Cosa si intende per "scopo" del trattamento dei dati personali nel contesto della blockchain? Si include solo la transazione iniziale o comprende anche il trattamento continuo dei dati personali (come la sua memorizzazione e il suo utilizzo per consenso) una volta che è stato messo in catena.

::: Blockchain vs GDPR (3/9)

È in corso un dibattito sul fatto che

- ***In caso di controversie, quali leggi devono essere applicate e di chi è la giurisdizione?*** In situazioni in cui non è possibile identificare l'entità di elaborazione dei dati personali e il luogo in cui i dati vengono elaborati (probabilmente ci sono tante di queste entità e luoghi quanti sono i nodi di rete), è difficile individuare la giurisdizione cui dovrebbe competere una eventuale valutazione legale del trattamento dei dati

Le I (ossia, in parole semplici, la legge nazionale applicabile).

crescono continuamente man mano che vengono aggiunti nuovi dati, che vengono replicati su molti computer diversi! Ciò pone problemi circa la minimizzazione dei dati e limitazione delle finalità.

- Cosa si intende per "scopo" del trattamento dei dati personali nel contesto della blockchain? Si include solo la transazione iniziale o comprende anche il trattamento continuo dei dati personali (come la sua memorizzazione e il suo utilizzo per consenso) una volta che è stato messo in catena.

::: Blockchain vs GDPR (4/9)

Il GDPR introduce il Data Protection Officer (DPO), che deve assistere colui che li controlla o li gestisce al fine di verificare l'osservanza interna al regolamento.

In una Blockchain, chi è il responsabile del trattamento dei dati personali? Nel GDPR, il responsabile del trattamento determina le finalità e i mezzi del trattamento dei dati personali. Può esistere una simile entità nel contesto di una Blockchain distribuita?

Il modello di governance decentralizzato di Blockchain e la molteplicità degli attori coinvolti rendono più ostica la definizione dei ruoli.

- I partecipanti, che scrivono sul canale e inviano dati alla convalida dei miners, possono essere considerati i responsabili.
- Qualora un gruppo di partecipanti decida di attuare un trattamento con uno scopo comune, il responsabile va identificato tra loro. In caso contrario, tutti i partecipanti dovrebbero essere considerati come contitolari del trattamento (ex art. 26 GDPR).

::: Blockchain vs GDPR (5/9)

Sicuramente non possono essere ritenuti titolari:

- i miner, in quanto il loro operato è circoscritto alla convalida delle transazioni, senza avere voce in merito all'oggetto di queste transazioni, non determinando né le finalità né i mezzi da attuare;
- le persone fisiche che immettono dati personali nella blockchain, al di fuori da un'attività professionale o commerciale (cioè quando l'attività è esclusivamente personale).

Il responsabile del trattamento andrebbe ricercato tra:

- gli sviluppatori degli Smart Contracts, in quanto trattano i dati personali per conto del titolare;
- i minatori, poiché eseguono le istruzioni del titolare quando verificano che la transazione soddisfano i criteri tecnici.

Entrambi dovrebbero quindi definire, con il titolare del trattamento, un contratto che specifichi gli obblighi di entrambe le parti e che incorpori le disposizioni dell'articolo 28 del GDPR.

::: Blockchain vs GDPR (6/9)

Per quanto riguarda l'ambito degli obblighi di Privacy by Design (articolo 25), il titolare del trattamento deve pensare, in via preliminare, alla pertinenza della scelta di questa tecnologia per l'attuazione del suo trattamento.

Qualsiasi transazione sulla blockchain implica:

- l'invio di una richiesta a tutti i minatori blockchain per la convalida di una transazione (contenente potenzialmente dati personali);
- un aggiornamento della blockchain aggiungendo il nuovo blocco nella catena di blocchi a tutti i partecipanti.

In aggiunta i partecipanti, possono essere ubicati in paesi al di fuori dell'UE sollevando la questione della conformità con gli obblighi di trasferimento extra UE (capo V GDPR).

::: Blockchain vs GDPR (7/9)

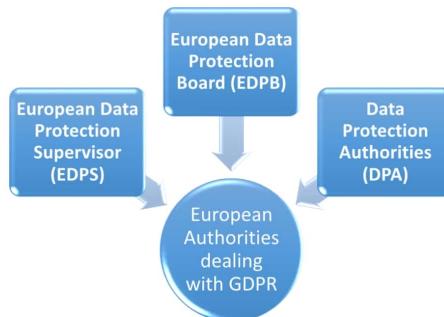
Per quanto riguarda l'identificabilità, la blockchain ha il vantaggio che ogni partecipante ha un identificativo costituito da una serie di caratteri alfanumerici apparentemente casuali e non identificabili con reali identità. Quanto ai dati aggiuntivi memorizzati sulla blockchain, nel caso in cui si tratti di dati personali, essi dovrebbero essere registrati preferibilmente in modalità crittografata.

È necessario determinare le finalità del trattamento e la valutazione d'impatto (DPIA), al fine di identificare come perseguitibile l'uso di blockchain pubbliche, private, con o senza cifratura del contenuto dei blocchi, così da dimostrare i rischi residui di una scelta tecnologica e la loro accettabilità.

La blockchain non è una tecnologia ma è una classe di tecnologie e l'esame di compatibilità con il GDPR va effettuato caso per caso.

::: Blockchain vs GDPR (8/9)

Attualmente, è allo studio una duplice linea d'azione per risolvere i problemi tra blockchain e GDPR:



- Le istituzioni dovrebbero condurre un'attività di orientamento regolatorio (una sorta di interpretazione autentica) di alcuni principi del GDPR per renderli applicabili alla tecnologia blockchain.
- I fornitori di servizi blockchain potrebbero studiare congiuntamente con le istituzioni dei codici di condotta e sistemi di certificazione delle catene a seconda dei settori di produzione nei quali la tecnologia è applicata.



Ciò sarebbe condotto in maniera similare al Cloud computing conduct code, ed è previsto dallo stesso GDPR (artt. 40 e 42).

::: Blockchain vs GDPR (9/9)

Per aumentare la certezza del diritto a sostegno della leadership digitale europea è necessario rafforzare il dialogo tra le autorità di regolamentazione e gli innovatori. La **European Blockchain Regulatory Sandbox** risponde a questa esigenza offrendo un ambiente affidabile per il coinvolgimento di autorità di regolamentazione e fornitori di tecnologie DLT.



European Blockchain Services Infrastructure (EBSI) è la prima iniziativa paneuropea di blockchain per supportare servizi pubblici migliori per tutta Europa. Il registro blockchain può essere utilizzato per archiviare informazioni in modo affidabile e decentralizzato, consentendo nuove forme di verifica, tracciabilità e trasparenza per i cittadini.