HEADLINES
12 STEPS ALLA CONFORMITA' GDPR

1 -Informative
L'informativa diventa uno strumento più efficace di trasparenza riguardo al trattamento dei dati personali e all'esercizio dei diritti

2- Consenso
Il consenso dell'interessato al trattamento dei dati personali deve essere "preventivo" ed "inequivocabile", anche quando espresso attraverso mezzi elettronici, ad esempio selezionando una casella su un sito web.
Per il Regolamento europeo il consenso è necessario che sia anche "esplicito" e "granulare"

3- Limiti al trattamento automatizzato dei dati
Regolamento europeo, aumentano i limiti alla possibilità per il titolare del trattamento di adottare decisioni solo sulla base di un trattamento automatizzato di dati.

4- Diritti dell'interessato
L'interessato ha il diritto di richiedere al titolare del trattamento l'accesso ai dati personali, la rettifica o la cancellazione degli stessi o alla limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati

5- Trasferimento Dati
Resta vietato il trasferimento di dati personali verso Paesi situati al di fuori dell'Unione europea o organizzazioni internazionali che non rispondono agli standard di adeguatezza in materia di tutela dei dati.

6- Data Breach
Il titolare del trattamento dovrà comunicare eventuali violazioni dei dati personali (data breach) all'Autorità nazionale di protezione dei dati.

7- Privacy by default & by design
Il Regolamento promuove la responsabilizzazione (accountability) dei titolari del trattamento e l'adozione di approcci e politiche che tengano conto costantemente del rischio che un determinato trattamento di dati personali può comportare per i diritti e le libertà degli interessati

8- Nomine
La designazione del Responsabile del trattamento, del responsabile per la protezione dei dati e dell'addetto al trattamento deve essere espressa, specifica, scritta e riferibile a determinate mansioni

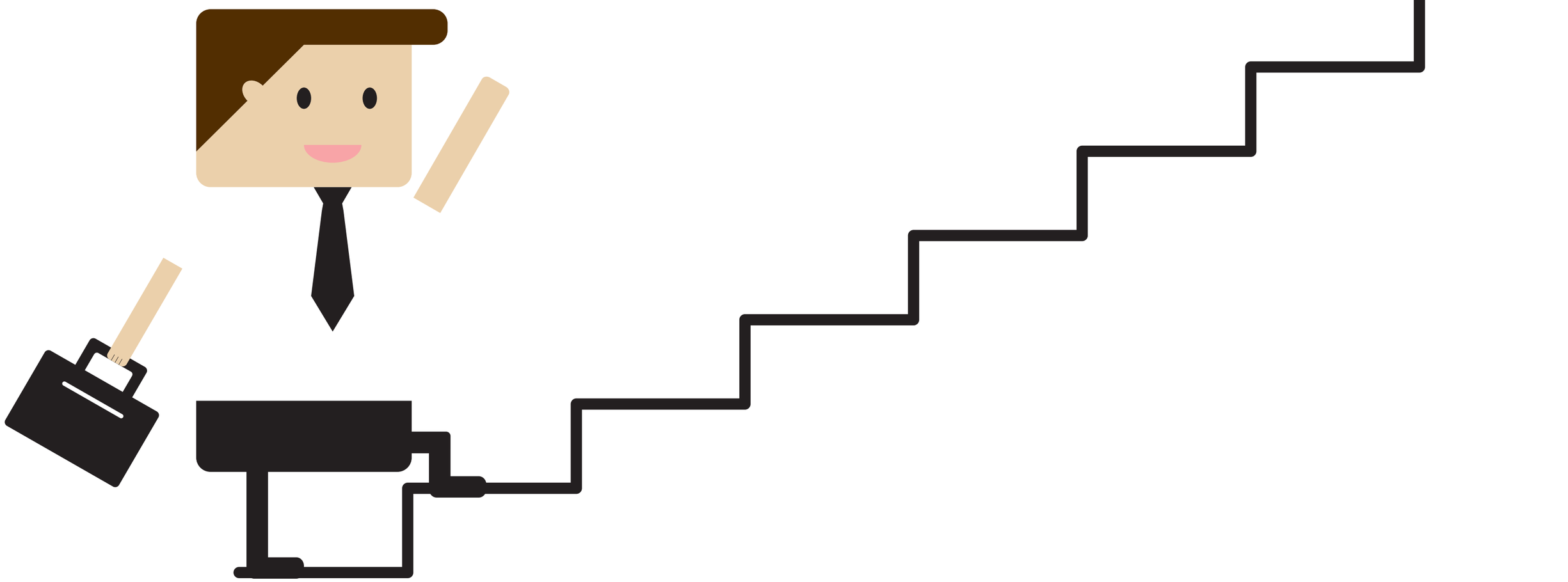
9- Misure idonee
Le misure di sicurezza idonee progettate e realizzate devono assicurare un adeguato livello di sicurezza, bilanciando da un lato lo stato dell'arte e i costi di attuazione e dall'altro i rischi

10- Registro delle attività
È un a dempime nto for male che va a sos tituire l'obbliga di notifica del trattamento all'autorità Garante. è un adempimento che in coordinato con la valutazione d'impatto è funzionale alla definizione delle misure tecniche organizzative adeguate

11- Valutazione rischi - Valutazione d'impatto
Nella valutazione dei rischi si deve tener conto della eventuale distruzione accidentale o illegale, perdita, modifica, rivelazione, o accesso non autorizzato ai dati personali trasmessi, conservati o comunque elaborati.
Bisogna tener conto di: danni fisici, materiali o immateriali

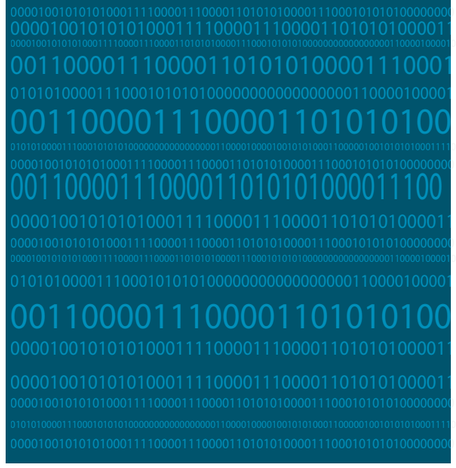
12- Piano d'emergenza
Nel'ottica dell'importanza della circolazione dei dati e della correlata necessità di gestirne il flusso e il lecito trattamento, bisogna provvedere a porre in essere azioni al seguito del verificarsi di eventuali eventi dannosi o pericolosi per il trattamento dei dati personali.

I 12 STEPS ALLA CONFORMITA' GDPR



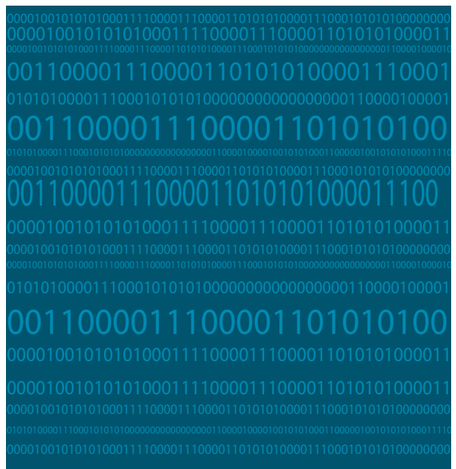
GUIDELINES

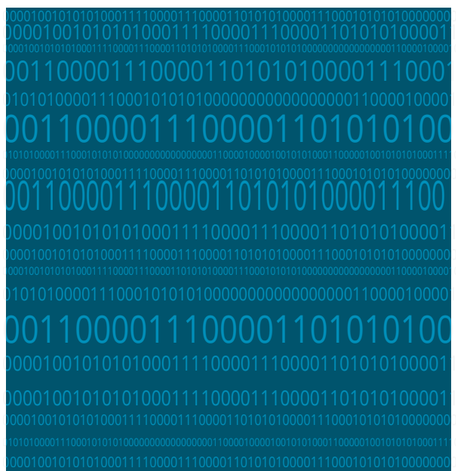
IL NUOVO REGOLAMENTO EUROPEO SUL TRATTAMENTO DEI DATI PERSONALI



INTRODUZIONE

L’obiettivo del nuovo regolamento europeo è quello di semplificare, per quanto possibile, le modalità di trattamento dei dati, pur essendo – gli adempimenti richiesti dallo stesso regolamento – più corposi e stringenti di quelli previgenti.
Nessuno può dubitare del fatto che oggi lo scambio di dati sia una componente fondamentale della crescita economica e molti programmi di sviluppo sono, infatti, basati su un libero scambio di dati.
Il regolamento altro non fa che trasformare questo libero scambio in uno scambio sicuro.
Essendo il concetto di dato personale stato allargato in misura significativa, con l’introduzione dell’IP e dei cookies nel novero dei dati personali per il semplice fatto che lasciano una traccia che potrebbe ricondurre a una persona fisica, è opportuno sottolineare in primo luogo l’importanza della pseudonomizzazione che consente una diminuzione degli obblighi in materia di protezione dati perché crea un collegamento meno diretto fra persona fisica e dato; in secondo luogo assume ancora più rilevanza la finalità della raccolta dati che sia determinata, esplicita e legittima e che consenta l’utilizzo dei dati solo nel contesto di riferimento in cui sono stati raccolti.





INFORMATIVE

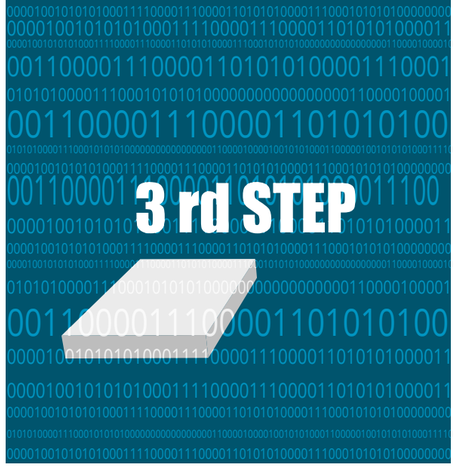
Informative più chiare sul Trattamento dei Dati

L'informativa diventa uno strumento più efficace di trasparenza riguardo al trattamento dei dati personali e all'esercizio dei diritti.
Potrà essere arricchita da icone per facilitare la comprensione dei contenuti per soggetti di etnie diverse.
Gli interessati dovranno essere a conoscenza del fatto che i loro dati siano, eventualmente, trasmessi al di fuori dell'Ue e con quali garanzie tale diffusione dei dati viene effettuata.
L'informativa deve essere resa prima del trattamento dei dati e prima della manifestazione del consenso dell'interessato. Non è necessario rinnovarla a meno che non sussistano situazioni che producano un mutamento della struttura de trattamento. L'informativa deve contenere:
L'identità e i dati di contatto del titolare del trattamento e del suo eventuale rappresentante;
I dati di contatto del responsabile della protezione dei dati (art 13):
Le finalità del trattamento cui sono destinati i dati nonché la base giuridica del trattamento (art 13);
Tali finalità devono essere conformi alla legge, ragionevoli e trasparenti, oltre che specifiche, esplicite e legittime. (art 5);
I legittimi interessi perseguiti dal titolare del trattamento (art 13); I destinatari dei dati personali (art 13);
L'intenzione del titolare del trattamento di trasferire i dati presso un paese terzo o un'organizzazione aziendale (art 13);
Il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare questo periodo (art 13); oltre che tutti i diritti concessi agli interessati sui loro propri dati personali.

CONSENSO

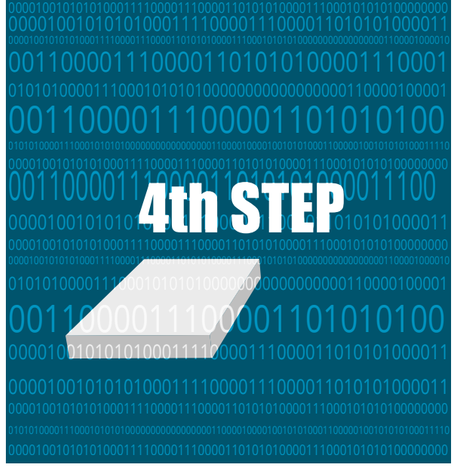
STRUMENTO DI GARANZIA ANCHE ON LINE

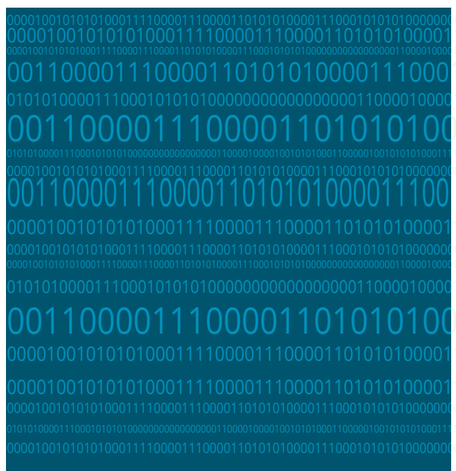
Il consenso dell'interessato al trattamento dei dati personali deve essere "preventivo" ed "inequivocabile", anche quando espresso attraverso mezzi elettronici, ad esempio selezionando una casella su un sito web.
Per il Regolamento europeo il consenso è necessario che sia anche "esplicito" e "granulare".
Il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei dati personali. (art 7 co1). Il consenso è obbligatorio sia per i dati convenzionali che per i dati sensibili. (Art 7 co1). Il consenso può essere prestato anche in modo chiaramente distinguibile dalle altre materie – consenso granulare. (art 7 co.2). il consenso, purchè sia effettivo ed inequivocabile, può essere formulato con varie metodologie: per iscritto, attraverso mezzi elettronici, verbale, mediante selezione di apposita casella su un sito web. Non consiste consenso il silenzio assenso, l'inattività o la preselezione di caselle.
Non è più consentita alcuna forma di consenso tacito, il silenzio assenso quindi non è più considerato una forma di consenso. Non lo è neanche il consenso ottenuto proponendo all'interessato una serie di opzioni già selezionate.
Il consenso potrà essere revocato in ogni momento, ma i trattamenti effettuati dal titolare del trattamento fino alla revoca rimarranno comunque legittimi perché fondati sul consenso precedentemente prestato.
I fornitori di servizi internet e social media dovranno richiedere il consenso ai genitori o a chi esercita la potestà genitoriale per trattare i dati personali dei minori di 16 anni.



LIMITI al trattamento dei dati automatizzato

Con il regolamento europeo aumentano i limiti alla possibilità per il titolare del trattamento di adottare decisioni solo sulla base di un trattamento automatizzato di dati.
Infatti, le decisioni che producono effetti giuridici, come ad esempio la concessione di un prestito, non possono essere basate esclusivamente sul trattamento automatizzato dei dati.
Ne deriva che non è consentita la profilazione, ad eccezione dei casi in cui l'interessato abbia rilasciato il consenso esplicito al trattamento automatizzato dei propri dati o nel caso in cui questo tipo di trattamento risulti strettamente necessario per la definizione di un contratto o avvenga in base a specifici obblighi di legge.
L'interessato ha, comunque, il diritto di opporsi alla decisione adottata sulla base di un trattamento automatizzato e il diritto di ottenere anche l'intervento umano rispetto alla decisione stessa.
Se il trattamento dei dati è finalizzato ad attività di marketing diretto l'interessato ha sempre il diritto di opporsi alla profilazione.





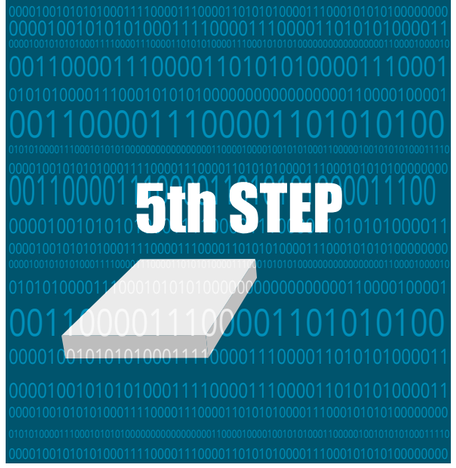
DIRITTI

I Diritti dell'Interessato Aumentano le tutele e le libertà

L'interessato ha il diritto di richiedere al titolare del trattamento lâ€™accesso ai dati personali, la rettifica o la cancellazione degli stessi o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati. (art 13);
oltre ch il diritto di proporre reclamo ad un'autorità di controllo (art 13).
Grazie all'introduzione del cosiddetto «diritto all'oblio», gli interessati potranno ottenere la cancellazione dei propri dati personali anche on line da parte del titolare del trattamento qualora i dati sono trattati solo sulla base del consenso;
se i dati non sono più necessari per gli scopi rispetto ai quali sono stati raccolti; se i dati sono trattati illecitamente; oppure se l'interessato si oppone legittimamente al loro trattamento.
A questo diritto si accompagna l'obbligo per il titolare del trattamento che ha pubblicato i dati di comunicare la richiesta di cancellazione a chiunque li stia trattando, nei limiti di quanto tecnicamente possibile.
Il diritto all'oblio potrà essere limitato solo in alcuni casi specifici: per esempio, per garantire l'esercizio della libertà di espressione o il diritto alla difesa in sede giudiziaria; per tutelare un interesse generale (ad esempio, la salute pubblica); oppure quando i dati, resi anonimi, sono necessari per la ricerca storica o per finalità statistiche o scientifiche.

PORTABILITY

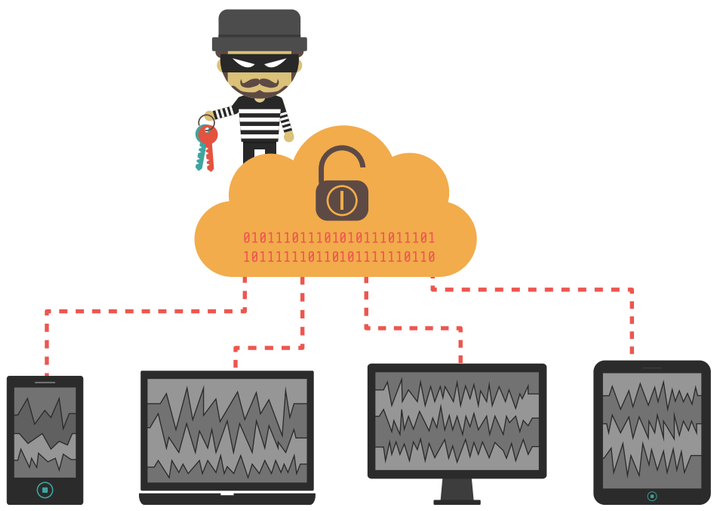
Liberi di inserire i propri dati in un mercato digitale più aperto alla concorrenza e attivo nei servizi digitali.
Il Regolamento introduce il diritto alla «portabilità» dei propri dati personali per trasferirli da un titolare del trattamento ad un altro.
Ad esempio, si potrà cambiare il provider di posta elettronica senza perdere i contatti e i messaggi salvati.
Ci saranno però alcune eccezioni che non consentono l'esercizio del diritto: in particolare, quando si tratta di dati contenuti in archivi di interesse pubblico, come ad



DATA TRANSFER

Garanzie rigorose per il trasferimento di dati

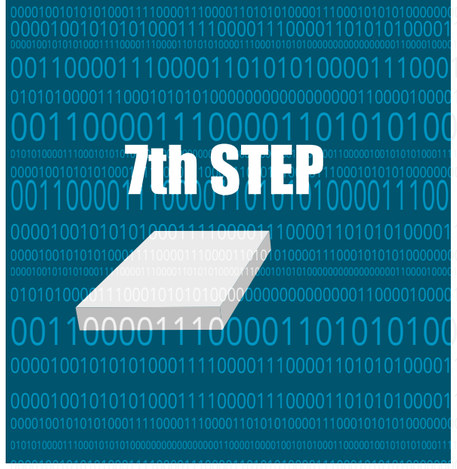
Resta vietato il trasferimento di dati personali verso Paesi situati al di fuori dell'Unione europea o organizzazioni internazionali che non rispondono agli standard di adeguatezza in materia di tutela dei dati, rispetto ai quali il Regolamento introduce criteri di valutazione più stringenti.
I titolari possono utilizzare per il trasferimento specifiche garanzie contrattuali, per le quali il Regolamento prevede norme dettagliate e vincolanti.
In assenza di garanzie contrattuali o riconoscimenti di adeguatezza, i dati potranno essere trasferiti solo con il consenso esplicito dell'interessato, oppure qualora ricorrano particolari condizioni (ad esempio, quando il trasferimento è indispensabile per rispettare specifici obblighi contrattuali, per importanti motivi di interesse pubblico, per esercitare o difendere un diritto in sede giudiziaria, ecc.).
Il trasferimento o la comunicazione di dati personali di un cittadino dell'Ue ad autorità giudiziarie o amministrative di Paesi terzi potranno avvenire solo sulla base di accordi internazionali di mutua assistenza giudiziaria o attraverso strumenti analoghi.

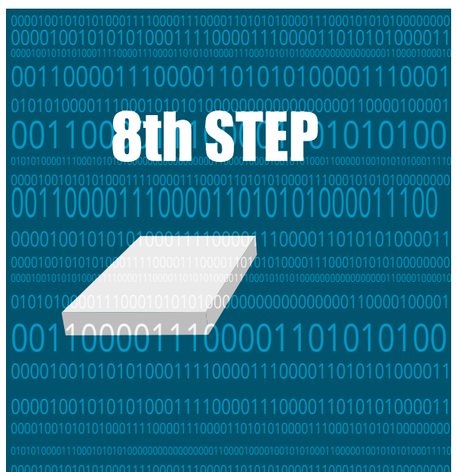


DATA BREACH

Obbligo di comunicazione per qualunque violazione di dati personali

Il titolare del trattamento dovrà comunicare eventuali violazioni dei dati personali (data breach) all'Autorità nazionale di protezione dei dati. Se la violazione dei dati rappresenta una minaccia per i diritti e le libertà delle persone, il titolare dovrà informare in modo chiaro, semplice e immediato anche tutti gli interessati e offrire indicazioni su come intende limitare le possibili conseguenze negative.
Il titolare del trattamento potrà decidere di non informare gli interessati se riterrà che la violazione non comporti un rischio elevato per i loro diritti (quando non si tratti, ad esempio, di frode, furto di identità, danno di immagine, ecc.); oppure se dimostrerà di avere adottato misure di sicurezza (come la cifratura) a tutela dei dati violati; oppure, infine, nell'eventualità in cui informare gli interessati potrebbe comportare uno sforzo sproporzionato (ad esempio, se il numero delle persone coinvolte è elevato). In questo ultimo caso, è comunque richiesta una comunicazione pubblica o adatta a raggiungere quanti più interessati possibile (ad esempio una comunicazione sul sito web del titolare).
L'Autorità di protezione dei dati potrà comunque imporre al titolare del trattamento di informare gli interessati sulla base di una propria autonoma valutazione del rischio associato alla violazione.
Il concetto dei dati personali è stato ampliato fino a comprendere dati (indirizzo ip) che prima non erano considerati personali. Da ciò deriva la necessità di predisporre informative ad hoc con i dettagli sulla modalità del trattamento dati e sui diritti concessi all'interessato relativi al trattamento.
Le competenze e le responsabilità richieste alle figure che coordinano e gestiscono il trattamento dati sono più specialistiche e dettagliate. Ne deriva l'obbligo di formazione del personale e la predisposizione di nomine scritte.
Non esistono più misure minime di sicurezza che erano facilmente individuabili (perché già prescritte dalla legge). Ne deriva che per porre in essere misure idonee di sicurezza occorre procedere obbligatoriamente ad una valutazione dei rischi a seguito della quale predisporre le misure minime da fare per garantire la sicurezza.
Le azioni negative forti che possono creare un evento dannoso per il trattamento dei dati vanno previste, pianificare ed associate ad azioni correttive che consentano di bloccare, arginare, risolvere il problema e contestualmente notificarlo a chi di competenza.



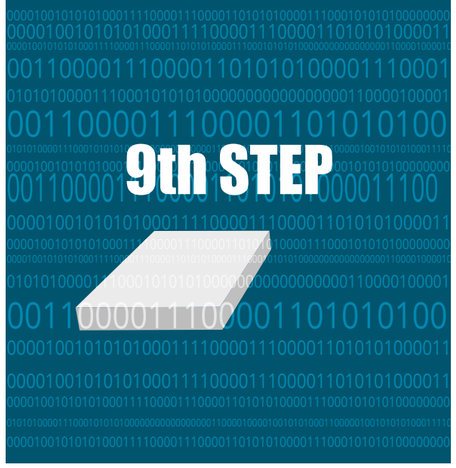


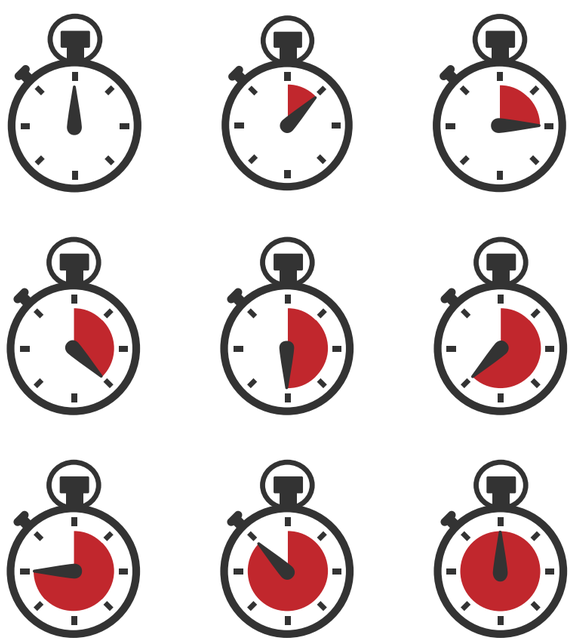
PRIVACY BY DESIGN & BY DEFAULT

Il Regolamento promuove la responsabilizzazione (accountability) dei titolari del trattamento e l'adozione di approcci e politiche che tengano conto costantemente del rischio che un determinato trattamento di dati personali può comportare per i diritti e le libertà degli interessati.
Il principio-chiave è «privacy by design» e " privacy by default" che introducono, rispettivamente, la necessità di predisporre delle procedure specifiche e differenti su ogni diversa tipologia di trattamento dati e di farlo in modo predefinito, cioè ancor prima di iniziare il trattamento stesso

LE NOMINE

La designazione del Responsabile del trattamento, del responsabile per la protezione dei dati e dell'addetto al trattamento deve essere espressa, specifica, scritta e riferibile a determinate mansioni. Il responsabile del trattamento o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso ai dati personali, non può trattare tali dati se non è istruito in tal senso dal responsabile del trattamento. (artt 29 e 30 co.2ter).
Il dpo, Responsabile per la protezione dei dati, è una figura che ha compiti consultivi, di assistenza e di vigilanza del rispetto della disciplina del regolamento Ue sulla privacy.
Può essere contattato direttamente dagli interessati e dal garante della privacy.
Nomina obbligatoria. In alcuni casi la nomina del dpo è obbligatoria. In sintesi si tratta degli enti pubblici e dei soggetti privati che effettuano monitoraggio delle persone su larga scala oppure trattano dati sensibili su larga scala. Gli indici generali per individuare i requisiti della larga scala sono: numero degli interessati; volume dei dati e tipi di dati trattati, durata del trattamento, ambito geografico dell'attività.
Alcuni esempi di trattamenti su larga scala: gli ospedali, i sistemi di traporto pubblico, geo-localizzazione dei clienti di una catena commerciale internazionale, le compagnie di assicurazione, le banche, i fornitori di servizi di telecomunicazioni, i motori di ricerca per trattamenti di dati per pubblicità mirata al comportamento delle persone. Enti pubblici. Tutti gli enti pubblici, tranne gli organi giudiziari, devono nominare il Dpo: i ministeri come le università, i comuni come le regioni. Ci sono enti, diversi dagli enti pubblici istituzionali, cui si applica diritto pubblico, e che operano per il pubblico interesse. Per esempio le public companies nel settore dei servizi pubblici (energia, ambiente ecc.). Per questi enti la nomina del Dpo non è obbligatoria, ma è consigliato come buona pratica. I Dpo abbiano competenza sulla normativa nazionale ed europea e sulle prassi relative alla materia della protezione di dati, una profonda conoscenza del regolamento europeo. È utile anche prevedere programmi di aggiornamento continuo. A queste competenze sulla normativa specifica della privacy è utile aggiungere la conoscenza del settore commerciale del titolare del trattamento. Il Dpo dovrebbe avere sufficiente conoscenza delle operazioni di trattamento, e altrettanta sufficiente conoscenza del sistema informativo, della sicurezza de dati e delle esigenza di protezione dei dati. Nel caso di ente pubblico, il Dpo dovrebbe avere una solida conoscenza dell'ordinamento e del Responsabilità. In riferimento alla responsabilità del Dpo, in caso di trattamenti non conformi al regolamento europeo, il Dpo non è personalmente responsabile. Il Regolamento, infatti, esige la dimostrazione di osservanza del regolamento sesso solo a carico del titolare e del responsabile del trattamento.





MEASURES IDONEE

Le misure di sicurezza idonee progettate e realizzate devono as sicurare un adeg uato livello di sicurez za, bila nciando da un lato lo stato dell'arte e i costi di attuazione e dall'altro i rischi che presentano i trattamenti e la natura dei dati personali stessi. (art 25 co. 1) Sulla base di questi parametri, quindi, il titolare del trattamento mette in atto misure tecniche organizzative adeguate quali ad esempio:

l'uso dei soli dati necessari per una certa finalità. Tale obbligo vale per la quantità dei dati, la portata del trattamento, il periodo di conservazione e l'accessibilità. (privacy by default);

La pseudonomizzazione, volta ad attuare in modo efficace la protezione dei dati creando un rapporto meno diretto tra interessato e dato. La minimizzazione, utile al fine di selezionare solo i dati strettamente necessari al raggiungimento del fine per cui sono stati raccolti, in ossequio dei principi dell'uso minimo e indispensabile del dato. (privacy by design);

Trasparenza sulle funzioni e sul trattamento dei dati.

Consentire l'accesso all'interessato al fine di controllare il trattamento dei dati.

Capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico.

Consentire all'interessato la cancellazione di dati divenuti inesatti. Obbligo per il titolare del trattamento di creare e migliorare le caratteristiche di sicurezza attraverso l'analisi dei rischi ed il vaglio dell'adeguatezza delle misure di tutela.

Prevedere l'efficienza e l'efficacia di un piano d'emergenza da attivare nel caso di violazione di dati.

Obbligo di effettuare una valutazione dei rischi.

Il livello di sicurezza risulta adeguato se risulta in grado di contrastare i seguenti rischi:

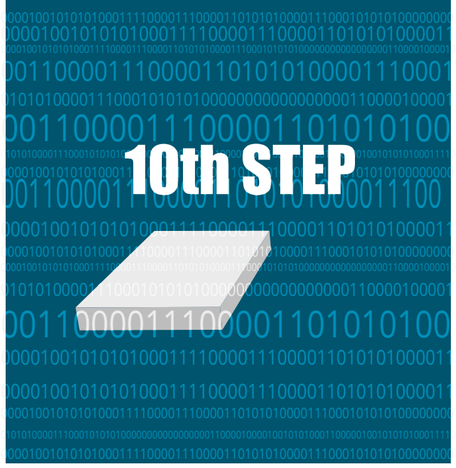
Distruzione

Perdita

Modifica

Divulgazione non autorizzata

Accesso accidentale o illegale

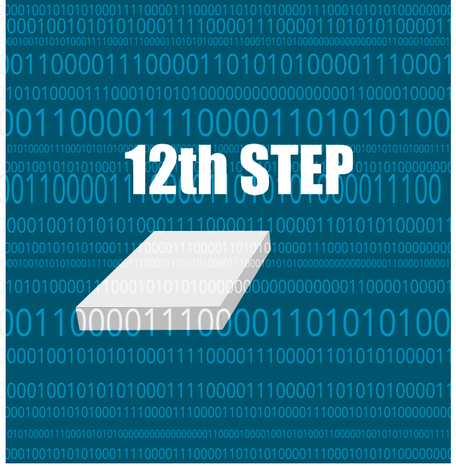


REGISTRO DELLE ATTIVITA'

È un adempimento formale che va a sostituire l'obbliga di notifica del trattamento all'autorità Garante. Un adempimento che in coordinato con la valutazione d'impatto è funzionale alla definizione delle misure tecniche organizzative adeguate. L'espletamento di entrambi consente di privarli di appesantimenti burocratici (verifica del garante) inserendoli in logiche di programmazione e audit interni.
Seppur non obbligatori per le imprese sotto i 250 dipendenti è vivamente consigliato per avere una rappresentazione chiara del trattamento dei dati
in sede di controllo.

VALUTAZIONE DI IMPATTO

Nella valutazione dei rischi si deve tener conto della eventuale distruzione accidentale o illegale, perdita, modifica, rivelazione, o accesso non autorizzato ai dati personali trasmessi, conservati o comunque elaborati. Bisogna tener conto di: danni fisici, materiali o immaterali.
La valutazione dei rischi è sempre necessaria, come è sempre necessaria la sicurezza dei trattamenti.
La valutazione d'impatto è invece un'attività non sempre necessaria ma riservata alla presenza di rischi elevati e presuppone il coinvolgimento,
nelle ipotesi più delicate, dell'autorità garante. Per i trattamenti che presentano un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento deve svolgere una valutazione d'impatto per determinare, in particolare, l'origine, la natura, la particolarità e la gravità di tale rischio. Se la tecnologia disponibile o i costi di attuazione non rendano possibile l'adozione di misure di gestione del rischio elevato, prima del trattamento si deve consultare l'autorità di controllo. (es. rilevazione biometrica – no accesso alternativo).



PIANO DI EMERGENZA

Nel'ottica dell'importanza della circolazione dei dati e della correlata necessità di gestirne il flusso e il lecito trattamento, bisogna provvedere a porre in essere azioni al seguito del verificarsi di eventuali eventi dannosi o pericolosi per il trattamento dei dati personali. Esempio: nel caso si verifiche un danneggiamento dei dati personali trattati da un'azienda a seguito di un trasferimento o di una comunicazione non autorizzata all'esterno bisogna provvedere ad avvisare il Garante entro 72 ore e gli interessati.

Per ottemperare a tale obbligo occorre definire procedure che consentano di fare azioni correttive a seguito dell'evento dannoso. Cio significa che bisogna formalizzare tutte le azioni possibili che possano correggere e/o comunicare l'evento anomalo ed esterno che ha comportato il danno.

Predisporre un piano d'emergenza significa, quindi, definire le azioni consentite e quelle non consentite in fase di formazione ma significa anche inquadrare gli eventi sentinella e le correlative azioni riparatrici.

Si definiscono eventi sentinella tutte quelle azioni negative forti che mettono in pericolo il trattamento dei dati nonché il prestigio reputazionale dell'azienda.

Sono azioni negative tutte quelle inquadrabili come intromissione effrazione nei sistemi aziendali: attacco di un virus, aceraggio,furto dati, programmatore che sbaglia una query ed estrae tutti i dati personali.

Tali azioni sono, come detto negative; perché le stesse azioni siano configurabili come forti (e quindi come eventi sentinella che necessitano di azione correttiva standardizzata – es. comunicazione al garante) occorre definirne l'entità, l'ambito, il dominio, l'effetto.

Definire le azioni sentinella e le correlative azioni correttive significa, quindi, individuare e rendere note le procedure da attivare per risolvere o contenere l'effetto negativo scaturito dall'evento dannoso.

È opportuno far presente che l'art 83 del Regolamento europeo nel prevedere le condizione e le circostanze che possono formare esenzione dalla responsabilità del trattamento illecito, prevede anche che in sede di controllo da parte dell'autorità vengano valutate le misure adottate dal titolare del trattamento per attenuare il danno subito dagli interessati; tali misure adottate, altro non sono che la predisposizione delle le procedure

da attivare per risolvere o contenere l'effetto negativo scaturito dall'evento dannoso, di cui si parlava prima.