GDPR & Dati Personali

- Andrea Alfieri -

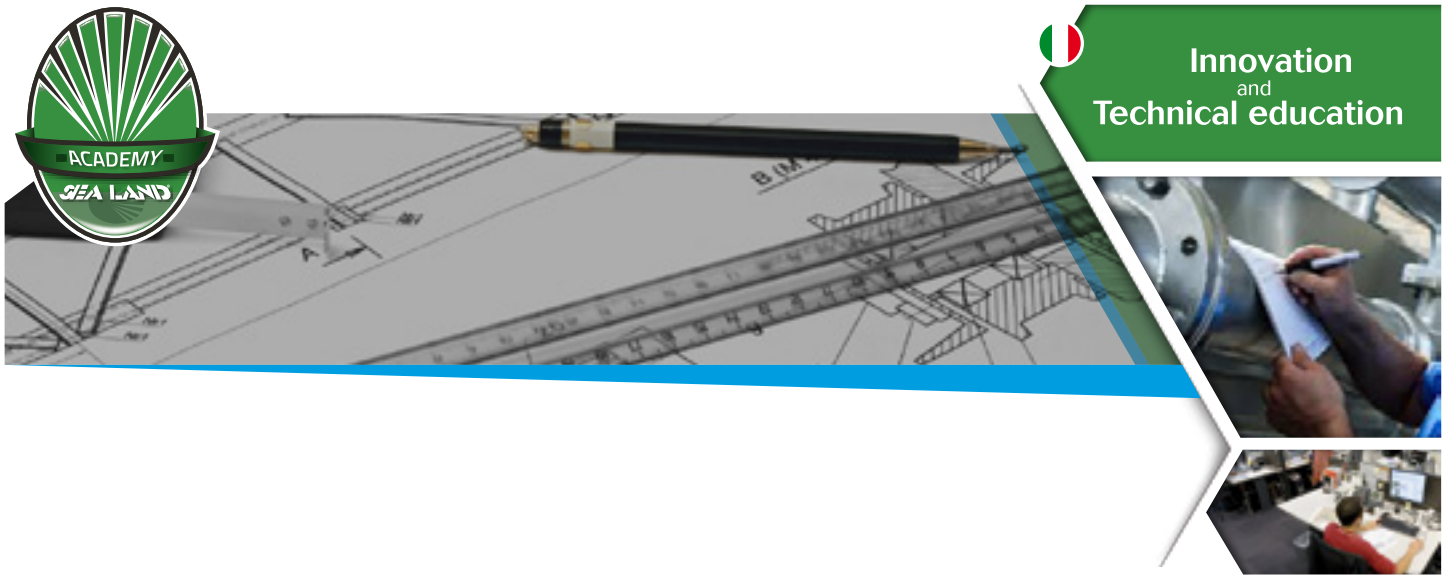
Attività formativa svolta il 30 gennaio 2018

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI PADOVA

LEN GRUPPO

FuturSkill ManpowerGroup

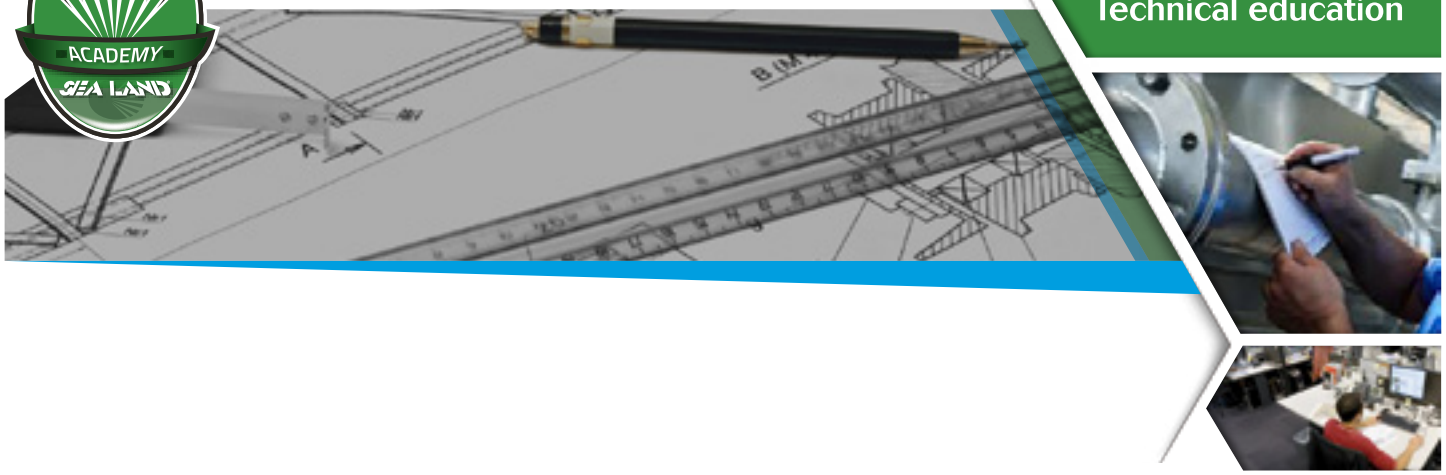
Manpower



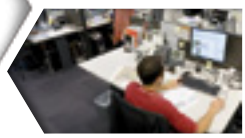
UN BUON MOTIVO PER...

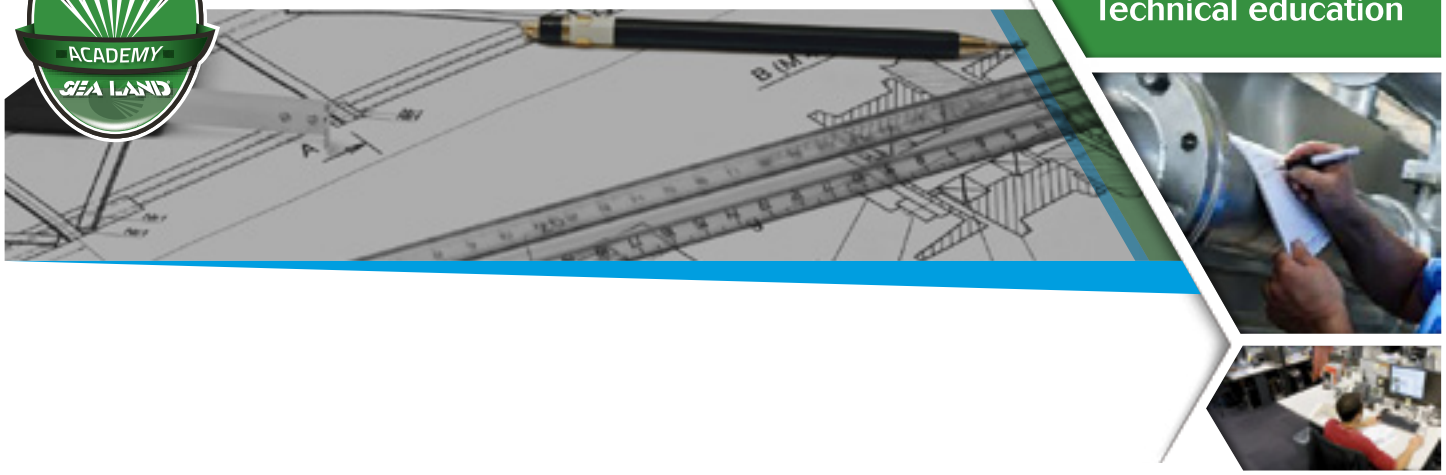
L'abilità di prendere decisioni con il supporto dei dati è considerata una delle competenze principali per i professionisti del Digital Marketing, ed una opportunità fondamentale per qualsiasi organizzazione commerciale che voglia affrontare la Digital Trasformation. Oggi tramite la rete e grazie a nuove tecniche di marketing come l'inbound marketing, Lead generation, Marketing automation ogni azienda è un grado di aprire nuovi mercati ed opportunità.

Esiste spesso però un forte gap tra la conoscenza dei concetti e degli strumenti e la reale efficacia dell'utilizzo dei dati per approfondire le analisi sul comportamento dei clienti. Inoltre l'imminente arrivo della normativa GDPR General Data Protection Regulation già deliberato il 24 Maggio 2016 che diventerà effettivo in tutti gli Stati Europei dal 25 maggio 2018 sembra voler porre serie barriere alle opportunità aziendali di utilizzo strategico dei dati a fini commerciali.



INDICE:

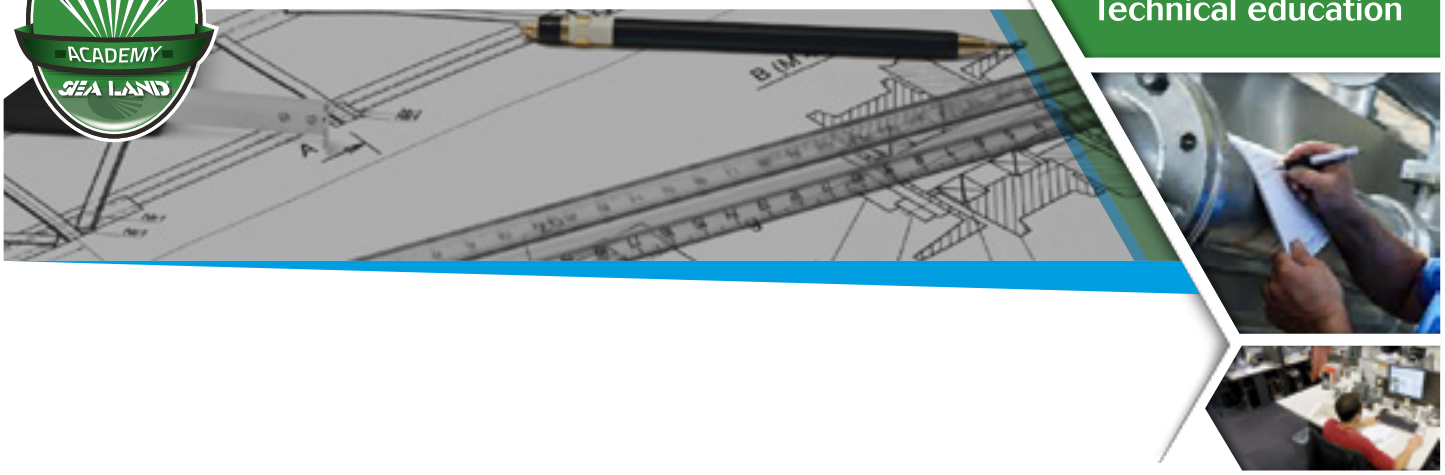




1. GDPR

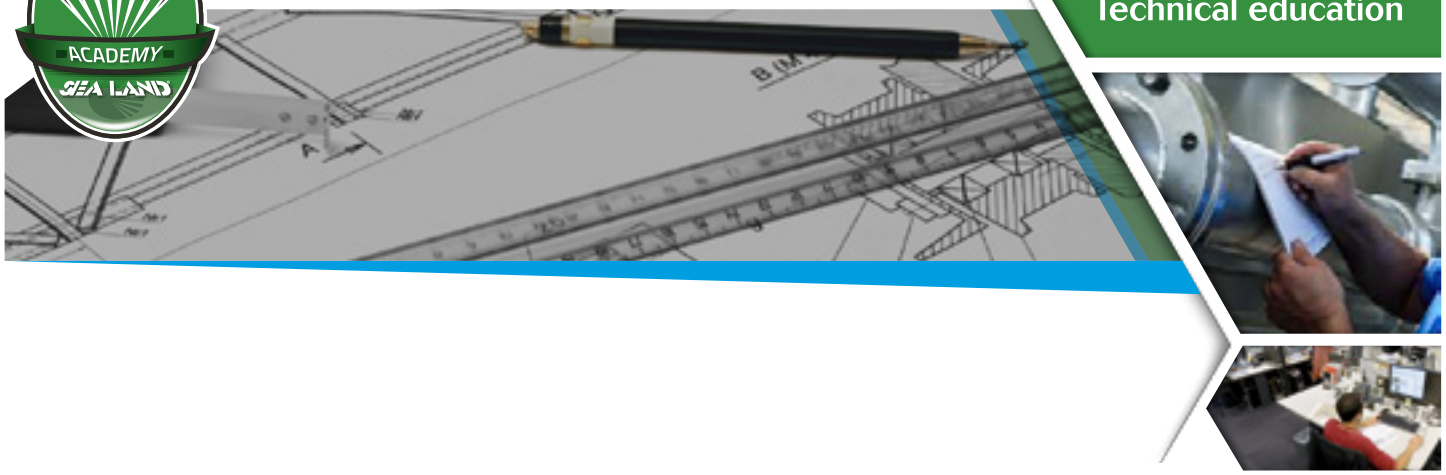
1.1 COS'È GDPR IN BREVE

- **GDPR** è l'acronimo di General Data Protection Regulation;
- Fa riferimento al nuovo Regolamento Europeo (UE) 2016/679 emanato il 27 Aprile 2016 in Gazzetta Ufficiale;
- Il regolamento stabilisce le regole applicabili in tutti i paesi dell'**Unione Europea** in materia di Dati Personali;
- Il regolamento non necessita di leggi nazionali di recepimento;
- Il GDPR è quindi un nuovo **statuto di norme**, che delineano un set di regole condivise, nuovi processi aziendali e nuove figure aziendali;
- Segna l'inizio di una nuova era nelle norme che tutelano il diritto a esercitare un controllo di informazioni che riguardano una persona fisica;
- Gestione Dati in azienda diventa un modello organizzativo specifico, definito e strutturato (no improvvisazione, no opinabilità, no sanatorie);
- Il GDPR diventa pienamente operativo dal **25 maggio 2018**.



1.2 CONTESTO E CRITICITÀ

- Il regolamento UE 2016/679 abroga la precedente direttiva UE 1995/46 in tema di trattamento di dati personali (privacy).
- La precedente direttiva UE 1995/46 è stata recepita dall'Italia in due momenti: il primo codice privacy formalizzato nel decreto legislativo 675/1995 e la sua seconda versione, nota comunemente come «Testo unico sulla privacy», nel decreto legislativo 196/2003 che ha sostituito il precedente 675/1995.
- La direttiva è un atto legislativo che sancisce un obiettivo che tutti i paesi della comunità europea devono raggiungere. Spetta tuttavia ai singoli paesi definire attraverso leggi nazionali e disposizioni come tali obiettivi vadano raggiunti.
- Viceversa, **il regolamento è un atto legislativo vincolante**, una volta approvato diventa una **normativa cogente** e deve essere applicato in tutti i paesi membri.
- La capillare diffusione dei servizi legati alle tecnologie digitali ha cambiato profondamente le attività quotidiane delle persone, trasformando i dati personali in una fonte di profitti per molti settori d'impresa.
- I dati personali sono in grado di raccontare in dettaglio la vita di ogni cittadino: usi, costumi, vita privata, vita pubblica, orientamento sessuale, politico e religioso.
- Sono quotidiane le notizie di cronaca che raccontano come un non corretto utilizzo delle nuove tecnologie, ovvero un errato trattamento dei dati personali, produca effetti spesso drammatici nella vita delle persone: è infatti illusorio pensare che esistano barriere tra la vita digitale e quella reale, gli eventi prodotti on-line producono impatti al di fuori di Internet, nella vita quotidiana e nei rapporti con gli altri.

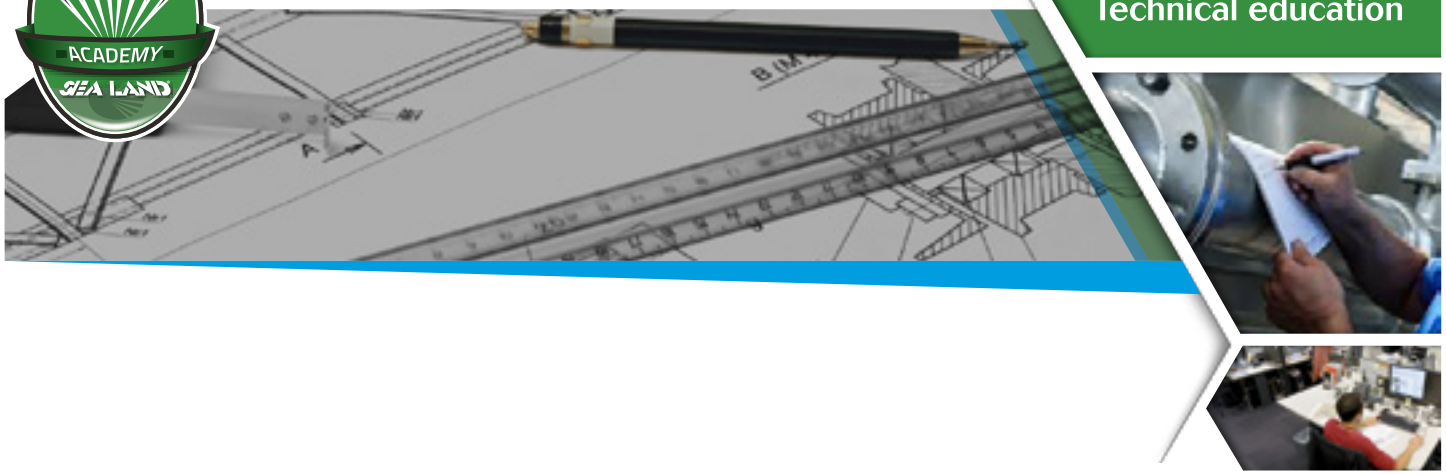


1.3 COSA COMPORTA PER L'AZIENDA

I dati sono il petrolio dell'era digitale e saper raccogliere, leggere e utilizzare dati personali è una chiave per **generare business**. I dati danno la capacità di sapere come si genera, si comunica e si trasferisce valore ai clienti. Siamo solo all'inizio dell'era **BIG DATA**, nei prossimi anni si svilupperà molto.

Attraverso dati personali le aziende possono:

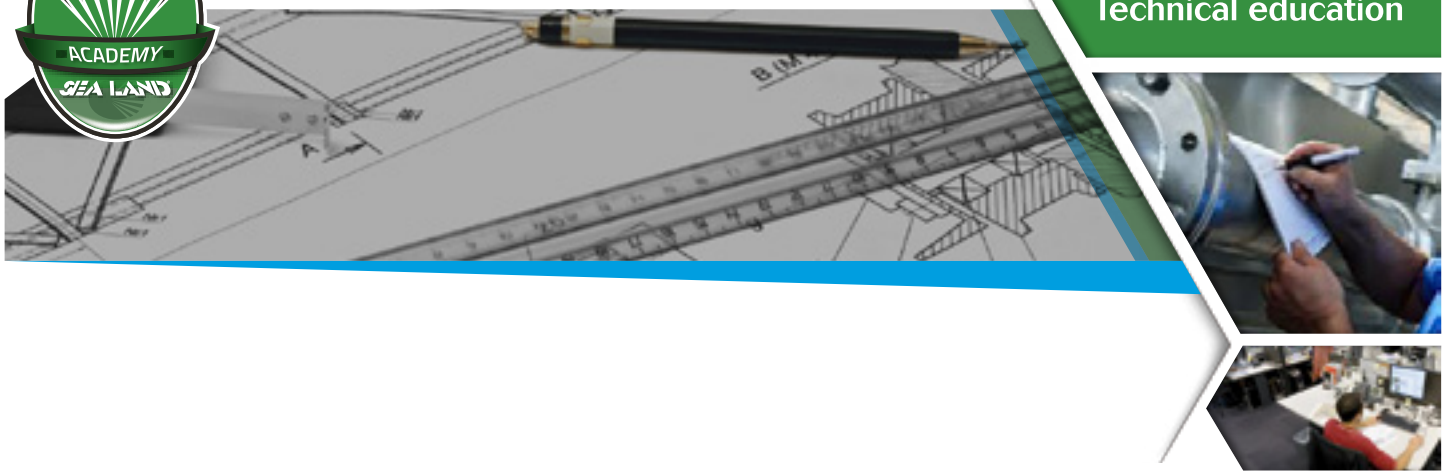
- Creare prodotti innovativi;
- Formulare offerte mirate a buyer personas;
- Controllare, profilare e analizzare dati per adattare comunicazioni marketing e commerciali;
- Gestire un patrimonio di utenti collegati, profilati e suddivisi in «clusters»;
- Aziende possono inoltre acquisire e vendere dati personali a terze parti;
- Possono organizzare eventi, concorsi, contest e attività di Lead generation (acquisizione contatti).



1.4 QUALI DATI RIGUARDA

"Dato" = informazione alfanumerica, immagine, suono o qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»). Non tutti i dati sono da proteggere in quanto tali, spesso la loro protezione deriva dalla capacità di interpretazione dei dati di cui sono capaci le aziende e la loro interpretazione è:

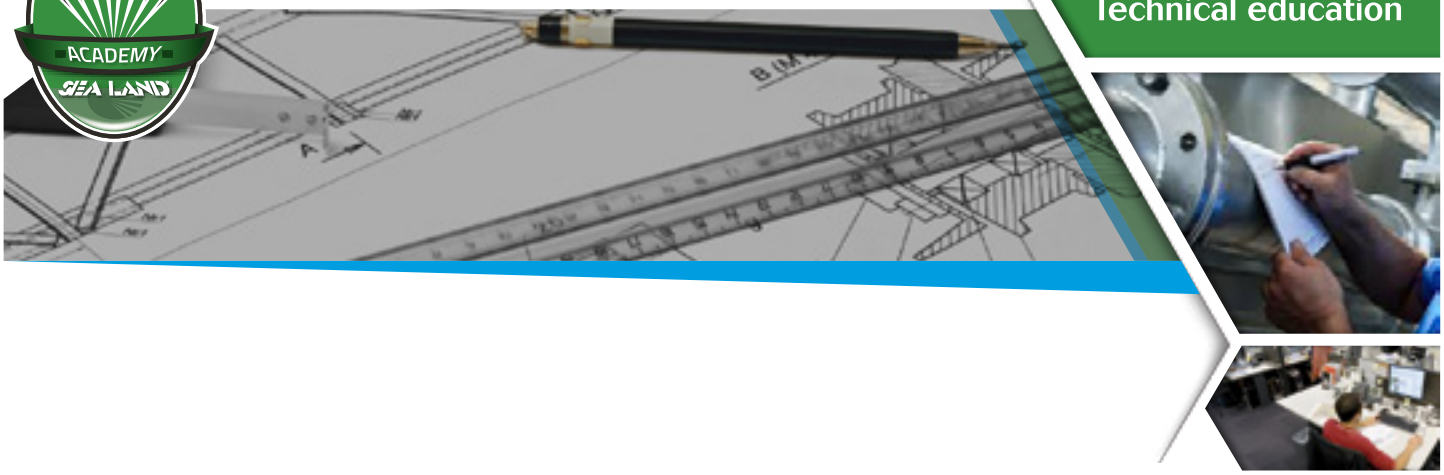
- **DATI PERSONALI**: Dati comuni (nome, anagrafica, codice fiscale, indirizzo, mail, telefono...) e qualunque informazione riconducibile ad una persona fisica.
- **DATI SENSIBILI**: Dati idonei a rivelare convinzioni (religiose, filosofiche, politiche...) e condizioni (ricchezza, condizioni di salute...).
- **DATI GIUDIZIARI**: Dati che rivelano la presenza di atti giudiziari o provvedimenti.
- **DATI SUPERSENSIBILI**: Dati medici come i dati biometrici. Sono relativi ad alcune caratteristiche fisiche uniche dell'individuo: ad esempio l'impronta digitale, l'impronta dei denti, l'immagine del volto, etc.
- **DATI DI GEO-REFERENZIAZIONE**: sono sia dati personali che dati sensibili, idonei infatti anche a rivelare condizioni o convinzioni sulla base dei luoghi frequentati.



1.5 QUALI FUNZIONI AZIENDALI RIGUARDA

Il GDPR ha potenzialmente un impatto su varie funzioni aziendali, ad esempio:

1. **Marketing**, raccolta dati da siti, social network, newsletter, inbound marketing, couponing, e-commerce, iscrizioni eventi.
2. **Vendite** (sales) raccolta e monitoraggio dati clienti (CRM).
3. **Acquisti** (purchasing) raccolta dati fornitori se con dati personali.
4. **Risorse Umane** (HR) raccolta dati personali e sensibili di candidati, dipendenti e collaboratori contrattualizzati.
5. **Customer Service** raccolta dati e tracciamento assistenza clienti.
6. **Sistemi Informativi** (IT), raccolta, stoccaggio, accesso e protezione dati nei sistemi informatici azienda, videosorveglianza.
7. **Top Management** (Titolare azienda) responsabilità penale a persona fisica (non azienda) passibile di sanzioni pecuniarie.



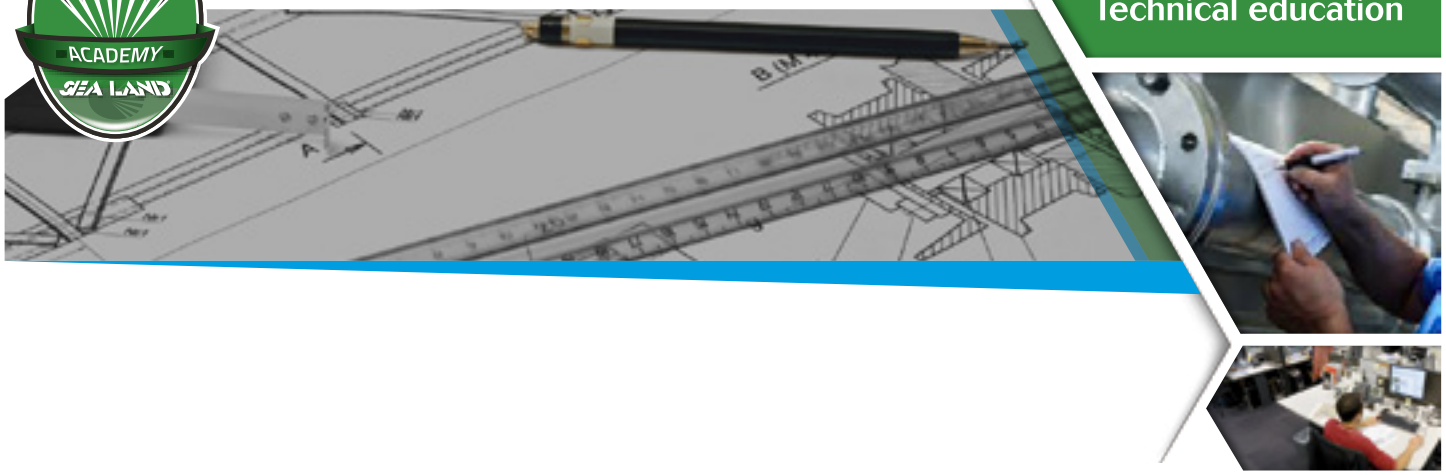
1.6 QUALI DATI HANNO LE AZIENDE

Ho chiesto ad alcune aziende quali Dati personali hanno o raccolgono:

- Dipendenti?
- Referenti commerciali di clienti e fornitori?
- Consulenti esterni?
- Consumatori finali in caso di raccolta dati e-commerce?
- Cliente finale - in caso di complain/lamentele che tracciamo (ticket)?
- Cliente finale – se ci scrive via mail?
- Cliente finale – se chiama numero verde?
- Contatti raccolti in fiere o eventi?
- Modulo raccolta dati su sito?
- Lavora con noi o curriculum?
- Campagne di Lead Generation con Landing Pages e Marketing automation?
- Geolocalizzazione di mezzi trasporto e personale?
- Dati raccolti da miei dipendenti in aziende altrui (es. pulizie)
- Altri?

1.7 QUALI SONO I PROTAGONISTI DEL GDPR

1. L'INTERESSATO
2. IL TITOLARE DEL TRATTAMENTO
3. IL RESPONSABILE DEL TRATTAMENTO
4. L'ADDETTO AUTORIZZATO AL TRATTAMENTO
5. L'AUTORITÀ' DI CONTROLLO
6. IL DATA PROTECTION OFFICER (DPO o RPD)



1.8 PRINCIPI FONDANTI DEL GDPR

1) **Principio della Accountability**: Onere di dimostrare l'adozione, senza convenzionalismi, di tutte le misure di sicurezza (analisi dei rischi) necessarie al trattamento secondo norma. Redigere e conservare adeguate documentazioni attestante il "modello organizzativo e di sicurezza privacy", e "valutazioni di impatto sulla protezione dei dati personali".

2) **Privacy by design e Privacy by default**: Privacy by design - nel momento in cui approcciamo un nuovo trattamento necessariamente dobbiamo farci delle domande e progettare e farlo partire, pensando già alle rischiosità che esso comporta. Privacy by default - quando parto devo avere il processo blindato, garantendo il massimo livello di protezione e tutela possibile. Poi gradualmente posso rilassare il sistema ma sempre e solo a fronte del consenso dell'interessato

3) **DPO Data Protection Officer**: Nasce una figura di indirizzo, organizzazione, e controllo. Non è un operativo ma lavora come organo di controllo (come un auditor), vigila, verifica i processi, figura di raccordo tra i proprietari delle informazioni (interessati) e colui che si pone da interfaccia con il garante.

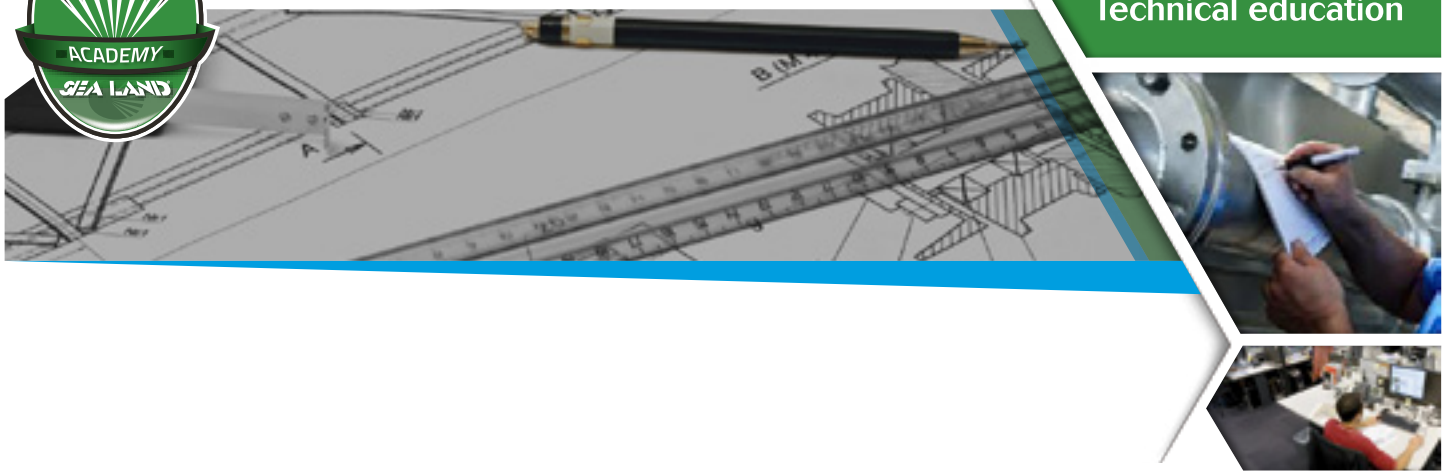
4) **Co-responsabilità tra Titolare/Controller e responsabile**: Le responsabilità ricadono anche sul responsabile se lui non ha messo in atto tutti i processi a norma di legge. Il titolare deve quindi formare in maniera attenta e specifica, fornire in maniera scritta/esplicita, dei mansionari e modus operandi ai responsabili per assicurarsi che lavori a norma di legge.

Il GDPR impone un approccio **Risk Based**, e organico, seguendo le normative ISO 27000 ad esempio.

Nella normativa si parla di **tecnologia di sicurezza** (DARI), **Tecnologie di Protezione** (Anonimizzazione, Pseudonomizzazione, Formazione continua) e **Procedure** (controlli, monitoraggio, gestione eventi, cifrature).

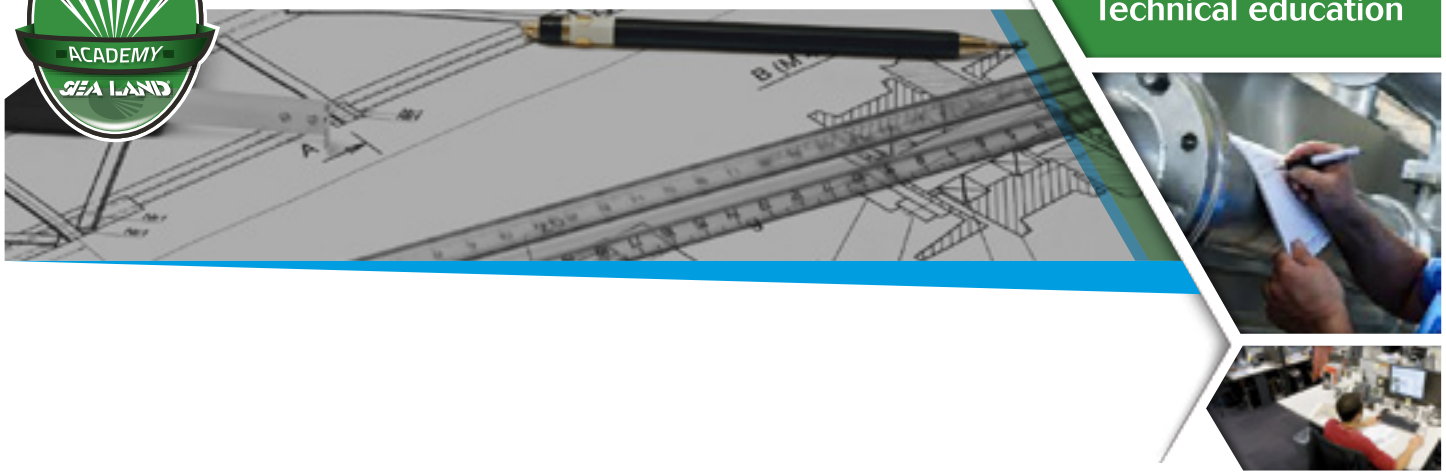
Il modello di gestione dei processi previsto nella normativa è:

- Scope: identificare il perimetro, il flusso dei dati;
- Model: capire i livelli di criticità per ogni categoria di dati;



- Process: implementazione di un processo di analisi rischi, essere misurabile, identifica ambiti dove concentrare i controlli;
- Decision: Si decide le operazioni di mitigazioni che contengono i rischi sotto una certa soglia;
- Review: Rivedere il processo con misurazione performance per poter migliorare i processi continuamente;

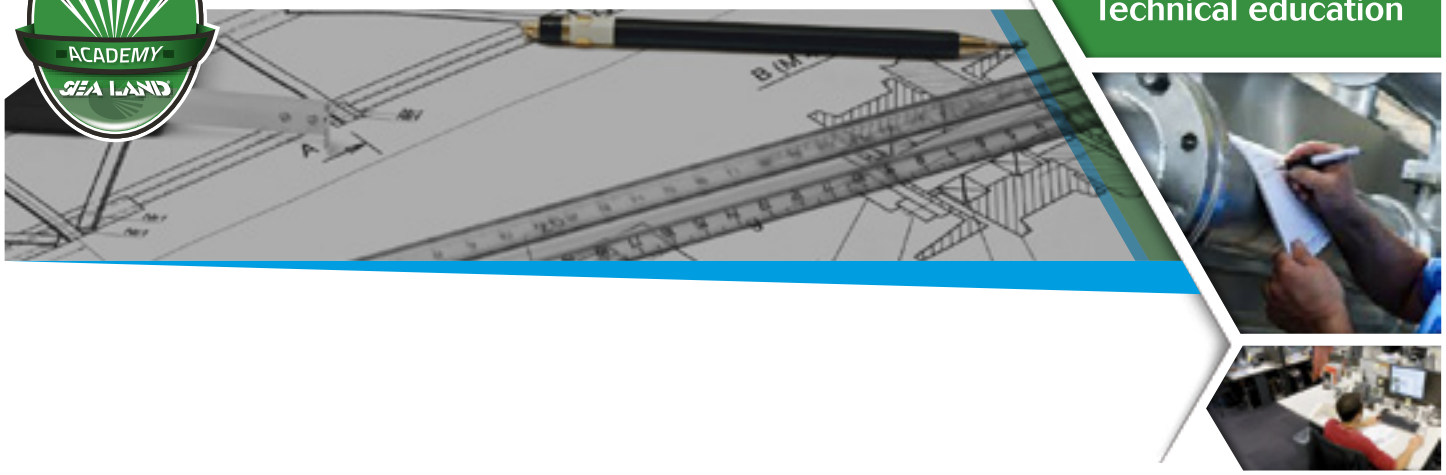
Questo è un pattern metodologico consolidato per chi gestisce processi. Tutto questo va **OBBLIGATORIAMENTE documentato per iscritto.**



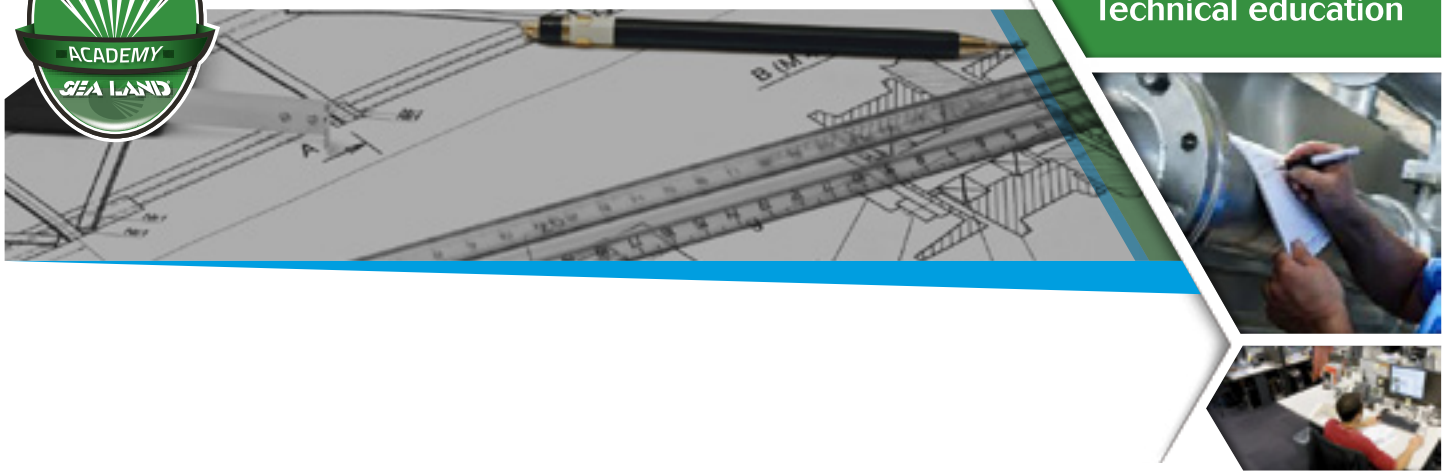
1.9 ADEMPIMENTI A CARICO DEL TITOLARE

Entro il 25 maggio 2018 deve:

1. Attribuire «ruoli» e definire «modello organizzativo» gestione dati;
2. Se Trattamento si basa su consenso, essere in grado di dimostrare che interessato ha concesso benestare;
3. Dimostrare che i dati sono usati «solo» per le finalità definite in consenso (cancellati, non conservati in caso contrario);
4. Adottare nuovo modello conforme per fornire «informativa» a interessato;
5. Saper fornire in formato appropriato a interessato i dati che lo riguardano, fornire anche ad altro titolare se richiesto (portabilità);
6. Adottare «codici condotta» o «certificazioni» e «linee guida di governance» per dimostrare rispetto obblighi di legge;
7. Opportunità di «formare» adeguatamente i dipendenti alla nuova normativa (riduce i propri rischi personali);
8. Tenere un registro delle attività di Trattamento svolte;
9. Analizzare rischi e dotarsi di misure tecniche per la sicurezza dei dati;
10. Limitare accesso ai dati «solo» a personale formato e «autorizzato» dal titolare stesso per iscritto;
11. Dotarsi di procedura notifica al Garante entro 72 ore in caso di violazione;
12. Documentare ogni violazione dati personali, circostanze, conseguenze e provvedimenti adottati;
13. Saper comunicare con l'interessato senza ritardi in caso di violazione o rischi per i suoi diritti e libertà personali;
14. Svolgere una valutazione di impatto e rischi (risk analysis);
15. Raccogliere, ascoltare e ricevere le opinioni degli interessati in materia trattamento dei propri dati;



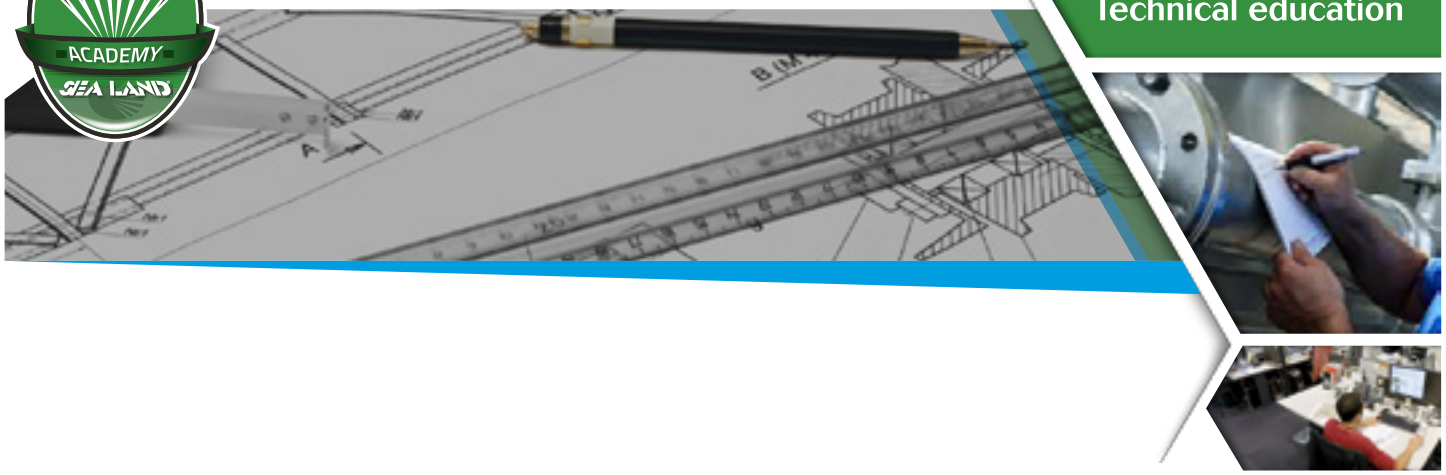
16. Aprire un canale con l'autorità di controllo, confrontarsi in caso di rischi e ottemperare ad ogni parere ricevuto;
17. Designare un Data Protection Officer (DPO) e coinvolgerlo in tutte le questioni riguardanti protezione dati;
18. Fornire al DPO tutte gli accessi e le risorse necessarie per svolgere il suo ruolo di vigilanza all'interno della azienda;
19. Non rimuovere o penalizzare il DPO e assicurarsi di conoscere tutte le istruzioni che riceve per l'esecuzione del proprio ruolo;
20. Fornire al DPO e tutti i dipendenti coinvolti nella gestione dei dati dei «mansionari dettagliati» per iscritto (non verbale).



1.10 SANZIONI A CARICO DEL TITOLARE:

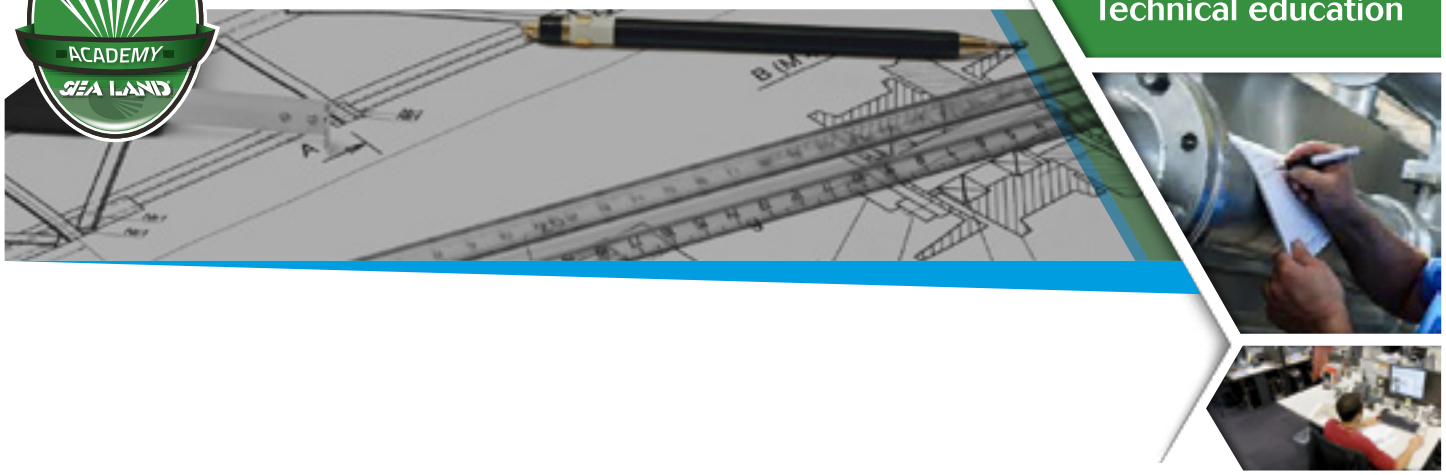
Dal 25 maggio 2018:

- Il mancato adempimento alla normativa, quando causa violazioni comporta **sanzioni PENALI** per i Titolari o altri responsabili (se il titolare riesce a dimostrare la loro colpa e nessuna propria mancanza);
- Sanzioni amministrative pecuniarie **fino a 10 milioni di Euro** (o fino al 2% del fatturato mondiale anno precedente) per violazioni agli obblighi del titolare trattamento o propri responsabili e DPO;
- Sanzioni amministrative pecuniarie **fino a 20 milioni di Euro** (o fino al 4% del fatturato mondiale anno precedente) per violazioni al principi di base del trattamento, diritti degli interessati, trasferimento di dati personali a un destinatario di un paese terzo. Anche per la mancata osservanza di un ordine dell'autorità di controllo.



1.11 DA DOVE PARTIRE

- Fare un inventario di tutte le proprietà aziendali (dipendenti, siti, software, gestionali, eventi…) che raccolgono, conservano, usano dati personali (sia interni che esterni);
- Fare un inventario di tutte le «Informative» che vengono fornite e valutare come potrebbero cambiare in funzione delle nuove regole (indicazioni, finalità, responsabili, tempo di conservazione…);
- Confrontarsi con il management aziendale per coinvolgerli nel processo (HR, IT, Sales, Marketing, Contabilità…). Capire quali dati personali, sensibili, giudiziari posseggono (anche storici);
- Verificare su quali server sono posizionati i dati (eventuali flussi extra-europei di dati usando servizi cloud?);
- Iniziare a sperimentare Privacy by Design (analisi rischi) ed effettuare il Privacy Impact Assessment, per minimizzare impatti e contenere costi gestione;
- Valutare se necessario introdurre in azienda un Data Privacy Officer (DPO);
- Fornire a tutti i dipendenti accesso ad un percorso formativo (in FAD) per dimostrare di aver «formato» adeguatamente alla nuova normativa il personale (e ridurre rischi per Titolare);
- Analizzare gli effetti del diritto alla Portabilità dei dati e adottare cautele organizzative per evitare impatti gravi sui database aziendali;
- Definire nuove regole di acquisizione e documentazione del consenso.



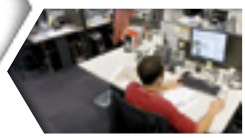
2. DPO

2.1 QUANDO SERVE UN DPO

Esistono 3 casi in cui la designazione del DPO è **obbligatoria**, vengono riportate di seguito le ipotesi previste nella sezione 4 dall'articolo 37 "Designazione del responsabile della protezione dei dati":

- Il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali (esercitano le loro funzioni giurisdizionali);
- Le attività principali del Titolare del trattamento o del Responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
- Le attività principali del Titolare del trattamento o del Responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 (dati giuridici | sensibili) o di dati relativi a condanne penali e a reati di cui all'articolo 10.

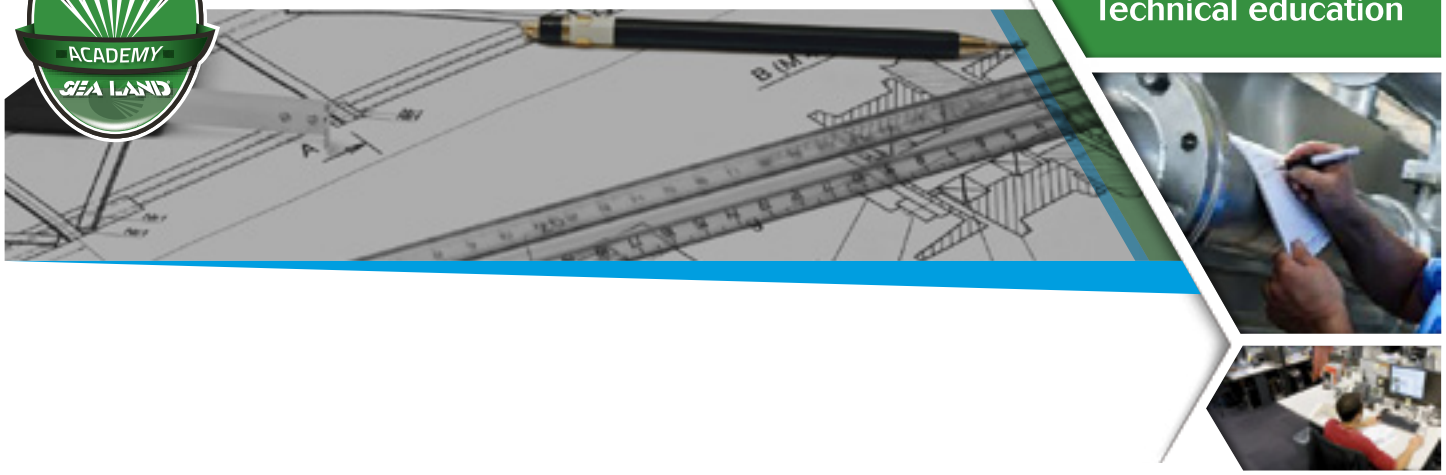
In tutti gli altri casi la nomina è dunque facoltativa.



2.2 COME SCEGLIERE UN DPO

Il DPO Data Processor Officer o RPD Responsabile della Protezione Dati

1. Dovranno avere un'approfondita conoscenza della normativa e delle prassi in materia di privacy, nonché delle norme e delle procedure amministrative che caratterizzano lo specifico settore di riferimento (Link Garante Privacy);
2. Privilegiare soggetti che possano dimostrare qualità professionali adeguate alla complessità del compito da svolgere, magari documentando le esperienze fatte;
3. La normativa attuale non prevede l'obbligo per i candidati di possedere attestati formali delle competenze professionali. Tali attestati, rilasciati anche all'esito di verifiche al termine di un ciclo di formazione, possono rappresentare un utile strumento per valutare il possesso di un livello adeguato di conoscenza della disciplina ma, tuttavia, non equivalgono a una "abilitazione" allo svolgimento del ruolo del RPD;
4. La normativa non prevede l'istituzione di un albo dei "Responsabili della protezione dei dati" che possa attestare i requisiti e le caratteristiche di conoscenza, abilità e competenza di chi vi è iscritto. Enti pubblici e società private dovranno quindi comunque procedere alla selezione del RPD o DPO, valutando autonomamente il possesso dei requisiti necessari per svolgere i compiti da assegnati.
5. Il DPO lavora in team, coinvolgendo e coordinando settori diversi d'azienda e deve avere conoscenze legali sulla normativa ma non solo da un punto di vista legale.
6. Deve essere coinvolto e informato in modo costante su ogni Progetto aziendale che possa avere una ricaduta sul Trattamento dati (i.e. campagne marketing, Digital Marketing, newsletter, nuovo sito, informativa privacy, Lead Generation su Landing page, Job posting per raccogliere candidati, evento aziendale con registrazione, realizzazione video o foto con clienti o persone per pubblicazione)
7. Il DPO deve saper individuare differenti rischi di privacy e fornire soluzioni basate sulla rispettiva

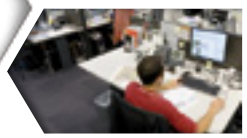


area di interesse o di esperienza ma senza bloccare le attività aziendali

8. Il DPO mantiene traccia di tutti i PIA eseguiti su progetti diversi e nel tempo diviene la memoria storica che può contaminare le implicazioni derivanti nella nuove molto rapidamente.

2.3 REGISTRO ATTIVITÀ DI TRATTAMENTO

- La compilazione del Registro delle Attività di trattamento o comunque della mappatura dei dati trattati è uno dei primi passi necessari per poter adempiere alle prescrizioni del GDPR come da articolo 30.
- Obbligatorio per aziende con più di 250 dipendenti. Consigliato per le altre.
- Il Registro serve per Mappare le Attività di Trattamento (non i singoli Trattamenti). E' un documento dinamico, aggiornabile e deve rispondere a domande specifiche.
- Il modello di DPS proposto dall'Autorità Garante richiedeva un elenco delle attività di trattamento. Chi ha DPS parte quindi da lì.
- Serve per dimostrare (accountabilty) di operare secondo un principio di privacy by design. Avere un registro non aggiornato evidenzierebbe di fatto la mancanza di un presidio nel continuo del proprio modello privacy.



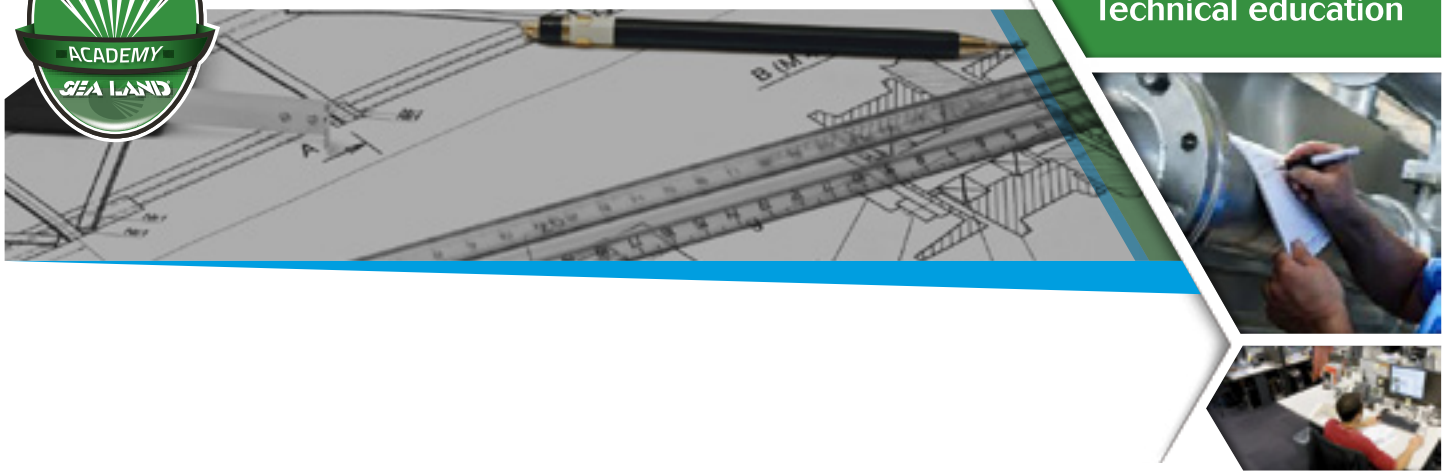
3. PIA

3.1 PIA PRIVACY IMPACT ASSESSMENT

- Il PIA (Privacy Impact Assessment) è uno strumento operativo richiesto dalla nuova normativa GDPR.
- Il processo è codificato e strutturato in fasi, e deve aiutare le aziende ad analizzare con sistematicità, ad individuare e a ridurre i rischi privacy per gli individui interessati coinvolti dal rilascio di ogni progetto, soluzione o regola.
- La valutazione d'impatto del trattamento dei dati personali costituisce parte integrante dell'approccio Privacy by Design imposto dalla normativa.
- Aiuta a garantire e dimostrare che i problemi potenziali siano identificati negli stadi iniziali della progettazione.
- Si compone in 6 fasi le quali hanno un ciclo ricorsivo. Le fasi permettono di attualizzare la valutazione iniziarla e apportare modifiche man a mano che il progetto si sviluppa.

3.2 QUANDO SERVE

1. **Valutazione personale** basata sulla profilazione personale
2. Decision making automatizzato con effetti legali sulle persone (i.e. **marketing automation**)
3. Monitoraggio (video sorveglianza) su vasta scala
4. **Dati sensibili o di natura altamente personale** (ad esempio, le opinioni politiche, fedina penale, dati sanitari personali, dati finanziari, documenti personali, email, codici di login personale)



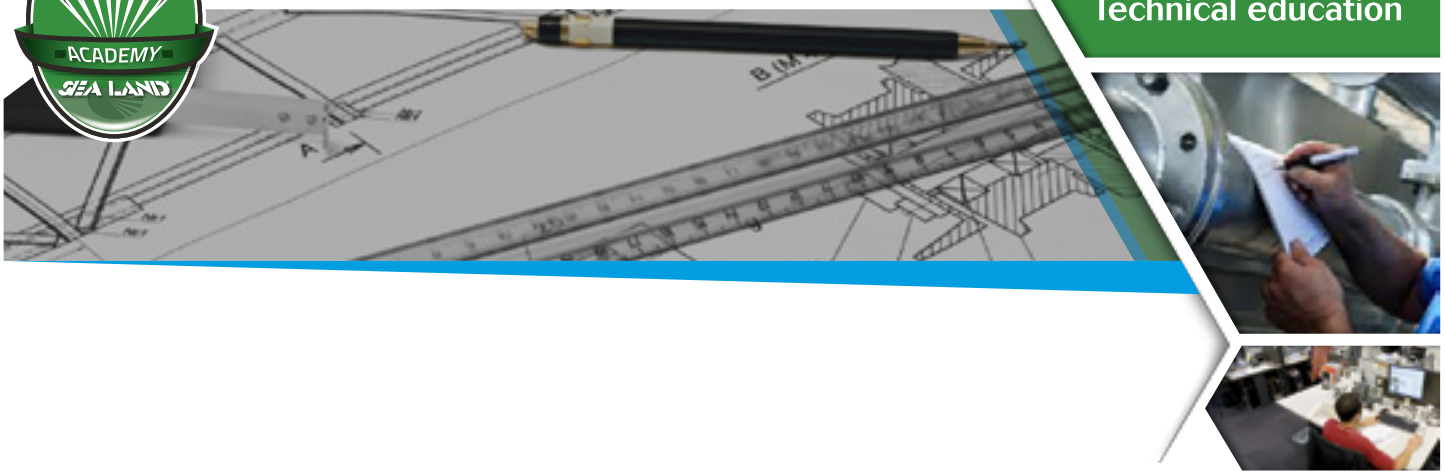
5. Trattamento dati su **larga scala** (ad esempio durata del trattamento, area geografica, volume dei dati trattati in relazione alla popolazione)
6. Il **matching e la combinazione di dataset diversi** (ad esempio, provenienti da database diversi e raccolti in origine per scopi diversi, la cui combinazione rischia di eccedere la portata del consenso originario)
7. Dati che riguardano categorie di **soggetti deboli** (bambini, anziani, malati, malati di mente, richiedenti asilo)
8. Utilizzo innovativo dei dati e nuove tecnologie in azienda di cui non si conoscono le conseguenze personali e sociali (ad esempio, **impronte digitali, riconoscimento facciale, Internet of Things**)
9. Quando il trattamento stesso impedisce ai soggetti titolari dei dati di esercitare un diritto o di usare un servizio o un contratto (ad esempio, nel caso in cui una **banca controlli l'affidabilità di un cliente consultando un database che raccoglie le referenze di credito**).

3.3 VALUTAZIONE PERSONALE

Questa fase serve ad un'organizzazione a:

- Spiegare ciò che il progetto intende realizzare, quali sono i benefici attesi per l'organizzazione, per gli individui e per le altre parti
- Decidere, in base ad un insieme di domande mirate di screening, se un PIA sia necessario
- Dimensionare le risorse a seconda dell'entità del progetto e il tempo necessario alla valutazione
- Capire gli impatti potenziali e i passi che potrebbero essere richiesti per identificare e ridurre il rischio.

Qui si valuta se per il progetto è necessario integrare la PIA all'interno delle fasi di sviluppo del progetto stesso (ci sono rischi e considerazioni legate a dati e privacy?).



3.4 DESCRIZIONE FLUSSI E COINVOLGIMENTO PARTECIPANTI

Questa fase serve ad un'organizzazione a capire:

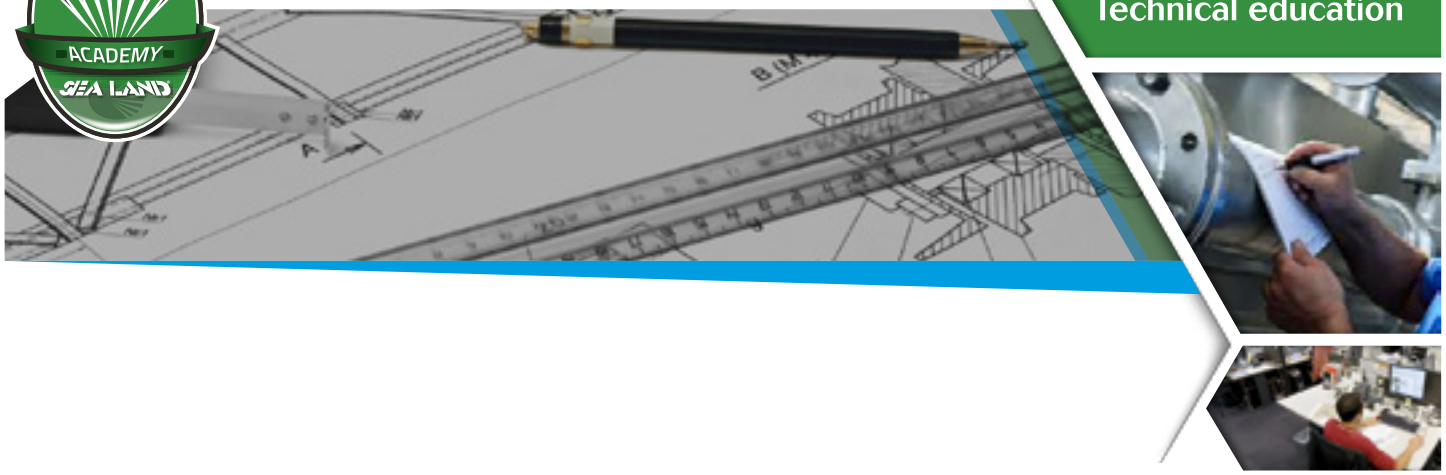
- quali informazioni sono utilizzate; come vengono trattate nelle singole fasi; cosa servono, ovvero per quale finalità; da chi sono ottenute, a chi sono comunicate; chi ne deve avere accesso.
- Questa fase del processo PIA può essere supportata da fonti informative già disponibili all'interno dell'organizzazione per descrivere come i dati saranno utilizzati.
- Il DPO ha un ruolo chiave, con l'autorità di rivolgersi a chi è in grado di guidare le fasi del PIA sui processi esistenti. Questa figura infatti mantiene traccia di tutti i PIA eseguiti su progetti diversi e può contaminare le implicazioni derivanti nella nuove.

Il DPO lavora in team, coinvolgendo e coordinando settori diversi d'azienda. Serve per individuare differenti rischi di privacy e fornire soluzioni basate sulla rispettiva area di interesse o di esperienza.

3.5 IDENTIFICAZIONE RISCHI PRIVACY E CORRELATI

Questa fase serve ad un'organizzazione a capire:

- aspetti di Privacy che espongono il progetto in esame a rischi di Privacy.
- che il processo PIA è insieme una forma di risk assessment e di risk management. Un progetto che è intrusivo sul fronte del pubblico aumenta anche i rischi di multe, di danni reputazionali, o di perdite di business se rilasciato con carenze o soluzioni inappropriate.
- un set di quesiti che consenta di far emergere le vulnerabilità e le minacce e su queste determinare gli effetti su cui quantificare gli impatti.



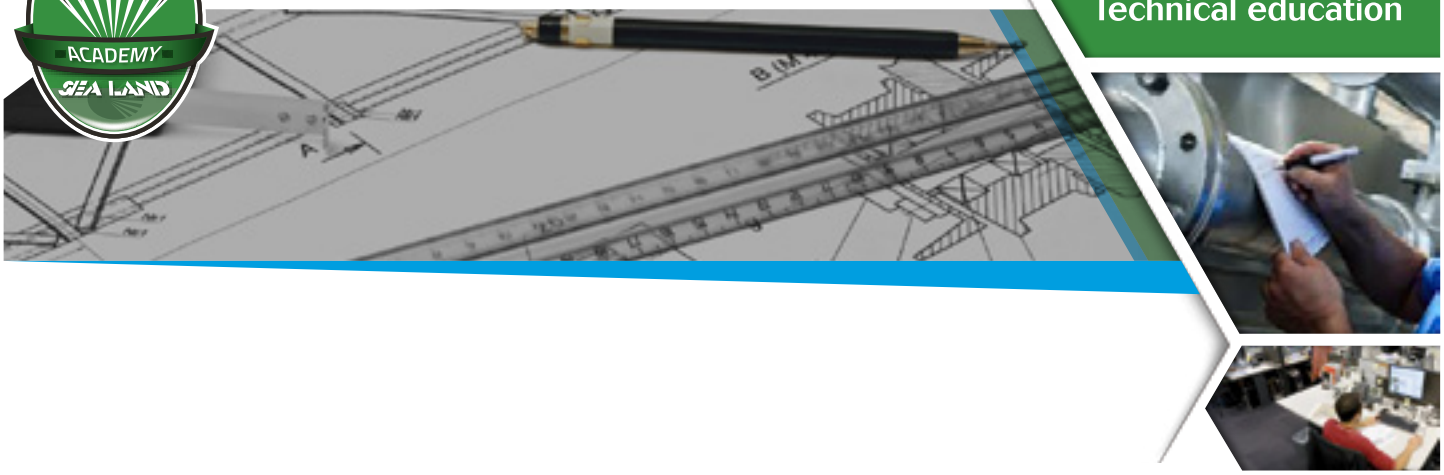
Il documento centrale di questa fase è il Privacy Risk Register dove sono riportate le descrizioni delle valutazioni fatte, al fine di dettagliare la mappatura dei rischi integrabile nel Risk Register di progetto.

3.5 IDENTIFICAZIONE SOLUZIONI E MISURE

Questa fase serve ad un'organizzazione a:

- Identificare quali soluzioni possono essere intraprese per i rischi. Il PIA dovrebbe offrire una serie di possibili opzioni per indirizzare ciascun rischio
- lo scopo non è quello di eliminare completamente l'impatto ma è quello di ridurre l'impatto ad un livello accettabile pur consentendo di realizzare un'iniziativa.
- soppesare se gli scopi e i risultati del progetto sono proporzionati con l'impatto previsto sugli interessati. Ci possono essere costi per elaborare soluzioni. Valutare i costi e i benefici delle possibili soluzioni.

I costi vanno da acquisto di software a stampe liberatorie, a fronte del rischio di sanzioni o provvedimenti o di essere esposti ad effetti reputazionali. Ne vale la pena?



3.6 APPROVAZIONE DECISIONI E REGISTRAZIONE RISULTATI

Questa fase serve ad un'organizzazione a:

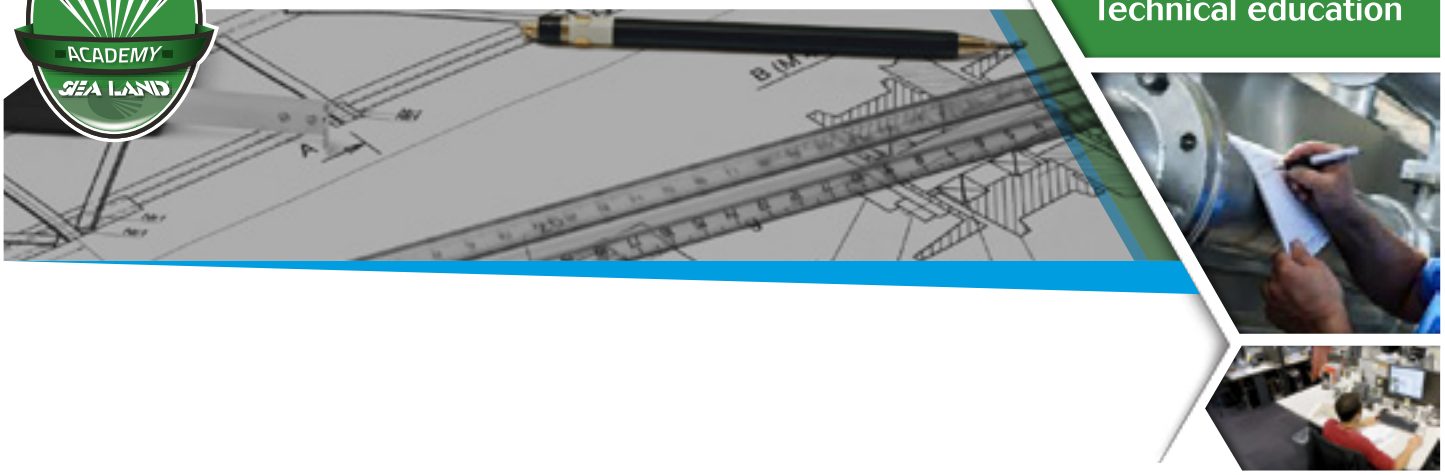
- tener traccia dei passi seguiti nel processo decisionale, compreso chi li abbia approvati, inclusa l'esplicita argomentazione sostenuta per accettare rischi e l'assunzione di responsabilità dei responsabili
- Per concludere l'attività si produce un report finale, da allegare alla documentazione di progetto, per riassumere il processo e i passi compiuti per mitigare il rischio privacy e per consentire di ricostruire a posteriori i motivi delle scelte fatte sulla base dei rischi individuati
- Il report può anche costituire una forma di comunicazione e di trasparenza verso gli interessati che ne richiedano la consultazione e diventare così integrante alla strategia di comunicazione

Questo documento quindi deve essere pensato «verso» l'esterno (interessati) ma anche sostenere una difesa in caso di richiamo dell'autorità di controllo.

3.7 INTEGRAZIONE DEL PIA NEL PIANO DI PROGETTO

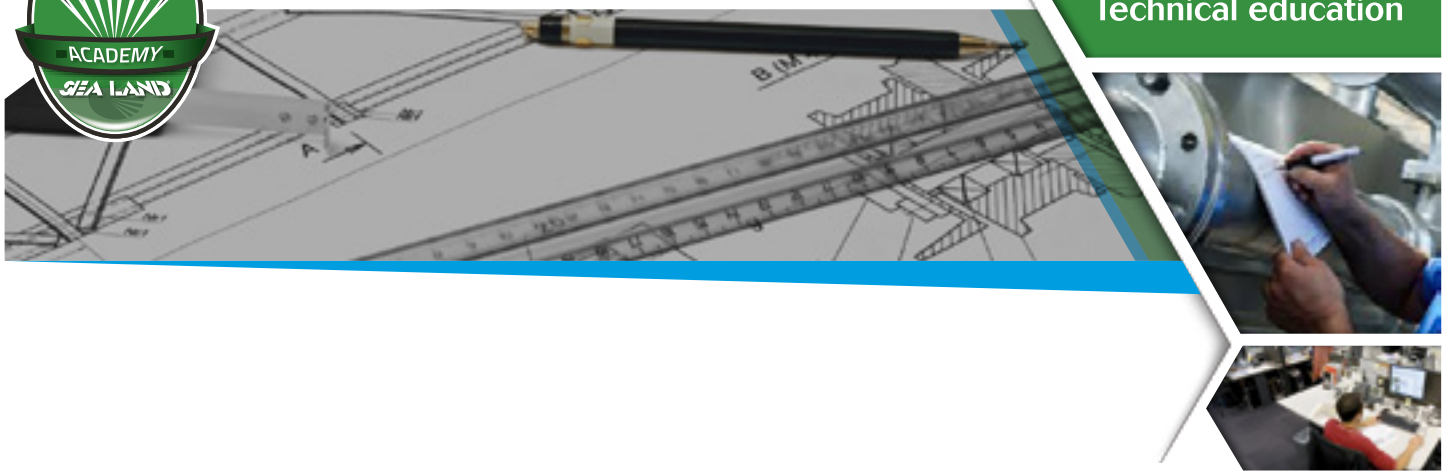
Questa fase serve ad un'organizzazione a:

- integrare il PIA con il Piano progetto
- Il PIA non è quindi un documento marginale o a se stante, ma deve essere integrato e affiancato al piano progetto, sin dall'inizio.
- Considerare il PIA durante tutta l'elaborazione del Piano Progettuale implica che man a mano che il progetto si sviluppa, servirà rivalutare l'impatto sul PIA stesso in vari momenti di progettazione



- Un PIA potrebbe generare azioni che continuano dopo che la valutazione è finita per cui è necessario che queste azioni vengano monitorate

Il PIA diviene quindi una traccia su cui costantemente migliorare e imparare per progetti futuri.



4. RISK BASED

4.1 ANALISI DI IMPATTO PRIVACY

Articolo 35 del GDPR prevede che la valutazione d'impatto della rischiosità sia una azione a carico del controller di sorveglianza. Tale attività non riguarda solo il «set-up» iniziale (non solo fatta una volta all'inizio) ma è protratta nel tempo e con modelli e procedure definite nella normativa stessa.

Il GDPR impone un approccio Risk Based, e organico, seguendo le normative ISO 27000 (ISO27001-ISO27005). Si parla di:

- Tecnologia di sicurezza (DARI),
- Tecnologie di Protezione (Anonimizzazione, Pseudonomizzazione, cifratura),
- Formazione continua
- Procedure definite (controlli, monitoraggio, gestione eventi)

4.2 GDPR E VALUTAZIONE RISCHIO

La norma GDPR poi affronta l'analisi dei rischi e li definisce riprendendo la Definizione del Rischio definito nella ISO 27005 del 2011:

«la possibilità che una determinata minaccia ha di sfruttare delle vulnerabilità di una risorsa (asset, dati, sistemi etc) e quindi causare impatti indesiderati all'organizzazione (danni economici)».

Il rischio può essere: accettato, eluso, mitigato o traferito. Servono quindi contromisure (Trattamento del rischio) ovvero azioni (procedurali, tecnologiche, assicurative etc) in grado di mitigare e diminuire gli impatti e di conseguenza i danni all'organizzazione stessa.

Anche la 196/2003 prevedeva Misure di sicurezza idonee a ridurre al minimo i rischi di "distruzione, perdita, accesso non autorizzato, o trattamento dati non consentito, o non conforme alla finalità dichiarata".