G.E.N.I. s.r.l.
Gestione Esercizi Navali Industriali

Regolamento (UE) 679/2016

Affrontare il GDPR come un Sistema di Gestione

Ing. Stefania Pusateri e
Ing. Massimo Giambarresi

G.E.N.I. s.r.l.
Gestione Esercizi Navali Industriali

Affrontare il GDPR come un Sistema di Gestione

Affrontare il GDPR come un Sistema di Gestione

Questo intervento nasce:

- Dalle personali esperienze di Consulenti di sistemi di gestione, di RSPP e di OdV;
- Dal ricordo, durante le attività lavorative, della difficoltà di dialogo che può venirsi a creare tra OdV, RSPP, Consulenti di Gestione e la Governance aziendale sotto forma di linguaggio, obiettivi e loro modalità di ottenimento

Affrontare il GDPR come un Sistema di Gestione

La mancanza di rapporto comporta una serie di problematiche che si riversano sulla qualità dell'attività lavorativa (comprensiva dei risultati) e sui rapporti interpersonali, con evidente nocumento per tutti gli attori partecipanti

Affrontare il GDPR come un Sistema di Gestione

- Il consulente lavora male e rende peggio;
- Il cliente non ottiene quanto auspicato o (ancora peggio) si convince (fino a reale necessità) di essere coperto dal punto di vista legislativo/normativo

Affrontare il GDPR come un Sistema di Gestione

Principio fondamentale che deve avere il cliente, per ottenere reale beneficio dalle attività di consulenza è

La Consapevolezza = "condizione di chi è consapevole. L'avere conoscenza, il rendersi conto di qualcosa".

Affrontare il GDPR come un Sistema di Gestione

1. Consapevolezza da parte del cliente
2. Competenza da parte del consulente
3. Comunicazione da parte del consulente
4. Coinvolgimento da parte del cliente
5. Miglioramento Organizzativo da parte del cliente
6. Raggiungimento dell'Obiettivo da parte del cliente

Affrontare il GDPR come un Sistema di Gestione

Il REG. N.679/16, per sua costituzione, risente molto di questo tipo di approccio.

Affrontare il GDPR come un Sistema di Gestione

In un contesto di questo tipo, nasce la necessità che il concetto di Consapevolezza collettiva all'interno dell'organizzazione sia sempre più praticato.

Affrontare il GDPR come un Sistema di Gestione

Cosa ci chiede di fare il GDPR (Regolamento UE 2016/679)?

Chiede di fare un sistema di gestione dei dati (similare a quelli normati come la ISO 9001 o di legislazione come richiesto dal DLgs 231/01)

Affrontare il GDPR come un Sistema di Gestione

Cosa ci chiede di fare il GDPR (Regolamento UE 2016/679)?

Affrontare il GDPR come un Sistema di Gestione

Cosa ci chiede di fare il GDPR (Regolamento UE 2016/679)?

Affrontare il GDPR come un Sistema di Gestione

Cosa ci chiede di fare il GDPR (Regolamento UE 2016/679)?

Affrontare il GDPR come un Sistema di Gestione
Principali Denominazioni e Concetti del GDPR

Interessato al Trattamento:
la persona fisica oggetto del trattamento dati

Titolare del Trattamento:
la persona
fisica o giuridica (azienda/ente)
titolare del trattamento

Affrontare il GDPR come un Sistema di Gestione
Principali Denominazioni e Concetti del GDPR

Responsabile del Trattamento: la persona fisica o giuridica responsabile di un determinato trattamento.

Autorizzato al Trattamento: la persona fisica che tratta(es: raccolta, distruzione,ecc) materialmente il dato

Affrontare il GDPR come un Sistema di Gestione
Il Principio di RESPONSABILITÀ nel GDPR

Il GDPR pone l'accento sui concetti di **"Responsabilizzazione"** *(Accountability)* e di **"Misure Adeguate"** in quanto, il Titolare del trattamento deve **garantire** ed essere sempre in grado di **dimostrare** di rispettare i principi del Regolamento nonché, di aver messo in atto le misure ritenute idonee dal Titolare stesso

Affrontare il GDPR come un Sistema di Gestione
Il Principio di RESPONSABILITÀ nel GDPR

Nel GDPR (in cui sparisce il concetto di "Misure Minime", presente nel D.lgs 196/2003), si possono prevedere un minimo insieme di azioni per soddisfare le esigenze di Accountability come:

1. **Assessment:** valutazione iniziale legale, organizzativa, storica e informatica
2. **Registro dei Trattamenti:** non obbligatorio fino a 250 dipendenti, a meno di particolarità, ma consigliato

Affrontare il GDPR come un Sistema di Gestione Il Principio di RESPONSABILITÀ nel GDPR

3. **Funzionigramma privacy:** definizione Ruoli e Compiti ed impostazione flussi di informazione evitando conflitti di interesse
4. **Risk Assessment:** valutazione del rischio sui dati da trattare

Affrontare il GDPR come un Sistema di Gestione
Il Principio di RESPONSABILITÀ nel GDPR

5. Privacy Impact Assessment: distinte valutazioni sull'impatto privacy relative a particolari processi, servizi, prodotti, sistemi che il Titolare può adottare, installare o fornire (ad es: installazione di impianti di videosorveglianza; raccolta punti per marketing; ecc.)

6. Gestione: mediante monitoraggio (es:audit periodici di controllo; analisi di obiettivi e risultati raggiunti)

Affrontare il GDPR come un Sistema di Gestione Privacy by design e privacy by default

Per definizione:

Il principio di **privacy by design** è volto a tutelare il dato protetto "sin dal momento della progettazione";

Il principio di **privacy by default** è volto a tutelare la vita privata per "impostazione predefinita"

Affrontare il GDPR come un Sistema di Gestione
Diritto all'oblio

Il regolamento n. 679/2016 (GDPR) in materia di trattamento di dati personali ha introdotto un **nuovo diritto** a favore degli interessati del trattamento, ovvero dei soggetti proprietari dei dati trattati.

Si tratta in estrema sintesi del diritto **ad ottenere la cancellazione definitiva e completa dei propri dati trattati da un titolare del trattamento**

Affrontare il GDPR come un Sistema di Gestione
Il registro dei trattamenti dei dati

E' un documento cartaceo/informatico che permette di avere un quadro aggiornato dei trattamenti in essere all'interno di un'azienda o di un soggetto pubblico al fine di effettuare un monitoraggio, con relativa valutazione, dei rischi

Affrontare il GDPR come un Sistema di Gestione
Il registro dei trattamenti dei dati

Cosa deve contenere il registro dei trattamenti

L'art. 30 del GDPR fornisce anche una lista di contenuti obbligatori

Affrontare il GDPR come un Sistema di Gestione
Il registro dei trattamenti dei dati

A cosa serve il registro dei trattamenti

E' uno strumento attraverso il quale si ha la possibilità di beneficiare di una più efficace **gestione della data protection**

Affrontare il GDPR come un Sistema di Gestione la Valutazione d'impatto: DPIA

E' la procedura per la valutazione di impatto sulla protezione dei dati personali trattati dalle aziende,

Affrontare il GDPR come un Sistema di Gestione diritto alla portabilità dei dati personali

L'art. 20 del GDPR riporta che ogni soggetto potrà chiedere ad un'organizzazione di **ricevere** i propri dati personali forniti in precedenza in un formato di uso **comune e leggibile** e di ottenerne la **trasmissione** da un titolare del trattamento a un altro se non sono presenti particolari impedimenti tecnologici.

Affrontare il GDPR come un Sistema di Gestione la verifica dei diritti

Tra i cosiddetti **diritti individuali**, infatti, il General Data Protection Regulation include i seguenti: Il diritto a essere Informati; Il diritto all'accesso; Il diritto alla correzione; Il diritto alla cancellazione; Il diritto alla limitazione del trattamento; Il diritto alla portabilità dei dati; Il diritto all'obiezione; Il diritto a non essere oggetto di scelte automatizzate (inclusa la profilazione).

Affrontare il GDPR come un Sistema di Gestione
Il DPO

Il GDPR prevede l'inserimento di un nuovo ruolo nell'organigramma: il Responsabile della Protezione Dati o meglio conosciuto come DPO (Data Protection Officer)

Affrontare il GDPR come un Sistema di Gestione
Principali Denominazioni e Concetti del GDPR

DPO (Data Protection Officer) o RPD (Responsabile Protezione Dati):

è la nuova figura introdotta nel 2016 dal GDPR.

Affrontare il GDPR come un Sistema di Gestione
Il DPO

Viene nominato dal Titolare del Trattamento e, il suo compito, è quello di **supportare** il **Titolare** nell'applicazione delle procedure che riguardano il nuovo regolamento fungendo anche da interfaccia fra le Autorità di Controllo e i diretti interessati.

La nomina ed il suo incaricato devono essere comunicati al garante della Privacy che lo collega (dandogli anche responsabilità) con la vita dei dati dell'organizzazione che lo ha nominato

Affrontare il GDPR come un Sistema di Gestione
Il DPO

Viene nominato dal Titolare del Trattamento e, il suo compito, è quello di **supportare** il **Titolare** nell'applicazione delle procedure che riguardano il nuovo regolamento fungendo anche da interfaccia fra le Autorità di Controllo e i diretti interessati.

La nomina ed il suo incaricato devono essere comunicati al garante della Privacy che lo collega (dandogli anche responsabilità) con la vita dei dati dell'organizzazione che lo ha nominato

Affrontare il GDPR come un Sistema di Gestione
I COMPITI del DPO

Informare e fornire consulenza al titolare del trattamento nonché ai dipendenti; **S**orvegliare l'osservanza del Regolamento GDPR; **F**ornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati; **C**ooperare con l'Autorità di controllo (il Garante Privacy); **F**ungere da punto di contatto per l'Autorità di controllo per questioni connesse al trattamento

Affrontare il GDPR come un Sistema di Gestione

QUANDO devo nominare un DPO

Regolamento (art. 37), la nomina del DPO è obbligatoria:

a) Se il trattamento è svolto da un'autorità pubblica o da un organismo pubblico, con l'eccezione delle autorità giudiziarie nell'esercizio delle funzioni giurisdizionali; **b)** Se le attività principali del titolare o del responsabile consistono in trattamenti che richiedono il monitoraggio regolare e sistematico di interessati su larga scala; **c)** Se le attività principali del titolare o del responsabile consistono nel trattamento su larga scala di categorie particolari di dati o di dati personali relativi a condanne penali e reati

Affrontare il GDPR come un Sistema di Gestione
QUANDO devo nominare un DPO

Si lascia all'organizzazione la responsabilità dell'idoneità professionale e/o formativa e/o operativa della risorsa scelta come DPO

Il DPO assume un ruolo fondamentale, in caso di violazione dei dati (Data Breach) da parte di entità esterne, come interfaccia con le Autorità di Controllo

Affrontare il GDPR come un Sistema di Gestione

QUANDO devo nominare un DPO

Nelle ipotesi sub lettere b) e c) dell'art. 37, paragrafo 1 del Regolamento risulta dirimente, al fine di valutare se sussista o meno l'obbligo di nomina di un DPO, è che il trattamento avvenga su "larga scala".

Affrontare il GDPR come un Sistema di Gestione

QUANDO devo nominare un DPO

Anche il concetto di "**monitoraggio regolare e sistematico degli interessati**" non trova definizione nel Regolamento; tale nozione include non solo tutti i vari strumenti di tracciatura elettronica e profilazione on line, ma anche qualsiasi forma di tracciatura in un ambiente off-line

Affrontare il GDPR come un Sistema di Gestione
INQUADRAMENTO del DPO

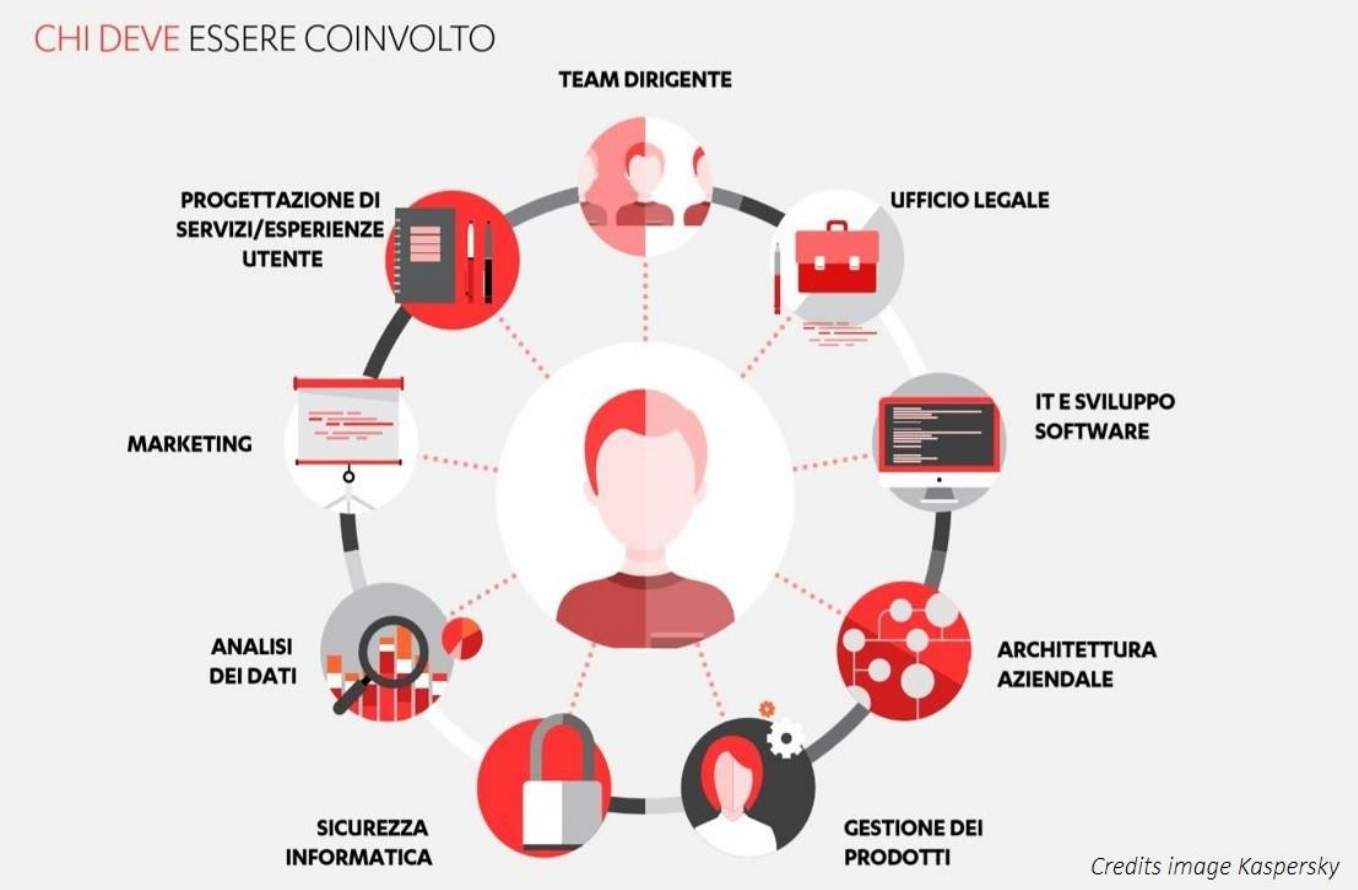
Il DPO può essere:

un **dipendente** del titolare del trattamento o del responsabile del trattamento

oppure assolvere i suoi compiti in base a un **contratto di servizi**

Affrontare il GDPR come un Sistema di Gestione

AREE e RUOLI di un PIANO PRIVACY

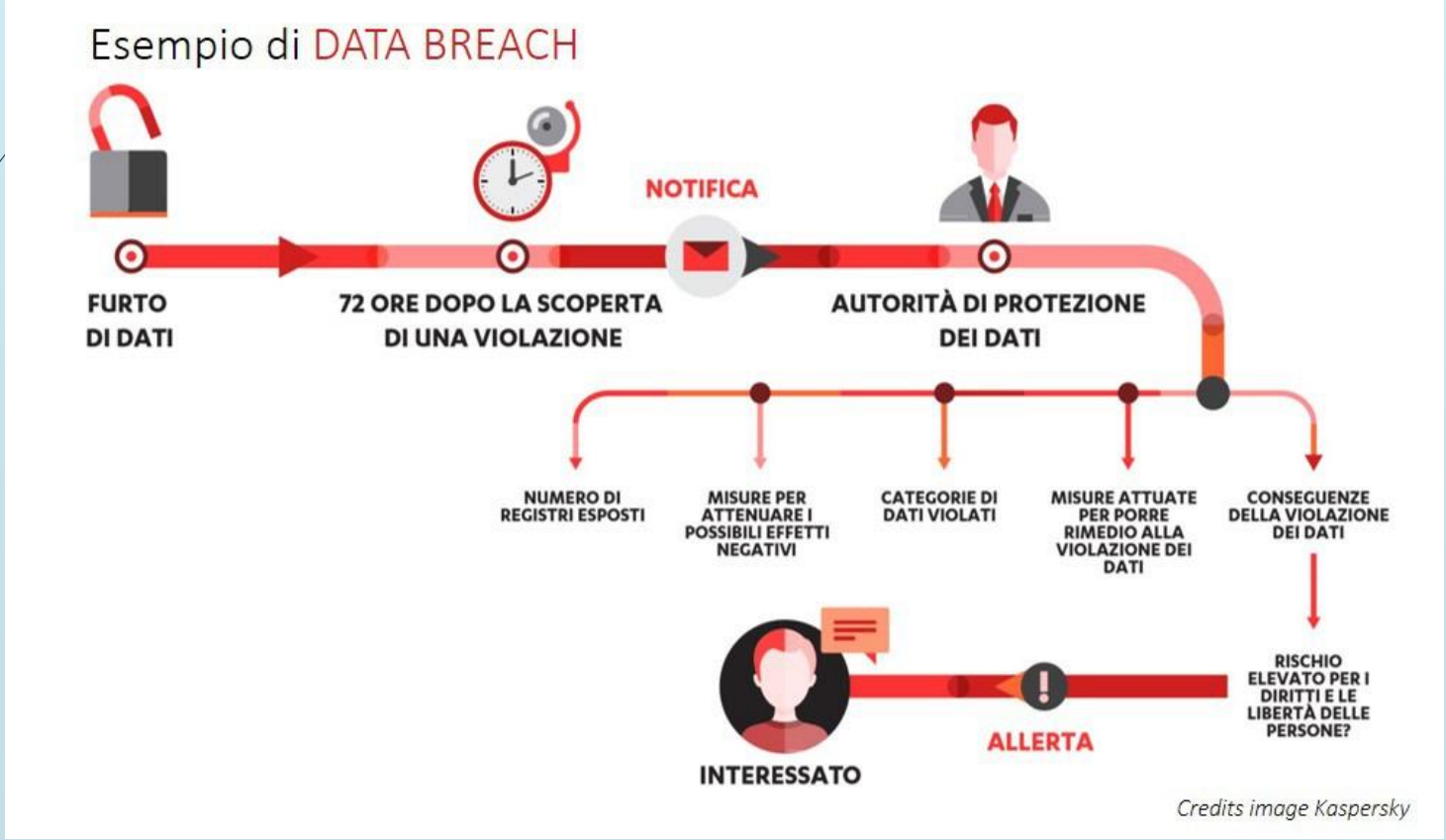


Affrontare il GDPR come un Sistema di Gestione

COME PROCEDERE per un piano Privacy GDPR – La Fase Iniziale

Affrontare il GDPR come un Sistema di Gestione

OBBLIGO di NOTIFICA o DATA BREACH NOTIFICATION



Affrontare il GDPR come un Sistema di Gestione

Costo della perdita dei Dati

Affrontare il GDPR come un Sistema di Gestione
FOIA E REG. 679

la trasparenza totale e la privacy.

La prima, il cosiddetto Foia italiano, è stata introdotta dal decreto 97/2016, di riforma del decreto 33/2013, e prescrive che ogni atto o documento detenuto dalla PA sia accessibile a chiunque ne faccia richiesta, indipendentemente dagli obblighi di pubblicazione e da interessi specifici del richiedente (accesso generalizzato), e salvo un rigoroso elenco di "esclusioni e limiti" da interpretare peraltro in modo restrittivo.

Affrontare il GDPR come un Sistema di Gestione
FOIA E REG. 679

Si potrebbe prefigurare, in definitiva, un conflitto concettuale e operativo fra due direzioni di marcia inconciliabili: la Pa-casa di vetro e la Pa che interviene in modo organico per bloccare la pubblicazione e la produzione di informazioni che possano, anche solo potenzialmente, provocare violazioni nel trattamento dei dati personali.

Affrontare il GDPR come un Sistema di Gestione

Sanzioni

Di seguito sono riportate tutte le sanzioni (c.d. **multe**) previste dal Regolamento Europeo che, ai sensi dell'art. 83 del Reg. UE/2016/679 devono avere carattere di effettività, proporzionalità e dissuasività.

Le Sanzioni Amministrative pecuniarie possono essere **integrative**, oppure **completamente sostitutive** delle Sanzioni Correttive.

Affrontare il GDPR come un Sistema di Gestione

SANZIONI DI CARATTERE ECONOMICO

Nel caso di: **I**nosservanza degli obblighi del titolare e del responsabile del trattamento; **I**nosservanza degli obblighi dell'organismo di certificazione (secondo la EN-ISO/IEC 17065/2012 e ai requisiti aggiuntivi stabiliti dall'autorità di controllo competente ai sensi degli articoli 55 o 56); **I**nosservanza degli obblighi dell'organismo di controllo: fino a **10 milioni di Euro**, o per le imprese, fino al **2% del fatturato** annuo mondiale dell'esercizio precedente.

Affrontare il GDPR come un Sistema di Gestione
SANZIONI CORRETTIVE

Essi consistono nel:

Rivolgere avvertimenti al titolare del trattamento o al responsabile del trattamento sul fatto che i trattamenti previsti possono violare il GDPR;

Rivolgere ammonimenti al titolare e del trattamento o al responsabile del trattamento ove i trattamenti abbiano violato le disposizioni del GDPR;

Affrontare il GDPR come un Sistema di Gestione
SANZIONI CORRETTIVE

Essi consistono nel:

Ingiungere al titolare del trattamento o al responsabile del trattamento di soddisfare le richieste dell'interessato di esercitare i relativi diritti;

Ingiungere al titolare o al responsabile del trattamento di conformare i trattamenti alle disposizioni del GDPR, anche specificando in che modo ed entro quale termine;

In conclusione …

Alla luce di quanto sin qui visto,

- Le PA, così come le aziende, per loro natura intrinseca, non possono non avere dati o non trattarli;
- Esse, e chi le rappresenta, non possono non applicare quanto previsto dal Regolamento 679/2016, nella misura più idonea alla propria struttura, in funzione delle proprie peculiarità;
- Ecco che il GDPR (General Data Protection Regulation) si profila, più di ogni altro sistema di gestione, estremamente simbiotico con la PA così come con l'azienda e con i processi e attività che esse definiscono.

G.E.N.I. s.r.l.
Gestione Esercizi Navali Industriali

GRAZIE PER L'ATTENZIONE

Ing. Stefania Pusateri e
Ing. Massimo Giambarresi