



Visionary Day

Tecnologia e Dati Personali: quando occorre il DPO

Webinar - 6 Ottobre 2020

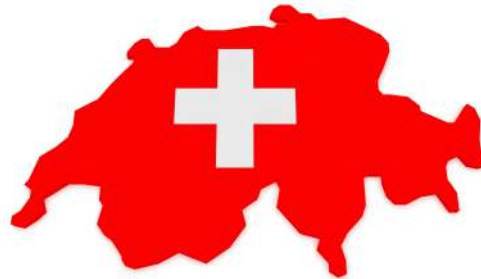
Contenuti del Webinar

- **Privacy Officer, DPO, Consulente per la protezione dei dati;**
- **Competenze e requisiti;**
- **La nomina: obbligo, facoltà...opportunità;**
- **Compiti e attività;**
- **Indipendenza e assenza di conflitto d'interessi;**
- **Conclusioni**

Privacy Officer, DPO, Consulente per la protezione dei dati



- The Health Insurance Portability and Accountability Act
- Fair Credit Reporting Act



- Legge Federale sulla protezione dei dati (LPD)
- Ordinanza relativa alla Legge Federale sulla protezione dei dati (OLPD)



- Gdpr (artt. 37 e ss; Considerando 97)
- Linee Guida WP Art. 29 (ora EDPB, EDPS)

Competenze e requisiti

CHI si occupa di «data protection» per un'organizzazione deve essere dotato di competenze multidisciplinari:

- Competenze informatiche;
- Conoscenza del funzionamento dei processi aziendali;
- Conoscenza specialistica della normativa;
- Determinate qualità personali.



Competenze e requisiti

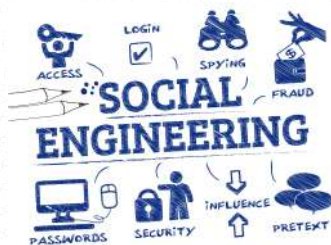
➤ Competenze informatiche e familiarità con i sistemi informatici:



Hacking



*Asset Informativi
incustoditi*



Social engineering

DATA BREACH



*Malfunzionamento
HW e SW*

Competenze e requisiti

➤ Conoscenza del funzionamento dei processi aziendali:

E' fondamentale la conoscenza dello specifico settore di attività della struttura organizzativa di riferimento, comprendendo in concreto «come funziona quell'azienda»: **NON E' POSSIBILE RIMANERE SUL PIANO DELLA TEORIA!**



Competenze e requisiti

- Conoscenza specialistica della normativa in materia di protezione dei dati personali e non solo:

*Normativa in materia
di data protection*

Rapporto di lavoro



Videosorveglianza



Biometria



Marketing



Competenze e requisiti

➤ Determinate qualità personali:



Leadership



*Capacità
organizzative*



*Capacità
comunicative*



Integrità

Competenze e requisiti

➤ «Certificazioni del DPO»:



La nomina: obbligo, facoltà...opportunità 1/6



LPD
FACOLTATIVA



GDPR
OBBLIGATORIA



La nomina: obbligo, facoltà...opportunità 2/6

Art. 37 capoverso 1 GDPR

- a) Quando il trattamento è effettuato da **un'autorità pubblica o da un organismo pubblico**, salvo le autorità giurisdizionali nell'esercizio delle loro funzioni;
- b) Quando le **attività principali** del Titolare/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**;

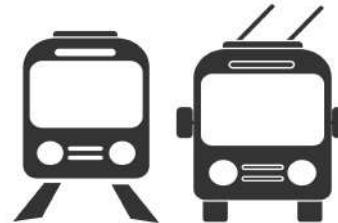
OPPURE

- c) Le attività principali del Titolare/Responsabile del trattamento consistono nel **trattamento su larga scala**, di categorie particolari di dati (art. 9 GDPR) o di dati relativi a condanne penali e reati di cui all'art. 10 GDPR.

La nomina: obbligo, facoltà...opportunità 3/6

LARGA SCALA

Gli elementi che ci permettono di identificare tale concetto sono il numero degli interessati, il volume e le diverse tipologie di dati trattati, la durata dell'attività di trattamento, l'estensione geografica del trattamento (Linee Guida WP 29)



La nomina: obbligo, facoltà...opportunità 4/6

MONITORAGGIO SISTEMATICO E REGOLARE

REGOLARE:

- Quando avviene in modo continuo ovvero a intervalli definiti per un arco di tempo definito;
- Quando è ricorrente o ripetuto ad intervalli costanti;
- Quando avviene in modo costante o a intervalli periodici.

SISTEMATICO:

- Quando avviene per sistema;
- Quando è predeterminato, organizzato o metodico;
- Quando ha luogo nell'ambito di un progetto complessivo di raccolta di dati;
- Quando è svolto nell'ambito di una strategia.

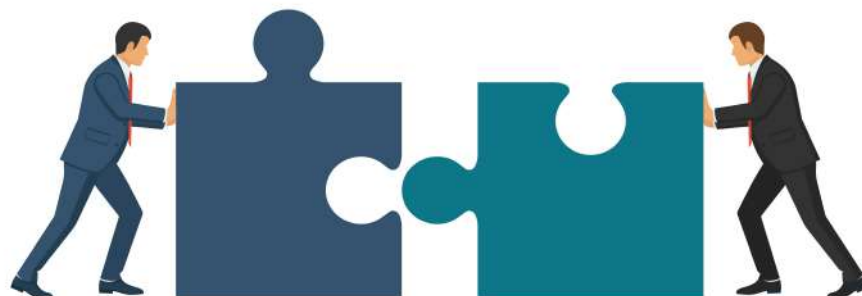


La nomina: obbligo, facoltà...opportunità 6/6

PERCHE' LA **NOMINA DI UN DPO/CONSULENTE** PER LA PROTEZIONE DEI DATI, ANCHE SE NON OBBLIGATORIA, RAPPRESENTA IN OGNI CASO **UN'OPPORTUNITA'** PER L'ORGANIZZAZIONE?

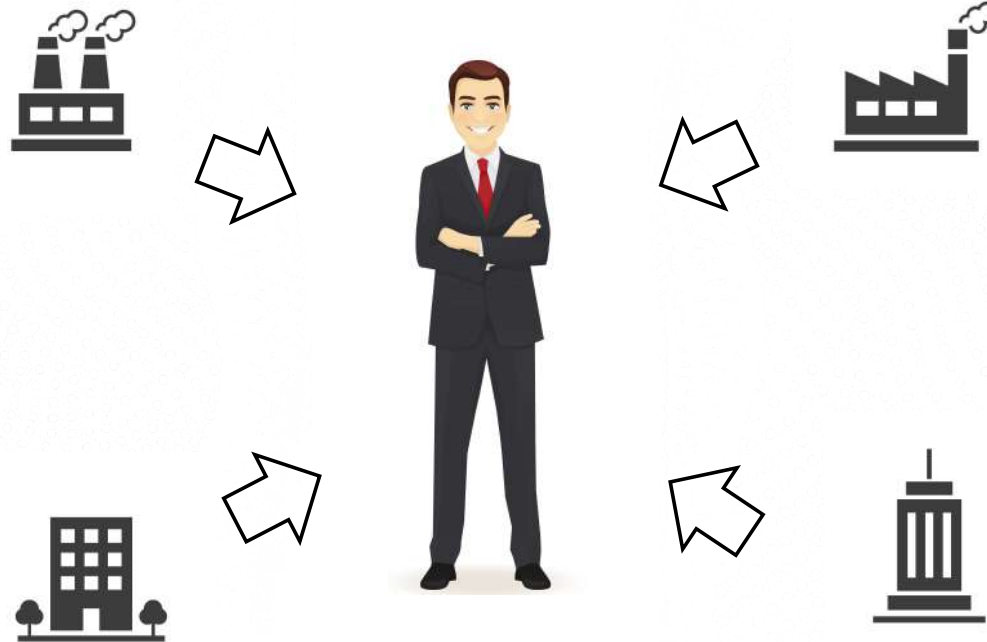
- Accountability;
- Misura organizzativa sostanziale;
- Semplificazione in caso di ispezioni, data breach, richieste degli interessati;

E' UN «ALLEATO IN CASA»



La nomina: obbligo, facoltà...opportunità 5/6

NOMINA DEL DPO PER PIÙ ORGANISMI



Contenuti del Webinar

- Privacy Officer, DPO, Consulente per la protezione dei dati;
- Competenze e requisiti;
- La nomina: obbligo, facoltà...opportunità;
- **Compiti e attività;**
- Indipendenza e assenza di conflitto d'interessi;
- Conclusioni

Ruolo del DPO: Riferimenti legislativi

- Legge Protezione Dati (LPD)
- Ordinanza relativa alla LPD (OLPD)
- Indicazioni Incaricato Federale per la Protezione Dati e Trasparenza (IFPDT)

- Regolamento UE 2016/679 (GDPR)
- Linee Guida WP-29 (European Data Protection Board)

Ruolo del DPO: Compiti e attività principali

1

**SORVEGLIARE
L'APPLICAZIONE
DELLE NORMATIVE**

2

**INFORMARE E
FORNIRE
CONSULENZA**

3

**FUNGERE DA
REFERENTE PER
L'AUTORITA' DI
CONTROLLO E
PUNTO DI
CONTATTO PER
GLI INTERESSATI**

Sorvegliare: Ambiti di Controllo

1

Registro dei Trattamenti

2

Modulistica/Contrattualistica

3

**Gestione delle richieste
degli interessati e dei
data breach**

4

**Sistema di gestione della
sicurezza dei dati
(Data Security Governance)**

Registro dei trattamenti

Servizio	Attività di trattamento	Autorizzati al Trattamento (personale interno)	Responsabili del Trattamento	Dato personale	Interessato	Tempo di conservazione dei dati	Trasferimento Paesi Terzi (extra CH-UE)	Archivio IT	Archivio non IT
Risorse Umane	Selezione personale	Reparto HR	Azienda Selezione Persnale	CV Dati anagrafici	Candidato Referente ex-datore lavoro	24 mesi	NO	Dropbox Archivio G-Suite	NA
Risorse Umane	Gestione personale	Reparto HR	Fiduciaria	Dati anagrafici Dati bancari Dati relativi la salute Oneri sociali Casellario giudiziaro Dati anagrafici famiglia Dati relativi le competenze	Dipendente	5-10 anni	NO	Dropbox Archivio G-Suite	Classeur dipendente
Amministrazione	Gestione relazioni con terze parti	Reparto Finanze	NA	Dati di contatto	Terze Parti	NA	NO	Dropbox Archivio G-Suite	NA
Informatico	Gestione utenti IT	Reparto IT	NA	Profili IT	Dipendente	6 mesi dopo cessazione contratto	NO	Archivio iCloud Archivio Dropbox	NA
Informatico	Gestione backup	Reparto IT	NA	Dati personali raccolti durante le diverse attività di trattamento	Candidato Dipendente Riferimenti contatto Fornitore	10 anni	NO	Archivio iCloud Archivio G-Suite Archivio Dropbox	NA

Modulistica / Contrattualistica

- ✓ **Informative e richieste di consenso**
- ✓ **Nomine interne (Autorizzati al trattamento / Nomina Administrator)**
- ✓ **Nomine esterne (Data Protection Agreement)**
- ✓ **Modulistica Siti Web (Privacy & Cokiee Policy, Richieste Consenso, sezione Career, ecc.)**

Richieste Interessati e Data Breach

1

**Procedura di gestione
delle richieste degli
interessati**

2

**Procedura di gestione
e notifica dei data
breach**

Sorvegliare: Data Security Governance

Data Security Governance

Risk
Management

Privacy by
design

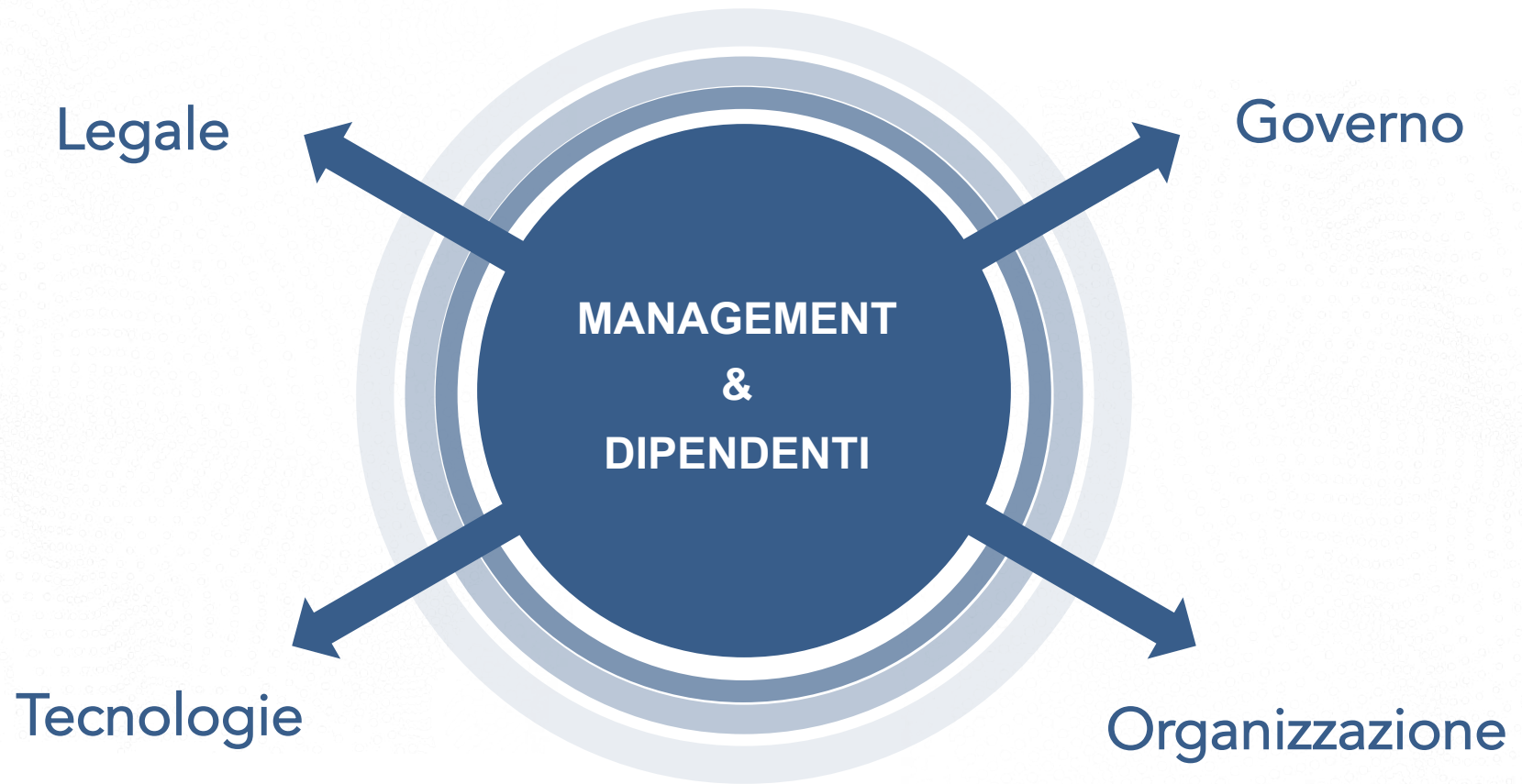
Sicurezza nelle
attività
operative

Training

Organization,
Testing,
Management

Standard and best practice (Enisa, ISO, NIST ecc.)

Informare e fornire consulenza



DPO Referente per l'Autorità di Controllo

1

Facilitazione dell'accesso ai documenti e alle informazioni necessarie da parte dell'Autorità di Controllo (poteri di indagine, correttivi, autorizzativi e consultivi) e cooperazione con l'Autorità di Controllo

2

Attivazione «consultazioni preventive» verso l'Autorità di controllo (nel rispetto delle norme in materia di segreto/riservatezza)

DPO Punto di contatto per gli interessati

3

Pubblicazione dei dati di contatto del DPO da parte del Titolare o del Responsabile del trattamento

4

Gli interessati possono contattare il DPO per le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti

Piano attività del DPO

➤ *Piano attività prioritarie del DPO*

Il DPO deve dare massima priorità alle sue attività che hanno diretto impatto e che concretamente supportano l'implementazione di misure di sicurezza che consentano di ridurre i rischi e prevenire i danni per gli interessati e per l'azienda stessa.

➤ *Piano attività di sorveglianza del DPO*

Le attività di sorveglianza hanno carattere di minore urgenza. Il piano deve prevedere la verifica di tutti gli elementi necessari in un tempo ragionevole, secondo specifiche priorità. Il Piano è aggiornamento annualmente.

➤ *Condivisione del Piano con il Management*

Report e Pareri del DPO

➤ Report sulle attività

- Attività svolte e specifici controlli effettuati
- Risultati emersi (casi di mancata o inadeguata applicazione delle normative vigenti e/o carenze del sistema di gestione della sicurezza)
- Considerazioni e suggerimenti del DPO

➤ Pareri del DPO

- Formalizzazione dei pareri emessi
- Evidenza di eventuali opinioni diverse del Management, con motivazioni sulle scelte fatte

➤ Responsabilità del DPO

- Nessuna responsabilità in caso di non conformità.
- Responsabilità “contrattuali” nei confronti dell’Organizzazione

Coinvolgimento del DPO nella vita aziendale

Per poter svolgere i compiti ad esso affidati, è **fondamentale che il DPO/Consulente sia tempestivamente ed adeguatamente coinvolto dal Management**, in tutte le questioni riguardanti la protezione dei dati personali.

In concreto, il DPO deve essere coinvolto in occasione di:

- **Cambiamenti organizzativi/tecnologici** o altre iniziative che prevedono un impatto sui dati personali
- **Riunioni manageriali** dove possono essere prese decisioni sull'avvio di progetti/attività che potrebbero impattare sui dati personali (il parere del DPO dovrà ricevere le dovute considerazioni)
- **Data breach** rilevanti che possano richiedere la notifica all'IFPDT

Risorse necessarie e a supporto

- Tempo (gestione delle priorità)
- Risorse finanziarie, infrastrutture e personale (se opportuno)
- Formazione permanente
- Ufficio o gruppo di lavoro
- Accesso a tutte le collezioni e trattamenti di dati
- Comunicazione ufficiale della nomina a tutto il personale
- Indicazione dei casi in cui è necessaria la consultazione del DPO e modalità operative su come procedere.

Indipendenza e assenza di conflitto d'interessi

Sia per quanto concerne la normativa Ue che in base al parere dell'IFPDT, il DPO/Consulente può essere:

INTERNO

ESTERNO (in base ad un contratto di servizi)

In entrambi i casi deve operare in maniera **INDIPENDENTE** senza incappare «**NEL CONFLITTO DI INTERESSI**»



- *Individuare qualifiche e funzioni incompatibili con quelle del DPO/Consulente;*
- *Redigere regole interne a tale scopo onde evitare conflitti di interesse;*
- *Dichiarare espressamente che il DPO/Consulente non versa in alcuna situazione di conflitto di interessi con riguardo alla funzione di DPO/Consulente, al fine di sensibilizzare rispetto al requisito in questione.*

Indipendenza e assenza di conflitto d'interessi

Le garanzie esistenti, che consentono al DPO/Consulente di operare in maniera indipendente sono:

1. *Assenza di istruzioni;*
2. *Nessuna penalizzazione, rimozione dall'incarico, licenziamento in rapporto allo svolgimento dei compiti affidati*
3. *Nessun conflitto di interessi con eventuali compiti e funzioni*

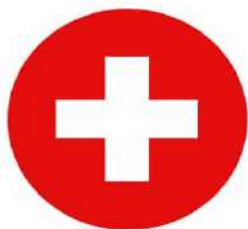
Ma quando sussistono in concreto situazioni di conflitto di interessi?



Linee Guida WP 29

Sanzioni delle Autorità di Controllo (Es. Garante Belga e Bavarese)

Conclusioni



**CONSULENTE PER LA
PROTEZIONE DEI DATI**



DPO

Grazie per l'attenzione!



siro.migliavacca@sec-lab.com

francesca.colombo@sec-lab.com

www.sec-lab.com