Scuola Internazionale

Etica&Sicurezza

Milano - L'Aquila

Statuto professionale, poteri e norme di riferimento per l'attività del Data Protection Officer

Scuola Internazionale
Etica&Sicurezza
Milano - L'Aquila

© Copyright Scuola Etica e Sicurezza 2018

Agenda

1. Il Data Protection Officer
   - Definizione, compiti e obblighi
   - Responsabilità connesse
   - Poteri istruttori, ispettivi e di accertamento
2. Standard professionali per il DPO

© Copyright Scuola Etica e Sicurezza 2018

SESSIONE 1 – LA FIGURA DEL DPO: STATUTO E FUNZIONI

© Copyright Scuola Etica e Sicurezza 2018

La base: Carta dei Diritti fondamentali dell'Unione Europea (200/C 364/01) – La «Carta di Nizza»

Articolo 8

Protezione dei dati di carattere personale

1. Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano.

2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica.

3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente.

© Copyright Scuola Etica e Sicurezza 2018

Caratteri della protezione dei sati

1. Effettività
2. Controllabilità
3. Responsabilità
4. Controlli

Il sistema delineato nei principi fondamentali presuppone che il «sistema di gestione della privacy» nelle organizzazioni sia effettivo e non meramente nominale

© Copyright Scuola Etica e Sicurezza 2018

Pregressi storici

Nella normativa previgente al GDPR)DPR 196/2003) non vi è aùlcun riferimento ad autorità interne di controllo. Gli unici soggetti identificati sono:

a. Il titolare del trattamento
b. Il responsabile del trattamento (art. 29), *designato dal titolare* ***facoltativamente*****.** Se designato, il responsabile è individuato tra soggetti che, per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni..

2 aspetti salienti rispetto al DPO:

- **La facoltatività della nomina**
- **L'assenza di una definizione dei poteri**

© Copyright Scuola Etica e Sicurezza 2018

In sintesi

Passaggio dall'affidamento sul binomio titolare /responsabile ad una più marcata distinzione di ruolo con caratteri tutti suoi tipici

© Copyright Scuola Italiana Sicurezza 2018

39

Ruolo disegnato dalla legge per il DPO

© Copyright Scuola Etica e Sicurezza 2018

«almeno» - il contenuto minimo del ruolo

a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
b) sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;
d) cooperare con l'autorità di controllo; e
e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

© Copyright Scuola Etica e Sicurezza 2018

Poliziotto o consigliere privilegiato?

Copyright Scuola Etica e Sicurezza 2018

Titolare e responsabile del trattamento non sono deresponsabilizzati

Il titolare del trattamento o il responsabile del trattamento mantengono la piena responsabilità dell'osservanza della normativa in materia di protezione dei dati e devono essere in grado di dimostrare tale osservanza (Gruppo di lavoro art. 29)

Il DPO non è il «parafulmine» o terminale di responsabilità.
La sua funzione è quella di sostenere e supportare il titolare e il responsabile nella gestione coerente ed effettiva del sistema di gestione della protezione dei dati personali

© Copyright Scuola Etica e Sicurezza 2018

Ruolo interno – governo del sistema basato sulla gestione del rischio

Art. 39 comma 2: il DPO *considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo*

La gestione del rischio è l'attività primaria e qualificante del DPO che serve a definire esattamente il perimetro della gestione del trattamento dei dati personali.
In ragione dell'architettura delle responsabilità e degli interessi di terzi, si richiede un approccio sistemico e per priorità ed una visone continua del processo

© Copyright Scuola Etica e Sicurezza 2018

Ruolo interno – sorveglianza sull'osservanza del GDPR

il titolare del trattamento o il responsabile del trattamento dovrebbe essere «assistito» DPO nel controllo del rispetto a livello interno del GDPR (art. 39 comma 1 lett. f)

Tra i compiti di controllo:

- La piena condivisione, l'analisi e le valutazioni connesse al registro dei trattamenti;
- la raccolta di informazioni per la verifica della legittimità, proporzionalità e continenza dei trattamenti e le modalità di raccolta;
- I poteri ispettivi connessi, funzionali all'esercizio della missione

© Copyright Scuola Etica e Sicurezza 2018

Ruolo interno – Il ruolo sulla Valutazione di impatto (DPIA)

il titolare del trattamento è il responsabile della valutazione di impatto e non spetta al DPO questo compito. Tuttavia, secondo la lettera c) dell'art. 30 spetta al DPO «*fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35*»

Tra le funzioni che può svolgere il DPO:

- Contribuire alla valutazione sulla necessità o meno della DPIA;
- Collaborare all'individuazione della metodologia;
- Se la DPIA possa essere svolta da risorse interne o se sia opportuno dare in outsourcing per competenze e capacità;
- Valutare la completezza e correttezza della DPIA svolta

© Copyright Scuola Etica e Sicurezza 2018

Ruolo interno – i rapporti tra titolare/responsabile e DPO

In materia di diritti forma e sostanza non hanno confini netti. Il DPO agisce per atti formali, così come il titolare e il responsabile
Le funzioni istruttorie del DPO richiedono che i suoi giudizi vengano valutati e ponderati e se il titolare/responsabile intende distaccarsi da tali valutazioni, deve coerentemente motivare le ragioni dello scostamento.
Tale funzione è direttamente connessa al profilo delle responsabilità ed al bilanciamento dei ruoli come disegnati dall'architettura del GDPR e da come nell'ente devono essere effettivamente definiti

© Copyright Scuola Etica e Sicurezza 2018

Ruolo esterno – Cooperazione con autorità di controllo e punto di contatto

Altro punto cruciale del sistema. Il ruolo del DPO con le autorità di contratto ha una natura e una genesi «ibrida» che lo porta ad essere una sorta di «longa manus» dell'autorità.

Questo è evidente:

a) Nel processo di designazione
b) Nelle fasi di gestione del processo, anche attraverso richieste di pareri e consulenza
c) Nell'adempimento degli obblighi di segnalazione

© Copyright Scuola Etica e Sicurezza 2018

Nel dettaglio – Quando è necessario il DPO

L’articolo 37 definisce una figura complessa e precedentemente sconosciuta, quando ricorrano le condizioni previste:

a) Trattamento effettuato da autorità pubblica o organismo pubblico
b) Le attività principali del titolare o responsabile del trattamento consistono in «trattamenti che, per la 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 o responsabile del trattamento consistono nel trattamento, su larga scala,, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all’articolo 10

© Copyright Scuola Etica e Sicurezza 2018

Tipologia 1

Posizione legata a pubblica funzione.

Si tratta di:
- Pubbliche amministrazioni
- Soggetti equiparabili alla pubblica amministrazione
- Gestori di servizi pubblici essenziali

L'identificazione di questa tipologia di soggetti deve essere formale ma soprattutto sostanziale.

© Copyright Scuola Etica e Sicurezza 2018

Tipologia 1 – segue

Non vi è alcuna definizione di «autorità pubblica» o di «organismo pubblico» e dunque essa va ricavata dall'interpretazione sistematica dell'Ordinamento nazionale.

Lo svolgimento di funzioni pubbliche e l'esercizio di pubblici poteri non pertengono esclusivamente alle autorità pubbliche e agli organismi pubblici, potendo riferirsi anche ad altre persone fisiche o giuridiche, di diritto pubblico o privato, in ambiti che variano a seconda delle disposizioni fissate nel diritto interno di ciascuno Stato membro: trasporti pubblici, forniture idriche ed elettriche, infrastrutture stradali, emittenti radiotelevisive pubbliche, istituti per l'edilizia pubblica o organismi di disciplina professionale.

© Copyright Scuola Etica e Sicurezza 2018

Tipologia 2 – definizione di «attività principali»

Riferimento al *Considerando* 97: operazioni che «*riguardano le sue attività primarie ed esulano dal trattamento dei dati personali come attività accessoria*»→ attività necessarie al raggiungimento degli obiettivi dichiarati ed effettivamente perseguiti dal titolare
Sono comprese però quelle attività che sono parte inscindibile del complesso delle operazioni svolte dal responsabile del trattamento e che ne caratterizzano il suo «core service»
Es.: un istituto di vigilanza che svolge attività di protezione fisica non può prescindere dal trattamento dei dati dei clienti o delle immagini raccolte dai sistemi TVCC

© Copyright Scuola Etica e Sicurezza 2018

Tipologia 2 – definizione di «Larga Scala»

Riferimento al *Considerando* 91: *trattamenti su larga scala, che mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato*→ Valutazione del rischio con riferimento ad indicatori quali:

- il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;
- il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;
- la durata, ovvero la persistenza, dell'attività di trattamento;
- la portata geografica dell'attività di trattamento.

© Copyright Scuola Etica e Sicurezza 2018

Tipologia 2 – definizione di «Larga Scala» - esempi

- Gestione della profilazione della navigazione internet da parte dei gestori di servizi digitali;
- Trattamento dati nell'ambito delle imprese bancarie o assicurative;
- Profilazione delle abitudini di consumo degli utenti nelle catene di grande distribuzione;
- Trattamento dati dei servizi telefonici e telematici;
- Attività nel settore sanitario;

© Copyright Scuola Etica e Sicurezza 2018

Tipologia 2 – definizione di «Monitoraggio regolare e sistematico»

Riferimento al *Considerando* 24: «*Per stabilire se un'attività di trattamento sia assimilabile al controllo del comportamento dell'interessato, è opportuno verificare se le persone fisiche sono tracciate su internet, compreso l'eventuale ricorso successivo a tecniche di trattamento dei dati personali che consistono nella profilazione della persona fisica, in particolare per adottare decisioni che la riguardano o analizzarne o prevederne le preferenze, i comportamenti e le posizioni personali.*»→ attività continua o ad intervalli constanti che avviene secondo una metodologia predeterminata e organizzata, che presuppone un «progetto complessivo» di raccolta dati nel quadro di una determinata strategia

© Copyright Scuola Etica e Sicurezza 2018

Tipologia 2 – definizione di «Monitoraggio regolare e sistematico» - Segue

NOTATE BENE: non si tratta solo di attività che vengano messe in capo nel mondo cibernetico: si pensi a:

- Attività di marketing svolte anche con inchieste e osservazioni,
- Utilizzo dei dati della videosorveglianza;
- Programmi di fidelizzazione
- Pubblicità selettiva
- Dispositivi connessi
- Mondo della telefonia fissa e mobile

© Copyright Scuola Etica e Sicurezza 2018

Tipologia 3 condanne penali e reati

Riferimento all'articolo 9 ed al trattamento di «categorie particolari» doi dati personali
Necessità di leggere l'insieme dei trattamenti connessi a condanne penali e reati con la funzione dell'organizzazione
Evidente necessità di apprestare una tutela rafforzata a queste tipologie di trattamenti

© Copyright Scuola Etica e Sicurezza 2018

La figura del DPO – Posizionamento e ruolo

Articolo 38 :

La figura del DPO è intrinsecamente connessa con i ruoli e le responsabilità del titolare e del responsabile del trattamento e i profili di *accountability* si definiscono vicendevolmente

© Copyright Scuola Etica e Sicurezza 2018

Effettività del ruolo del DPO – privacy by design e nel ciclo di vita

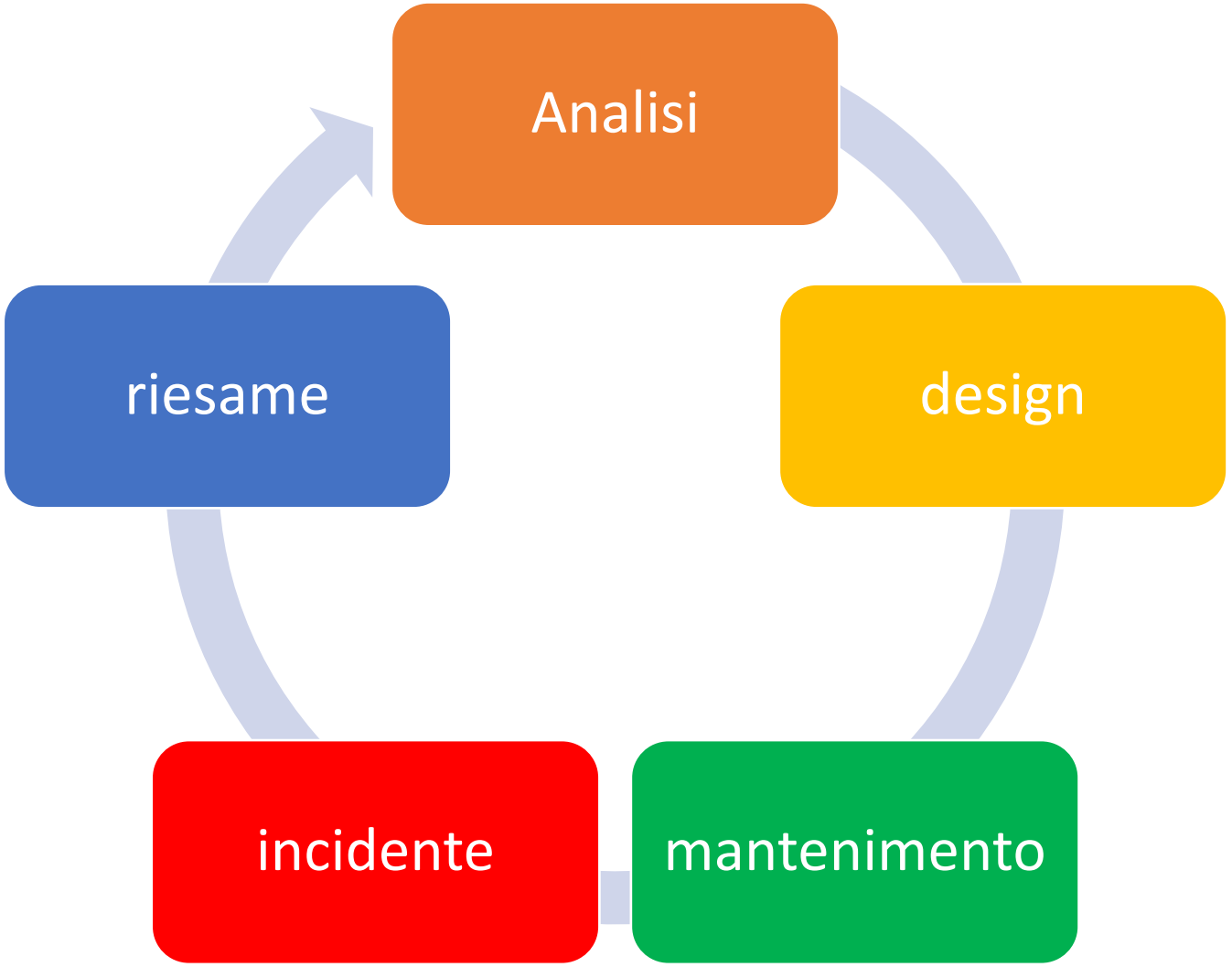
1. Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.

Il principio della «privacy by design» rappresenta la chiave di volta del sistema. Il modello voluto dal legislatore richiede che il processo di protezione delle informazioni ai fini della salvaguardia della privacy.

La protezione ha un carattere ciclico e continuativo e richiede la costante verifica secondo un processo PDCA

© Copyright Scuola Etica e Sicurezza 2018

Aree e tempi di coinvolgimento del DPO



- Coinvolgimento nelle attività di analisi e delle scelte strategiche
- Nella definizione delle policy, processi e procedure
- Valutazione degli impatti (DPIA)
- Architetture e sistemi
- Nei processi di mantenimento
- Nella gestione degli incidenti
- Nel riesame

© Copyright Scuola Etica e Sicurezza 2018

Effettività del ruolo del DPO - committment

Il titolare e del trattamento e il responsabile del trattamento sostengono il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 39 fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica. .

Il ruolo del DPO non può essere soltanto nominale o di figura. Ad esso devono essere associati poteri puntuali, risorse umane e strumentali e poter garantire la continua formazione.

© Copyright Scuola Etica e Sicurezza 2018

In concreto:

- supporto attivo delle funzioni del RPD da parte del senior management (per esempio, a livello del consiglio di amministrazione);
- tempo sufficiente per l'espletamento dei compiti affidati al DPO
- supporto adeguato in termini di risorse finanziarie, infrastrutture (sede, attrezzature, strumentazione) e, ove opportuno, personale;
- comunicazione ufficiale della nomina del RPD per garantirne il riconoscimento;
- accesso garantito ad altri servizi (risorse umane, ufficio giuridico, IT, sicurezza, ecc.)
- formazione permanente
- Definizione chiara di ruoli, responsabilità e poteri (Sistema di gestione)

Vale tanto per il DPO interno che esterno!

© Copyright Scuola Etica e Sicurezza 2018

Effettività del ruolo del DPO – autonomia ed indipendenza

Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti. Il responsabile della protezione dei dati non è rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti. Il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento

E’ un ruolo scomodo ed è esattamente questo ciò che vuole la norma

© Copyright Scuola Etica e Sicurezza 2018

«assenza di istruzioni»

Il concetto di indipendenza è complesso e richiede un'attenta valutazione.
Questo significa che, se da un lato il DPO deve essere posto in grado di esercitare un potere autonomo con libertà di determinazioni e piena consapevolezza di giudizio, dall'altro deve trovare rifermento sempre e soltanto nel perimetro delle funzioni che l'art. 39 gli attribuisce.
Il titolare del trattamento o il responsabile del trattamento mantengono la piena responsabilità dell'osservanza della normativa in materia di protezione dei dati e devono essere in grado di dimostrare tale osservanza. Se il titolare del trattamento o il responsabile del trattamento assumono decisioni incompatibili con i principi normativi e le indicazioni fornite dal DPO, quest'ultimo dovrebbe avere la possibilità di manifestare il proprio dissenso al più alto livello del management e ai decisori.
Nelle organizzazioni più complesse, il DPO deve poter avere diretto accesso ai vertici aziendali ed informare i CdA e il management non esecutivo dei possibili rischi e delle circostanze critiche

© Copyright Scuola Etica e Sicurezza 2018

Il delicato posizionamento all'interno dell'organizzazione

Occorre dare risposta ad una domanda: è possibile che il DPO sia un soggetto con ruolo gerarchico e funzionale sottordinato a coloro verso i quali debba esercitare le funzioni di controllo?

La risposta è «ad assetto variabile» e dipende dalle organizzazioni e dai poteri che sono disegnati

Casistica varia:

a. Posizione di dipendenza gerarchica «pura»
b. Posizione di coordinamento e controllo
c. Soggetto appartenente a struttura esterna o dipendente «part time»

© Copyright Scuola Etica e Sicurezza 2018

Poteri ispettivi

L’esercizio delle funzioni del DPO deve poter essere effettivo.
Per rispondere a questa esigenza, il DPO e la sua struttura deve poter avere ampi spazi di capacità istruttoria ed avere accesso ai documenti essenziali per le operazioni di privacy.
Questo può tradursi in:

- Richieste di documentazione;
- Accesso diretto a data-base
- Verifica dell’esercizio dei poteri degli amministratori di sistema
- Analisi degli indicatori di rispetto delle regole del GDPR

© Copyright Scuola Etica e Sicurezza 2018

La figura del DPO – Conoscenze e competenze

Articolo 37 comma 5:

il DPO «è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39».

Nel considerando 97 si prevede che il livello necessario di conoscenza specialistica dovrebbe essere determinato in base ai trattamenti di dati effettuati e alla protezione richiesta per i dati personali oggetto di trattamento

© Copyright Scuola Etica e Sicurezza 2018

Definizione di «competenze» e «conoscenze» nel quadro del sistema EQF

“conoscenze”: risultato dell’assimilazione di informazioni attraverso l’apprendimento. Le conoscenze sono un insieme di fatti, principi, teorie e pratiche relative ad un settore di lavoro o di studio. Nel contesto del Quadro europeo delle qualifiche le conoscenze sono descritte come teoriche e/o pratiche;

“competenze”: comprovata capacità di utilizzare conoscenze, abilità e capacità personali, sociali e/o metodologiche, in situazioni di lavoro o di studio e nello sviluppo professionale e personale. Nel contesto del Quadro europeo delle qualifiche le competenze sono descritte in termini di responsabilità e autonomia.

© Copyright Scuola Etica e Sicurezza 2018

Terms of reference – la soluzione italiana

- Assenza di indicazioni di sostanza nel quadro normativo, contrapposta all'assoluto bisogno di individuare i criteri di professionalità del DPO
- Evitare il far west
- Fornire alle imprese e agli enti/organismi pubblici dei chiari termini di riferimento

UNI 11697 - Attività professionali non regolamentate - Profili professionali relativi al trattamento e alla protezione dei dati personali - Requisiti di conoscenza, abilità e competenza

© Copyright Scuola Etica e Sicurezza 2018

Finalità della norma

La norma definisce i requisiti relativi all'attività professionale di soggetti operanti nell'ambito del trattamento e della protezione dei dati personali – professione intellettuale che viene esercitata a diversi livelli di complessità e in diversi contesti organizzativi, pubblici e privati.

Nello specifico, la norma si orienta alla definizione dello «statuto di qualificazione» del DPO di cui all'art. 39 del Reg. 679/2016 , che supporta il titolare o responsabile del trattamento dei dati in applicazione del GDPR

© Copyright Scuola Etica e Sicurezza 2018

Commento ai requisiti UNI 11697

Secondo il modello di standardizzazione, per ogni attività specifica è necessario individuare le competenze necessarie e successivamente, per ogni competenza identificata, individuare le relative abilità e conoscenze.

Le attività del DPO sono modellate sul profilo normativo e sono disegnati i risultati attesi.

© Copyright Scuola Etica e Sicurezza 2018

Commento ai requisiti UNI 11697

Compiti principali

- informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
- sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
- fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
- cooperare con l'autorità di controllo;
- fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento.

© Copyright Scuola Etica e Sicurezza 2018

Dallo schema di certificazione di un ente di certificazione - competenze

Le competenze richieste al Responsabile della protezione dei dati personali sono elencate al prospetto 1 della Norma UNI 11697.

- Pianificazione di Prodotto o di Servizio
- Sviluppo della Strategia per la Sicurezza Informatica
- Gestione del Contratto
- Sviluppo del Personale
- Gestione del Rischio
- Gestione delle Relazioni
- Gestione della Sicurezza dell'Informazione
- Governance dei sistemi informativi

© Copyright Scuola Etica e Sicurezza 2018

Dallo schema di certificazione di un ente di certificazione – abilità (punto 5.1 della norma)

- Contribuire alla strategia per il trattamento e per la protezione dei dati personali
- Gestire l'applicazione dei codici di condotta e delle certificazioni applicabili in materia di trattamento e protezione dei dati personali.
- Capacità di comunicare
- Capacità di analisi
- Autogestione e controllo dello stress
- Capacità di autosviluppo
- Capacità di controllo
- Capacità di convincimento
- Capacità di gestione dei conflitti
- Iniziativa
- Idoneità alla negoziazione
- Capacità organizzative
- Pensiero prospettico
- Pianificazione e programmazione
- Atteggiamento costruttivo nella soluzione dei problemi
- Tenacia

© Copyright Scuola Etica e Sicurezza 2018

Dallo schema di certificazione di un ente di certificazione – conoscenze (punto 5.1) -1

- I principi di privacy e protezione dei dati by design e by default
- I diritti degli interessati previsti da leggi e regolamenti vigenti
- Le responsabilità connesse al trattamento dei dati personali
- Norme di legge italiane ed europee in materia di trattamento e di protezione dei
- dati personali
- Norme di legge in materia di trasferimento di dati personali all'estero e
- circolazione dei dati personali extra UE/SEE
- Le metodologie di valutazione d'impatto sulla protezione dei dati e PIA
- Le possibili minacce alla protezione dei dati personali
- Le norme tecniche ISO/IEC per la gestione dei dati personali
- I codici di condotta e le certificazioni applicabili in materia di trattamento e
- protezione dei dati personali.
- Tecniche e strumenti di comunicazione (relazione con Istituzioni, autorità, Forze
- dell'ordine, enti locali e stampa)
- Le tecniche crittografiche
- Le tecniche di anonimizzazione

© Copyright Scuola Etica e Sicurezza 2018

Dallo schema di certificazione di un ente di certificazione – conoscenze (punto 5.1) - 2

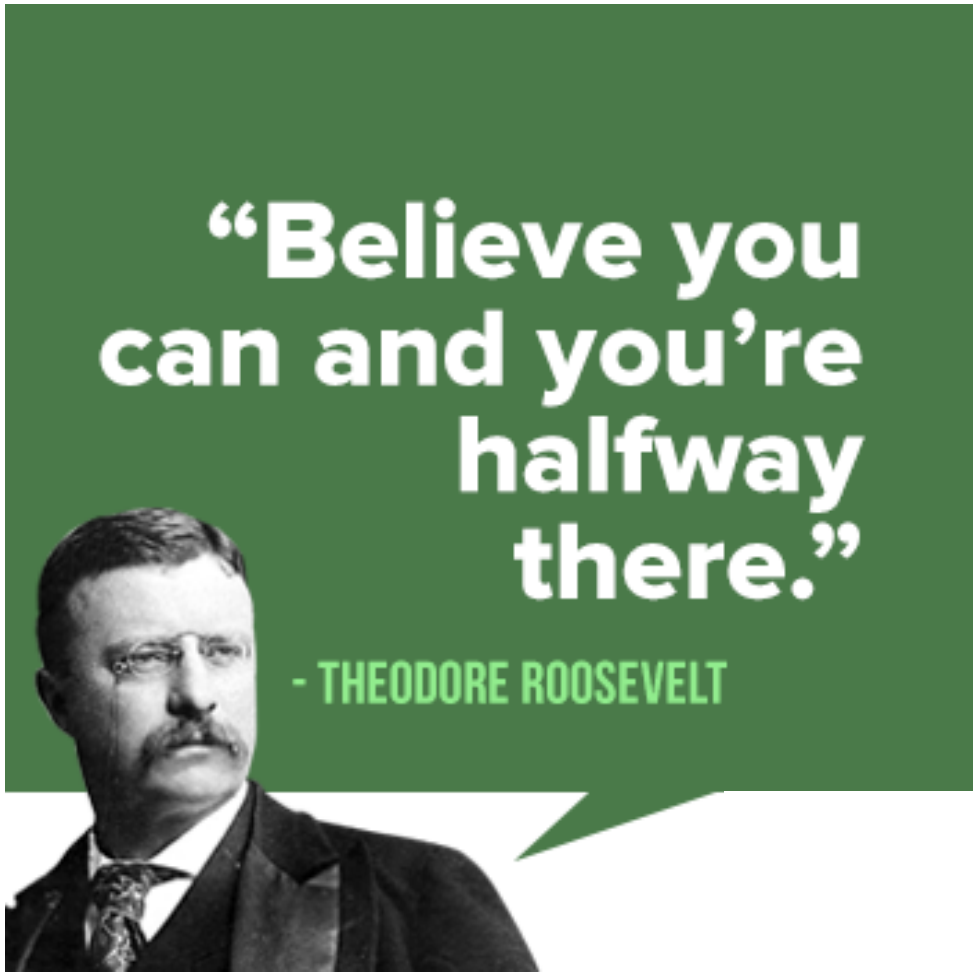
- Le tecniche di pseudonimizzazione
- Sistemi e tecniche di monitoraggio e "reporting"
- gli strumenti di controllo della versione per la produzione di documentazione
- i metodi di sviluppo delle competenze
- i processi dell'organizzazione ivi inclusi le strutture decisionali, di budget e di gestione.
- i rischi critici per la gestione della sicurezza
- i tipici KPI (key performance indicators)
- il potenziale e le opportunità offerte dagli standard e dalle best practices più rilevanti.
- il ritorno dell'investimento comparato all'annullamento del rischio
- l'impatto dei requisiti legali sulla sicurezza dell'informazione
- la computer forensics (analisi criminologica di sistemi informativi)
- la politica di gestione della sicurezza nelle aziende e delle sue implicazioni con gli impegni verso i clienti, i fornitori e i sub-contraenti

© Copyright Scuola Etica e Sicurezza 2018

Dallo schema di certificazione di un ente di certificazione – conoscenze (punto 5.1) - 3

- la strategia dell'informazione nell'organizzazione
- le best practice (metodologie) e gli standard nella analisi del rischio
- le best practice e gli standard nella gestione della sicurezza delle informazioni
- le metodologie di analisi dei fabbisogni di competenze e skill
- le norme legali applicabili ai contratti
- le nuove tecnologie emergenti (es. sistemi 375 distribuiti, modelli di virtualizzazione, sistemi di mobilità, data sets)
- le possibili minacce alla sicurezza
- le problematiche legate alla dimensione dei data sets (es. big data)
- le problematiche relative ai dati non strutturati (es. data analytics)
- le tecniche di attacco informatico e le contromisure per evitarli

© Copyright Scuola Etica e Sicurezza 2018



© Copyright Scuola Etica & Sicurezza 2018