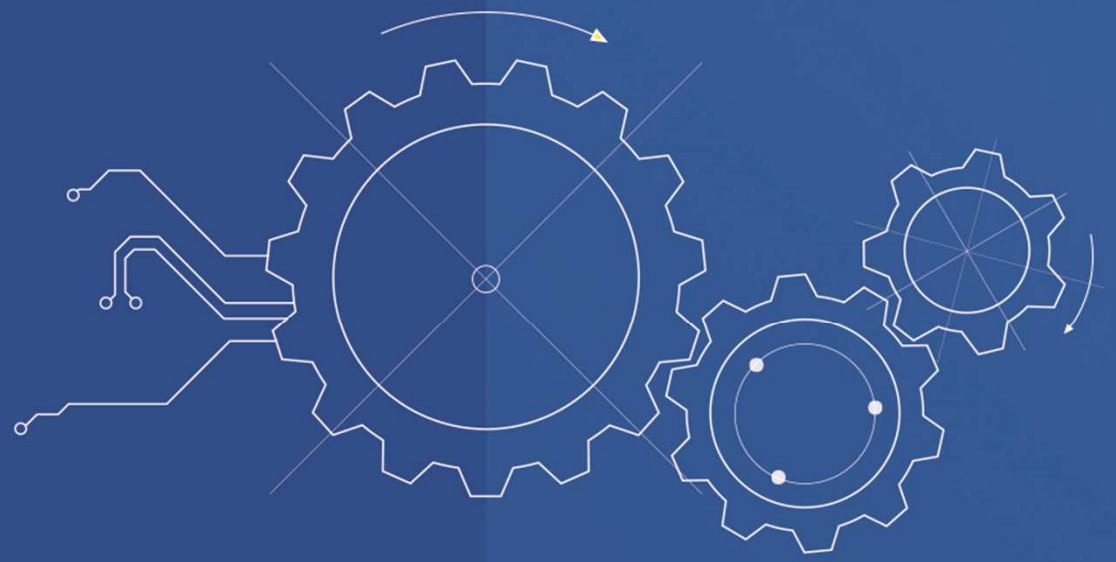
Comuni attrezzati per il GDPR

Incontro con le Pubbliche Amministrazioni Locali a Novara

La cassetta degli attrezzi: Registro dei trattamenti, Data Breach, DPO interno, Informativa e Norme contrattuali

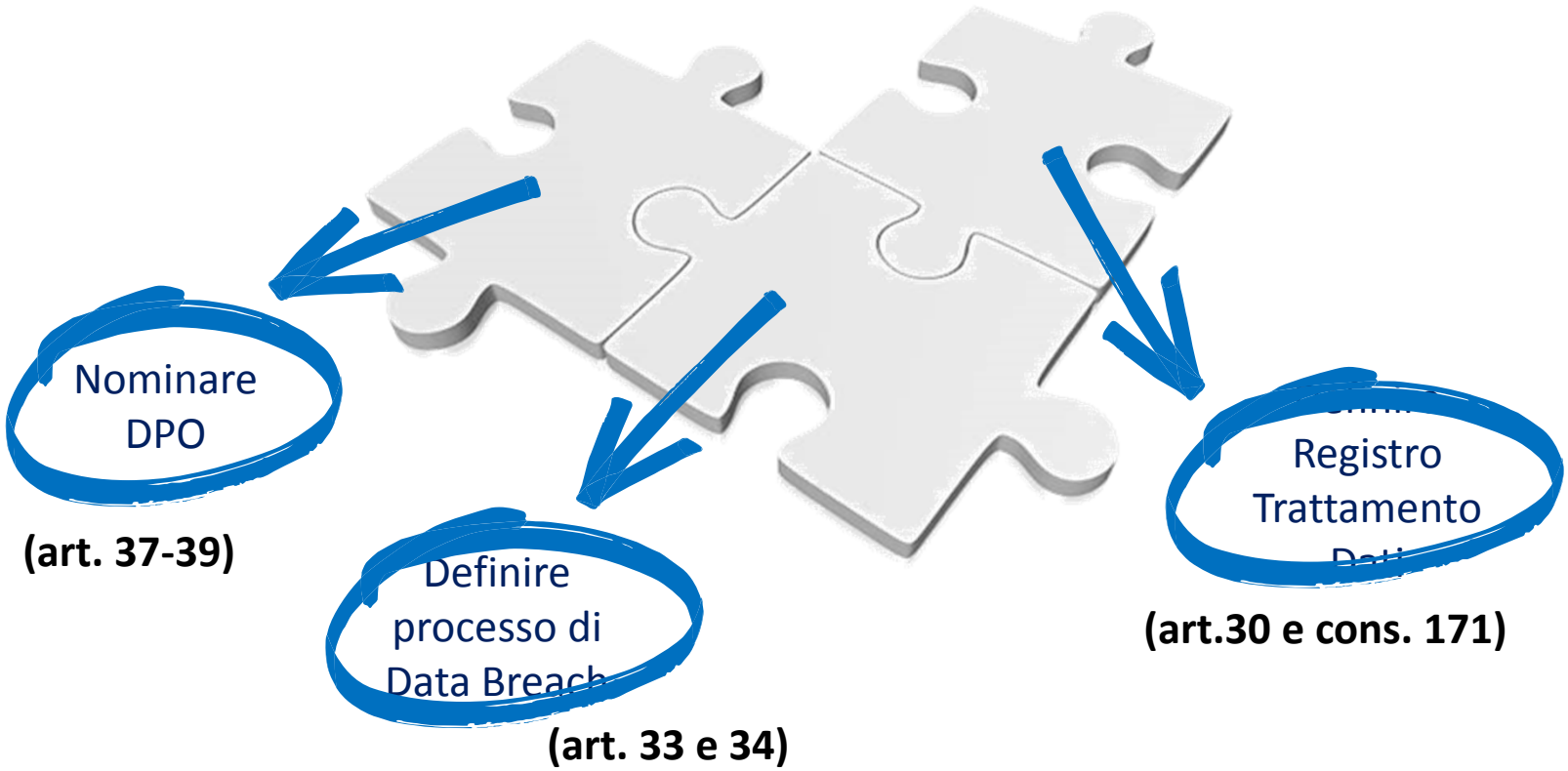
Torino 06/04/2018

Enzo Veiluva
Responsabile Sicurezza e Privacy
CSI Piemonte



PUBBLICA AMMINISTRAZIONE

LE TRE PRIORITA' INDICATE DAL GARANTE



IL REGISTRO DEI TRATTAMENTI

ART.30 GDPR

1) Ogni **titolare del trattamento** e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità…..

2) Ogni **responsabile del trattamento** e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento…..

3) I registri di cui ai paragrafi 1 e 2 sono tenuti in **forma scritta, anche in formato elettronico**

4) Su richiesta, il titolare del trattamento o il responsabile del trattamento e, ove applicabile, il rappresentante del titolare del trattamento o del responsabile del trattamento **mettono il registro a disposizione dell'autorità di controllo**

5) Gli obblighi di cui ai paragrafi 1 e 2 non si applicano alle imprese o organizzazioni con meno di 250 dipendenti, a meno che **il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1,** o i dati personali relativi a condanne penali e a reati di cui all'articolo 10.

Cosa contiene il Registro dei Trattamenti

a)il nome e i dati di contatto **del titolare del trattamento** e, ove applicabile, del **contitolare del trattamento**, del rappresentante del **titolare del trattamento** e del **responsabile della protezione dei dati**;

b) **le finalità del trattamento**;

c) una descrizione delle **categorie di interessati** e delle **categorie di dati personali**;

d) le **categorie di destinatari** a cui i dati personali sono stati o saranno comunicati, compresi i **destinatari di paesi terzi** od **organizzazioni internazionali**; ,

e) ove applicabile, i trasferimenti di dati personali verso **un paese terzo o un'organizzazione internazionale**, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;

f) ove possibile, i **termini ultimi previsti per la cancellazione** delle diverse categorie di dati;

g) ove possibile, una descrizione generale delle **misure di sicurezza tecniche e organizzative** di cui all'articolo 32, paragrafo 1

Es la proposta di ANCI (Quaderno 11)

REGISTRO ATTIVITA' DI TRATTAMENTO (art. 30, c.1, GPRD)

ENTE TITOLARE DEL TRATTAMENTO		**Responsabile protezione dati**	
Indirizzo		Indirizzo	
N. telefono		N. telefono	
Mail		Mail	
PEC		PEC	
Delegato dal Titolare (eventuale)		**Registro tenuto da**	
Indirizzo		**Data di creazione**	
N. telefono		**Ultimo aggiornamento**	
Mail		**N. schede compilate**	
PEC		**Prossima revisione**	

	TRATTAMENTO			DATI PERSONALI			INTERESSATI		DESTINATARI		TRASFERIMENTI	SICUREZZA
n. ordine	Descrizione	Finalità	Contitolare (eventuale Rappres.nte)	Categoria	Dati sensibili (SI/NO)	Termine ultimo cancell.ne	Categoria	Consenso (SI/NO)	Categoria	Paesi terzi, org.ni int.li (eventuale) (SI/NO)	Paesi terzi, org.ni int.li (eventuale)	Misure tecniche ed organizzative adottate

Quali Trattamenti ?

E’ POSSIBILE INDIVIDUARE UN ELENCO TIPICO DI TRATTAMENTI DI UNA AMMINISTRAZIONE COMUNALE?

QUALI RIFERIMENTI ADOTTARE?

Come si è operato

Su organizzazione della Regione Piemonte si è costituito un primo gruppo di volontari (GDL) appartenenti a ANCI, CSI Piemonte , Comune Di Biella, Comune di Alessandria, Unione Comuni Alta Langa , Comune di Vercelli, Comune di Cuneo, a cui si stanno aggiungendo ulteriori interessati

Punti di Partenza

1) Il DPS Documento Programmatico delle Sicurezza (obbligatorio sino al 2012) doveva riportare elenco dei trattamenti di dati personali sensibili e giudiziari in capo alla Pubblica Amministrazione

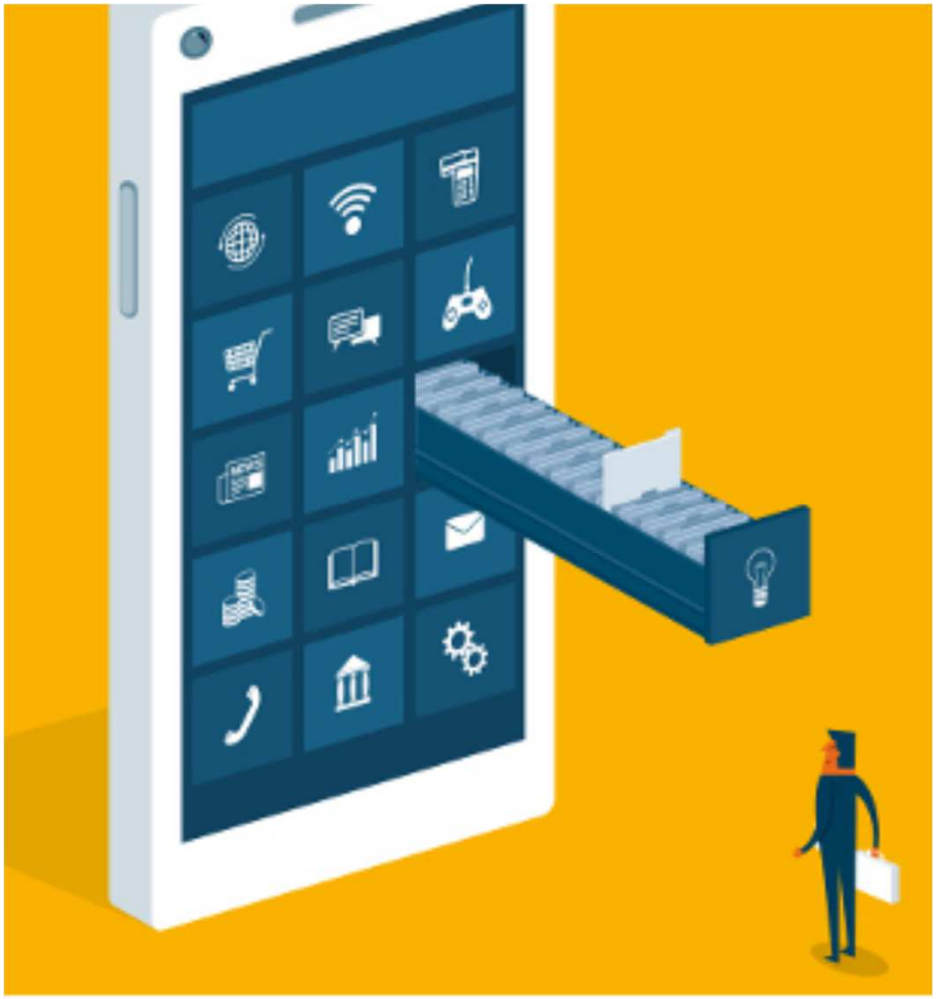
2) Elenco dei Procedimenti Amministrativi di competenza dell'Amministrazione Comunale

3) Coincidenza fra i contenuti della notifica dei trattamenti di cui all'art. 38 del Codice e quelli che devono costituire il registro dei trattamenti art. 30 regolamento (*Fonte Garante Privacy*)

4) Schema tipo regolamento trattamento dati sensibili e giudiziari (*parere Garante privacy 19 settembre 2005)*

Primo attrezzo della «cassetta»

Il GDL ha provato, confrontandosi sulle varie «esperienze casalinghe» ed in base alle fonti disposizione a produrre una proposta di elenco standardizzato di Trattamenti Dati tipici di una Amministrazione Comunale



Uno stralcio della proposta

	TRATTAMENTO		INTERESSATI
n	MACRO AREA	DESCRIZIONE	CATEGORIA
1	ACCERTAMENTI POLIZIA MUNICIPALE	Esposti e Segnalazioni a Organo di Polizia Municipale	Cittadini, Imprese
2	ACCESSO CIVICO	Accesso agli atti	Cittadini, Imprese
3	ACCORDI/CONVENZIONI	Stipula di accordi e convenzioni con enti pubblici o privati	Cittadini, Imprese, Enti
4	ALBO PRETORIO	Albo pretorio - Pubblicazioni dell'ente e di istanze da altri enti	Cittadini, Imprese, Enti
5	AMBIENTE	Tutela ambientale e decoro urbano	Cittadini, Imprese, Enti
6	AMBIENTE - ANIMALI	Gestione Anagrafe canina e Benessere Animale	Cittadini
7	AMBIENTE - RIFIUTI	Gestione smaltimento rifiuti (servizio, sanzioni, segnalazioni)	Cittadini, Imprese, Enti
8	ASILI NIDO	Asili Nido (iscrizione, rinuncia, decadenza, rette, ...)	Cittadini
9	ASSEGNAZIONI	Assegnazioni di beni e spazi a titolo gratuito	Cittadini, Imprese, Enti
10	ASSICURAZIONI	Gestione Assicurazioni (stipula, pratiche risarcimento, ecc..)	Cittadini, Imprese, Enti
11	BIBLIOTECA	Biblioteca (consultazione e prestito, prestito	Cittadini

Obiettivo

La proposta non vuole assolutamente rappresentare un elenco esaustivo o certificato , ma un elemento di supporto e di verifica per tutte le amministrazioni comunali e potrebbe essere auspicabile possa costituire anche un primo elemento di proposta di standardizzazione in termini di nomenclatura.

Lo «strumento» è pienamente aperto a proposte di miglioramento ed integrazione

IL DPO

Indicazioni del Garante: Schema di atto di designazione del RDP

Il GDPR prevede l'obbligo per il titolare o il responsabile del trattamento di designare il *RPD* «***quando il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizi****onali*» (art. 37, paragrafo 1, lett a);

Le predette disposizioni prevedono che il RPD «***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***» (art. 37, paragrafo 6) e deve essere individuato «***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***» (art. 37, paragrafo 5) *e* «***il livello necessario di conoscenza specialistica dovrebbe essere determinato in base ai trattamenti di dati effettuati e alla protezione richiesta per i dati personali trattati dal titolare del trattamento o dal responsabile del trattamento***» (considerando n. 97 del RGPD);

Atto di Nomina (Fonte www.garanteprivacy.it)

---- ;»

Nel caso in cui si opti per la designazione di un RPD condiviso si dovrà aggiungere

- Le disposizioni prevedono inoltre che *«un unico responsabile della protezione dei dati può essere designato per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione»* (art. 37, paragrafo 3);

Considerato che *l'Ente X*:

- è tenuto alla designazione obbligatoria del RPD nei termini previsti, rientrando nella fattispecie prevista dall'art. 37, par. 1, lett a) del RGPD;

Nel caso in cui si opti per la designazione di un RPD condiviso si dovrà aggiungere

- ha ritenuto di avvalersi della facoltà, prevista dall'art. 37, paragrafo 3, del Regolamento, di procedere alla nomina condivisa di uno stesso RPD con gli *Enti X, Y, Z*, sulla base delle valutazioni condotte di concerto con i predetti Enti in ordine a … (es. dimensioni, affinità tra le relative strutture organizzative, funzioni (attività) e trattamenti di dati personali, razionalizzazione della spesa);

- all'esito di … (*indicare la procedura selettiva interna o esterna, gara, altro*) ha ritenuto che il la/il ……., sia in possesso del livello di conoscenza specialistica e delle competenze richieste dall'art. 37, par. 5, del RGPD, per la nomina a RPD, e non si trova in situazioni di conflitto di interesse con la posizione da ricoprire e i compiti e le funzioni da espletare;

Atto di Nomina (Fonte www.garanteprivacy.it)

DESIGNA

(*generalità della persona individuata*), Responsabile della protezione dei dati personali (RPD) per l'*Ente X*,

Il predetto, nel rispetto di quanto previsto dall'art. 39, par. 1, del RGPD è incaricato di svolgere, in piena autonomia e indipendenza, i seguenti compiti e funzioni:

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 RGPD, nonché da altre disposizioni nazionali o dell'Unione relative alla protezione dei dati;

b) sorvegliare l'osservanza del RGPD, di altre disposizioni nazionali o dell'Unione 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 del RGPD;

d) cooperare con il Garante per la protezione dei dati personali;

e) fungere da punto di contatto con il Garante per la protezione dei dati personali 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;

(è possibile inserire di seguito anche ulteriori compiti, purché non incompatibili, quali ad es..

f) tenere il registro delle attività di trattamento sotto la responsabilità del titolare o del responsabile ed attenendosi alle istruzioni impartite…)

Atto di Nomina (Fonte www.garanteprivacy.it)

I compiti del Responsabile della Protezione dei Dati personali attengono all'insieme dei trattamenti di dati effettuati dall'Ente X.

L'*Ente X* si impegna a:

a) mettere a disposizione del RPD le seguenti risorse al fine di consentire l'ottimale svolgimento dei compiti e delle funzioni assegnate ... (*specificare, ad es. se è stato istituito un apposito Ufficio o gruppo di lavoro, le relative dotazioni logistiche e di risorse umane, nonché i compiti o le responsabilità individuali del personale*);

b) non rimuovere o penalizzare il RPD in ragione dell'adempimento dei compiti affidati nell'esercizio delle sue funzioni;

c) garantire che il RPD eserciti le proprie funzioni in autonomia e indipendenza e in particolare, non assegnando allo stesso attività o compiti che risultino in contrasto o conflitto di interesse;

DELIBERA

di designare ..... come Responsabile dei dati personali (RPD) per *l'Ente X*

Data .....

Modello di comunicazione al Garante (Fonte www.garanteprivacy.it)

Allegato B Nuove Faq sul Responsabile della Protezione dei dati (RPD) in ambito pubblico (in aggiunta a quelle adottate dal Gruppo Art. 29 in Allegato alle Linee guida sul RPD

MODELLO COMUNICAZIONE AL GARANTE DEI DATI DELL'RPD AI SENSI DELL'ART. 37, PAR. 1, LETT. A) E PAR. 7, DEL RGPD

DATI DEL TITOLARE/RESPONSABILE DEL TRATTAMENTO

Denominazione ente: .....

Codice Fiscale / P.Iva .....

Via / Piazza ..... N. civico .....

Città ..... Cap. ..... Provincia .....

Telefono ..... Fax .....

Email ..... Pec .....

Sito istituzionale .....

Atto di Notifica al Garante (Fonte www.garanteprivacy.it)

DATI DEL RESPONSABILE DELLA PROTEZIONE DEI DATI

Nome e cognome: .....

Data e luogo di nascita: .....

Sede (solo ove diversa da quella del titolare)

Via / Piazza ..... N. Civico .....

Città ..... Cap. ..... Provincia .....

Telefono ..... Fax .....

Email ..... Pec .....

In caso di stipulazione del contratto di servizio con una persona giuridica, indicare anche i seguenti dati della medesima:

Denominazione: .....

Via / Piazza ..... N. Civico .....

Città ..... Cap. ..... Provincia .....

Telefono ..... Fax .....

Email ..... Pec ..... Sito web .....

IMPORTANTE !

Ricordarsi che le **informazioni di contatto** (non l'identità) del **Responsabile della Protezione Dati** (es. e-mail, telefono ufficio, indirizzo postale, etc) DEVONO OBBLIGATORIAMENTE essere sempre presenti nelle informative rilasciate agli interessati per le attività di trattamento

DPO INTERNO O ESTERNO

Considerando che il GDPR esplicitamente prevede la possibilità di ricorrere a un servizio fornito da terzi, cosa è meglio tra designare un dipendente aziendale e acquistare un servizio da una fornitore specializzato?

La risposta, naturalmente, dipende da molti fattori: la dimensione dell'organizzazione, l'esistenza delle competenze richieste all'interno, la tipologia di dati trattati e di trattamenti e così via. Alcuni di questi fattori dipendono anche dal servizio offerto: la competenza specifica per il settore di attività del titolare sembra davvero un elemento chiave perchè un servizio esterno possa essere utile, in particolare per quei settori con minore cultura ed esperienza della privacy.

DPO Interno o Esterno?

«Il DPO va, infatti, considerato come un manager del cambiamento digitale (che è il presupposto su cui è fondato l'intero GDPR) **che deve acquisire conoscenze multidisciplinari per poter garantire in piena autonomia l'assistenza necessaria ai Titolari e/o Responsabili del trattamento nella costruzione di adeguati modelli organizzativi che siano, a loro volta, animati dai principi fondamentali della privacy by default e della privacy by design, nell'ambito dell'accountability che permea tutta l'attuale normativa europea**.»

Andrea Lisi - Avvocato, Presidente ANORC Professioni;

Direttore Master Unitelma La Sapienza "I professionisti della digitalizzazione e della privacy"

Fonte: https://www.anorc.eu/news/item/data-protection-officer-interno-o-esterno-il-dpo-sara-una-figura-strategica-per-ogni-tipo-di-organizzazione-non-affidiamola-al-caso

IL DPO

Agenda Digitale.eu

Cittadinanza digitale | Sicurezza Informatica | Sanità digitale

DATI PERSONALI

Documenti digitali | Scuola digitale | Cultura digitale | Mercat

Gdpr, attenti: fare il DPO non è un mestiere. Ecco le sue vere funzioni

Home > Sicurezza Digitale

Troppi equivoci, nel mercato, su cosa sia il responsabile della protezione dei dati (DPO). E' una figura rilevante, ma certamente non è il "centro" del sistema posto in essere dal GDPR, che nel nuovo ordinamento è sempre il Titolare del trattamento. Ecco quali sono le sue funzioni, le competenze e il ruolo

29 Set 2017

Franco Pizzetti, Professore ordinario di Diritto Costituzionale presso la Facoltà di Giurisprudenza dell'Università di Torino

IL PROCESSO DI DATA BREACH

ART 34
"Comunicazione di una violazione dei dati personali all'interessato«

Comma 1: Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.

Per **“Violazione di dati**” si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l’accesso ai dati personali trasmessi, conservati o comunque trattati (Art. 4 p.12 GDPR).

Da non dimenticare che già oggi…

Violazioni di dati personali *(data breach)*

Gli adempimenti previsti

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Il Garante per la protezione dei dati personali ha adottato una serie di provvedimenti che fissano per amministrazioni pubbliche e aziende l'obbligo di comunicazione nei casi in cui - a seguito di attacchi informatici, accessi abusivi, incidenti o eventi avversi, come incendi o altre calamità - si dovesse verificare la perdita, la distruzione o la diffusione indebita di dati personali conservati, trasmessi o comunque trattati. La scheda, che ha mere finalità divulgative, riassume i casi finora esaminati.

DOSSIER SANITARIO ELETTRONICO

Provvedimento n. 331 del 4 giugno 2015 [doc. web n. 4084632]

- **Entro 48 ore** dalla conoscenza del fatto, le strutture sanitarie pubbliche e private sono tenute a comunicare al Garante *(tramite il modello allegato al provvedimento)* tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui dati personali trattati attraverso il dossier sanitario.

AMMINISTRAZIONI PUBBLICHE

Provvedimento n. 392 del 2 luglio 2015 [doc. web n. 4129029]

- **Entro 48 ore** dalla conoscenza del fatto, le amministrazioni pubbliche sono tenute a comunicare al Garante *(tramite il modello allegato al provvedimento)* tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui dati personali contenuti nelle proprie banche dati.

Fonte: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/5031339

Notifica Data Breach GDPR 2016/679

Dato che l'obbligo di notifica **spetta al titolare**, è molto importante che, nell'affidare servizi a responsabili del trattamento, questi, preliminarmente, si accerti della capacità del fornitore nel gestire tempestivamente e adeguatamente un incidente di sicurezza (art. 28 p.1 GDPR) e, quindi, preveda **idonee clausole contrattuali** (art. 28 p.3 GDPR) che regolino il rapporto di fornitura in modo da garantire il rispetto del GDPR.

L'art. 33 p.2 GDPR prevede espressamente **il dovere** per il responsabile, quando viene a conoscenza di una violazione, di informare, senza ingiustificato ritardo, il titolare.

Scoprire l'incidente non è sufficiente, il titolare deve essere **in grado di valutare la portata di questo in termini di impatto rispetto ai dati personali ed ai diritti e la libertà degli interessati**.

Quando la notifica non deve essere effettuata anche all’interessato

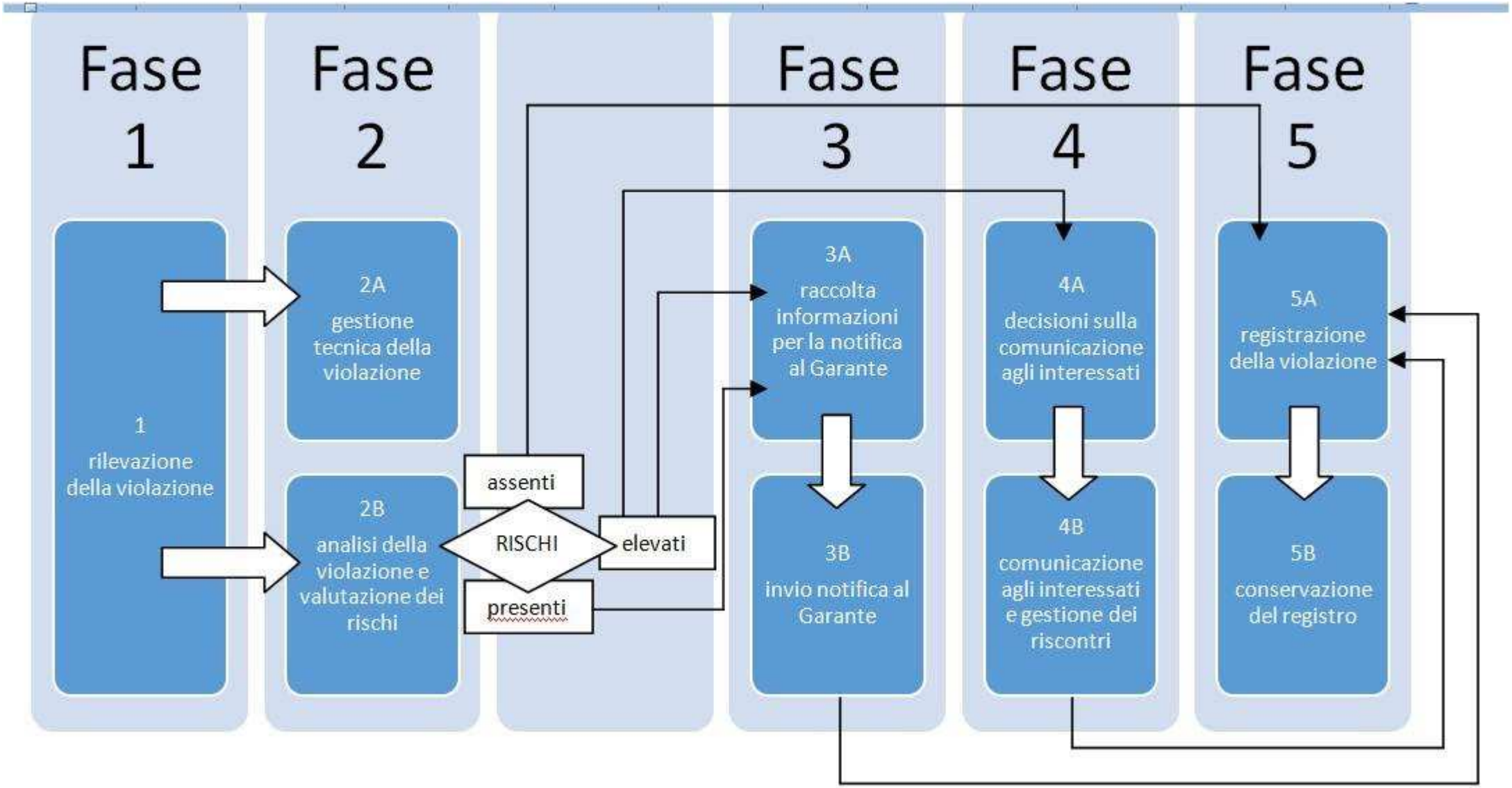
Se il titolare ritiene che il **rischio per i diritti e le libertà degli interessati è elevato, allora si dovranno informare anche gli interessati**, sempre "senza ingiustificato ritardo". Non è richiesta la comunicazione all'interessato nei casi indicati dall'art. 34:

a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la **cifratura**;

b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;

c) la **comunicazione richiederebbe sforzi sproporzionati**. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

Quindi …Processo Data Breach



Fonte: http://europrivacy.info/it/2017/11/13/italiano-data-breach-non-solo-notifica/

Registro delle violazioni (art.33 Comma 5)

*«Tutti i titolari di trattamento (imprese, studi professionali, **enti pubblici**) dovranno in ogni caso **documentare le violazioni di dati personali** subite, anche se non notificate all'autorità di controllo e non comunicate agli interessati, nonché le relative circostanze e conseguenze e i provvedimenti adottati.*

L'obbligo non è diverso, nella sostanza, da quello attualmente previsto dall'art. 32-bis, comma 7, del Codice della privacy. Il Garante italiano raccomanda, pertanto, ai titolari di trattamento di adottare le misure necessarie a documentare eventuali violazioni, essendo peraltro tenuti a fornire tale documentazione, su richiesta, al Garante in caso di accertamenti.»

Fonte: Federprivacy da Italia Oggi del 13 novembre 2017 – Articolo a cura di Antonio Ciccia Messina

Cosa si puo fare ?

Esempi di passi organizzativi all’interno dell’amministrazione comunale:

- Scegliere un fornitore in grado di offrire la predisposizione di «misure tecniche ed organizzative» adeguate (valutare anche certificazioni offerte)
- Definire norme contrattuali e le modalità di supporto
- Agire sul personale interno con opportuna formazione
- Predisporre disciplinari /regolamenti interni
- Definire un flusso interno per le fasi di valutazione e notifica
- Tenere un registro delle violazioni
- Valutare polizze assicurative

I CONTRATTI

Responsabilità solidale

RESPONSABILITA' SOLIDALE (art. 82)

Il Responsabile è responsabile in solido con il Titolare per l'intero ammontare dell'eventuale danno causato dal trattamento, al fine di garantire l'effettivo risarcimento dell'interessato.

L'eventuale azione di regresso sarà possibile se il Responsabile:

- ✓ non ha adempiuto agli obblighi del GDPR o
- ✓ ha agito in modo difforme o contrario rispetto alle istruzioni formalizzate nel contratto

culpa in eligendo e culpa in vigilando

I rapporti tra Titolare e Responsabile

CONTRATTO O ALTRO ATTO GIURIDICO SCRITTO che disciplini:

- ✓ La materia oggetto del trattamento
- ✓ Durata, natura, finalità del trattamento
- ✓ Tipo di dati trattati e categorie di interessati
- ✓ Obblighi e diritti del titolare e del Responsabile
- ✓ Modalità del trattamento con le misure tecniche ed organizzative adeguate a consentire il rispetto delle istruzioni impartite dal Titolare e delle disposizioni del GDPR

(art. 28 c. 3 del GDPR e art. 29 Codice Privacy novellato dalla Legge 167/2017)

Contratto: obbligo e garanzia contrattuale

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

ico.
Information Commissioner's Office

DATA PROCESSING AGREEMENT

(o Atto di nomina)

Premesso che:

- (L'ENTE)..... ha affidato a..... con la **convenzione/atto**..... stipulata in data ..... le attività ivi descritte che comportano il trattamento di dati personali, sensibili (o particolari) e giudiziari ai sensi del D. Lgs. 196/03 e s.m.i "Codice in materia di protezione dei dati personali" (di seguito anche solo "Codice") e del GDPR 679/2016 (Regolamento europeo in materia di privacy, di seguito anche solo GDPR);
- **l'art. 29** del Codice e **l'art. 28** del GDPR attribuiscono al Titolare del trattamento la facoltà di ricorrere ad un **Responsabile** che presenti, per **esperienza, capacità ed affidabilità** garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate in modo tale che il trattamento soddisfi i requisiti previsti dalle vigenti disposizioni in materia di trattamento dati, ivi compreso il profilo relativo alla sicurezza e garantisca la tutela dei diritti dell'interessato;
- l'art. 4 comma 1 lett. g) del Codice e l'art. 4 comma 1 n. 8), del GDPR individua quale **Responsabile del Trattamento** la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;
- considerata l'idoneità di..... rispetto alle caratteristiche di **esperienza, capacità ed affidabilità**, richieste dalla legge per la tutela del trattamento dei dati, in relazione alle attività affidategli

L’INFORMATIVA

L’INFORMATIVA

DEVE CONTENERE

a**) l’identità e i dati di contatto del titolare del trattamento** e, ove applicabile, del suo rappresentante;

b) **i dati di contatto** del responsabile della protezione dei dati, ove applicabile;

c) **le finalità del trattamento , nonché la base giuridica del trattamento**;

d) qualora il trattamento si basi sull’articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi;

e) **gli eventuali destinatari** o le eventuali **categorie di destinatari** dei dati personali;

f) ove applicabile, l’intenzione del titolare del trattamento di trasferire dati personali **a un paese terzo o a un’organizzazione internazionale** e l’esistenza o l’assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all’articolo 46 o 47, o all’articolo 49, secondo comma, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili.

IN AGGIUNTA

a) **il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;**

b) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso , la rettifica o la cancellazione o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati, se consentito ;

c) l'esistenza del diritto **di revocare il consenso** in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;

d) il diritto di proporre **reclamo a un'autorità di controllo**;

e) se la comunicazione di dati personali **è un obbligo legale o contrattuale** oppure un requisito necessario per la conclusione di un contratto

f) l'esistenza di un processo decisionale automatizzato, **compresa la profilazione** di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

In SINTESI

Modalità dell'informativa

Il regolamento specifica molto più in dettaglio rispetto al Codice le caratteristiche dell'informativa, che deve avere forma **concisa, trasparente, intelligibile per l'interessato e facilmente accessibile**; occorre utilizzare un linguaggio **chiaro e semplice**, e per i minori occorre prevedere informative idonee *(si veda anche considerando 58)*.

L'informativa è data, **in linea di principio, per iscritto** e **preferibilmente in formato elettronico** (soprattutto nel contesto di servizi online: *si vedano art. 12, paragrafo 1, e considerando 58*), anche se sono ammessi "altri mezzi", quindi può essere fornita anche oralmente, ma nel rispetto delle caratteristiche di cui sopra *(art. 12, paragrafo 1)*. Il regolamento ammette, soprattutto, l'utilizzo di **icone** per presentare i contenuti dell'informativa in forma sintetica, **ma solo "in combinazione" con l'informativa estesa** *(art. 12, paragrafo 7)*; queste icone dovranno essere identiche in tutta l'Ue e saranno definite prossimamente dalla Commissione europea.

Sono inoltre **parzialmente diversi i requisiti che il regolamento fissa per l'esonero dall'informativa** *(si veda art. 13, paragrafo 4 e art. 14, paragrafo 5 del regolamento, oltre a quanto previsto dall'articolo 23, paragrafo 1, di quest'ultimo)*, anche se occorre sottolineare che **spetta al titolare**, in caso di dati personali raccolti da fonti diverse dall'interessato, **valutare se la prestazione dell'informativa agli interessati comporti uno sforzo sproporzionato** *(si veda art. 14, paragrafo 5, lettera b))* – a differenza di quanto prevede l'art. 13, comma 5, lettera c) del Codice.

Raccomandazioni del garante privacy

RACCOMANDAZIONI

E' opportuno che i titolari di trattamento **verifichino la rispondenza delle informative** attualmente utilizzate a tutti i criteri sopra delineati, con particolare riguardo ai **contenuti obbligatori** e alle **modalità di redazione**, in modo da apportare le modifiche o le integrazioni eventualmente necessarie ai sensi del regolamento.

Il regolamento supporta chiaramente il concetto di **informativa "stratificata"**, più volte esplicitato dal Garante nei suoi provvedimenti [si veda **http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1712680** relativo all'utilizzo di un'icona specifica per i sistemi di videosorveglianza con o senza operatore; **http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1246675** contenente prescrizioni analoghe rispetto all'utilizzo associato di sistemi biometrici e di videosorveglianza in istituti bancari], in particolare attraverso l'impiego di icone associate (in vario modo) a contenuti più estesi, che devono essere facilmente accessibili, e promuove **l'utilizzo di strumenti elettronici** per garantire la massima diffusione e semplificare la prestazione delle informative.

EVOLUZIONE DELLA CASETTA DEGLI ATTREZZI

COMUNI PIEMONTESI ATTREZZATI PER IL GDPR

STRUMENTI DI LAVORO

Questi materiali vengono incrementati e aggiornati periodicamente.

Il GDPR

Guida all'applicazione del GDPR

Quaderno ANCI n.11. Il GDPR negli Enti Locali: istruzioni, linee guida e modulistica (pdf)

Pillole video

Le novità introdotte dalla normativa GDPR

Protezione e gestione della password: come difendere il pc dagli hacker

Malware tramite e-mail: sicurezza e gestione della posta indesiderata

Gestione dei dati e logiche di backup

Alcune idee…

- Esempi/modello per l'applicazione della DPIA
- Esempi di Informativa per i servizi dell'Amministrazione Comunale
- Linee Guida e Check List per l'applicazione della privacy by design
- Esempi/modello di disciplinare interno
- Esempi di registro delle violazioni
- Modello di comunicazione di Data Breach (*aggiornamento annunciato dal Garante privacy)*
- ……..

Il GDL è aperto a tutti coloro che intendono contribuire ….

La Privacy è un problema di tutti !

Ritrovarsi insieme è un inizio, restare insieme è un progresso, ma riuscire a lavorare insieme è un successo. (Henry Ford)

Grazie

enzo.veiluva@csi.it