ISACA®

Sistemi informativi: averne fiducia e trarne valore

Rome Chapter

GDPR dopo 5 mesi dalla sua applicazione: evoluzione e prime considerazioni

GDPR nel settore bancario, finanziario ed assicurativo

Cesare De Santis

Roma 19/10/2018

Agenda

- Presentazione relatore
- GDPR nel settore bancario, finanziario ed assicurativo
- Bibliografia & sitografia
- Q&A

Agenda

Presentazione relatore

- GDPR nel settore bancario, finanziario ed assicurativo
- Bibliografia & sitografia
- Q&A

Presentazione relatore

Cesare De Santis

Ho lavorato a lungo per Enti della P.A. (Difesa) ed aziende private (banca e alcune società di consulenza di emanazione bancaria) prima di intraprendere, nel 2008, un autonomo percorso professionale.

Attualmente sono amministratore unico di PRIMAe srl, che opera sui temi della privacy, della sicurezza, dell'auditing dei S.I., della compliance e della organizzazione. Tra i clienti di PRIMA*e* srl si annoverano banche, finanziarie, società di leasing, compagnie di assicurazione e riassicurazione, fondi pensione, società immobiliari, altre società di consulenza.

Titoli/certificazioni/attestati

Laureato in Scienze statistiche ed attuariali, abilitato alla professione di attuario, CISM, iscritto nel registro dei consulenti privacy di KHC (http://www.khc.it/)

Agenda

- Presentazione relatore
- GDPR nel settore bancario, finanziario ed assicurativo
- Q&A
- Bibliografia & sitografia

Agenda

- Presentazione relatore
- **GDPR nel settore bancario, finanziario ed assicurativo**
- Q&A
- Bibliografia & sitografia

Premessa: il nostro «osservatorio» e il ruolo che svolgiamo

Primae srl gioca diversi ruoli presso le aziende del c.d. «osservatorio»:

- Società di consulenza a supporto del piano di adeguamento
- Consulente azienda per verifica piano di adeguamento supportato da altra società
- DPO
- Supporto al DPO
- Supporto a verifica di compliance sulla protezione dei dati personali

«Osservatorio»

Aziende	***Contesto***	***Dipendenti***
Banche		
Banca 1	Azienda autonoma	< 1.000
Banca 2	Capogruppo di gruppo italiano	> 1.000
Banca 3	Azienda autonoma	< 1.000
Banca 4	Azienda autonoma	< 100
Banca 5	Azienda autonoma	< 100
Banca 6	Azienda Autonoma	< 100
Banca 7	Componente gruppo italiano	< 1.000
Banca 8	Azienda autonoma	< 1.000
Banca 9	Azienda autonoma	> 1.000
Finanziarie		
Finanziaria 1	Azienda autonoma	< 1.000
Finanziaria 2	Azienda autonoma	< 100
Compagnie assicurazione/riassicurazione		
Compagnia 1	Componente gruppo europeo	< 1.000
Rappresentanza 1	Componente gruppo europeo	< 100
Rappresentanza 2	Componente gruppo europeo	< 100
Fondi Pensione		
Fondo pensioni 1	Componente gruppo europeo	< 100
Real Estate		
Gruppo RE 1	Componente gruppo europeo	< 100

Premessa: il ruolo di outsourcer informatici & Capogruppo

- Presso gli outsourcer sono stati attivati diversi Cantieri, con la partecipazioni di aziende utenti della piattaforma applicativa, che hanno prodotto metodologie e indicazioni tecnico/organizzative
- Gli outsourcer hanno fornito in genere il registro dei trattamenti del responsabile
- Nel caso di alcuni outsourcer i Cantieri hanno prodotto anche modelli di documenti rappresentativi di adempimenti (documenti di nomina, policy, informativa clientela)
- Le Capogruppo dei gruppi multinazionali, con il supporto di società di consulenza internazionali, hanno prodotto metodologie, indicazioni tecnico/organizzative, policy, informativa clientela e dipendenti ed hanno individuato il DPO di gruppo, in qualche caso a livello di Paese

Uno sguardo al GDPR: i principali adempimenti

I principali adempimenti previsti dal GDPR riguardano:

- **Principio di responsabilizzazione e altri principi**
- **Responsabile del trattamento (esterno)**
- **Persone autorizzate (incaricati) al trattamento**
- **Responsabile della protezione dei dati (DPO)**
- **Informativa**
- **Consenso**
- **Diritti dell'interessato (portabilità)**
- **Privacy by design e by default**
- **Valutazione d'impatto sulla protezione dei dati**
- **Registro dei trattamenti**
- **Analisi dei rischi e misure di sicurezza**
- **Violazione dei dati personali**
- **Trasferimento di dati all'estero**

Principio di responsabilizzazione e altri principi

Sintesi adempimenti

Il Titolare(1) del trattamento, che determina le finalità e i mezzi per il trattamento, deve garantire (principio di responsabilizzazione) attraverso adeguate misure - che possono comprendere l'attuazione di politiche adeguate - riesaminate e aggiornate qualora necessario, per garantire ed essere in grado di dimostrare la conformità al GDPR. Tale dimostrazione può avvenire anche attraverso certificazioni privacy ed adesione a codici di condotta approvati, che alla data non sono ancora disponibili. Sulla certificazione c'è stato un comunicato congiunto Accredia/Garante(2)

I principi che riguardano i requisiti dei dati sono: principi di **liceità**; correttezza e trasparenza; limitazione delle finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; sicurezza, integrità e riservatezza

.

Problematiche emerse & linea d'azione

Le aziende hanno emanato una **policy GDPR** nella quale si promuovono i principi della protezione dei dati personali, che è attuata da specifiche norme operative interne (**Regolamento privacy aziendale e relativi allegati**). Al termine dell'adeguamento del sistema di gestione della privacy, l'azienda potrà scegliere se procedere a richiedere una certificazione privacy (sottoponendosi al processo di certificazione) ovvero aderire a codici di condotta, nel frattempo approvati.

(1) Nel Regolamento UE sia il Titolare che il Responsabile possono essere persone fisiche, persone giuridiche, Autorità pubblica, servizio o altro organismo

(2) http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6621723

Responsabile del trattamento (esterno)

Sintesi adempimento & linea guida

Il Responsabile del trattamento, tratta i dati personali per conto del Titolare del trattamento. In caso di esternalizzazione dei trattamenti la società esterna opera quale Responsabile. Il Responsabile deve essere istruito dal Titolare e deve garantire che le persone autorizzate al trattamento siano impegnate alla riservatezza o ne abbiano obbligo legale. E' importante sottolineare che il Responsabile deve essere scelto, con un contratto o altro atto giuridico, dal Titolare tra soggetti che presentino garanzie sufficienti (ad esempio con certificazioni e adesione a codici di condotta) a mettere in atto misure che soddisfino i requisiti del Regolamento UE e in caso di sub-responsabili garantisce per essi. Utile per stabilire il ruolo privacy di soggetti (fornitori, partner commerciali, outsourcer) è il «*Parere 1/2010 sui concetti di "responsabile del trattamento" e "incaricato del trattamento*" (WP169).

Problematiche emerse & linee di azione

Nelle aziende è stato effettuato un **censimento** dei fornitori/outsourcer cui è stato inviato un c.d. **contratto di nomina**, in qualche caso corredato da allegato tecnico, da ritornare controfirmato rinnovando la eventuale nomina pregressa. Alcune aziende sono state **nominate responsabili del trattamento da partner commerciali** (ad esempio da parte di Compagnie di assicurazione nel caso di collocamento di prodotti assicurativi effettuato da banche sulla propria clientela) e questo implica per tali aziende **la tenuta di un separato Registro dei trattamenti** (vedi appresso)

Persone autorizzate (incaricati) al trattamento

Sintesi adempimento

La figura previgente dell'incaricato del trattamento non è prevista specificatamente nel GDPR ma viene indicato che chiunque agisca sotto l'autorità del Responsabile o del Titolare deve essere istruito dal Titolare (art. 29). Il Garante privacy nella sua Guida *"… ritiene opportuno che titolari e responsabili del trattamento mantengano in essere la struttura organizzativa e le modalità di designazione degli incaricati di trattamento così come delineatesi negli anni anche attraverso gli interventi del Garante …"*

L'art. 2-quaterdecies (Attribuzione di funzioni e compiti a soggetti designati) del d.lgs. 196/2003 così come modificato dal d.lgs. 101/2018 prevede che "*Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità*."

Problematiche emerse & linee d'azione

Le nomine degli incaricati sono state rinnovate, nelle realtà più piccole attraverso lettere nominative e in quelle più grandi attraverso specifici ordini di servizio. La problematica dei responsabili del trattamento interni, molto usati nella realtà italiana, appare superata dall'individuazione di nuove figure (referenti privacy) con compiti organizzativi relativamente agli adempimenti. Per quanto riguarda la formazione degli incaricati, nelle realtà più piccole, ed anche per la formazione dei referenti privacy, è privilegiata la formazione in aula mentre nelle realtà più grandi si ricorre ai prodotti di e-learning corroborati, in qualche situazione, da apposite «pillole» formative.

Responsabile della protezione dei dati (DPO)

Sintesi adempimento & linea guida

Sulla figura del **Responsabile della protezione dei dati** il Garante privacy ha pubblicato delle apposite FAQ nelle quali individua «*istituti di credito; imprese assicurative; sistemi di informazione creditizia; società finanziarie*» tra i soggetti tenuti alla nomina. Pubblicate «Linee guida sui responsabili della protezione dati» (WP243).

Linea d'azione (segue)

Aziende	***DPO***
Banche	
Banca 1	Interno (compliance)
Banca 2	Interno (compliance)
Banca 3	Interno (organizzazione)
Banca 4	Interno (controlli interni)
Banca 5	Esterno (Primae srl)
Banca 6	Esterno (Primae srl)
Banca 7	Di gruppo (compliance)
Banca 8	Interno (controlli interni)
Banca 9	Interno (compliance)
Finanziarie	
Finanziaria 1	Interno (risk management)
Finanziaria 2	Interno (organizzazione)
Compagnie assicurazione/riassicurazione	
Compagnia 1	Interno (compliance)
Rappresentanza 1	Di gruppo (compliance)
Rappresentanza 2	Di Gruppo (compliance)
Fondi Pensione	
Fondo pensioni 1	Di gruppo territoriale (compliance)
Real Estate	
Gruppo RE 1	Di gruppo territoriale (compliance)

Responsabile della protezione dei dati (DPO): nomina

Linea d'azione

La nomina può riguardare un soggetto esterno, ingaggiato attraverso un contratto di servizio, o un soggetto interno che possieda le caratteristiche indicate nelle linee guida WP29 e non presenti conflitti di interessi nelle attività svolte. La soluzione interna dovrebbe garantire una maggiore conoscenza dei processi aziendali e dei relativi trattamenti di dati personali (mentre una soluzione esterna potrebbe presentare un minor rischio di condizionamenti «ambientali») ed una maggiore facilità di coinvolgimento nelle decisioni da assumere in materia di protezione dei dati personali.

Occorre evitare i conflitti d'interesse anche attraverso la individuazione dei conflitti stessi nella normativa interna.

La individuazione del soggetto interno ha in genere implicato una integrazione delle sue conoscenze di base con specifiche azioni formative mentre una certificazione delle competenze non appare in questo momento necessaria.

Il DPO funge da contatto con l'Autorità di controllo (vedi anche meccanismo dello «sportello unico»)

Informativa ai soggetti interessati

Sintesi adempimento & linea guida

L'informativa, sia per raccolta dei dati presso l'interessato che presso terzi, anche con contenuti più specifici (quali il periodo di conservazione dei dati o criteri per determinarlo) rispetto a quelli previgenti, è un adempimento previsto dal GDPR ove è precisato che l'informativa deve essere fornita "*in forma concisa, trasparente, intelligibile, e facilmente accessibile usando un linguaggio chiaro e semplice* ", anche utilizzando apposite icone. Confermate in Guida GDPR del Garante icone videosorveglianza. L'esonero informativa per sforzo sproporzionato è da valutare da parte del Titolare.
Sono state emanate le «Linee guida sulla trasparenza ai sensi del regolamento 2016/679» (WP260)

Problematiche emerse & linea d'azione

Come indicato dal Garante privacy nella sua Guida « *… 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 prima del 25 maggio 2018 …».* E' stata necessaria le revisione delle informative (e dei consensi, vedi appresso) verso tutti i soggetti interessati, sia nell'approccio [vedi in proposito l'articolo di Alberto Fuccello(1)] verso l'interessato sia nei contenuti (es. indicazione tempo di conservazione, basi giuridiche, ecc.) . Le aziende hanno predisposto la informativa per la clientela che è stata posta sul sito aziendale e sono stati utilizzati vari metodi per segnalare tale modifica (avvisi cartacei in agenzia, totem, avvisi nelle schermate del bancomat, home banking, comunicazione periodica nonché, in qualche caso l'invio della informativa al cliente). Sono state altresì predisposte tutte le altre informative gestite (vedi slide seguente).

(1) https://www.linkedin.com/pulse/gdpr-lalba-delle-nuove-informative-privacy-alberto-fuccello/?trackingId=wWE9Hm1GAvgofu52MyEqeg%3D%3D

Quali informative sono rese e in quale modo

Tipo informativa	Modalità di resa	U.O. competente
Clienti	In documentazione contrattuale	Filiale
Informativa SIC	In richiesta credito	Filiale
Esponenti societari	All'atto della nomina	Segreteria generale
Dipendenti	All'atto dell'assunzione	Uffico del Personale
Candidati all'assunzione	Alla selezione	Segreteria generale
Lavoratori interinali	All'atto dell'ingresso in azienda	Ufficio del Personale
Tirocinanti	All'atto dell'ingresso in azienda	Ufficio del Personale
Fornitori e professionisti	In lettera d'ordine o contratto	U.O. interessata
Videosorveglianza sintesi	vetrofanie	Ufficio Organizzazione
Videosorveglianza estesa	affissione	Ufficio Organizzazione
Sottoscrittori documenti	All'accettazione del servizio	Filiale
Navigatori Internet	Sul sito internet	Banca Online
Soci	All'atto dell'adesione	Segreteria generale

Consenso al trattamento

Sintesi adempimento & linea guida

Il consenso è definito nel GDP come "*qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento*". Tipicamente il consenso deve essere raccolto per la promozione commerciale e per la profilazione. C'è da segnalare, in alternativa al consenso l'introduzione del c.d. legittimo interesse del Titolare tra le condizioni di liceità del trattamento oltre all'obbligo di legge e all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali prese su richiesta dello stesso, già presenti nel Codice privacy. Non occorre che l'interessato presti nuovamente il suo consenso, se questo è stato espresso secondo modalità conformi al GDPR (considerando 171). Il consenso dei minori, nel caso di offerta diretta di servizi della società dell'informazione (1), è valido a partire dai 14 anni (2) ; al di sotto di tale età occorre raccogliere il consenso dei genitori o di chi ne fa le veci. Il Titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso, in caso sia utilizzata tale condizione di liceità.

Sono state emanate «Linee guida sul consenso ai sensi del regolamento (UE) 2016/679» (WP259) .

Linea d'azione (segue)

In parallelo all'adeguamento dei testi delle informative **è stata adeguata l'articolazione dei consensi** ed è stata stabilita una **corrispondenza con l'articolazione dei consensi previgente** nelle procedure di gestione dei consensi privacy dei clienti. Nel comunicare la nuova informativa è stato riportato che i **consensi prestati rimanevano validi** a meno di diversa decisione del cliente.

(1) Disciplinata dalla Direttiva UE 2015/1535
(2) Art. 2 quinquies Codice privacy novellato

Quali consensi sono gestiti

CONSENSO AI SENSI DEL REGOLAMENTO EUROPEO, PER LA PROTEZIONE DEI DATI, 679/2016

Profilazione (3.3)
□ do il consenso □ nego il consenso

Decisioni automatizzate (3.4)
□ do il consenso □ nego il consenso

Marketing (3.5)
□ do il consenso □ nego il consenso

Attività di marketing per prodotti di terzi (3.6)
□ do il consenso □ nego il consenso

Cessione di dati personali a terzi (3.7)
□ do il consenso □ nego il consenso

Controllo della qualità dei servizi (3.8)
□ do il consenso □ nego il consenso

Trattamento di categorie particolari di dati personali ("dati sensibili") (3.9)
□ do il consenso □ nego il consenso

DATA FIRMA

Diritti dell'interessato

Sintesi adempimenti & linea guida

Il GDPR prevede specificatamente i diritti alla rettifica, cancellazione ed opposizione (già previsti dal Codice privacy) nonché il diritto alla limitazione(1) del trattamento ed alla portabilità (2) dei dati (da un Titolare ad un altro). Il limite temporale indicato per il riscontro all'esercizio di tali diritti è di un mese. Il Garante privacy nella sua Guida indica che *« … E' opportuno che i titolari di trattamento adottino le misure tecniche e organizzative eventualmente necessarie per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati, che – a differenza di quanto attualmente previsto – dovrà avere per impostazione predefinita forma scritta (anche elettronica) … «* e che « *… i titolari possono consentire agli interessati di consultare direttamente, da remoto e in modo sicuro, i propri dati personali (si veda considerando 68) …».* Per quanto riguarda il contributo spese l'Autorità intende valutare l'opportunità di definire linee-guida specifiche. E' stata emanata da WP29 una «Linea guida sul diritto alla portabilità» (WP242) e «Linee guida elaborate dal Gruppo Art. 29 in materia di processi decisionali automatizzati e profilazione, definite in base alle previsioni del Regolamento (UE) 2016/679» (WP251)

Problematiche emerse & linea d'azione (segue)

Sono state **riviste le procedure per il riscontro dell'esercizio dei diritti** degli interessati individuando altresì, eventualmente in sinergia con l'outsourcer, soluzioni tecniche per realizzare il contrassegno relativo alla limitazione di trattamento e gli aspetti tecnici della portabilità considerando che il Garante nella sua Guida indica « *… Poiché la trasmissione dei dati da un titolare all'altro prevede che si utilizzino formati interoperabili, i titolari che ricadono nel campo di applicazione di questo diritto dovrebbero adottare sin da ora le misure necessarie a produrre i dati richiesti in un formato interoperabile secondo le indicazioni fornite nel considerando 68 e nelle linee-guida del Gruppo WP29 …».* E' stato definito un **perimetro dei dati interessati ai vari diritti** e in particolare alla portabilità. Il d.lgs. 101/2018 ha introdotto limitazioni (es. antiriciclaggio nell'esercizio dei diritti. Problema aperto il discorso del **periodo di conservazione** dei dati (vedi appresso) e **cancellazione** dei dati

(1) il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro

(2) Se il trattamento si basa su consenso o su un contratto ed è effettuato con mezzi automatizzati *" … L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti "*

Esempi di tempi di conservazione

TABELLA DEI TEMPI DI CONSERVA

*(**nota bene**: i punti in giallo riguardano solo banche e soggetti obbligati, quelli c*

Tipologia dati	***Tempo di conservazione***
dati relativi alle scritture contabili	10 anni
dati relativi alle operazioni poste in essere dal cliente	10 anni
e-mail a contenuto e rilevanza giuridica e commerciale	10 anni
dati centrali rischi (**sui SIC**)	max 5 anni scadenza rapporto
dati relativi al dettaglio degli acquisti (marketing)	24 mesi da registrazione
dati relativi al dettaglio degli acquisti (profilazione)	12 mesi da registrazione
dati richiesta finanziamento respinta/rinunciata **sui SIC**	6 mesi/1 mese
log Amministratori di sistema (c.d. Garante I)	almeno 6 mesi
log tracciamento operazioni bancarie (c.d. Garante II)	almeno 24 mesi
account di posta elettronica aziendale	da determinare (1)
immagini da videosorveglianza	24 ore (7 giorni solo banche)
dati di curriculum	da determinare (2)
dati di navigazione (sul sito)	7 giorni (3)
log di accesso al sistema informativo	12 mesi [dato medio banche(4)]
log della posta elettronica e di accesso a Internet	da determinare(5)
Dati relativi ai sinistri (**su banche dati istituzionali**)	5 anni/10 anni
Dati adeguata verifica antiriciclaggio	10 anni dalla chiusura rapporto
Cartella sanitaria lavoratore	10 anni(6) da cessazione lavoratore

Privacy by design e by default

Sintesi adempimento

"Privacy by design"(analizzare contesto, caratteristiche, ambito applicazione, finalità nonché rischi del trattamento fin dal momento della determinazione dei mezzi del trattamento allo scopo di adottare misure adeguate, quali la pseudonimizzazione) e "Privacy by default" (adozione di misure adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati necessari ad ogni specifica finalità del trattamento) sono nuovi adempimenti che costituiscono secondo il Garante « … *un'analisi preventiva e un impegno applicativo da parte dei titolari che devono sostanziarsi in una serie di attività specifiche e dimostrabili* …»

Problematiche emerse & linea d'azione

Sono state predisposte delle **procedure aziendali (anche sotto forma di questionario)** affinchè i nuovi progetti siano preventivamente sottoposti alle analisi richieste da documentare opportunamente ed allegare alla documentazione di progetto ed in particolare **valutare il rischio inerente** (ad esempio tenendo conto di tipologie di interessati, e numerosità di essi, e di tipo dati trattati, di caratteristiche – cartaceo, elettronico, misto, di profilazione, finalizzato ad assumere decisione completamente automatizzata – del trattamento, di presenza outsourcing nonché di trasferimenti all'estero) che se superiore al livello di accettabilità richiede l'esecuzione di DPIA. In caso di valore accettabile occorre comunque **confrontare il trattamento con le 9 circostanze di rischio** di cui alla linea guida WP29 su DPIA .

Necessità PbD & DPIA

Necessità PbD

- la progettazione di una nuova iniziativa che preveda il trattamento di dati personali;
- l'estensione di un trattamento già previsto a nuove categorie di interessati o dati personali;
- qualsiasi modifica della struttura organizzativa della società;
- la sottoscrizione di contratti di fornitura che comportino la nomina a responsabile esterno della controparte;
- le categorie di destinatari cui i dati personali oggetto del trattamento sono comunicati;
- la necessità di trasferire i dati personali trattati all'esterno dell'Unione Europea;
- qualsiasi modifica dei sistemi informativi adottati;
- l'adozione di nuove misure tecniche e/o organizzative.

Necessità DPIA (almeno due)

1. Valutazione o scoring (es. valutazione merito creditizio)
2. Processo decisionale automatizzato con significativi effetti di natura legale o similari
3. Monitoraggio sistematico
4. Uso di particolari categorie di dati
5. Dati trattati su larga scala (es. di larga scala: attività ordinaria di banche/assicurazioni)
6. Archivi elettronici confrontati o combinati
7. Uso di dati di soggetti vulnerabili (es.: minori)
8. Uso innovativo o applicazioni tecnologiche o soluzioni organizzative
9. Trattamento che impedisce a soggetti esercizio diritto/uso servizio/contratto

Valutazione d'impatto sulla protezione dati

Sintesi adempimento & Linea guida

Il Data Protection Impact Assessment (DPIA), che può riguardare un singolo trattamento o un insieme di trattamenti similari, è necessario quando un trattamento può presentare un rischio elevato (vedi le 9 situazioni già citate) per i diritti e le libertà fondamentali delle persone fisiche, allorchè prevede in particolare l'uso di nuove tecnologie e considerando natura, oggetto, contesto e finalità del trattamento (art. 35 comma 1 GDPR).

Sono state pubblicate «*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*» (WP248) In tale linea guida sono indicate 9 circostanze, già citate, che rendono obbligatoria la DPIA che dovrebbero essere alla base dell'elenco nazionale delle tipologie di trattamenti in obbligo di tale adempimento(1). Nella linea guida è indicato lo standard ISO/IEC 29134:2017.

Problematiche emerse & linea d'azione

E' stata predisposta una **procedura aziendale per predisporre tale analisi preventiva** nei casi previsti ma in alternativa può essere utilizzato un sw specifico sulla DPIA pubblicato dal Garante francese (CNIL) denominato **PIA** https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil (anche in italiano).
Gli outsourcer informatici, in qualche caso, hanno fornito le DPIA (che riguardano però sostanzialmente il rischio informatico) per le applicazioni/servizi che hanno ritenuto in obbligo di tale adempimento.

(1) https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9044761

Il software PIA del CNIL

Registro dei trattamenti

Sintesi adempimento & istruzioni Garante

Il Registro dei trattamenti è obbligatorio per aziende oltre(1) i 250 dipendenti e, a richiesta, deve essere reso disponibile al Garante. Specifica Titolare e DPO nonchè finalità (e base giuridica), categorie interessati/dati personali, categorie destinatari, se applicabile trasferimento di dati all'estero e garanzie adeguate per il trasferimento, termini per la cancellazione dei dati, descrizione misure di sicurezza del trattamento. Nella Guida GDPR il Garante invita comunque " *… tutti i titolari di trattamento e i responsabili, a prescindere dalle dimensioni dell'organizzazione, a compiere i passi necessari per dotarsi di tale registro …*". E' tenuto " *… in forma scritta, anche in formato elettronico …* " . Di recente il Garante ha pubblicato delle FAQ su questo aspetto (https://www.garanteprivacy.it/regolamentoue/registro)

Problematiche emerse & linea d'azione

I Registri dei trattamenti predisposti sia dagli outsourcer informatici sia dalle Capogruppo sono costituiti da **fogli excel molto complessi** che arrivano a contenere fino a 50 colonne.

Esistono prodotti, italiani e internazionali, di gestione del Registro dei trattamenti e di altri adempimenti privacy (suite)

Quali sono le modalità di conservazione e aggiornamento del Registro dei trattamenti ?

Il Garante precisa che «*Il Registro dei trattamenti è un documento di censimento e analisi dei trattamenti effettuati dal titolare o responsabile. In quanto tale, il registro deve essere mantenuto costantemente aggiornato poiché il suo contenuto deve sempre corrispondere all'effettività dei trattamenti posti in essere. Qualsiasi cambiamento, in particolare in ordine alle modalità, finalità, categorie di dati, categorie di interessati, deve essere immediatamente inserito nel Registro, dando conto delle modifiche sopravvenute*.

Il Registro può essere compilato sia in formato cartaceo che elettronico ***ma deve in ogni caso recare, in maniera verificabile, la data della sua prima istituzione (o la data della prima creazione di ogni singola scheda per tipologia di trattamento) unitamente a quella dell'ultimo aggiornamento.***

(1) 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 idati personali relativi a condanne penali e a reati di cui all'articolo 10.

Il modello di registro dei trattamenti del Garante (PMI)

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

SCHEDA REGISTRO DEI TRATTAMENTI *[per i contenuti vedi Faq sul registro delle attività di trattamento: https://www.garanteprivacy.it/regolamentoue/registro]*

TITOLARE/CONTITOLARE/RAPPRESENTANTE DEL TITOLARE *[inserire la denominazione e i dati di contatto]*

RESPONSABILE DELLA PROTEZIONE DEI DATI *[inserire la denominazione e i dati di contatto]*

TIPOLOGIA DI TRATTAMENTO	FINALITA' E BASI LEGALI DEL TRATTAMENTO	CATEGORIE DI INTERSSATI	CATEGORIE DI DATI PERSONALI	CATEGORIE DI DESTINATARI *[indicare eventuali responsabili del trattamento o altri titolari cui i dati siano comunicati]*	TRASFERIMENTO DATI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI *[indicare il Paese terzo o l'organizzazione internazionale cui i dati sono trasferiti e le "garanzie" adottate ai sensi del capo V del RGPD]*	TERMINI ULTIMI DI CANCELLAZIONE PREVISTI	MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE

Analisi dei rischi e misure di sicurezza

Sintesi adempimenti

Nel GDPR il Titolare del trattamento, tenuto conto di stato dell'arte e costi attuazione nonché natura, oggetto, contesto, finalità e rischio per i diritti/libertà delle persone fisiche, mette in atto misure tecniche/organizzative adeguate (che comprendono se del caso: pseudonimizzazione(1), cifratura, garanzia di riservatezza/integrità/disponibilità/resilienza, rispristino tempestivo disponibilità/accesso dati, procedura per testare/verificare/valutare regolarmente efficacia misure tecniche/organizzative) per garantire un livello di sicurezza adeguato ai rischi (che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati). Secondo il Garante « *… non potranno sussistere dopo il 25 maggio 2018 obblighi generalizzati di adozione di misure "minime" di sicurezza (ex art. 33 Codice) poiché tale valutazione sarà rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificamente individuati come da art. 32 del regolamento …* «

Problematiche emerse & linea d'azione

L'analisi del rischio è stata predisposta secondo le metodologie in uso nelle aziende Occorre verificare l'approccio prescelto per la predisposizione dell'analisi dei rischi tenendo conto degli standard utilizzabili. Di utilità appaiono gli standard ISO:

- ISO/IEC 29134 Privacy Impact Assessment
- ISO 29100 – 29101 Privacy Framework
- ISO 29151 Code of practice for Personally Identified Information protection
- ISO 27001/2 Information Security Management System
- ISO 31000:2009, Risk management — Principles and guidelines

nonchè "*Guidelines for SMEs on the security of personal data processing*" di ENISA (2) (dicembre 2016).
Inoltre a fronte della valutazione dei rischi, individuare le misure di sicurezza adeguate (quali la crittografia) anche in relazione alla probabilità di violazione (vedi punto successivo). **Sono in corso cantieri con outsourcer**.

(1) il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile

(2) (www.enisa.europa.eu)

Violazione dei dati personali

Sintesi adempimenti & linea guida

In caso di violazione(1) dei dati personali, e soltanto se si ritiene probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati, il Titolare la notifica entro 72 ore all'Autorità di controllo e, in caso di rischio elevato per i diritti/libertà, anche all'interessato. E' interessante segnalare che la comunicazione all'interessato può essere omessa se (in alternativa) il Titolare: ha messo in atto misure tecniche/organizzative adeguate (crittografia) , ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato, la comunicazione richiederebbe sforzi sproporzionati (ricorrendo in alternativa a comunicazione pubblica o misura simile). Tutti i titolari di trattamento 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. La violazione dei dati personali può provocare infatti danni fisici, materiali o immateriali alle persone fisiche e pertanto questo aspetto assume una grande rilevanza nel GDPR. Sono state emanate «Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679» (WP250)

Problematiche emerse & linea d'azione

Sono stati predisposti **protocolli di comunicazione con outsourcer (ticket), metodologie per valutare gravità della violazione, modelli di comunicazione al Garante/interessato, registro delle violazioni**.

(1) 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;

Trasferimento all'estero di dati personali

Sintesi adempimenti

Il trasferimento di dati all'estero è consentito in presenza di particolari condizioni ovvero deroghe a tali condizioni (tra cui il consenso dell'interessato informato dei rischi).

Come detto nella Guida del Garante *«In primo luogo, viene meno il requisito dell'autorizzazione nazionale (si vedano art. 45, paragrafo 1, e art. 46, paragrafo 2). Ciò significa che il trasferimento verso un Paese terzo "adeguato" ai sensi della decisione assunta in futuro dalla Commissione, ovvero sulla base di clausole contrattuali modello, debitamente adottate, o di norme vincolanti d'impresa approvate attraverso la specifica procedura di cui all'art. 47 del regolamento, potrà avere inizio senza attendere l'autorizzazione nazionale del Garante - a differenza di quanto attualmente previsto dall'art. 44 del Codice. Tuttavia, l'autorizzazione del Garante sarà ancora necessaria se un titolare desidera utilizzare clausole contrattuali ad-hoc (cioè non riconosciute come adeguate tramite decisione della Commissione europea) oppure accordi amministrativi stipulati tra autorità pubbliche – una delle novità introdotte dal regolamento.»*

Suggerimenti di azione

La possibilità di trasferire dati all'estero in Paesi non adeguati **è previsto nelle informative rese**. L'utilizzo delle clausole contrattuali tipo emanate dalla Commissione UE appare oggi la modalità più utilizzata in caso di trasferimenti all'estero in Paesi non adeguati dal punto di vista della normativa sulla protezione dei dati personali. Per gli Stati Uniti vige l'accordo denominato «Privacy Shield[1] » cui le aziende statunitensi posso aderire (https://www.privacyshield.gov/list) volontariamente.

(1) http://194.242.234.211/documents/10160/0/Privacy+shield.+Lo+Scudo+per+la+privacy+fra+Ue+e+USA+-+Infografica

Agenda

- Presentazione relatore
- GDPR nel settore bancario, finanziario ed assicurativo
- Bibliografia & sitografia
- Q&A

Agenda

- Presentazione relatore
- GDPR: lavori in corso
- **Bibliografia & sitografia**
- Q&A

Bibliografia

«Il Regolamento Privacy Europeo – Commentario alla nuova disciplina sulla protezione dei dati personali» di Luca Bolognini, Enrico Pelino, Camilla Bistolfi – Giuffrè Editore - 2016

«Privacy e il diritto europeo alla protezione dei dati personali – Il Regolamento europeo 2016/679 (volume secondo)» di Francesco Pizzetti - G. Giappichelli Editore – 2016

«Privacy e Regolamento europeo» di Antonio Ciccia Messina e Nicola Bernardi – Wolters Kluwer – 2016

«Il responsabile della protezione dei dati (Data Protection Officer-DPO)» di Stefano Comellini – Maggioli Editore – 2018

"Privacy by design – The 7 Foundamental Principles" di Ann Cavoukian , che è alla base della "Resolution on Privacy by design" adottata alla 32^ Conferenza internazionale dei Garanti privacy svoltasi a Gerusalemme nel 2010
https://edps.europa.eu/sites/edp/files/publication/10-10 27_jerusalem_resolutionon_privacybydesign_en.pdf

"Privacy and Data Protection by Design" pubblicato da ENISA e scaricabile gratuitamente da https://www.enisa.europa.eu/

Sitografia

Guida applicativa del Garante privacy (http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6302257)

Linee guida EDPB (ex WP29) (http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1360)

Download GDPR con considerando (https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6264597)

Download Codice Privacy novellato (https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9042678)

Download decreto armonizzazione d.lgs. 101/2018
http://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2018-09-04&atto.codiceRedazionale=18G00129&elenco30giorni=true

Agenda

- Presentazione relatore
- GDPR: lavori in corso
- Bibliografia & sitografia
- Q&A

Agenda

- Presentazione relatore
- GDPR: lavori in corso
- Bibliografia & sitografia
- **Q&A**

Q&A

Contatti

- cesare.desantis@primaedintorni.it

Grazie...

Portabilità dei dati (scheda Garante privacy)

Il diritto alla portabilità dei dati (art. 20 RGPD)

La scheda presenta gli elementi generali del diritto alla «portabilità dei dati» introdotto dal Regolamento (UE) 2016/679, entrato ufficialmente in vigore il 24 maggio 2016 e che sarà direttamente applicato in tutti gli Stati membri a partire dal 25 maggio 2018

COSA È?

È un diritto innovativo previsto dall'**articolo 20** del Regolamento che consente all'interessato di **ricevere** i dati personali forniti a un titolare, in **un formato strutturato, di uso comune e leggibile da dispositivo automatico,** e di **trasmetterli** ad un **altro titolare del trattamento senza impedimenti.**

QUALI VANTAGGI PUO' OFFRIRE?

- facilitare il **passaggio da un fornitore di servizi all'altro** fungendo, quindi, da fattore di promozione della concorrenza fra i singoli fornitori;
- consentire la **creazione di nuovi servizi** nel quadro della strategia per il mercato unico digitale;
- offrire la possibilità di **«riequilibrare» il rapporto fra interessati e titolari del trattamento** tramite l'affermazione dei diritti e del controllo spettanti agli interessati in rapporto ai dati personali che li riguardano.

COSA PERMETTE DI FARE?

- **ricevere dati personali** trattati da un titolare e **conservarli** su un supporto personale in vista di un utilizzo ulteriore per scopi personali, senza trasmetterli a un altro titolare *(ad es., recuperare l'elenco dei brani musicali preferiti detenuto da un servizio di musica in streaming, per scoprire quante volte si sono ascoltati determinati brani)*;
- **trasmettere dati personali da un titolare del trattamento a un altro titolare del trattamento** *(ad es., un diverso fornitore di servizi)*.

L'esercizio del diritto alla portabilità dei dati **non pregiudica** nessuno degli altri diritti dell'interessato che può, ad esempio,

- continuare a fruire del servizio offerto dal titolare anche dopo un'operazione di portabilità;
- esercitare il diritto di cancellazione.

QUANDO TROVA APPLICAZIONE?

Occorre siano soddisfatte **tre condizioni:**

1. i dati personali devono essere **trattati attraverso strumenti automatizzati** (quindi sono esclusi gli archivi cartacei), sulla base del **consenso preventivo dell'interessato** o per l'**esecuzione di un contratto** di cui è parte l'interessato;
2. i dati personali di cui si chiede la portabilità devono **riguardare l'interessato** ed essere quelli **forniti dall'interessato consapevolmente e in modo attivo** *(ad es., i dati di registrazione - indirizzo postale, nome utente, età, ecc.- inseriti compilando un modulo online)*. Sono compresi anche i dati **generati e raccolti** attraverso le **attività dell'utente** che fruisce di un servizio o utilizza un dispositivo.
   Il diritto alla portabilità **non** si applica invece ai dati personali che sono **derivati o dedotti** dalle informazioni **fornite dall'interessato** *(ad es., il profilo-utente creato analizzando i dati grezzi di un contatore intelligente)*, poiché non si tratta di dati forniti dall'interessato bensì creati dal titolare del trattamento.
3. l'esercizio del diritto alla portabilità **non deve ledere i diritti e le libertà altrui.** Ad es., se l'insieme dei dati trasferiti su richiesta dell'interessato contiene dati personali che riguardano altre persone fisiche, il nuovo titolare deve trattarli solo in presenza di un'idonea base giuridica.

La scheda ha un mero valore illustrativo ed è in continuo aggiornamento in base all'evoluzione delle indicazioni applicative del Regolamento.
Per un quadro completo si invita a consultare la pagina www.garanteprivacy.it/portabilita

Liceità del trattamento (art. 6) nel nuovo Regolamento

Il trattamento è lecito se ricorre una delle seguenti condizioni::

a) l'interessato ha manifestato il **consenso al trattamento** dei propri dati personali per una o più specifiche finalità;

b) il trattamento è necessario **all'esecuzione di un contratto** di cui l'interessato è parte o all'esecuzione di **misure precontrattuali** prese su richiesta dello stesso;

c) il trattamento è necessario per adempiere obbligo legale al quale è soggetto il Titolare;

d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di altra PF;

e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare;

f) il trattamento è necessario per il **perseguimento del legittimo interesse del Titolare** o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore. Ciò non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esercizio dei loro compiti.

Responsabile del trattamento: obblighi contrattuali (art.28) nel Regolamen

L'esecuzione dei trattamenti su commissione svolti da un Responsabile è disciplinato da **contratto/accordo** di diritto Ue/Stati membri contenente materia disciplinata, durata, natura, finalità del trattamento, tipo di dati e categorie di interessati e i diritti/obblighi del Titolare e che prevede che il Responsabile:

a) tratti i dati **solo su istruzione documentata del Titolare** incluso il trasferimento verso Paesi terzi/organizzazioni internazionali, a meno che non sia previsto dalla legge; in tal caso il Responsabile deve informare il Titolare a meno che la legge lo proibisca (interesse pubblico)

b) impieghi **solo personale che si sia impegnato alla riservatezza** (o ne abbia obbligo legale)

c) prenda tutte **le misure di sicurezza prescritte** (art. 32)

d) rispetti **le condizioni per il ricorso ad altri Responsabili**

e) tenendo conto natura trattamento **assista il Titolare**, con idonee misure tecniche/organizzative, a dare seguito a richieste di **esercizio diritti degli Interessati** (capo III)

f) **assista il Titolare** nel garantire il rispetto delle **misure di sicurezza** (art. da 32 a 36), tenendo conto natura trattamento e info a disposizione

g) a scelta del Titolare, **restituisca/cancelli i dati personali, previsti nel contratto, e cancelli le copie esistenti, al cessare della prestazione** di servizio salvo obblighi di legge

h) metta a disposizione le **informazioni idonee a dimostrare il rispetto degli obblighi del Regolamento** e **collabori con gli audit** , incluse le ispezioni, del Titolare, o di altro auditor inviato dal Titolare

i) **informi immediatamente il Titolare qualora a suo giudizio qualche istruzioni violi il Regolamento o altre disposizioni nazionali/UE**

Informazioni da fornire per raccolta presso interessato (art. 13)

- Informazioni che Titolare fornisce all'atto raccolta (**in caso di raccolta presso interessato**):
  - ✓ **identità/coordinate** contatto del **Titolare** e se designati **Rappresentante e Data Protection Officer (DPO)**
  - ✓ **finalità** trattamento per le quali sono destinati i dati nonché **le basi giuridiche** del trattamento
  - ✓ **il legittimo interesse** del Titolare o di terzi (art. 6 c. 1 f)
  - ✓ i **destinatari o le categorie di destinatari** dei dati personali
  - ✓ dove applicabile l'intenzione di **trasferire i dati in Paesi terzi** e l'esistenza/assenza di **decisioni adeguatezza** o in caso di altri tipi di trasferimenti (art. 46, 47 o 49 c. 2) le **garanzie** e i mezzi per ottenerne copia o dove sono state rese disponibili
- Inoltre occorre fornire
  - ✓ **periodo di conservazione** dei dati, o criterio usato per determinarlo
  - ✓ esistenza **diritto di richiedere accesso e rettificare/cancellare** dati o limitazioni di trattamento o opporsi trattamento di tali dati nonché **diritto alla portabilità** di essi
  - ✓ in caso di dati art. 6 c. 1a e art. 9 c. 2a l'esistenza **del diritto di revocare il consenso** in qualsiasi momento senza conseguenze su legittimità trattamento prima della revoca
  - ✓ **diritto a presentare reclamo** all'Autorità di controllo
  - ✓ se la comunicazione di dati è **requisito imposto da legge o contrattuale**, o necessario per stipula contratto nonché se interessato è obbligato a fornire i dati e conseguenze rifiuto
  - ✓ esistenza di **decisioni automatizzate, inclusa profilazione**, (art. 22 c.1 e c.4), e almeno in quei casi informazioni comprensibili intorno alla logica usata nonché importanza/conseguenze previste per interessato
- Se Titolare intende procedere a **ulteriori trattamenti** informa interessato prima di iniziarli dando informazioni su ulteriori finalità
- Quanto sopra **non si applica se l'Interessato ha già le informazioni**

Data Protection Officer (scheda Garante privacy)

Il Responsabile della protezione dei dati (RPD) o Data Protection Officer (DPO)

La scheda presenta la figura del Responsabile della protezione dei dati (RPD), o Data Protection Officer (DPO), in base a quanto previsto dal Regolamento (UE) 2016/679 e dalle Linee-guida del WP29

QUALI SONO I REQUISITI?

Il Responsabile della protezione dei dati, nominato dal titolare del trattamento o dal responsabile del trattamento, dovrà:

1. **possedere un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali**, anche in termini di misure tecniche e organizzative o di misure atte a garantire la sicurezza dei dati;
2. **adempiere alle sue funzioni in piena indipendenza e in assenza di conflitti di interesse** . In linea di principio, ciò significa che il RPD non può essere un soggetto che decide sulle finalità o sugli strumenti del trattamento di dati personali;
3. **operare alle dipendenze del titolare o del responsabile oppure sulla base di un contratto di servizio** (RPD/DPO esterno).

Il titolare o il responsabile del trattamento dovranno mettere a disposizione del Responsabile della protezione dei dati le risorse umane e finanziarie necessarie all'adempimento dei suoi compiti.

IN QUALI CASI E' PREVISTO?

Dovranno designare obbligatoriamente un RPD:

a) amministrazioni ed enti pubblici, fatta eccezione per le autorità giudiziarie;
b) tutti i soggetti la cui attività principale consiste in trattamenti che, per la loro natura, il loro oggetto o le loro finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
c) tutti i soggetti la cui attività principale consiste nel trattamento, su larga scala, di dati sensibili, relativi alla salute o alla vita sessuale, genetici, giudiziari e biometrici.

Anche per i casi in cui il regolamento non impone in modo specifico la designazione di un RPD, è comunque possibile una nomina su base volontaria.

Un gruppo di imprese o soggetti pubblici possono nominare un unico RPD.

QUALI SONO I COMPITI?

Il Responsabile della protezione dei dati dovrà, in particolare:

a) **sorvegliare l'osservanza del regolamento**, valutando i rischi di ogni trattamento alla luce della natura, dell'ambito di applicazione, del contesto e delle finalità;
b) collaborare con il titolare/responsabile, laddove necessario, nel condurre una **valutazione di impatto sulla protezione dei dati (DPIA);**
c) **informare e sensibilizzare** il titolare o il responsabile del trattamento, nonché i dipendenti di questi ultimi, riguardo agli obblighi derivanti dal regolamento e da altre disposizioni in materia di protezione dei dati;
d) **cooperare con il Garante e fungere da punto di contatto per il Garante** su ogni questione connessa al trattamento;
e) **supportare** il titolare o il responsabile in ogni attività connessa al trattamento di dati personali, anche con riguardo alla tenuta di un **registro delle attività di trattamento** .

Nomina DPO : indicazioni delle linee guida WP29

- **Conoscenze specialistiche**: il livello di conoscenza specialistica deve essere proporzionato alla sensibilità, complessità e quantità dei dati sottoposti a trattamento
- **Qualità professionali**: riguarda la conoscenza da parte del DPO della normativa e delle prassi nazionali ed europee in materia di protezione dei dati e un'approfondita conoscenza del GDPR. Proficua anche la promozione di una formazione adeguata e continua rivolta ai DPO da parte delle Autorità di controllo E' utile la conoscenza dello specifico settore di attività e della struttura organizzativa del titolare; inoltre, il DPO dovrebbe avere sufficiente familiarità con le operazioni di trattamento svolte nonché con i sistemi informativi ed esigenze di sicurezza e protezione dati manifestate dal titolare
- **Capacità di assolvere ai propri compiti**: si deve intendere sia quanto è legato alle qualità personali e alle conoscenze del DPO, sia quanto dipende dalla posizione del RPD all'interno dell'azienda. Le qualità personali dovrebbero comprendere, per esempio, l'integrità ed elevati standard deontologici
- **Conflitti di interesse**: L'assenza di conflitti di interessi è strettamente connessa agli obblighi di indipendenza. Anche se un RPD può svolgere altre funzioni, l'affidamento di tali ulteriori compiti e funzioni è possibile solo a condizione che essi non diano adito a conflitti di interessi. Ciò significa, in modo particolare, che un RPD non può rivestire, all'interno dell'organizzazione del titolare o del responsabile, un ruolo che comporti la definizione delle finalità o modalità del trattamento di dati personali. A grandi linee, possono sussistere situazioni di conflitto all'interno dell'organizzazione del titolare o del responsabile riguardo a ruoli manageriali di vertice (amministratore delegato, responsabile operativo, responsabile finanziario, responsabile sanitario, direzione marketing, direzione risorse umane, responsabile IT), ma anche rispetto a posizioni gerarchicamente inferiori se queste ultime comportano la determinazione di finalità o mezzi del trattamento.

Meccanismo dello «sportello unico»

Adempimenti

Nel GDPR è previsto un maggior coordinamento tra Autorità di controllo con il meccanismo dello sportello unico/Autorità capofila. Infatti nei casi transfrontalieri importanti in cui sono coinvolte diverse autorità di controllo nazionali, si adotterà una decisione di controllo unica. In base a questo principio, noto appunto come »sportello unico», una società con controllate in diversi Stati membri dovrà interagire solo con l'Autorità preposta alla protezione dei dati nello Stato membro in cui ha lo stabilimento principale (Autorità di controllo capofila), o il centro decisionale sui trattamenti, che collaborerà con le altre Autorità di controllo interessate. E' prevista altresì la creazione del Comitato Europeo per la Protezione dei Dati (ex WP29), con i rappresentanti di tutti i Garanti UE, EDPS e Commissione UE. Su tali aspetti è stata emanata una linea guida(1) .

(1) Linee-guida per l'individuazione dell'autorità di controllo capofila in rapporto a uno specifico titolare o responsabile del trattamento (*http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6386159*)

Violazione dati personali nel Regolamento: notificazione ad Autorità (art. 33)

- In caso di **violazione dei dati personali**, il **Titolare**, senza ritardo ingiustificato, e dove possibile, **non più tardi di 72 ore** dopo averne preso atto notifica la violazione all'Autorità di controllo competente (art. 55), **a meno sia improbabile che comporti un rischio per diritti/libertà delle persone fisiche**
- Qualora non sia effettuata entro 72 ore, la notifica è corredata di una **giustificazione motivata**.
- **Responsabile deve informare il Titolare** senza ritardo ingiustificato dopo avere preso atto della violazione
- La notifica contiene almeno:
  a) descrizione della **natura della violazione** includendo se possibile le categorie e **il numero approssimativo dei soggetti interessati** nonché categorie e **numero approssimativo di registrazioni di dati** relativi alla violazione
  b) i **riferimenti DPO** o altro punto di contatto ove ottenere informazioni
  c) descrizione **conseguenze probabili della violazione**
  d) la **descrizione misure adottate o di cui si propone l'adozione** da parte del Titolare per porre rimedio alla violazione incluso dove possibile di attenuare i possibili effetti negativi
- Ove e nella misura in cui non sia possibile fornire le informazioni nello stesso momento esse possono essere **fornite in diverse fasi** senza ulteriore ingiustificato ritardo
- Il Titolare **documenta ogni violazione di dati personali incluse le circostanze, le conseguenze, le misure di rimedio prese**. Tale documentazione deve essere resa disponibile all'Autorità di controllo per consentire la verifica del rispetto del Regolamento

Violazione dati personali nel Regolamento: comunicazione a Interessato

- In caso di violazione dei dati personali suscettibile di presentare un **rischio elevato** per diritti/libertà delle persone fisiche, **il Titolare deve comunicare violazione all'Interessato** senza ingiustificato ritardo
- **La comunicazione descrive con un linguaggio semplice e chiaro la natura della violazione di dati personali e contiene almeno i punti b), c) e d) della slide precedente**
- La comunicazione non è richiesta se:
  - **a) Il Titolare aveva adottato opportune misure tecniche/organizzative di protezione** e tali misure erano state applicate ai dati oggetto di violazione in particolare quelle destinate a rendere i dati incomprensibili (cifratura) a chiunque non sia autorizzato ad accedervi , o
  - **b) Il Titolare ha adottato successivamente misure atte a scongiurare il sopraggiungere di un rischio elevato** per diritti/libertà degli interessati, o
  - c) Implica **un impegno sproporzionato** (es. per l'alto numero dei soggetti interessati) e si procede per comunicazioni pubbliche o misure similari tali da assicurare una efficace comunicazione a detti soggetti
- Se il Titolare non ha effettuato la comunicazione all'interessato, **l'Autorità di controllo**, considerando la probabilità della violazione di comportare un alto rischio**, può richiedere che vi provveda** o può decidere che una delle condizioni sopra descritte sia soddisfatta

Registro attività di trattamento per Titolare (art. 30) nel Regolamento

- Ogni Titolare, e suo Rappresentante, tengono un **registro delle attività di trattamento** sotto la propria responsabilità che contenga:
  a) nome e **coordinate contatto del Titolare e di ogni Contitolare, del Rappresentante,** del Responsabile e eventualmente **del DPO**
  b) finalità del trattamento
  c) categorie di interessati e di dati personali
  d) destinatari/categorie di destinatari a cui dati sono stati/saranno comunicati in particolare in **Paesi terzi**
  e) dove applicabile, **trasferimenti di dati verso Paesi terzi/organizzazioni internazionali**, incluso la loro identificazione e la documentazione di garanzie adeguate in caso art. 49 c. 2
  f) termini ultimi per cancellare diverse categorie di dati, ove possibile
  g) descrizione generale delle misure di sicurezza (tecniche/organizzative) di cui art. 32 c. 1
- I registri sono tenuti in **forma scritta, anche in formato elettronico** e a richiesta sono messi a disposizione dell'Autorità di controllo
- Gli obblighi suddetti **non si applicano a imprese o organismi con meno di 250 dipendenti** a meno di rischi elevati per diritti/libertà interessato, o il trattamento è non occasionale o il trattamento include speciali categorie di dati (art. 9 c. 1) o trattamento dati di condanne penali o reati (art. 10)

Profilazione

Adempimenti

- Nel GDPR viene data una specifica attenzione al trattamento di profilazione(1) dell'esistenza del quale e delle sue conseguenze l'interessato deve essere informato, e i dati derivanti da essa possono essere utilizzati per assumere decisioni sotto specifiche condizioni, tra le quali figurano la necessità di concludere/eseguire un contratto o il consenso esplicito dell'interessato. L'interessato a diritto di opporsi anche quando essa sia connessa al direct marketing ed a un processo decisionale automatizzato. Può essere necessaria una preventiva DPIA (vedi il punto «Valutazione d'impatto sulla protezione dei dati»)

(1) « *qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica* «

Legittimo interesse & direct marketing

GDPR/1: Legittimo interesse & direct marketing → Vi segnalo sul tema del legittimo interesse da applicarsi al *direct marketing* un articolo da cui sono tratti i brani che seguono [" … *L'interesse legittimo può quindi secondo il WP29 costituire un fondamento giuridico adeguato da utilizzare per alcuni tipi di attività di marketing, sia online che offline, purché sussistano adeguate garanzie (compreso, fra l'altro, un meccanismo efficace che permetta di opporsi a tale trattamento)* ***Il punto è: fino a dove può spingersi l'interesse legittimo del titolare nel conoscere le preferenze dei suoi clienti per poter meglio indirizzare la pubblicità sui propri beni e servizi o personalizzare le proprie offerte creando beni e servizi che meglio soddisfano le loro necessità?*** *Quali sono invece le pratiche di marketing più sofisticate e intrusive che richiedono uno specifico consenso degli interessati ai sensi dell'art. 6.1, (a) of the GDPR ? …*] un articolo degli avvocati Francesca Lonardo e Gabriele Faggioli (CEO della società P4I ed esperto molto noto in tema di privacy), precisandovi che "… *P4I-Partner4Innovation ha* ***chiesto proprio al WP29, partecipando alla consultazione pubblica da quest'ultimo indetta sulle recenti Linee Guida sulla trasparenza e il consenso, di esprimersi chiaramente – in attesa e in vista dell'approvazione del Regolamento ePrivacy – sui casi in cui il Titolare può ricorrere, per effettuare attività di marketing, all'interesse legittimo****, comunque soggetto al test di bilanciamento di interessi, esemplificando le ipotesi di marketing più invasive che richiedono invece il consenso degli interessati."* https://www.zerounoweb.it/techtarget/searchsecurity/gdpr-informativa-e-consenso/

I trasferimenti di dati all'estero: principio generale e garanzie (art. 44/45/46/47)

Il **trasferimento di dati personali** oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento **verso un paese terzo o un'organizzazione internazionale**, compreso il trasferimento successivo di dati personali da un paese terzo o un'organizzazione internazionale verso un altro paese terzo o un'altra organizzazione internazionale**, è ammesso soltanto** se il Titolare/Responsabile, fatte salve le altre disposizioni, rispettano le seguenti condizioni:

- Conformità alle **decisioni di adeguatezza** della Commissione UE
- Adozione di garanzie adeguate quali:
  - **strumento vincolante** giuridicamente tra Autorità/Enti pubblici
  - **norme vincolanti d'impresa** (art. 47), approvate dall'Autorità di controllo competente
  - **clausole tipo** di protezione dei dati adottate **dalla Commissione UE** (art 93)
  - **clausole tipo** di protezione dei dati adottate da **Autorità di controllo** e approvate dalla Commissione UE (art . 93)
  - un **codice di condotta approvato** (art. 40) insieme a un impegno vincolante ed esecutivo da parte Titolare/Responsabile ad applicare opportune garanzie comprese quelle relative a diritti interessati
  - un **meccanismo di certificazione approvato** (art. 42) insieme a un impegno vincolante ed esecutivo da parte Titolare/Responsabile ad applicare opportune garanzie comprese quelle relative a diritti interessati
- Salvo l'autorizzazione dell'Autorità di controllo competente possono costituire garanzie adeguate:
  - **Clausole contrattuali** tra Titolare/Responsabile e Titolare/Responsabile/Destinatario in paese terzo;
  - Disposizioni in **accordi amministrativi tra autorità pubbliche con diritti effettivi/azionabili** degli Interessati

I trasferimenti di dati all'estero: validità sentenze e deroghe (art. 48, 49 e 50)

- **Nessuna sentenza** di una corte o tribunale, né alcuna decisione presa da un'autorità amministrativa di un Paese terzo che disponga trasferimento/comunicazione, da parte di Titolare/Responsabile**, è riconosciuta o assume in alcun modo un carattere esecutivo**, fatti salvi trattati di mutua assistenza legale ovvero accordi internazionali in vigore tra il Paese terzo richiedente e UE o un suo Stato membro.
- In assenza di condizioni di cui alla slide precedente il trasferimento può avvenire solo a condizione:
  - **consenso dell'interessato** dopo adeguata informazione sui rischi
  - trasferimento **è necessario per la conclusione di un contratto** tra interessato e Titolare o per l'esecuzione di misure pre-contrattuali prese su istanza dell'interessato
  - trasferimento **è necessario per la conclusione di un contratto tra Titolare e un'altra PF/giuridica** a favore dell'interessato
  - trasferimento **è necessario per importanti motivi di interesse pubblico**
  - trasferimento **è necessario per accertare, esercitare o difendere un diritto** in sede giudiziaria
  - trasferimento **è necessario per salvaguardare un interesse vitale** dell'interessato o di altre persone, qualora l'interessato si trovi nell'incapacità fisica/giuridica di dare il consenso
  - trasferimento **è effettuato a partire da un registro** che, a norma diritto UE/Stato membro, mira a fornire informazioni al pubblico e **può essere consultato dal pubblico** o da chiunque in possesso di legittimo interesse (purché sussistano requisiti per consultazione previsti dalla legge)
  - per trasferimenti, **non su larga scala né frequenti, necessari per il perseguimento di legittimi interessi cogenti** del Titolare su cui non prevalgano interessi/diritti interessato e il Titolare abbia offerto adeguate garanzie (il Titolare informa l'Autorità di controllo e l'interessato, quest'ultimo anche dei legittimi interessi)
- La Commissione e le Autorità di controllo adottano misure appropriate per:
  - sviluppo cooperazione internazionale per applicazione legislazione protezione dati, per assistenza reciproca su protezione dati (notificazione/deferimento reclami, assistenza indagini, scambio info), coinvolgimento parti interessate su promozione cooperazione internazionale, per promuovere scambio/documentazione di legislazione/pratiche protezione dati e conflitti giurisdizione)

Problematica del Responsabile interno del trattamento

Francesco Pizzetti
Professor of Constitutional Law, Turin University. Former President of the Italian D...
2m

Attenzione.Dopo 25 maggio 2018 si potrà (e dovrà) indicare esistenza di un responsabile dei trattamenti distinto dal titolare ex GDPR solo se esso è esterno alla impresa del titolare, e legato al titolare da contratto o altro atto giuridico vincolante per entrambi che definisca le rispettive responsabilita'.
La figura di responsabile interno non è compatibile con art.28 GDPR e non solleva il titolare da alcuna responsabilità né assume alcuna responsabilità se non quella proprie di un dipendente verso il suo datore di lavoro.
Dal 25 maggio chiunque induca un titolare a credere di poter dividere le sue responsabilità di Controller con un suo dipendente solo perché gli assegna una responsabilità interne di qualunque tipo rispetto a trattamenti che restano tutti imputati al titolare assume una grave responsabilità professionale.Il Processor/Responsabile ai sensi GDPR deve essere sempre esterno e legato a titolare da contratto o atto giuridico vincolante per entrambi.
Continuare, volutamente o no, a fare confusione e' pericolosissimo e può provocare gravi rischi e possibili sanzioni e danni ai titolari

Consigliato 221 volte · 43 commenti

5. Responsabile interno / esterno. Nella prassi applicativa italiana si distingue tra responsabile interno ed esterno, a seconda che l'individuazione avvenga tra dipendenti e collaboratori del titolare oppure riguardi un soggetto terzo. Ugualmente, possono essere responsabili interni uffici e altre ripartizioni strutturali del titolare, ove non assumano i connotati di una vera e propria titolarità. Ebbene, ci si può domandare se la figura del responsabile interno sia compatibile con il Regolamento. Ancorché gli elementi di analisi a questo proposito siano scarsi, chi scrive propende per la soluzione negativa, che peraltro ha il pregio di una maggiore linearità concettuale: i ruoli subalterni interni sono quelli del per-

Citazione tratta da «Il Regolamento privacy Europeo – Commentario alla nuova disciplina sulla protezione dei dati personali» in bibliografia

I rischi per l'interessato

I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, **furto o usurpazione d'identità**, **perdite finanziarie**, **pregiudizio alla reputazione**, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.