ISACA®

Sistemi informativi: averne fiducia e trarne valore

Rome Chapter

GDPR: lavori in corso

Cesare De Santis

Roma 27/0372018

Agenda

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

Agenda

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

Agenda

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

Evoluzione normativa

OLD

- Dal 1 gennaio 2004 la protezione dei dati personali è disciplinata in Italia dal d.lgs. 196/2003 denominato «Codice in materia di protezione dei dati personali» (conosciuto anche come Codice privacy) , approvato il 27 giugno 2003 dal Consiglio dei ministri, in Gazzetta Ufficiale n.123/L del 29 luglio 2003 e che ha abrogato la legge 675/1996 ed alcuni decreti successivi, nonchè dai suoi allegati (Disciplinare tecnico in materia di misure minime di sicurezza e codici deontologici, tra i quali quello sui S.I.C.)
- Negli ultimi anni sono state introdotte alcune importanti “semplificazioni” negli adempimenti previsti dalla normativa italiana sulla protezione dei dati personali quali l’esclusione dei dati delle persone giuridiche, Enti e associazioni e l’eliminazione dell’obbligo di tenuta di un aggiornato Documento programmatico sulla sicurezza;

NEW

- Nel 2012 la Commissione europea ha presentato una riforma della protezione dei dati nell'UE per adeguare l'Europa all'era digitale.
- La riforma si compone di due strumenti:
  - ✓ il **regolamento generale sulla protezione dei dati** (acronimo inglese GDPR)
  - ✓ la direttiva sulla protezione dei dati trattati dalla polizia e dalle autorità giudiziarie penali
- Il 15 dicembre 2015 è stato raggiunto l'accordo tra Commissione, Parlamento e Consiglio UE dopo i negoziati finali tra le tre istituzioni (cosiddette riunioni di "trilogo").
- Il Regolamento(1) è stato approvato in via definitiva e pubblicato nella G.U. della UE n. L 119/1 del 4 maggio 2016
- E’ entrato in vigore il 25 maggio 2016 e **sarà applicato a partire dal 25 maggio 2018**
- Il governo ha avuto la delega **(**legge 25 ottobre 2017, n. 163) per attuazione GDPR ed ha approvato il 21 marzo 2018 un decreto legislativo di attuazione dell’art. 13 di tale legge

(1) Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE (regolamento generale sulla protezione dei dati)

Cosa cambia rispetto alla attuale normativa: sintesi (1/2)

- Unica normativa in UE - con l'obiettivo di rafforzare il mercato unico digitale - che si applica ai trattamenti (1) (interamente o parzialmente automatizzati nonché non automatizzati) di dati personali(2) relativi a **persone fisiche**(3), con esclusione dei **deceduti** (vedi considerando 27) che si trovano nella UE, effettuati da titolari e responsabili del trattamento stabiliti nella UE ma anche fuori UE, quando i trattamenti riguardano offerta di beni e servizi e monitoraggio di comportamenti nella UE. Esclusi i trattamenti svolti per attività a carattere personale e domestico.
- La notificazione del trattamento viene abolita.
- Confermate le figure del Contitolare del trattamento e del Rappresentante, per Titolare/Responsabile non UE
- Attenzione alla definizione delle responsabilità (anche in solido con rivalsa) per soggetti che trattano i dati e delle possibilità di **ricorso/risarcimento** previste per l'interessato
- Inasprimento delle sanzioni di tipo amministrativo (**fino a 20 mln di euro e al 4% del fatturato mondiale totale dell'azienda, se superiore**)
- Il Garante privacy ha pubblicato sul proprio sito una «*Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali*» che sarà continuamente aggiornata
- Il GdL dei Garanti europei (WP29), che costituirà lo *European Data Protection Board* , pubblica linee guida sulla nuova normativa europea

(1) Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

(2) Qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale

(3) « … *Il presente regolamento non disciplina il trattamento dei dati personali relativi a persone giuridiche, in particolare imprese dotate di personalità giuridica, compresi il nome e la forma della persona giuridica e i suoi dati di contatto* … « (considerando 14)

Cosa cambia rispetto alla attuale normativa: sintesi (2/2)

I principali adempimenti previsti dal GDPR riguardano:

- **Principi della disciplina**
- **Particolari categorie di dati e dati relativi a condanne penali, reati e connesse misure**
- **Responsabilizzazione (accountability) del Titolare del trattamento**
- **Responsabile del trattamento**
- **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**
- **Sanzioni**

Principi della disciplina

Adempimenti

- Sono confermati i principi (1) che riguardano i requisiti dei dati: principi di **liceità**; correttezza e trasparenza; limitazione delle finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; sicurezza, integrità e riservatezza
- Tra le condizioni di liceità viene però ad assumere particolare importanza il «legittimo interesse» del Titolare del trattamento o del terzo, che deve prevalere sui diritti e le libertà fondamentali dell'interessato per costituire un valido fondamento di liceità (nella Guida del Garante sono indicati i provvedimenti in materia di biometria, videosorveglianza e utilizzo di sistemi di rilevazione informatica anti-frode come riferimento per i principi da applicare nel «bilanciamento di interessi»):

  *« … In ogni caso, l'esistenza di legittimi interessi richiede **un'attenta valutazione** (2) anche in merito all'eventualità che l'interessato, al momento e nell'ambito della raccolta dei dati personali, **possa ragionevolmente attendersi** che abbia luogo un trattamento a tal fine … Può essere considerato legittimo interesse trattare dati personali per finalità di **marketing diretto** …» (considerando 47)*

Suggerimenti di azione

Oltre a verificare il rispetto dei principi, con particolare riguardo alla minimizzazione e conservazione dei dati (da indicare anche in informativa e nel registro dei trattamenti), occorre valutare la possibilità di utilizzare il legittimo interesse (vedi anche il successivo punto «Consenso») ad es. per le azioni di marketing diretto da parte del Titolare del trattamento (sul punto vedi questo articolo)

(1) Per il principio di responsabilizzazione vedi il successivo punto «Responsabilizzazione del Titolare»
(2) Documento di utilità : Parere 6/2014 del WP29 sul concetto di interesse legittimo (test comparativo)
http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3815154

Particolari categorie dati e dati relativi a condanne/reati

Adempimenti

In presenza della regola generale di divieto, il trattamento di particolari categorie di dati (essenzialmente i già noti «dati sensibili» con l'aggiunta di dati genetici, biometrici per identificazione univoca di una persona nonché orientamento sessuale) è consentito con il consenso esplicito dell'interessato (a meno di impedimenti di legge) o in virtù di specifiche deroghe (quali ad esempio il caso di dati resi manifestatamente pubblici). I trattamento di dati personali relativi a condanne penali, reati e connesse misure di sicurezza deve avvenire sotto il controllo dell'Autorità pubblica o se autorizzato da diritto UE/Stati membri, con apposite garanzie.

Suggerimenti di azione

Confermata la necessità del consenso (vedi anche successivo punto sul «Consenso») già raccolto dalle Banche (per prodotti di banca assicurazione, pagamenti per prestazioni sanitarie) occorrerà attendere eventuali pronunciamenti del Garante in relazione al mantenimento dell'attuale meccanismo basato sulle Autorizzazioni generali(2). I dati relativi a condanne penali, reati e misure accessorie (oggi inquadrati nei c.d. dati «giudiziari») sono trattati in obbligo di legge. Importante verifica da fare nella predisposizione del Registro dei trattamenti (vedi punto successivo).

(1) Già presente nel modulo di consenso della clientela e dei dipendenti e, per i dati biometrici, nel modulo FEA (firma grafometrica)
(2) In relazione a tali autorizzazioni generali appare peraltro opportuno formalizzare le verifiche di indispensabilità dei dati sensibili e giudiziari trattati nelle U.O. deputate a tali trattamenti.

Responsabilizzazione (accountability) del Titolare

Adempimenti

La figura del Titolare(1) del trattamento, che determina le finalità e i mezzi per il trattamento, è prevista anche nel GDPR . E' di particolare importanza sottolineare che il Titolare deve garantire attraverso adeguate misure - che possono comprendere l'attuazione di politiche adeguate - riesaminate e aggiornate qualora necessario, 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 (2) Il Garante sta valutando i codici deontologici attualmente vigenti per alcune tipologie di trattamento (es. codice deontologico SIC) nell'ottica dei requisiti fissati nel GDPR. Sulla certificazione c'è stato un comunicato congiunto Accredia/Garante(3) . In ogni caso, anche il Gruppo WP29 sta lavorando sui temi ed emanerà una linea guida.

Suggerimenti di azione

Il Titolare emana una policy nella quale promuove i principi della protezione dei dati personali, che sarà attuata tramite specifiche norme operative (Regolamento privacy). Al termine dell'adeguamento del sistema di gestione della privacy, il Titolare 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) E' stata emanato una norma UNI sulla figura del DPO
(3) http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6621723

Responsabile del trattamento

Adempimenti

La figura del Responsabile del trattamento, che tratta i dati personali per conto del Titolare del trattamento, è prevista anche nel Regolamento UE. 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 (quali certificazioni e adesione a codici di condotta) a mettere in atto misure che soddisfino i requisiti del Regolamento UE e garantisca la tutela dei diritti degli interessati. Per quanto riguarda la compatibilità della figura di Responsabile del trattamento interno all'azienda con il GDPR, essa è negata da alcuni esperti (1) della materia. Il Garante privacy nella sua Guida indica che "*I titolari di trattamento dovrebbero verificare che i contratti o altri atti giuridici che attualmente disciplinano i rapporti con i rispettivi responsabili siano conformi a quanto previsto … La Commissione e le autorità nazionali di controllo stanno valutando la definizione di clausole contrattuali modello da utilizzare a questo scopo*". L'art. 29 del Codice privacy è stato di recente modificato (2) (Responsabili esterni, nomine tipo da Garante)

Suggerimenti di azione

Appare necessario un censimento dei fornitori/outsourcer e una verifica dei requisiti di conformità dei contratti esistenti per la presenza delle clausole prescritte (art. 28 GDPR) tra le quali figura l'obbligo di "*garantire che le persone autorizzate al trattamento si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza*". In caso di firma di nuovi contratti, la cui durata superi la data di applicazione del GDPR, è opportuno, fin d'ora, utilizzare un facsimile di nomina quale Responsabile del trattamento dell'outsourcer che tenga conto del GDPR.

(1) *« … Ebbene ci si può domandare se la figura del responsabile interno sia compatibile con il Regolamento. Ancorchè gli elementi di analisi a questo proposito siano scarsi chi scrive propende per la soluzione negativa … «* (vedi «Il Regolamento privacy europeo – Commentario alla nuova disciplina sulla protezione dei dati personali» di L. Bolognini, E.Pelino, C. Bistolfi – Giuffrè Editore 2016 – pag. 148)

(2) *Legge 20 novembre 2017 n. 167*

Persone autorizzate (incaricati) al trattamento

Adempimenti

- 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 Responsabile del trattamento garantische che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza
- 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 …"*

Suggerimenti di azione

- E' necessario pianificare la formazione sulle nuove regole di trattamento per tutto il personale. Inoltre appare opportuna una verifica (1) (aggiornamento) delle normative richiamate nelle nomine degli incaricati in relazione agli ambiti di trattamento consentiti. Da tenere in considerazione il fatto che le persone autorizzate (incaricati) presso i Responsabili del trattamento devono essere formate e devono firmare impegno alla riservatezza (nel contratto bancari art. 38 c. 2 prevede segreto d'ufficio)

(1) Lo schema di nomina che utilizza la «documentata preposizione della persona fisica a una unità per la quale è individuato, per iscritto, l'ambito di trattamento consentito agli addetti dell'unità medesima» (art. 30 comma 2 del Codice privacy attuale), secondo la «Guida alla privacy nel rapporto di lavoro» di P.Borghi e G. Mieli – Bancaria editrice 2005, pag 83, «*soddisfa la previsione normativa, a patto che nell'ambito dell'azienda sia stato realizzato e risulti comprovabile il censimento dei vari trattamenti svolti dalle singole unità organizzative*».

Responsabile della protezione dei dati (DPO): generalità

Adempimenti

E' introdotta la nuova figura del **Responsabile della protezione dei dati** , meglio nota come DPO(1) obbligatori oltre che per gli Enti pubblici anche nel caso in cui le attività principali del titolare consistono nel monitoraggio regolare e sistematico degli interessati su larga scala(2) . E' una figura di garanzia che « *… dovrebbe perseguire in via primaria l'osservanza delle disposizioni del GDPR …*» e che secondo il Garante privacy « *… riflette l'approccio responsabilizzante che è proprio del regolamento (si veda art. 39), essendo finalizzata a facilitare l'attuazione del regolamento da parte del titolare/del responsabile …*». Secondo le linee guida WP29, oltre a dare pareri sulla DPIA, « *… contribuisce a dare attuazione a elementi essenziali del regolamento quali i principi fondamentali del trattamenti, i diritti degli interessati, la protezione dei dati sin dalla fase di progettazione e per impostazione predefinita, i registri delle attività di trattamento, la sicurezza dei trattamenti e la notifica e comunicazione delle violazioni di dati personali. «*

Suggerimenti di azione

Occorre individuare il soggetto secondo le indicazioni delle linee guida (3) del WP29 con attenzione alle conoscenze specialistiche, qualità professionali, capacità di assolvere i propri compiti, conflitti di interesse.

(1) Data Protection Officer

(2) Esempio di trattamenti su larga scala (dalle Linee guida del WP29):

«***trattamento di dati relativi alla clientela da parte*** *di una compagnia assicurativa o* ***di una banca nell'ambito delle ordinarie attività***»

(3) http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/5930287

Responsabile della protezione dei dati (DPO): nomina

Riferimenti operativi

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.

La individuazione del soggetto interno da nominare dovrebbe essere effettuata in maniera precoce rispetto alla data di applicazione del GDPR. Infatti le sue conoscenze di base andranno integrate con specifiche azioni formative mentre una certificazione delle competenze possedute/acquisite appare altresì opportuna. La nomina effettiva è auspicabile al completamento di tale processo di adeguamento.

Quanto sopra ha un riflesso, in questa fase di avvio della nuova normativa, sulla predisposizione della DPIA (vedi avanti), per i trattamenti che ne hanno necessità, sulla quale il Titolare del trattamento può chiedere un parere al DPO (art. 35/39 del GDPR).

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

Informativa ai soggetti interessati

Adempimenti

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 agli attuali, 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.
Il WP29 ha emanato una linea guida sulla trasparenza.

Suggerimenti di 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' 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) . Le informative è opportuno contengano le icone (art. 12 comma 7 GDPR) standardizzate che saranno messe a disposizione dalla Commissione UE.

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

Consenso al trattamento

Adempimenti

Il consenso è un adempimento previsto dal GDPR che lo definisce 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 l'introduzione del c.d. legittimo interesse(1) del Titolare tra le condizioni di liceità del trattamento, alternative al consenso, 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 è valido a partire dai 16 anni; prima 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. WP29 ha emanato linea guida su consenso.

Suggerimenti di azione

In parallelo all'adeguamento dei testi delle informative occorrerà predisporre le coerenti articolazioni dei consensi prendendo in considerazione le decisioni relative alle condizioni di liceità del trattamento (legittimo interesse e obblighi contrattuali), la presenza di trattamenti suscettibili di particolari rischi (profilazione), l'utilizzo di particolari categorie di dati (ex dati sensibili).
Punto di attenzione: eventuale necessità adeguamento procedura gestione consensi
Per il pregresso occorre valutare le modalità di raccolta del consenso per stabilire la validità dei vecchi consensi. Punto di attenzione: consensi raccolti in particolari situazioni (es. su Internet, in occasione di campagne promozionali ovvero nel corso manifestazioni estemporanee quali fiere, mostre, convegni)

(1) Nella legge di bilancio 2018 (art. 1 commi da 1020 a 1025, vedi allegato), nell'ambito dell'adeguamento dell'ordinamento interno al regolamento (UE) 2016/679, al Garante vengo assegnati compiti di tutela dei diritti degli interessati in relazione all'utilizzo da parte dei titolari (informativa al Garante) del legittimo interesse in particolare con uso nuove tecnologie.

Diritti dell'interessato

Adempimenti

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 su portabilità e decisione completamente automatizzata (cui l'interessato ha diritto di opporsi)

Suggerimenti di azione

Occorre rivedere la procedura 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' opportuno definire un perimetro dei dati interessati alla portabilità

(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 "*

Privacy by design e by default

Adempimenti

"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* …»

Suggerimenti di azione

Occorre predisporre delle procedure aziendali 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 (tenendo conto di tipologie di interessati, e numerosità di essi, e di 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 cui alla linea guida WP29 su DPIA .

Valutazione d'impatto sulla protezione dati

Adempimenti

La valutazione dell'impatto delle operazioni di trattamento previste sulla protezione dei dati personali (DPIA) si rende necessaria se un tipo di trattamento, in particolare per l'uso di nuove tecnologie (ad es. app su mobile) e tenendo conto di natura, oggetto, contesto e finalità può produrre alti rischi per diritti e le libertà fondamentali dell'interessato, con particolare riguardo al trattamento di particolari categorie di dati e alla valutazione sistematica e globale degli aspetti personali relativi ad un interessato con significative conseguenze (es. giuridiche) e che sia fondata unicamente su un trattamento automatizzato, compresa la profilazione. Secondo il Garante « *… tali impatti dovranno essere analizzati attraverso un apposito processo di valutazione (si vedano artt. 35-36) tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare per mitigare tali rischi. All'esito di questa valutazione di impatto il titolare potrà decidere in autonomia se iniziare il trattamento (avendo adottato le misure idonee a mitigare sufficientemente il rischio) ovvero consultare l'autorità di controllo competente per ottenere indicazioni su come gestire il rischio residuale … « .* Il WP29 (1) ha pubblicato una linea guida nella quale viene indicato come esempio di trattamento da sottoporre a DPIA: « *… An example of this is where a bank screens its customers against a credit reference database in order to decide whether to offer them a loan …*" e sono specificati i criteri per una DPA accettabile . In tale linea guida sono indicate 9 circostanze che rendono obbligatoria la DPIA che dovrebbero essere alla base dell'elenco nazionale delle tipologie di trattamenti in obbligo di tale adempimento. Nella linea guida è indicato lo standard ISO/IEC 29134:2017.

Suggerimenti di azione

Occorre individuare una procedura aziendale per predisporre tale analisi preventiva nei casi previsti (dopo la nomina si può richiedere un parere su di essa al DPO) con particolare attenzione all'analisi dei rischi e tenendo presente che nelle linee guida WP29 sono date indicazioni su framework, cui si potrebbe fare riferimento, predisposti da altri Garanti privacy (DE,ES,FR,UK). Il CNIL ha pubblicato un sw specifico su DPIA https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment (anche in italiano)

Registro dei trattamenti

Adempimenti

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, categorie interessati/dati personali, categorie destinatari, se applicabile trasferimento di dati all'estero, 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 …* " ed è altresì indicato che "*l'Autorità sta valutando di mettere a disposizione un modello di registro dei trattamenti sul proprio sito, che i singoli titolari potranno integrare nei modi opportuni…*".

Suggerimenti di azione

Nella Guida il Garante « … *richiama l'attenzione sulla sostanziale coincidenza fra i contenuti della notifica dei trattamenti di cui all'art. 38 del Codice e quelli che devono costituire il registro dei trattamenti ex art. 30 regolamento …».*

Ma il Registro dei trattamenti richiama anche l'elenco dei trattamenti presente nel DPS che può essere una base di partenza ma occorre integrarla con gli attributi previsti dall'art. 30 del GDPR e farla confluire in una idonea rappresentazione automatizzata e conservata con le opportune garanzie di sicurezza nonché di aggiornamento e completezza. Il Garante privacy inglese (ICO) ha pubblicato delle indicazioni per la predisposizione del registro delle attività di trattamento :
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation/

Sono stati sviluppati dei prodotti di gestione del Registro dei trattamenti (e di altri adempimenti privacy connessi) che consentono ricerche «inverse».

(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.

Analisi dei rischi e misure di sicurezza

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 …* «

Suggerimenti di azioni

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). Appare necessario il confronto con outsourcer informatici

(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

Adempimenti

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(2) e pertanto questo aspetto assume una grande rilevanza nel GDPR. Sono state emanate linee guida da WP29 e Garante privacy aggiornerà modulo per inoltrare notifica di violazione

Suggerimenti di azione

Occorre predisporre una procedura aziendale per la notificazione, e la documentazione, della violazione (oggi prevista come misura opportuna nel tracciamento delle operazioni bancarie e misura obbligatoria in caso di trattamento di dati biometrici) al Garante e, se del caso, all'interessato

(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;

(2) Ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica

Trasferimento all'estero di dati personali

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

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

Sanzioni

Limiti

Le sanzioni pecuniarie possono arrivare a 20 milioni di euro o , per le imprese, al 4% del fatturato mondiale totale annuo dell'esercizio precedente se più alto

Criteri

Ogni Autorità di controllo garantisce che la imposizione di sanzioni amministrative pecuniarie siano, in ogni singolo caso, effettive, proporzionate e dissuasive

Circostanze che contribuiscono a determinare sanzione pecuniaria:

a) natura, gravità e durata della violazione considerata natura, oggetto e finalità del trattamento così come numero di soggetti interessati lesi e livello di danno subito
b) carattere colposo/doloso della violazione
c) misure prese da Titolare/Responsabile per attenuare danno subito da interessati
d) grado responsabilità di Titolare/Responsabile considerate le misure tecniche/organizzative messe in atto (artt. 25 e 32)
e) eventuali precedenti violazioni pertinenti commesse da Titolare/Responsabile
f) il grado di cooperazione con l'Autorità di controllo, al fine di porre rimedio alla violazione e attenuare possibili effetti negativi
g) le categorie specifiche di dati personali interessati dalla violazione
h) la maniera in cui l'Autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il Titolare/Responsabile ha notificato la violazione
i) qualora siano stati disposti provvedimenti (art. 58 c.2) nei confronti Titolare/Responsabile relativamente allo stesso oggetto e il rispetto di essi
j) adesione a codici di condotta o meccanismi di certificazione approvati
k) eventuali altri fattori aggravanti/attenuanti applicabili

DPO & RdT: analisi di un campione di aziende

Aziende	Contesto	DPO		Registro trattamenti	
Banche		Nomina	Provenienza	Stato	Strumento
Banca 1	Azienda autonoma	In corso, interno	Compliance	completato	si
Banca 2	Capogruppo di gruppo italiano	Da individuare		In corso	In esame
Banca 3	Azienda autonoma	Nominato, interno	Sicurezza	completato	si
Banca 4	Azienda autonoma	Da individuare		completato	no
Banca 5	Capogruppo di gruppo italiano	In corso, interno	Compliance	In corso	si
Banca 6	Componente gruppo italiano	Nominato, interno, di gruppo	Compliance	In corso	no
Banca 7	Azienda autonoma	Nominato, interno	Internal Audit	completato	si
Banca 8	Azienda autonoma	Da individuare			
Finanziarie					
Finanziaria 1	Azienda autonoma	In corso, interno	Compliance	In corso	In esame
Finanziaria 2	Azienda autonoma	Da individuare (esterno)		In corso	no
Compagnie assicurazione					
Compagnia 1	Componente gruppo europeo	Nominato, interno a componente	Compliance	In corso	Si, di gruppo
Rappresentanza 1	Componente gruppo europeo	Nominato, interno, di Gruppo		In corso	Si, di gruppo
Rappresentanza 2	Componente gruppo europeo	Da individuare		In corso	no
Fondi Pensione					
Fondo pensione	Componente gruppo europeo	Nominato, interno, di gruppo		completato	Si, di gruppo
Real Estate					
Gruppo italiano RE	Componente gruppo europeo	Nominato, interno di gruppo		completato	Sì, di gruppo

Agenda

- Presentazione relatore
- GDPR: lavori in corso
- 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)

Sito WP29 (http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083)

Download GDPR http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ITA&toc=OJ:L:2016:119:TOC nella lingua prescelta

Linea guida DPIA del Politecnico di Milano https://www.osservatori.net/it_it/pubblicazioni/linea-guida-per-la-data-protection-impact-assessment

Indicazioni da Commissione UE https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_it?pk_campaign=dataprotectionsme&pk_source=linkedin&pk_medium=paid&pk_content=IT#informazionisulr

GDPR Guidelines prepared by the WP29

Finalised GDPR Guidelines

- Guidelines on Data Protection Officers (DPO)
- Guidelines on the right to data portability
- Guidelines for identifying a controller or processor's Lead Supervisory Authority
- Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk"
- Guidelines on Automated individual decision-making and Profiling
- Guidelines on Data Breach Notifications
- Guidelines on Administrative fines
- BCR referential for data controllers
- BCR referential for data processors
- Adequacy referential

GDPR Guidelines currently to be open for public consultation for a period of 6 weeks

- Guidelines on Derogations for transfers
- Guidelines on Accreditation

GDPR Guidelines no longer under public consultation but still to be finally adopted by the WP29

- Guidelines on Consent
- Guidelines on Transparency

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

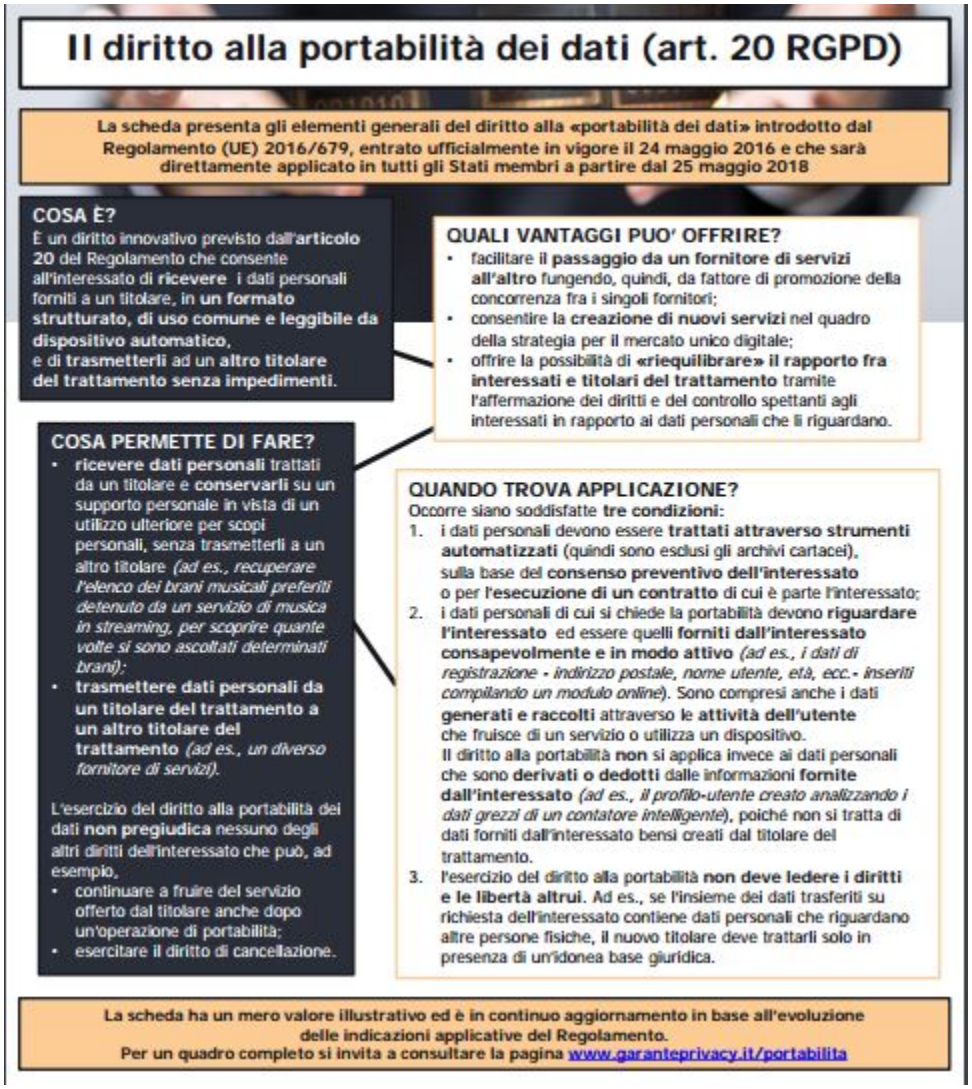
Grazie...

Legge delega per attuazione GDPR

- E’ stata pubblicata sulla Gazzetta Ufficiale Serie Generale n.259 del 6 novembre 2017 la legge 25 ottobre 2017, n. 163 "Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea - Legge di delegazione europea 2016-2017" che entrerà in vigore il 21 novembre 2017 e all'art. 13 riporta la delega al Governo per l'adeguamento della normativa nazionale al GDPR.

- Nell’ambito di tale delega verranno seguiti i seguenti principi:
  - abrogare espressamente le disposizioni del codice in materia di trattamento dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196, incompatibili con le disposizioni contenute nel regolamento (UE) 2016/679;
  - modificare il codice di cui al decreto legislativo 30 giugno 2003, n. 196, limitatamente a quanto necessario per dare attuazione alle disposizioni non direttamente applicabili contenute nel regolamento (UE) 2016/679;
  - coordinare le disposizioni vigenti in materia di protezione dei dati personali con le disposizioni recate dal regolamento (UE) 2016/679;
  - prevedere, ove opportuno, il ricorso a specifici provvedimenti attuativi e integrativi adottati dal Garante per la protezione dei dati personali nell'ambito e per le finalita' previsti dal regolamento (UE) 2016/679;
  - adeguare, nell'ambito delle modifiche al codice di cui al decreto legislativo 30 giugno 2003, n. 196, il sistema sanzionatorio penale e amministrativo vigente alle disposizioni del regolamento (UE) 2016/679 con previsione di sanzioni penali e amministrative efficaci, dissuasive e proporzionate alla gravita' della violazione delle disposizioni stesse.

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

Capo IV

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)