REGOLAMENTO EUROPEO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

Il Regolamento europeo (UE) 2016/679 concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati è entrato in vigore il 24 maggio 2016 e diventerà direttamente applicabile in tutti gli Stati membri a partire dal 25 maggio 2018

Più diritti e più opportunità per tutti

Omega Computer srl

Il Regolamento porterà significative innovazioni non solo per i cittadini, ma anche per le aziende, gli enti pubblici, le associazioni, i liberi professionisti

Omega Computer srl

Viale Augusto Daolio, 9/D
42012 Campagnola Emilia (RE)

Home Page: http://www.omegacomputer.it
E-mail: **info@omegacomputer.it**

Tel. +39 348 3226888

Cittadini più garantiti

Il Regolamento introduce regole più chiare in materia di informativa e consenso, definisce i limiti al trattamento automatizzato dei dati personali, pone le basi per l'esercizio di nuovi diritti, stabilisce criteri rigorosi per il trasferimento dei dati al di fuori dell'Ue e per i casi di violazione dei dati personali (data breach).

INFORMATIVA

Informazioni più chiare e complete sul trattamento

CONSENSO

Consenso, strumento di garanzia anche on line

TRATTAMENTI AUTOMATIZZATI

Limiti alla possibilità per il titolare di adottare decisioni solo sulla base di un trattamento automatizzato di dati

NUOVI DIRITTI

Più tutele e libertà con il diritto all'oblio e il diritto alla portabilità dei dati

TRASFERIMENTO DATI

Garanzie rigorose per il trasferimento dei dati al di fuori dell'Ue

DATA BREACH

Obbligo di comunicare i casi di violazione dei dati personali (data breach)

Novità per le imprese e gli enti

Imprese ed enti avranno più responsabilità, ma potranno beneficiare di semplificazioni. In caso di inosservanza delle regole sono previste sanzioni, anche elevate.

NORMATIVA UNICA

Un unico insieme di norme per tutti gli Stati dell'Unione europea

ACCOUNTABILITY

Approccio basato sulla valutazione del rischio che premia i soggetti più responsabili

CERTIFICAZIONI E CODICI DEONTOLOGICI

Semplificazioni per i soggetti che offrono maggiori garanzie e promuovono sistemi di autoregolamentazione

Il Regolamento punta a rispondere alle sfide poste dagli sviluppi tecnologici e dai nuovi modelli di crescita economica, tenendo conto delle esigenze di tutela dei dati personali sempre più avvertite dai cittadini dei Paesi dell'Unione europea.

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

GUIDA AL NUOVO

REGOLAMENTO EUROPEO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

Il Regolamento europeo (UE) 2016/679 concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati è entrato in vigore il 24 maggio 2016 e diventerà direttamente applicabile in tutti gli Stati membri a partire dal 25 maggio 2018

Più diritti e più opportunità per tutti

Il Regolamento porterà significative innovazioni non solo per i cittadini, ma anche per le aziende, gli enti pubblici, le associazioni, i liberi professionisti

Cittadini più garantiti

Il Regolamento introduce regole più chiare in materia di informativa e consenso, definisce i limiti al trattamento automatizzato dei dati personali, pone le basi per l'esercizio di nuovi diritti, stabilisce criteri rigorosi per il trasferimento dei dati al di fuori dell'Ue e per i casi di violazione dei dati personali (*data breach*).

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Informazioni più chiare e complete sul trattamento

L’informativa diventa sempre di più uno strumento di trasparenza riguardo al trattamento dei dati personali e all’esercizio dei diritti.

Per facilitare la comprensione dei contenuti, nell’informativa si potrà fare ricorso anche a icone, identiche in tutta l’Unione europea.

Gli interessati dovranno sapere se i loro dati sono trasmessi al di fuori dell’Ue e con quali garanzie; cosi come dovranno sapere che hanno il diritto di revocare il consenso a determinati trattamenti, come quelli a fini di marketing diretto.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Consenso, strumento di garanzia anche on line

Il consenso dell'interessato al trattamento dei dati personali dovrà essere, come oggi, preventivo e inequivocabile, anche quando espresso attraverso mezzi elettronici (ad esempio, selezionando un'apposita casella in un sito web).
Per trattare i dati sensibili, il Regolamento prevede che il consenso deve essere anche «esplicito».

Viene esclusa ogni forma di consenso tacito (il silenzio, cioè, non equivale al consenso) oppure ottenuto proponendo a un interessato una serie di opzioni già selezionate.

Il consenso potrà essere revocato in ogni momento.
I trattamenti effettuati fino a quel momento dal titolare sulla base del consenso rimarranno comunque legittimi.

I fornitori di servizi Internet e i social media, dovranno richiedere il consenso ai genitori o a chi esercita la potestà genitoriale per trattare i dati personali dei minori di 16 anni.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Limiti alla possibilità per il titolare di adottare decisioni solo sulla base di un trattamento automatizzato di dati

Le decisioni che producono effetti giuridici (come, la concessione di un prestito) non potranno essere basate esclusivamente sul trattamento automatizzato dei dati (ad esempio, la profilazione).

Faranno eccezione i casi in cui l'interessato abbia rilasciato un consenso esplicito al trattamento automatizzato dei suoi dati, oppure questo tipo di trattamento risulti strettamente necessario per la definizione di un contratto o avvenga in base a specifici obblighi di legge.

In ogni caso, sono previste garanzie per gli interessati, come il diritto di opporsi alla decisione adottata sulla base di un trattamento automatizzato o il diritto di ottenere anche l'intervento umano rispetto alla decisione stessa.

Se il trattamento è finalizzato ad attività di marketing diretto, l'interessato ha sempre il diritto di opporsi alla profilazione.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Più tutele e libertà con il diritto all'oblio

Grazie all'introduzione del cosiddetto «diritto all'oblio», gli interessati potranno ottenere la cancellazione dei propri dati personali anche on line da parte del titolare del trattamento qualora ricorrano alcune condizioni previste dal Regolamento: se i dati sono trattati solo sulla base del consenso; se i dati non sono più necessari per gli scopi rispetto ai quali sono stati raccolti; se i dati sono trattati illecitamente; oppure se l'interessato si oppone legittimamente al loro trattamento.

A questo diritto si accompagna l'obbligo per il titolare del trattamento che ha pubblicato i dati di comunicare la richiesta di cancellazione a chiunque li stia trattando, nei limiti di quanto tecnicamente possibile.

Il diritto all'oblio potrà essere limitato solo in alcuni casi specifici: per esempio, per garantire l'esercizio della libertà di espressione o il diritto alla difesa in sede giudiziaria; per tutelare un interesse generale (ad esempio, la salute pubblica); oppure quando i dati, resi anonimi, sono necessari per la ricerca storica o per finalità statistiche o scientifiche.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Portabilità dei dati: liberi di trasferire i propri dati in un mercato digitale più aperto alla concorrenza

Il Regolamento introduce il diritto alla «portabilità» dei propri dati personali per trasferirli da un titolare del trattamento ad un altro.
Ad esempio, si potrà cambiare il *provider* di posta elettronica senza perdere i contatti e i messaggi salvati.

Ci saranno però alcune eccezioni che non consentono l'esercizio del diritto: in particolare, quando si tratta di dati contenuti in archivi di interesse pubblico, come ad esempio le anagrafi.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Garanzie rigorose per il trasferimento dei dati al di fuori dell'Ue

Resta vietato il trasferimento di dati personali verso Paesi situati al di fuori dell'Unione europea o organizzazioni internazionali che non rispondono agli standard di adeguatezza in materia di tutela dei dati, rispetto ai quali il Regolamento introduce criteri di valutazione più stringenti.

Come avviene già oggi, in mancanza di un riconoscimento di adeguatezza da parte della Commissione europea, i titolari potranno utilizzare per il trasferimento specifiche garanzie contrattuali, per le quali il Regolamento prevede norme dettagliate e vincolanti.

In assenza di garanzie contrattuali o riconoscimenti di adeguatezza, i dati potranno essere trasferiti solo con il consenso esplicito dell'interessato, oppure qualora ricorrano particolari condizioni (ad esempio, quando il trasferimento è indispensabile per rispettare specifici obblighi contrattuali, per importanti motivi di interesse pubblico, per esercitare o difendere un diritto in sede giudiziaria, ecc.).

Il trasferimento o la comunicazione di dati personali di un cittadino dell'Ue ad autorità giudiziarie o amministrative di Paesi terzi potranno avvenire solo sulla base di accordi internazionali di mutua assistenza giudiziaria o attraverso strumenti analoghi.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Obbligo di comunicare i casi di violazione dei dati personali *(data breach)*

Il titolare del trattamento dovrà comunicare eventuali violazioni dei dati personali (*data breach*) all'Autorità nazionale di protezione dei dati.
Se la violazione dei dati rappresenta una minaccia per i diritti e le libertà delle persone, il titolare dovrà informare in modo chiaro, semplice e immediato anche tutti gli interessati e offrire indicazioni su come intende limitare le possibili conseguenze negative.

Il titolare del trattamento potrà decidere di non informare gli interessati se riterrà che la violazione non comporti un rischio elevato per i loro diritti (quando non si tratti, ad esempio, di frode, furto di identità, danno di immagine, ecc.);
oppure se dimostrerà di avere adottato misure di sicurezza (come la cifratura) a tutela dei dati violati; oppure, infine, nell'eventualità in cui informare gli interessati potrebbe comportare uno sforzo sproporzionato (ad esempio, se il numero delle persone coinvolte è elevato).
In questo ultimo caso, è comunque richiesta una comunicazione pubblica o adatta a raggiungere quanti più interessati possibile (ad esempio, tramite un'inserzione su un quotidiano o una comunicazione sul sito web del titolare).

L'Autorità di protezione dei dati potrà comunque imporre al titolare del trattamento di informare gli interessati sulla base di una propria autonoma valutazione del rischio associato alla violazione.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Le novità per le imprese e gli enti

Imprese ed enti avranno più responsabilità, ma potranno beneficiare di semplificazioni. In caso di inosservanza delle regole sono previste sanzioni, anche elevate.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Un unico insieme di norme per tutti gli Stati dell'Unione europea

Il Regolamento è direttamente applicabile e vincolante in tutti gli Stati membri dell'Unione europea e non richiede una legge di recepimento nazionale.

Inoltre, si applica integralmente alle imprese situate fuori dall'Unione europea che offrono servizi o prodotti a persone che si trovano nel territorio dell'Unione europea.
Tutte le aziende, ovunque stabilite, dovranno quindi rispettare le regole fissate nell'Ue.

Fra le principali novità del Regolamento c'è il cosiddetto «sportello unico» (*one stop shop*), che semplificherà la gestione dei trattamenti e garantirà un approccio uniforme.
Salvo casi specifici, le imprese stabilite in più Stati membri o che offrono prodotti e servizi in vari Paesi dell'Ue, per risolvere possibili problematiche sull'applicazione e il rispetto del Regolamento potranno rivolgersi ad un solo interlocutore: cioè all'Autorità di protezione dei dati del Paese dove si trova il loro stabilimento principale.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Approccio basato sulla valutazione del rischio che premia i soggetti più responsabili

Il Regolamento promuove la responsabilizzazione (*accountability*) dei titolari del trattamento e l'adozione di approcci e politiche che tengano conto costantemente del rischio che un determinato trattamento di dati personali può comportare per i diritti e le libertà degli interessati.

Il principio-chiave è *«privacy by design»*, ossia garantire la protezione dei dati fin dalla fase di ideazione e progettazione di un trattamento o di un sistema, e adottare comportamenti che consentano di prevenire possibili problematiche. Ad esempio, è previsto l'obbligo di effettuare valutazioni di impatto prima di procedere ad un trattamento di dati che presenti rischi elevati per i diritti delle persone, consultando l'Autorità di protezione dei dati in caso di dubbi. Viene inoltre introdotta la figura del «Responsabile della protezione dei dati» (*Data Protection Officer* o DPO), incaricato di assicurare una gestione corretta dei dati personali nelle imprese e negli enti.

In compenso, scompaiono alcuni oneri amministrativi come l'obbligo di notificare particolari trattamenti, oppure di sottoporre a verifica preliminare dell'Autorità i trattamenti considerati «a rischio».

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Semplificazioni per i soggetti che offrono maggiori garanzie e promuovono sistemi di autoregolamentazione

Il Regolamento promuove il ricorso a codici di condotta da parte di associazioni di categoria e altri soggetti, sottoposti all'approvazione dell'Autorità nazionale di protezione dei dati ed eventualmente della Commissione europea (nel caso dell'approvazione da parte della Commissione il codice di condotta avrà applicazione nell'intera Ue).

Il titolare potrà far certificare i propri trattamenti, in misura parziale o totale, anche ai fini di trasferimenti di dati in Paesi terzi. La certificazione potrà essere rilasciata da un soggetto abilitato oppure dall'Autorità di protezione dei dati.

L'adesione ai codici di condotta e la certificazione del trattamento saranno elementi di cui l'Autorità dovrà tenere conto, per esempio, nell'applicare eventuali sanzioni o nell'analizzare la correttezza di una valutazione di impatto effettuata dal titolare.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Il Regolamento punta a rispondere alle sfide poste dagli sviluppi tecnologici e dai nuovi modelli di crescita economica, tenendo conto delle esigenze di tutela dei dati personali sempre più avvertite dai cittadini dei Paesi dell'Unione europea.

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Per saperne di più

www.garanteprivacy.it/regolamentoue

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Giugno 2016

La guida ha mere finalità divulgative

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Scheda aggiornata in base alla versione delle Linee guida del WP29 emendata e adottata il 4 ottobre 2017

Valutazione di impatto sulla protezione dei dati (DPIA) – Art. 35 del Regolamento UE/2016/679

COSA È?

È una procedura prevista dall'**articolo 35 del Regolamento UE/2016/679 (RGDP)** che mira a descrivere un trattamento di dati per **valutarne la necessità e la proporzionalità nonché i relativi rischi**, allo scopo di approntare misure idonee ad affrontarli. Una DPIA **può riguardare un singolo trattamento oppure più trattamenti** che presentano **analogie** in termini di natura, ambito, contesto, finalità e rischi.

PERCHÉ?

La DPIA è uno strumento importante in termini di responsabilizzazione *(accountability)* in quanto aiuta il titolare non soltanto a rispettare le prescrizioni del RGPD, ma anche ad attestare di aver adottato misure idonee a garantire il rispetto di tali prescrizioni. In altri termini, **la DPIA è una procedura che permette di valutare e dimostrare la conformità con le norme in materia di protezione dei dati personali.** Vista la sua utilità, il Gruppo Art. 29 suggerisce di valutarne l'impiego **per tutti i trattamenti**, e **non solo** nei casi in cui il Regolamento la prescrive come obbligatoria.

IN CHE MOMENTO?

La DPIA deve essere condotta **prima** di procedere al trattamento. Dovrebbe comunque essere previsto un **riesame continuo** della DPIA, **ripetendo la valutazione a intervalli regolari.**

CHI?

La **responsabilità** della DPIA spetta al **titolare**, anche se la conduzione materiale della valutazione di impatto può essere affidata a un altro soggetto, interno o esterno all'organizzazione. Il titolare **ne monitora** lo svolgimento **consultandosi** con il **responsabile della protezione dei dati** (RPD, in inglese DPO) e acquisendo - se i trattamenti lo richiedono - il parere di esperti di settore, del **responsabile della sicurezza dei sistemi informativi** *(Chief Information Security Officer, CISO)* e **del responsabile IT**.

QUANDO LA DPIA E' OBBLIGATORIA?

In tutti i casi in cui un trattamento può presentare un **rischio elevato per i diritti e le libertà** delle persone fisiche.
Il Gruppo Art. 29 individua alcuni criteri specifici a questo proposito:
- trattamenti valutativi o di *scoring*, compresa la profilazione;
- decisioni automatizzate che producono significativi effetti giuridici (es: assunzioni, concessione di prestiti, stipula di assicurazioni);
- monitoraggio sistematico (es: videosorveglianza);
- trattamento di dati sensibili, giudiziari o di natura estremamente personale (es: informazioni sulle opinioni politiche);
- trattamenti di dati personali su larga scala;
- combinazione o raffronto di insiemi di dati derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dal consenso iniziale (come avviene, ad esempio, con i Big Data);
- dati relativi a soggetti vulnerabili (minori, soggetti con patologie psichiatriche, richiedenti asilo, anziani, ecc.);
- utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative (es: riconoscimento facciale, device IoT, ecc.);
- trattamenti che, di per sé, potrebbero impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto (es: screening dei clienti di una banca attraverso i dati registrati in una centrale rischi per stabilire la concessione di un finanziamento).

La DPIA è necessaria in presenza di almeno due di questi criteri, ma - tenendo conto delle circostanze - il titolare può decidere di condurre una DPIA anche se ricorre uno solo dei criteri di cui sopra.

QUANDO LA DPIA NON E' OBBLIGATORIA?

Secondo le Linee guida del Gruppo Art. 29, la DPIA **NON è necessaria** per i trattamenti che:
- non presentano rischio elevato per diritti e libertà delle persone fisiche;
- hanno natura, ambito, contesto e finalità molto simili a quelli di un trattamento per cui è già stata condotta una DPIA;
- sono stati già sottoposti a verifica da parte di un'Autorità di controllo prima del maggio 2018 e le cui condizioni (es: oggetto, finalità, ecc.) non hanno subito modifiche;
- sono compresi nell'elenco facoltativo dei trattamenti per i quali non è necessario procedere alla DPIA;
- fanno riferimento a norme e regolamenti, Ue o di uno stato membro, per la cui definizione è stata condotta una DPIA.

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: www.garanteprivacy.it/regolamentoue

CYBERATTACK DISRUPTION IN EUROPA

IDC Analyze the Future

#IDCSecurity17

60%

Percentuale di multinazionali con radici in Europa che entro il 2019 subirà significativi attacchi informatici finalizzati all'interruzione della distribuzione di beni materiali e immateriali

Questo significa che la maggior parte delle grandi aziende europee sarà sotto attacco continuo e sofisticato

L'Europa, grazie alla GDPR, sarà un passo avanti rispetto al resto del mondo, dove questa percentuale sarà del 70%

Le motivazioni di questi attacchi saranno soprattutto economiche, chiunque siano i mandanti

L'adozione dell'IoT se da una parte migliora lo scambio e la raccolta dei dati, dall'altra aumenta i rischi di falle

Le aziende non dovranno proteggere solo se stesse, ma anche e soprattutto la catena del valore

IDC Security Conference 2017
11 maggio 2017 | Milano

CYBERBULLISMO

IL 19 % DEI RAGAZZI ITALIANI SI CONNETTE AD INTERNET PER PIÙ DI 5 ORE AL GIOGNO

LA FOTOGRAFIA DEL FENOMENO SECONDO LA NOSTRA RICERCA.

MOTIVI PER CUI SI È PRESI DI MIRA

- IMMAGINE FISICA
- TIMIDEZZA
- ORIENTAMENTO SESSUALE
- NAZIONALITÀ
- DISABILITÀ

2 RAGAZZI SU 5 SONO VITTIME

I LUOGHI

COME AVVIENE

59% DIFFUSIONE FOTO DENIGRATORIE

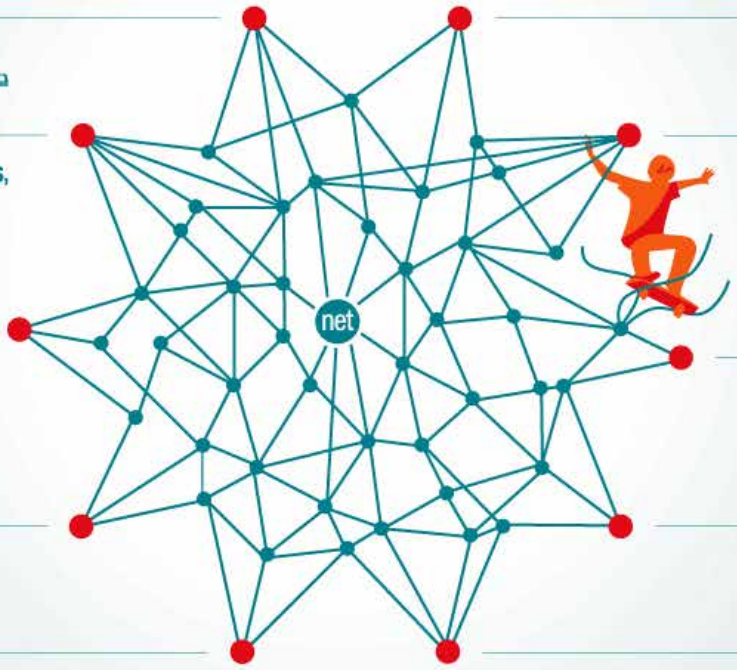
58% INFORMAZIONI FALSE O MINACCIOSE VIA SMS, MMS, E-MAIL @

61% ATTRAVERSO I SOCIAL NETWORK

f t You Tube

57% CREAZIONE DI GRUPPI "CONTRO"

48% HACKING DEI PROFILI PRIVATI



COME REAGISCONO LE VITTIME

67% SI ISOLANO SOCIALMENTE

33% NON CERCANO AIUTO ESTERNO

31% CERCANO L'AIUTO DI ADULTI

28% LASCIANO PASSARE IL TEMPO

9% SUBISCONO CONSEGUENZE NEGATIVE

LE CONSEGUENZE DEL CYBERBULLISMO

- TIMORE DI CONSEGUENZE TRAGICHE
- ISOLAMENTO
- DEPRESSIONE

IL PERICOLO

72% PER IL DEI RAGAZZI **IL BULLISMO RAPPRESENTA IL PERICOLO MAGGIORE**

INTERVENTI RICHIESTI DAI RAGAZZI

- INCONTRI DI PREVENZIONE CON ALTRI GIOVANI
- INCONTRI CON GENITORI
- MAGGIOR SENSIBILIZZAZIONE DEGLI INSEGNANTI

Save the Children
Italia ONLUS

www.garanteprivacy.it/flash

Consigli flash

X TUTELARE la tua privacy con buone password

1 COME E' FATTA UNA BUONA PASSWORD

Una **buona password**

- deve essere abbastanza **lunga** (almeno 8 caratteri);
- deve contenere **caratteri di almeno 3 diverse tipologie**, da scegliere tra le 4 seguenti: lettere maiuscole, lettere minuscole, numeri, caratteri speciali (punti, trattino, *underscore*, ecc.);
- **non** dovrebbe **contenere riferimenti** personali facili da indovinare (nome, cognome, data di nascita, ecc.);
- **andrebbe periodicamente cambiata**, almeno per i profili più importanti o quelli che usi più spesso (e-mail, *e-banking*, *social network,* ecc.).

2 UTILIZZA PASSWORD DIVERSE PER ACCOUNT DIVERSI (e-mail, *social network*, ecc.)

In caso di «furto» di una password eviterai così il rischio che anche gli altri profili che ti appartengono possano essere violati.

3 CONSERVA CON CURA LE PASSWORD

- Non conservare mai le password su biglietti che poi tieni nel portafoglio o indosso, oppure in *file* non protetti su pc, *smartphone* o *tablet.*
- **Evita di condividere** le password via e-mail, sms, *social network*, *instant messaging*, ecc.. Anche se le comunichi a persone conosciute, le credenziali potrebbero essere diffuse involontariamente a terzi o «rubate» da pirati informatici.
- Se usi pc, *smartphone* e altri *device* che non ti appartengono, **evita** che possano **conservare in memoria le password da te utilizzate.**

4 PROVA AD USARE SOFTWARE «GESTORI DI PASSWORD»

Si tratta di programmi specializzati che **generano password sicure** e **consentono di appuntare sul pc tutte le password salvandole in un database cifrato sicuro**.
Ce ne sono di vario tipo, gratuiti o a pagamento.

Ti suggeriamo di consultare anche le altre schede informative che trovi su www.garanteprivacy.it/flash e le nostre campagne di comunicazione «Social privacy», «Fatti smart» e «Connetti la testa».
Se hai dubbi e domande, puoi contattare l'URP del Garante: www.garanteprivacy.it/home/urp

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

www.garanteprivacy.it/flash

Consigli flash

XTUTELARE la tua privacy se metti immagini online

1

Rifletti bene prima di postare online foto o filmati.
Potrebbe poi essere molto difficile eliminarli, soprattutto se qualcuno li ha copiati, condivisi, o diffusi su altri siti o social network

2

Pubblica immagini di altre persone solo con il loro consenso. Potrebbero non voler apparire online o sentirsi in imbarazzo. Inserisci nelle immagini **tag** con i nomi di altre persone **solo** se sei sicuro che queste siano d'accordo

3

Controlla i tag con il tuo nome associati a foto e filmati.
Alcuni social network consentono eventualmente di applicare scelte come:
1) bloccare l'inserimento di **tag** con il tuo nome nelle immagini postate da altre persone;
2) autorizzare solo alcune persone a *taggare* le immagini con il tuo nome;
3) ricevere un messaggio di avviso se qualcuno collega il tuo nome ad un'immagine, in modo che tu possa approvare o rifiutare il tag

4

Controlla chi può vedere le tue immagini.
I principali social network consentono di scegliere se foto e immagini che pubblichi saranno visibili a tutti o solo da liste di persone scelte da te

5

Molte app richiedono l'accesso alle foto o ai filmati che conservi su smartphone o tablet. Prima di autorizzare l'accesso, cerca di capire a quale scopo potrebbero essere utilizzate o diffuse le tue immagini

Per ulteriori informazioni, contatta il Garante:
www.garanteprivacy.it/home/urp

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

www.garanteprivacy.it/flash

Consigli flash

TUTELARE la tua privacy su web e social network

1 RISPETTA SEMPRE GLI ALTRI

Chiediti **sempre** se quello che pubblichi *on line* può **offendere** o **danneggiare qualcuno.** Ricorda che sei responsabile di ciò che scrivi o diffondi su web e *social network*

2 RIFLETTI PRIMA DI PUBBLICARE QUALCOSA *ON LINE*

Foto, testi e filmati messi in Rete **possono restare** *on line* **per sempre** ed essere **visti da chiunque**. Ricorda: ciò che pubblichi oggi potrebbe non piacerti più domani, o potrebbe danneggiare la tua reputazione con datori di lavoro, colleghi, compagni di studio, ecc.

5 OCCHIO ALLE TRACCE CHE PUOI LASCIARE *ONLINE*

Puoi **verificare** le **informazioni legate al tuo nome** o alla **tua attività lavorativa** o **professionale** usando un motore di ricerca. Se lo ritieni necessario, puoi chiedere al sito web di cancellare o rettificare alcuni dati personali che ti riguardano (per informazioni, consulta: **www.garanteprivacy.it/home/diritti**). Controlla anche i ***cookie*** scaricati mentre navighi *on line*, e ricorda che puoi decidere se dare il consenso a quelli usati a scopo di profilazione (per approfondire, vedi: **www.garanteprivacy.it/cookie**)

3 ATTENTO A PIRATI TELEMATICI E LADRI DI IDENTITA' DIGITALE

Usa *password* differenti e complicate per i tuoi *account* e-mail e per i profili su web e *social network* e **non comunicarle** a nessuno. Altrimenti i tuoi dati personali e la tua identità *on line* potrebbero essere a rischio. Per informazioni, consulta anche la campagna **«Connetti la testa»** (**www.garanteprivacy.it/connettilatesta**)

4 PROTEGGITI DALLO SPAM TELEMATICO

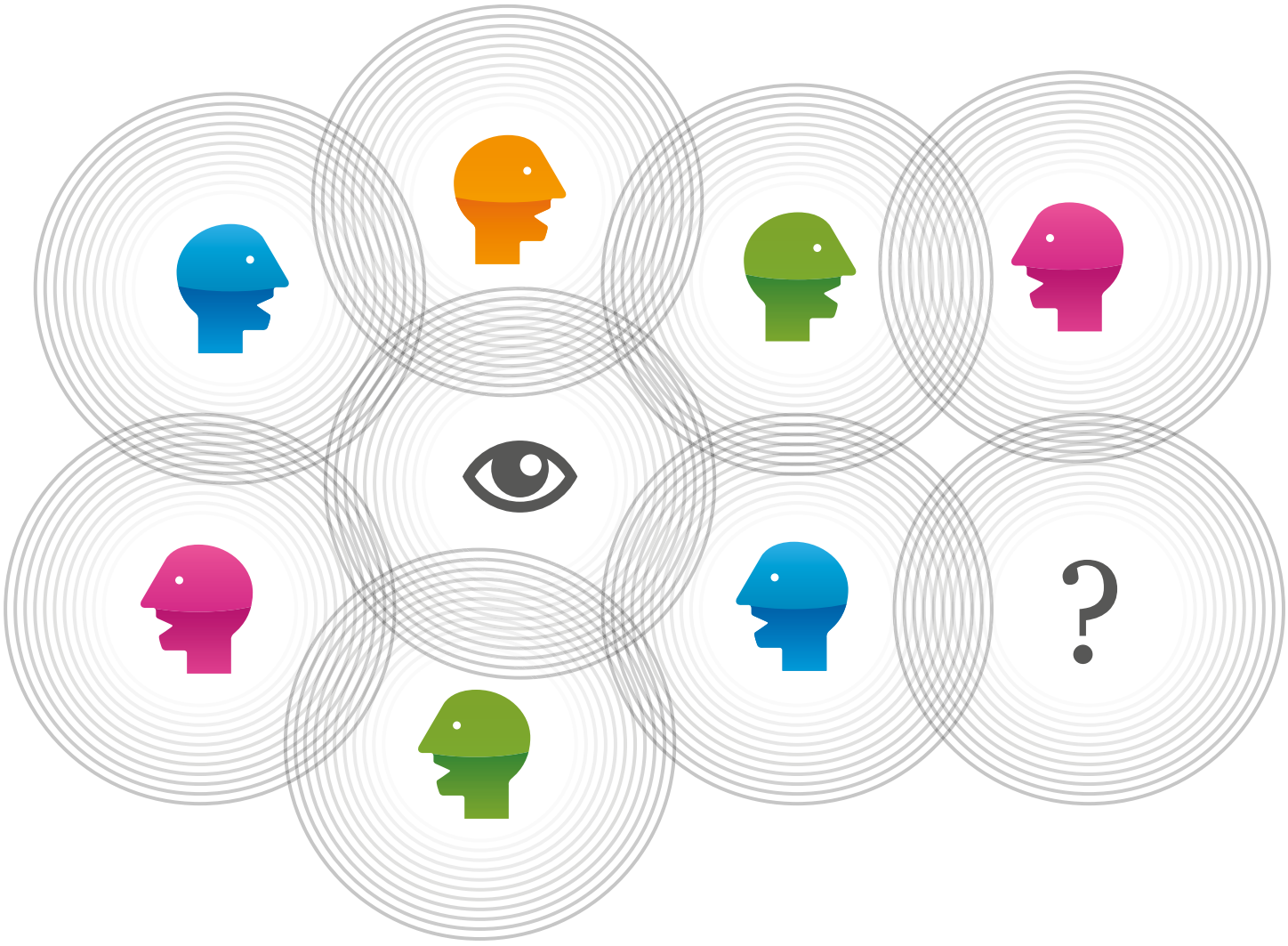
Leggi sempre con attenzione **l'informativa sul trattamento dei dati personali** prima di accedere a servizi *on line* o compilare *form* sul web. **Crea indirizzi e-mail diversi** da usare **solo** per fare acquisti *online*, accedere a servizi sul web, ricevere *newsletter*, ecc.. Così la tua posta elettronica personale o lavorativa sarà protetta dal rischio di «**contagio spam».** Per informazioni, consulta anche la pagina web: **www.garanteprivacy.it/spam**

Se hai dubbi e domande, puoi conttatare l'URP del Garante: www.garanteprivacy.it/home/urp

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

SOCIAL PRIVACY

COME TUTELARSI NELL'ERA DEI SOCIAL NETWORK



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

FACEBOOK & CO

AVVISI AI NAVIGANTI

TI SEI MAI CHIESTO?

10 CONSIGLI
PER NON RIMANERE
INTRAPPOLATI

IL GERGO DELLA RETE

PREMESSA:
DALLA VITA DIGITALE A QUELLA REALE

Il mondo delle reti sociali (da Facebook a Twitter, da Linkedin a Instagram) è in cambiamento incessante e il Garante per la protezione dei dati personali ne segue con attenzione gli sviluppi allo scopo di tutelare con efficacia giovani e adulti.

I social network offrono vantaggi significativi e immediati: semplificano i contatti, rendono possibili scambi di informazioni con un numero enorme di persone. Queste comunità on-line, però, amplificano i rischi legati a un utilizzo improprio o fraudolento dei dati personali degli utenti, esponendoli a danni alla reputazione, a furti di identità, a veri e propri abusi.

Non esistono più, infatti, barriere tra la vita digitale e quella reale: quello che succede on-line sempre più spesso ha impatto fuori da Internet, nella vita di tutti i giorni e nei rapporti con gli altri.

Proprio con l'obiettivo di aumentare la consapevolezza degli utenti e offrire loro ulteriori spunti di riflessione e strumenti di tutela, il Garante ha deciso di aggiungere nuovi contenuti alla guida ai social network pubblicata nel 2009, mantenendone però la struttura agile che ne ha favorito in questi anni la diffusione e il facile utilizzo.

FACEBOOK & CO

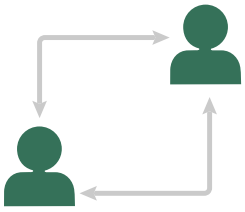
I SOCIAL NETWORK

I social network (a volte definiti social media per enfatizzare il loro impatto non solo come reti sociali ma come veri e propri media auto-organizzati) sono "piazze virtuali", cioè dei luoghi in cui via Internet ci si ritrova condividendo con altri fotografie, filmati, pensieri, indirizzi, amici e tanto altro. I social network sono lo strumento di condivisione per eccellenza e rappresentano straordinarie forme di comunicazione, anche se comportano dei rischi per la sfera personale degli individui coinvolti.

I primi social network sono nati in ambito universitario, tra colleghi che non si volevano "perdere di vista" e che desideravano "fare squadra" una volta entrati nel mondo del lavoro. Facebook, per citare uno dei più famosi, agli inizi era esattamente la traduzione virtuale dell'annuario, ovvero del "libro delle fotografie" della scuola. Una bacheca telematica dove ritrovare i colleghi di corso e scambiare con loro informazioni. Le più recenti evoluzioni della tecnologia consentono ai social network di integrarsi sempre più con i telefoni cellulari, trasformando i messaggi che pubblichiamo on-line in una sorta di sms multiplo che giunge istantaneamente a tutti i nostri amici.

Gli strumenti predisposti dalle reti sociali ci permettono di seguire i familiari che vivono in un'altra città. Espandono la nostra possibilità di comunicare, anche in ambito politico e sociale, trasformandoci in agenti attivi di campagne a favore di quello in cui crediamo. Possono facilitare lo scambio di conoscenze tra colleghi e tra colleghi e impresa.

Ai tradizionali social network si sono aggiunte numerose piattaforme di messaggistica sociale istantanea (come WhatsApp), la cui crescita è andata di pari passo con la rapidissima diffusione di smartphone e di altri strumenti (dai tablet ai phablet, alle cosiddette tecnologie indossabili come occhiali e orologi "intelligenti") che consentono la connessione alla rete in mobilità.



I social network sono strumenti che danno l'impressione di uno spazio personale, o di piccola comunità. Si tratta però di un falso senso di intimità che può spingere gli utenti a esporre troppo la propria vita privata e professionale, a rivelare informazioni confidenziali, orientamenti politici, scelte sessuali, fede religiosa o condizioni di salute, provocando gravi "effetti collaterali", anche a distanza di anni, che non devono essere sottovalutati. Tra l'altro, l'idea di impunità trasmessa dalla possibilità di utilizzare messaggi che si "autodistruggono" o di nascondersi dietro forme di anonimato può favorire in rete atteggiamenti aggressivi o violenti, in particolare verso le persone più giovani e indifese.

ALCUNI DEI SOCIAL NETWORK PIÙ DIFFUSI NEL MONDO

Facebook, Google Plus+, VKontakte, Qzone, WhatsApp, LinkedIn, Badoo, Twitter, LINE, WeChat, SinaWeibo, Orkut, Snapchat, Vine, Tencent QQ, Instagram, MySpace, Ask.fm, Tumblr.

IL GARANTE E LA PRIVACY SU INTERNET

La dignità della persona e il diritto alla riservatezza non perdono il loro valore su Internet. La tutela dei dati personali nel mondo interconnesso, per quanto più difficile, è pur sempre possibile, anche grazie alla collaborazione tra i Garanti della privacy, non soltanto europei, ma anche di altri Paesi. L'Autorità italiana interviene direttamente in caso di violazioni di propria competenza. Ma è anche costantemente impegnata per rafforzare gli strumenti a difesa degli utenti e per aumentare la loro consapevolezza sui loro diritti e doveri on-line.

AVVISI AI NAVIGANTI

VITA DIGITALE – VITA REALE
Non esiste più una separazione tra la vita "on-line" e quella "off-line". Quello che scrivi e le immagini che pubblichi sui social network hanno quasi sempre un riflesso diretto sulla tua vita di tutti i giorni, e nei rapporti con amici, familiari, compagni di classe, colleghi di lavoro. Ed è bene ricordare che l'effetto può non essere necessariamente immediato, ma ritardato nel tempo.

IL RICORDO DEL FAR WEST
Il web è spesso raccontato come un luogo senza regole dove ogni utente può dire o fare quello che vuole. In realtà, le stesse regole di civile convivenza, così come le norme che tutelano, ad esempio, dalla diffamazione, dalla violazione della tua dignità, valgono nella vita reale come sui social network, in chat o sui blog. Non esistono zone franche dalle leggi e dal buon senso.

PER SEMPRE... O QUASI
Quando inserisci i tuoi dati personali su un sito di social network, ne perdi il controllo. I dati possono essere registrati da tutti i tuoi contatti e dai componenti dei gruppi cui hai aderito, rielaborati, diffusi, anche a distanza di anni. A volte, accettando di entrare in un social network, concedi al fornitore del servizio la licenza di usare senza limiti di tempo il materiale che inserisci on-line... le tue foto, le tue chat, i tuoi scritti, le tue opinioni.

IL MITO DELL'ANONIMATO

Non è poi così difficile risalire all'identità di coloro che pubblicano testi, immagini, video su Internet con l'intento di danneggiare l'immagine o la reputazione di un'altra persona. L'anonimato in rete può essere usato per necessità, ma mai per commettere reati: in questo caso le autorità competenti hanno molti strumenti per intervenire e scoprire il "colpevole".

LA PRIVACY E IL RISPETTO DEGLI ALTRI

Quando metti on-line la foto di un tuo amico o di un familiare, quando lo "tagghi" (inserisci, ad esempio, il suo nome e cognome su quella foto), domandati se stai violando la sua privacy. Nel dubbio chiedigli il consenso. Non lasciarti trascinare dagli hater, dai troll, nel gioco perverso dei gruppi "contro qualcuno": la prossima volta potresti essere tu la vittima.

NON SONO IO!
Attenzione ai falsi profili. Basta la foto, il tuo nome e qualche informazione sulla tua vita per impadronirsi on-line della tua identità. Sono già molti i casi di attori, politici, personaggi pubblici, ma anche di gente comune, che hanno trovato su social network e blog la propria identità gestita da altri.

GIOCARE E FARSI MALE
Molti giovani, ma non soltanto loro, pensano che l'adozione di alcuni piccoli stratagemmi, come l'invio di messaggi che si "autodistruggono" dopo la lettura, possa metterli al riparo dai rischi di un uso inappropriato del materiale che viene così condiviso. Questa falsa sicurezza può spingerti a scambiare, senza pensarci troppo, messaggi sessualmente espliciti (sexting), insulti gratuiti o semplicemente inopportuni. Tutto quello che è condiviso, però, può sempre essere in qualche maniera salvato e riutilizzato. Se stai giocando, attento a non farti male.

E IL CONTO IN BANCA?
Attento alle informazioni che rendi disponibili on-line. La data e il luogo di nascita bastano per ricavare il tuo codice fiscale. Altre informazioni potrebbero aiutare un malintenzionato a risalire al tuo conto in banca o addirittura al tuo nome utente e alla password.

DISATTIVAZIONE O CANCELLAZIONE?
Se decidi di uscire da un social network spesso ti è permesso solo di "disattivare" il tuo profilo, non di "cancellarlo". I dati, i materiali che hai messo on-line, potrebbero essere comunque conservati nei server, negli archivi informatici dell'azienda che offre il servizio. Leggi bene cosa prevedono le condizioni d'uso e le garanzie di privacy offerte nel contratto che accetti quando ti iscrivi.

LE LEGGI APPLICATE

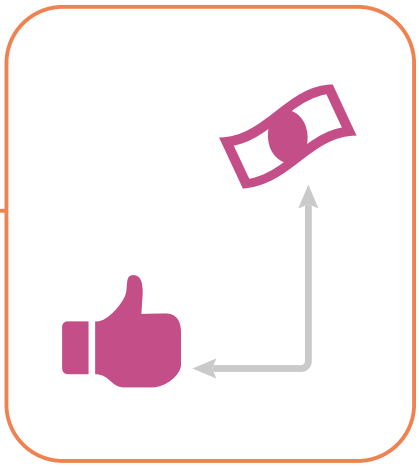
La maggior parte dei social network ha sede all'estero, e così i loro server. In caso di disputa legale o di problemi insorti per violazione della privacy, non sempre si è tutelati dalle leggi italiane ed europee. Se desideri essere più sicuro sul rispetto dei tuoi diritti, sappi che le società che ti offrono i loro servizi da sedi dislocate in uno dei Paesi dell'Unione Europea devono sempre rispettare la normativa comunitaria e in essi è presente un'autorità di protezione dati (Data Protection Authority) che potrà intervenire, anche tramite il Garante, nel caso subissi violazioni alla tua privacy.

CHI PUÒ FARE COSA

Rifletti bene prima di inserire on-line dati che non vuoi vengano diffusi o che possano essere usati a tuo danno. Segnala al Garante della privacy e alle altre autorità competenti le eventuali violazioni affinché possano intervenire a tua tutela. Ma ricorda: il miglior difensore della tua privacy sei innanzitutto tu.

LA LOGICA ECONOMICA:
NIENTE È GRATIS

Le aziende che gestiscono i social network generalmente si finanziano vendendo pubblicità mirate. Il valore di queste imprese è strettamente legato anche alla loro capacità di analizzare in dettaglio il profilo degli utenti, le abitudini e i loro hobby, ma anche le condizioni di salute e l'orientamento politico o sessuale, le reti di contatti, per poi rivendere le informazioni a chi se ne servirà per promuovere offerte commerciali specifiche o per sostenere campagne di vario genere.
Le informazioni raccolte su di te sono infatti usate per monitorare e prevedere i tuoi acquisti, le tue scelte, i tuoi comportamenti.
E ricorda: anche nel web, dietro l'offerta di un servizio "gratuito", si nasconde lo sfruttamento per molteplici scopi dei tuoi dati.



CI SONO AMICI E AMICI

Nelle amicizie esistono differenti livelli di relazione a seconda che ci si rapporti con amici stretti o semplici conoscenti, compagni di classe o professori, partner commerciali o datori di lavoro. Sui social network spesso poniamo tutti sullo stesso piano, rischiando di scrivere o mostrare la cosa sbagliata alla persona sbagliata. Impara a distinguere chi aggiungi alla tua rete di "amici" in base all'uso che ne fai. Se il social network a cui sei iscritto te lo consente, decidi quali tipi di informazioni possono essere consultate dai differenti tipi di amici.

LA REPUTAZIONE DELLE IMPRESE

Anche le società che offrono servizi on-line e di social network hanno una reputazione da mantenere di fronte all'opinione pubblica. Gran parte del loro valore di mercato e del numero di iscritti dipende anche dalla loro "immagine". Se una società adotta comportamenti scorretti nei confronti degli utenti o non risponde con celerità a richieste di aiuto – ad esempio contro il cyberbullismo e la diffamazione – parlane con gli altri utenti e segnalalo alle autorità competenti.

TI SEI MAI CHIESTO?

SEI UN RAGAZZO/A:

- Se sapessi che il vicino di casa o il tuo professore possono accedere al tuo profilo e al tuo diario on-line, scriveresti le stesse cose e nella stessa forma?
- Sei sicuro che le foto e le informazioni che pubblichi ti piaceranno anche tra qualche anno?
- Prima di caricare/postare la "foto ridicola" di un amico, ti sei chiesto se a te farebbe piacere trovarti nella stessa situazione?
- I membri dei gruppi ai quali sei iscritto possono leggere le informazioni riservate che posti sul tuo profilo?
- Sei sicuro che mostreresti "quella" foto con il tuo ex anche al tuo nuovo ragazzo/a?
- Vuoi veramente far sapere a chiunque dove ti trovi (si chiama geolocalizzazione) e chi stai incontrando in ogni momento della giornata?
- Prima di inviare, anche per gioco, un video sexy al tuo nuovo compagno, hai considerato che potrebbe essere condiviso con i suoi amici o con degli sconosciuti?

SEI UN GENITORE:

- Hai spiegato a tuo figlio che non deve toccare il fornello acceso, lo hai educato ad attraversare la strada, a “non prendere caramelle dagli sconosciuti”... ma gli hai insegnato a riconoscere i segnali di pericolo della rete?
- Gli hai insegnato a difendersi dalle aggressioni di potenziali provocatori o molestatori on-line? A non raccontare a tutti, anche a sconosciuti, particolari della sua vita privata e di quella degli amici?
- Hai mai provato a navigare insieme a tuo figlio? Gli hai chiesto di mostrarti come si usa Internet e le reti sociali alle quali è iscritto? Se vedi tua figlia turbata, le chiedi come è andata la giornata con i suoi gruppi sui social network?
- Provi mai a farti spiegare dai tuoi figli quali sono gli argomenti di discussione più interessanti sui social network in quel momento? Ti informi se i tuoi figli hanno conosciuto nuovi amici in chat?
- Hai cercato di capire se sono stati vittime di cyberbullismo o stalking o se fanno sexting?
- Sai come funzionano le “app” sociali e di messaggistica istantanea che i tuoi figli hanno caricato sullo smartphone?
- Conosci i rispettivi vantaggi e gli svantaggi che una persona ha nel collegarsi a un social network con la propria identità riconoscibile o in forma anonima? Ne hai discusso con i tuoi figli?

CERCHI LAVORO:

- Sai che le società di selezione del personale cercano informazioni sui candidati utilizzando i principali motori di ricerca on-line o accedendo direttamente ai profili pubblicati sui social network?
- Ti sei chiesto se le foto che hai pubblicato sui social network e i post che hai inserito potranno danneggiarti nella ricerca del tuo prossimo lavoro?
- Le informazioni contenute nel curriculum che hai spedito all'azienda corrispondono a quelle che hai pubblicato su Internet, magari sul tuo profilo?
- Quello che racconti della tua vita nelle tue "chiacchiere on-line" è coerente con le tue aspirazioni professionali?
- Lo sai che a volte basta cliccare un "mi piace" sui social network per essere "analizzati ed etichettati" in base alle proprie opinioni politiche, sessuali o religiose, con eventuali ripercussioni anche sul contesto lavorativo?

SEI UN UTENTE "ESPERTO":

- Hai verificato come sono impostati i livelli di privacy della tua identità?
- Hai violato il diritto alla riservatezza di qualcuno pubblicando "quel" materiale?
- Hai commesso un reato mostrando quelle foto a tutti, scrivendo quei post?
- Hai verificato chi detiene la "licenza d'uso", le "royalty" e la proprietà intellettuale della documentazione, delle immagini o dei video che hai inserito on-line?
- Prima di installare sul tuo smartphone o sul tuo tablet una nuova "app", hai verificato a quali dati personali accede il programma? E per quale motivo?

SEI UN PROFESSIONISTA:

- Il gruppo di persone abilitate a interagire con la tua identità corrisponde al target professionale che ti sei prefissato di raggiungere?
- I gruppi ai quali sei iscritto sui social network possono avere effetti negativi sul tuo lavoro?
- Se vieni contestato on-line da un componente iscritto alla tua rete sul social network, sei preparato a reagire in maniera appropriata?
- Hai valutato se stai condividendo informazioni con qualcuno che può danneggiarti?
- Sai che numerosi servizi di chat – inclusi quelli offerti dai siti di social network – permettono di registrare e conservare il contenuto della conversazione avvenuta con gli altri utenti?
- Quando offri un servizio ai tuoi clienti, chiedi di essere retribuito per il tuo lavoro. Ti sei mai domandato come paghi i servizi “gratuiti” e le “app” che utilizzi su Internet?

10 CONSIGLI PER NON RIMANERE INTRAPPOLATI

1

PENSARCI BENE, PENSARCI PRIMA

Pensa bene prima di pubblicare i tuoi dati personali (soprattutto nome, indirizzo, numero di telefono) in un profilo-utente, o di accettare con disinvoltura le proposte di amicizia. Ricorda che immagini e informazioni che posti in rete possono riemergere, complici i motori di ricerca, a distanza di anni. Fai attenzione a quello che fai on-line e alle informazioni che condividi (in particolare se riguardano la tua salute o altri aspetti ancora più intimi) anche in forum o chat, perché potrebbe avere "effetti collaterali" sulla tua vita reale.

2

NON SENTIRTI TROPPO SICURO

Prendi opportune precauzioni per tutelare la tua riservatezza, ma non illuderti di essere sempre al sicuro. Le foto e i video che scambi privatamente, magari di contenuto esplicito, possono essere sempre copiati e inoltrati ad altre persone "fuori dal giro dei tuoi amici". Non esistono, tra l'altro, messaggi che si autodistruggono con assoluta certezza.

3

RISPETTA GLI ALTRI

Astieniti dal pubblicare informazioni personali e foto relative ad altri (magari "taggandone" i volti) senza il loro consenso. Sui social network e nella messaggistica istantanea uno scherzo o una semplice ripicca può facilmente degenerare in un grave abuso, facendoti rischiare anche sanzioni penali.

4

SERRA LA PORTA DELLA TUA RETE E DEL TUO SMARTPHONE

Aggiorna l'antivirus del tuo smartphone. Usa login e password diversi da quelli utilizzati su altri siti web, sulla posta elettronica e per la gestione del conto corrente bancario on-line. Fai attenzione, inoltre, quando clicchi su uno dei tanti indirizzi internet abbreviati (ad esempio url tipo t.co, bit.ly oppure goo.gl) pubblicati sui social network, e verifica che non ti conducano a siti fasulli usati per rubarti i dati o per farti scaricare programmi con virus. Se possibile crea pseudonimi differenti in ciascuna rete cui partecipi. Non mettere la data di nascita (in particolare se sei minorenne) o altre informazioni personali nel nickname: così potrai rendere più difficile "tracciarti" o molestarti.

5

ATTENZIONE ALL'IDENTITÀ

Non sempre parli, chatti e condividi informazioni con chi credi tu. Chi appare come bambino potrebbe essere un adulto e viceversa. Sempre più spesso vengono create false identità (sia di personaggi famosi, sia di persone comuni) per semplice gioco, per dispetto o per carpire informazioni riservate. Basta la tua foto e qualche informazione sulla tua vita... e il prossimo "clonato" potresti essere tu.

6

OCCHIO AI CAVILLI

Informati su chi gestisce il social network e quali garanzie offre rispetto al trattamento dei dati personali. Ricorda che hai diritto di sapere come vengono utilizzati i tuoi dati: cerca sotto “privacy” o “privacy policy”.
Accertati di poter recedere facilmente dal servizio e di poter cancellare (eventualmente anche di poter salvare e trasferire) tutte le informazioni che hai pubblicato sulla tua identità.
Leggi bene il contratto e le condizioni d’uso che accetti quando ti iscrivi a un social network. Controlla con attenzione anche le frequenti modifiche che vengono introdotte unilateralmente dal fornitore del servizio: capita spesso che i social network comunichino di aver cambiato i livelli di privacy che tu hai scelto per la tua identità solo alla fine di una lunga nota.

7

ANONIMATO, MA NON PER OFFENDERE

Se lo ritieni opportuno, pubblica messaggi sotto pseudonimo o in forma anonima per tutelare la tua identità, non per offendere o violare quella degli altri. Difendi la libertà di parola, non di insulto. Ricordati che in caso di violazioni non è poi così difficile risalire agli autori di messaggi anonimi postati su Internet.

8

FATTI TROVARE SOLO DAGLI AMICI

Se non vuoi far sapere a tutti dove sei stato o dove ti trovi, ricordati di disattivare le funzioni di geolocalizzazione presenti sulle "app" dei social network, così come sullo smartphone e sugli altri strumenti che utilizzi per collegarti a Internet.

9

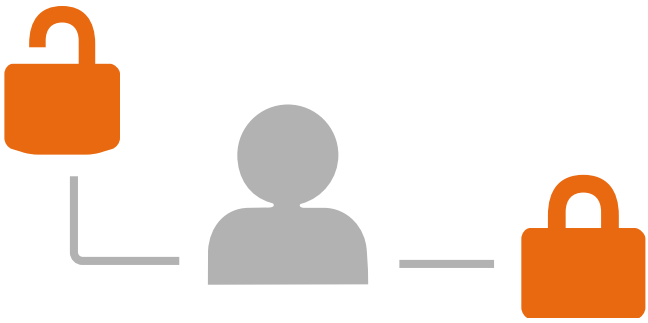
SEGNALA L'ABUSO E CHIEDI AIUTO

Se noti comportamenti anomali e fastidiosi su un social network, se vedi che un tuo amico è insultato e messo sotto pressione da individui o gruppi, non aspettare e segnala subito la situazione critica al gestore del servizio affinché possa intervenire immediatamente. A tale scopo, alcuni social network rendono accessibile agli utenti, sulle pagine del proprio sito, un'apposita funzione (una sorta di pulsante "panic button") per chiedere l'intervento del gestore contro eventuali abusi o per chiedere la cancellazione di testi e immagini inappropriate.
In caso di violazioni, segnala subito il problema al Garante e alle altre autorità competenti. Se sei tu la vittima di commenti odiosi a sfondo sessuale, di cyberbullismo o di sexting, se stanno violando la tua privacy, non aspettare che la situazione degeneri ulteriormente e chiedi aiuto alle persone a te care e alle autorità compenti.

10

PIÙ SOCIAL PRIVACY, MENO APP E SPAM

Controlla come sono impostati i livelli di privacy del tuo profilo: chi ti può contattare, chi può leggere quello che scrivi, chi può inserire commenti alle tue pagine, che diritti hanno gli utenti dei gruppi ai quali appartieni. Limita al massimo la disponibilità di informazioni, soprattutto per quanto riguarda la reperibilità dei dati da parte dei motori di ricerca.
Controlla quali diritti di accesso concedi alle App che installi sul tuo smartphone o sul tuo tablet affinché non possano utilizzare i tuoi dati personali (contatti, telefonate, foto...) senza il tuo consenso. Se non desideri ricevere pubblicità, ricordati che puoi rifiutare il consenso all'utilizzo dei dati per attività mirate di pubblicità, promozioni e marketing.



IL GERGO DELLA RETE

ALIAS / FAKE
Falsa identità assunta su Internet (ad esempio su siti di social network). L'utente può scegliere un nome di fantasia, uno pseudonimo, o appropriarsi dei dati di una persona realmente esistente. A volte il termine fake viene utilizzato per segnalare una notizia falsa.

APP
Un software che si installa su smartphone, tablet o altri dispositivi portatili. Può offrire funzionalità di ogni tipo, come l'accesso ai social network, le previsioni del tempo, il consumo di calorie, i videogiochi, le novità musicali. Il termine deriva dalla contrazione del termine "applicazione".

ASKARE
Descrive una pratica molto diffusa negli adolescenti iscritti al social network Ask.fm, ovvero quello di postare una domanda personale, quasi sempre in forma anonima, sulla bacheca di uno degli utenti registrati. Questo meccanismo può facilitare atteggiamenti aggressivi o di vero e proprio cyberbullismo.

BANNARE / BANDIRE
L'atto che l'amministratore di un sito o di un servizio on-line (chat, social network, gruppo di discussione...) effettua per vietare l'accesso a un certo utente. In genere si viene bannati/cancellati quando non si rispettano le regole di comportamento definite all'interno del sito.

CARICARE / UPLODARE / UPLOADARE
Inserire un documento di qualunque tipo (audio, video, testo, immagine) on-line, anche sulla bacheca del proprio profilo di social network.

CHATTARE
Termine mutuato dalla parola inglese "chat", letteralmente, una "chiacchierata". Il dialogo on-line, attraverso un sistema di messaggistica istantanea, può essere limitato a due persone o coinvolgere un gruppo più ampio di utenti.

CONDIVIDERE
Permettere ad altri utenti, amici/sconosciuti, di accedere al materiale (testi, audio, video, immagini) che sono presenti sul nostro computer o che abbiamo caricato on-line.

CONDIZIONI D'USO / USER AGREEMENT / TERMS OF USE
Le regole contrattuali che vengono accettate dall'utente quando accede a un servizio. È sempre bene stamparle e leggerle con attenzione quando si decide di accettarle. Possono essere modificate in corso d'opera dall'azienda.

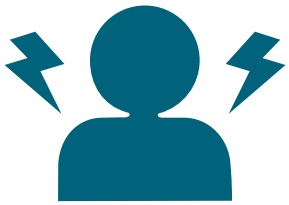
CYBERBULLISMO
Indica atti di molestia/bullismo posti in essere utilizzando strumenti elettronici. Spesso è realizzato caricando video o foto offensive su Internet, oppure violando l'identità digitale di una persona su un sito di social network. Si tratta di un fenomeno sempre più diffuso tra i minorenni.

IDENTITÀ / PROFILO / ACCOUNT
Insieme dei dati personali e dei contenuti caricati su un sito Internet o, più specificamente, su un social network. Può indicare anche solo il nome-utente che viene utilizzato per identificarsi e per accedere a un servizio on-line (posta elettronica, servizio di social network, chat, blog...).

GEOLOCALIZZAZIONE
Identificazione della posizione geografica di un utente. Tra le tante modalità con cui viene rilevata si ricordano: il segnale gps dello strumento che si sta utilizzando oppure la triangolazione delle reti wi-fi rilevate dallo strumento con cui l'utente si collega in rete.

HASHTAG
Il termine deriva dall'unione dei due termini inglesi hash (cancelletto) e tag (etichetta). Il carattere "#" viene anteposto dagli utenti di alcuni social network alle parole chiave dei propri messaggi. I messaggi così indicizzati possono essere raggruppati e ricercati in base all'argomento segnalato.

HATER
Letteralmente "chi odia". Il termine viene spesso utilizzato per indicare chi pubblica, spesso coperto dall'anonimato, messaggi offensivi o carichi di rabbia.



LOGGARE / AUTENTICARSI
Accedere a un sito o a un servizio on-line, facendosi identificare con il proprio nome-utente (login, username) e password (parola chiave).

NICKNAME
Pseudonimo.

POKARE / MANDARE UN POKE
È l'equivalente digitale di uno squillo telefonico fatto a un amico per attirarne l'attenzione. In origine, su Facebook, con un "poke" (cenno di richiamo) si chiedeva a uno sconosciuto il permesso di accedere temporaneamente al suo profilo per decidere se inserirlo nella propria rete di amici.

POSTARE
Pubblicare un messaggio (post) – non necessariamente di solo testo – all'interno di un newsgroup, di un forum, di una qualunque bacheca on-line.

PRIVACY POLICY / TUTELA DELLA PRIVACY / INFORMATIVA
Pagina esplicativa predisposta dal gestore del servizio – a volte un semplice estratto delle "condizioni d'uso" del sito – contenente informazioni su come

saranno utilizzati i dati personali inseriti dall'utente sul sito di social network, su chi potrà usare tali dati e quali possibilità si hanno di opporsi al trattamento. (Per una definizione completa del termine "informativa" e una spiegazione dei diritti e dei doveri in tema di privacy, consultare il sito Internet www.garanteprivacy.it).

SCARICARE /DOWNLODARE / DOWNLOADARE
Salvare sul proprio computer o su una memoria esterna (chiave usb, hard disk esterno...) documenti presenti su Internet. Ad esempio, le fotografie o i video trovati su siti quali Facebook o Youtube.

SELFIE
Indicano gli autoscatti o, comunque, le fotografie di se stessi. La pubblicazione di gallerie di "selfie" rappresenta una tendenza abbastanza comune in rete.

SERVER
Generalmente, si tratta di un computer connesso alla rete utilizzato per offrire un servizio (ad esempio per la gestione di un motore di ricerca o di un sito di social network). Sono denominati "client" i computer (come quello di casa) che gli utenti utilizzano per collegarsi al server e ottenere il servizio.

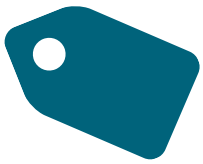
SEXTING
Consiste nell'invio di messaggi provocanti o sessualmente espliciti (eventualmente con foto o video). Il termine sexting deriva dall'unione di due parole inglesi: sex (sesso) e texting (inviare messaggi testuali). Lo scambio di messaggi a contenuto erotico direttamente tramite cellulare o attraverso altri strumenti connessi in rete (come social network e posta elettronica) è molto diffuso tra gli adolescenti.

SNAPCHATTARE
"Fare uno snapchat" o snapchattare indica lo scambio di messaggi che si autodistruggono sul social network Snapchat.

SPAM
Pubblicità e offerte commerciali indesiderate. Sui social network si diffondono spesso forme elaborate di “social spam”.

STALKING
Il termine stalking viene utilizzato con varie accezioni ma generalmente indica l'adozione di atti persecutori ripetuti (ad esempio tramite sms, telefonate o forme di pedinamento) nei confronti di qualcuno. In rete, tali attività moleste e intrusioni nella vita privata possono essere condotte con e-mail o altri tipi di "messaggi istantanei" oppure scambi indesiderati sui social network.

TAG
Marcatore, “etichetta virtuale”, parola chiave associata a un contenuto digitale (immagine, articolo, video).



TAGGARE
Attribuire una “etichetta virtuale” (tag) a un file o a una parte di file (testo, audio, video, immagine). Più spesso, sui social network, si dice che “sei stato taggato” quando qualcuno ha attribuito il tuo nome/cognome a un volto presente in una foto messa on-line. Di conseguenza, se qualcuno cerca il tuo nome, appare la foto indicata.

TROLLING
Definisce il comportamento di chi agisce on-line come un “troll”, provocando, insultando, aggredendo, pubblicando commenti negativi nei confronti di altri utenti della comunità virtuale.

TWEET
La traduzione inglese del termine “cinguettio”. Identifica un breve messaggio inviato sul social network Twitter.

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Piazza di Monte Citorio, 121 - 00186 Roma
tel. 06 696771 – fax 06 696773785
www.garanteprivacy.it

Per informazioni presso l'Autorità:
Ufficio per le relazioni con il pubblico
lunedì - venerdì ore 10.00 - 13.00
tel. 06 696772917
e-mail: urp@gpdp.it
pec: urp@pec.gpdp.it

**A cura del Servizio relazioni
con i mezzi di informazione**

Vertigo Design - Stampa: IAG Mengarelli - Maggio 2014

Violazioni di dati personali *(data breach)*

Gli adempimenti previsti

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

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

SOCIETA' TELEFONICHE E INTERNET PROVIDER

Art. 32-*bis* del Codice in materia di protezione dei dati personali (d. lgs. 196/2003), Regolamento UE 611/13, Provvedimento del Garante n. 161 del 4 aprile 2013 [doc. web n. 2388260]

- **L'obbligo di comunicazione al Garante** *(mediante un apposito modello di comunicazione)* riguarda i fornitori di servizi telefonici e di accesso a Internet (e non, ad esempio, i siti internet che diffondono contenuti, i motori di ricerca, gli *internet point*, le reti aziendali).
- In caso di violazione dei dati personali, società di tlc e Isp **devono**:
  a. **entro 24 ore** dalla scoperta dell'evento, fornire al Garante le informazioni necessarie a consentire una prima valutazione dell'entità della violazione
  b. **entro 3 giorni dalla scoperta,** informare anche ciascun utente coinvolto, comunicando gli elementi previsti dal Regolamento 611/2013 e dal provvedimento del Garante n. 161 del 4 aprile 2013.
- La comunicazione agli utenti **non è dovuta** se si dimostra di aver utilizzato misure di sicurezza nonché sistemi di cifratura e di anonimizzazione che rendono inintelligibili i dati. Nei casi più gravi, il Garante può comunque imporre la comunicazione agli interessati.
- Per consentire l'attività di accertamento del Garante, società telefoniche e provider devono tenere un **inventario** costantemente aggiornato delle violazioni subite.
- **SANZIONI AMMINISTRATIVE PREVISTE (art. 162-*ter* del Codice in materia di protezione dei dati personali)**
  - per mancata o ritardata comunicazione al Garante: da 25mila a 150mila euro;
  - per omessa o mancata comunicazione agli utenti: da 150 euro a 1000 euro per ogni società, ente o persona interessata;
  - per mancata tenuta dell'inventario delle violazioni aggiornato: da 20mila a 120mila euro.

BIOMETRIA

Provvedimento n. 513 del 12 novembre 2014 [doc. web n. 3556992]

- **Entro 24 ore** dalla conoscenza del fatto, i titolari del trattamento (aziende, amministrazioni pubbliche, ecc.) comunicano al Garante *(tramite il modello allegato al provvedimento)* tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui sistemi biometrici installati o sui dati personali custoditi.

DOSSIER SANITARIO ELETTRONICO

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

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

AMMINISTRAZIONI PUBBLICHE

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

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

Per approfondimenti, consultare i provvedimenti pubblicati sul sito: www.garanteprivacy.it

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

IL PHISHING: Attenzione ai «pescatori» di dati personali

Il phishing è una tecnica illecita utilizzata per appropriarsi di informazioni riservate relative a una persona o a un'azienda - username e password, codici di accesso (come il PIN del cellulare), numeri di conto corrente, dati del bancomat e della carta di credito – con l'intento di compiere operazioni fraudolente.

La truffa avviene di solito via e-mail, ma possono essere utilizzati anche sms, chat e social media. Il «ladro di identità» si presenta, in genere, come un soggetto autorevole (banca, gestore di carte di credito, ente pubblico, ecc.) che invita a fornire dati personali per risolvere particolari problemi tecnici con il conto bancario o con la carta di credito, per accettare cambiamenti contrattuali o offerte promozionali, per gestire la pratica per un rimborso fiscale o una cartella esattoriale, ecc..

In genere, i messaggi di phishing invitano a fornire direttamente i propri dati personali, oppure a cliccare un link che rimanda ad una pagina web dove è presente un *form* da compilare. I dati così carpiti possono poi essere utilizzati per fare acquisti a spese della vittima, prelevare denaro dal suo conto o addirittura per compiere attività illecite utilizzando il suo nome e le sue credenziali.

ALCUNI CONSIGLI PER DIFENDERSI

1. IL BUON SENSO PRIMA DI TUTTO

Dati, codici di accesso e password personali **non** dovrebbero mai essere comunicati a sconosciuti. E' bene ricordare che, in generale, banche, enti pubblici, aziende e grandi catene di vendita **non** richiedono informazioni personali attraverso e-mail, sms, social media o chat: quindi, meglio **evitare** di fornire dati personali, soprattutto di tipo bancario, attraverso tali canali. Se si ricevono messaggi sospetti, è bene **non** cliccare sui link in essi contenuti e **non** aprire eventuali allegati, che potrebbero contenere virus o programmi *trojan horse* capaci di prendere il controllo di pc e smartphone. Spesso dietro i nomi di siti apparentemente sicuri o le URL abbreviate che si trovano sui social media si nascondono link a contenuti **non sicuri**. Una **piccola accortezza consigliata** è quella di posizionare sempre il puntatore del mouse sui link prima di cliccare: in molti casi si potrà così leggere in basso a sinistra nel browser il vero nome del sito cui si verrà indirizzati.

2. OCCHIO AGLI INDIZI

I messaggi di phishing sono progettati per ingannare e spesso utilizzano imitazioni realistiche dei loghi o addirittura delle pagine web ufficiali di banche, aziende ed enti. Tuttavia, capita spesso che contengano anche **grossolani errori** grammaticali, di formattazione o di traduzione da altre lingue. E' utile anche **prestare attenzione al mittente** (che potrebbe avere un nome vistosamente strano o eccentrico) o al suo indirizzo di **posta elettronica** (che spesso appare un'evidente imitazione di quelli reali). Meglio diffidare **dei messaggi con toni intimidatori**, che ad esempio contengono minacce di chiusura del conto bancario o di sanzioni se non si risponde immediatamente: possono essere subdole **strategie per spingere il destinatario a fornire informazioni personali**.

3. PROTEGGERSI MEGLIO

E' utile installare e tenere aggiornato sul pc o sullo smartphone un programma **antivirus** che **protegga anche dal phishing**. Programmi e gestori **di posta elettronica** hanno spesso **sistemi di protezione** che indirizzano automaticamente nello **spam** la maggior parte dei messaggi di phishing: è bene controllare che siano attivati e verificarne le impostazioni. Meglio non **memorizzare dati personali e codici di accesso nei browser** utilizzati per navigare online. In ogni caso, è buona prassi **impostare password alfanumeriche complesse**, cambiandole spesso e scegliendo credenziali diverse per ogni servizio utilizzato: banca online, e-mail, social network, ecc. *[vedi anche la scheda del Garante con i consigli per gestire le password in sicurezza]*, a meno di disporre di sistemi di autenticazione forte (*strong authentication*).

4. ACQUISTI ONLINE IN SICUREZZA

Se si fanno acquisti online, è più prudente usare **carte di credito prepagate** o altri sistemi di pagamento che permettono di **evitare** la condivisione di dati del conto bancario o della carta di credito.

5. LA PRUDENZA NON E' MAI TROPPA

Per proteggere conti bancari e carte di credito è bene **controllare spesso le movimentazioni** e attivare **sistemi di *alert*** automatico che avvisano l'utente di ogni operazione effettuata. Nel caso si abbia il dubbio di essere stati vittime di phishing è consigliabile **contattare direttamente** la banca o il gestore della carta di credito attraverso i **canali di comunicazione conosciuti e affidabili**.

Per segnalazioni e richieste di ulteriori informazioni: urp@gpdp.it

SPAM: COME DIFENDERSI

Spamming* o *spam è l'invio, talora massiccio e ripetuto, tramite operatore o con modalità automatizzate, di **comunicazioni non richieste** (via telefono, *e-mail*, fax, sms o mms), senza che il destinatario abbia ricevuto un'**informativa** sul trattamento dei dati personali o abbia prestato il **consenso** a ricevere messaggi. Negli ultimi tempi, lo *spamming* sta interessando anche il mondo dei *social network* e quello dei sistemi di messaggistica per *smartphone* e *tablet*.
Lo ***spammer*** - cioè colui che invia lo *spam* - utilizza riferimenti (*e-mail*, numeri telefonici, ecc.) per l'invio di messaggi promozionali spesso raccolti in modo non lecito o in maniera automatica via Internet (su gruppi *Usenet*, *newsgroups*, *forum*, ecc.), mediante speciali programmi (*spambot*, ecc.) o, più semplicemente, facendo invii massivi a caso ad indirizzi *e-mail* basati sull'uso di nomi comuni
Scopo dello *spamming* è veicolare messaggi pubblicitari, ma tale pratica è legata anche a veri e propri tentativi di truffa, come il *phishing*. In Italia l'invio di messaggi automatizzati a fini promozionali non desiderati è soggetto a sanzioni amministrative e penali.

Come prevenire lo spam?

- **Non diffondere**, soprattutto *on-line*, il tuo indirizzo e-mail o il numero di telefono fisso o mobile;
- Se per ottenere un dato servizio (iscrizione a *newsletter*, acquisti *on-line*, ecc.) devi firmare un documento o iscriverti ad un sito web, **leggi sempre con attenzione le regole privacy e le condizioni d'uso del servizio**, e soprattutto verifica le modalità e le finalità del trattamento dei tuoi dati personali;
- Prendi in considerazione di **utilizzare più indirizzi *e-mail*** per le tue varie esigenze. Ad esempio, potresti crearne uno ad uso **esclusivamente** "commerciale", da impiegare per fare acquisti *on-line*, accedere a servizi su Internet, iscriverti a *newsletter*, ecc.. In questo modo, il rischio di «contagio spam» non coinvolgerebbe gli indirizzi di posta elettronica che utilizzi invece per le tue esigenze quotidiane più importanti (lavoro, amicizia, ecc.);
- Se hai un sito personale o un blog su cui vuoi pubblicare la tua *e-mail*, proteggila con accorgimenti che rendono la vita più difficile ai programmi (*i cosiddetti spider*) capaci di raccogliere in automatico gli indirizzi di posta elettronica per finalità di *spamming*;
- Se invii una *e-mail* a molti destinatari, **non rendere visibili gli indirizzi dei tuoi contatti** e usa la funzione *"destinatario in copia conoscenza nascosta (ccn)"*. Stessa precauzione se frequenti dei *newsgroups*, dove possono essere attivi dei programmi *spider* ;
- Prova ad usare i **filtri *anti-spam*** offerti, ad esempio, da alcuni programmi di posta elettronica, che possono aiutarti a bloccare tutti i messaggi provenienti da un particolare indirizzo. Tali funzioni possono essere disponibili anche per i *social network* e i servizi di messaggistica per *smartphone* e *tablet*;
- **Mantieni in efficienza il tuo pc,** scaricando periodicamente gli aggiornamenti (che contengono anche difese *anti-spam*) per il sistema operativo e gli applicativi più utilizzati, e installa eventualmente un programma *anti-virus* che offra anche una protezione *anti-spam*;
- **Se utilizzi i social network**:
  1) controlla le impostazioni privacy del tuo *account* eventualmente limitando la visibilità del tuo profilo;
  2) se disponibile, utilizza la funzione *"di blocco"* per i soggetti che inviano messaggi indesiderati;
  3) non dare l'amicizia a soggetti sconosciuti;
  4) evita di rendere pubblici sulla tua pagina personale il tuo indirizzo *e-mail* o il numero di cellulare.

Cosa non devi fare

- **Non rispondere allo *spam***: la risposta può consentire allo *spammer* di stabilire che il tuo indirizzo *e-mail* è valido e attivo. Così può continuare a «spammarti» o rivendere il tuo indirizzo verificato a terzi. Può anche tentare di utilizzare il contatto creato per portare avanti tentativi di truffa.
- **Non cliccare su eventuali link** per la cancellazione dell'invio e tantomeno non fornire i tuoi dati personali senza aver prima fatto delle verifiche. Questi link potrebbero essere collegati a sistemi che consentono truffe telematiche e furti di identità, ma potrebbero anche aprire la strada a *software spia* o a virus informatici. Per la stessa ragione, **non devi mai cliccare su collegamenti ipertestuali** inseriti nel corpo del testo o **aprire ed eseguire eventuali allegati**, soprattutto se contengono estensioni tipo «.exe». Per la stessa ragione, se non sei sicuro del mittente, evita di scaricare le immagini eventualmente contenute nel corpo del messaggio *e-mail*.

Differenze tra spam e invii leciti

- Se il contatto e-mail o telefonico è stato **raccolto** con il **consenso del destinatario** o secondo le **modalità previste dalla legge** (es: nell'ambito di un contratto per la fornitura di un qualche servizio), non si può parlare di *spam*.
- In ogni caso, **se le comunicazioni pubblicitarie o altro tipo richieste** (es: invio di *newsletter*, ecc.) **risultano ad un certo punto indesiderate**, è tuo diritto opporti al trattamento dei tuoi dati inviando una *e-mail* al mittente per chiedere la sospensione dell'invio o utilizzando, se disponibili, le procedure *on-line* per la cancellazione dei tuoi dati dal *database* di chi ti invia le comunicazioni.

Come agire contro lo spam?

Se sei una persona fisica puoi:
- presentare segnalazioni, reclami e ricorsi al Garante per la protezione dei dati personali
- rivolgerti al giudice ordinario per l'eventuale risarcimento del danno

Se sei una persona giuridica:
- puoi rivolgerti al giudice ordinario per il risarcimento del danno
- **non** puoi fare segnalazioni, reclami e ricorsi al Garante, che può però intervenire d'ufficio

Le indicazioni del Garante per tutelare la tua privacy quando usi smartphone e tablet

Non ci pensiamo quasi mai, forse. Smartphone e tablet ci accompagnano ovunque e custodiscono parti importanti e spesso delicate delle nostre vite, sotto forma di foto, filmati, messaggi e dati telematici. E noi stiamo sempre attenti a proteggere adeguatamente queste informazioni con piccole ma utili precauzioni?

In un video-tutorial il Garante per la protezione dei dati personali offre alcune utili indicazioni per tutelare la nostra privacy quando utilizziamo smartphone e tablet.

Attenzione ai dati conservati su smartphone e tablet

Non conservare su smartphone e tablet informazioni troppo personali che potrebbero essere smarrite o rubate, o perfino clonate o attaccate da pirati elettronici. Non si dovrebbero mai conservare, ad esempio, password personali, codici di accesso e dati bancari in chiaro.

Ricorda, poi, che smartphone e tablet venduti, regalati o buttati possono contenere ancora dati privati. Se te ne liberi, quindi, **cerca di adottare alcune piccole precauzioni di sicurezza** come:

- ripristinare le impostazioni di fabbrica
- rimuovere la scheda SIM e la scheda di memoria
- eliminare tutti i backup contenuti nella memoria.

Proteggi i tuoi dati

Se vuoi evitare che qualcuno legga di nascosto le tue e-mail e i tuoi sms o che usi a tua insaputa il tuo smartphone o il tuo tablet, usa alcune precauzioni.

Imposta sempre un codice PIN abbastanza complicato, evitando, ad esempio, di usare il tuo nome e cognome, la data di nascita, il nome dei figli o quello del gatto di casa, o comunque altre parole che ti renderebbero in qualche modo riconoscibile.

Magari imposta anche un **codice di blocco**, quello che si attiva automaticamente quando il cellulare è acceso ma non viene utilizzato per un po' di tempo. E anche in questo caso, evita codici un po' troppo facili da scoprire.

Alcuni sistemi operativi consentono anche di impostare password di sicurezza che bloccano completamente l'accesso ai dati personali. Per farlo, basta collegare smartphone e tablet con il pc e utilizzare il software per la gestione del prodotto.

Conserva con cura il codice IMEI, che trovi sulla scatola del prodotto che acquisti e che in caso di furto o smarrimento puoi utilizzare per bloccare a distanza l'accesso al tuo smartphone o tablet.

Quando navighi su smarthone e tablet

Se ti connetti a Internet e ai social network via smartphone e tablet, **verifica le impostazioni privacy e leggi le condizioni d'uso dei servizi**.

Per navigare sul web, inoltre, **installa sempre - se disponibile - software di sicurezza anti-virus informatici o contro le intrusioni da parte di pirati telematici e ladri d'identità digitali**.

Quando usi connessioni wi-fi gratuite, ad esempio nei locali pubblici, **verifica che la navigazione sia protetta con protocolli di scambio dati criptati** e che l'autenticazione ai siti che eventualmente vengono visitati utilizzi il **protocollo Https**. In caso contrario, se si utilizzano credenziali di accesso a siti e servizi come la posta elettronica o l'home banking, il rischio che non ci siano adeguate garanzie di sicurezza per i propri dati è reale.

APP-rova di privacy

Se scarichi delle applicazioni, **evita le fonti sconosciute e utilizza sempre i market ufficiali**, a meno che tu non sia in grado di valutare autonomamente l'affidabilità della fonte - ad esempio leggendo i commenti eventualmente lasciati dagli altri utenti - per comprendere se ci sono eventuali rischi o problematiche.

Una volta installata un'applicazione, verifica se richiede **l'accesso a contenuti presenti sul tuo smartphone o sul tuo tablet** (ad esempio, le tuo foto o i contatti in rubrica) e leggi con attenzione le **condizioni d'uso del servizio**, soprattutto per evitare di dover pagare servizi non richiesti o di vedere esposte oltremisura informazioni di carattere personale (ad esempio: foto, video, contatti, ecc.).

Occhio allo spam

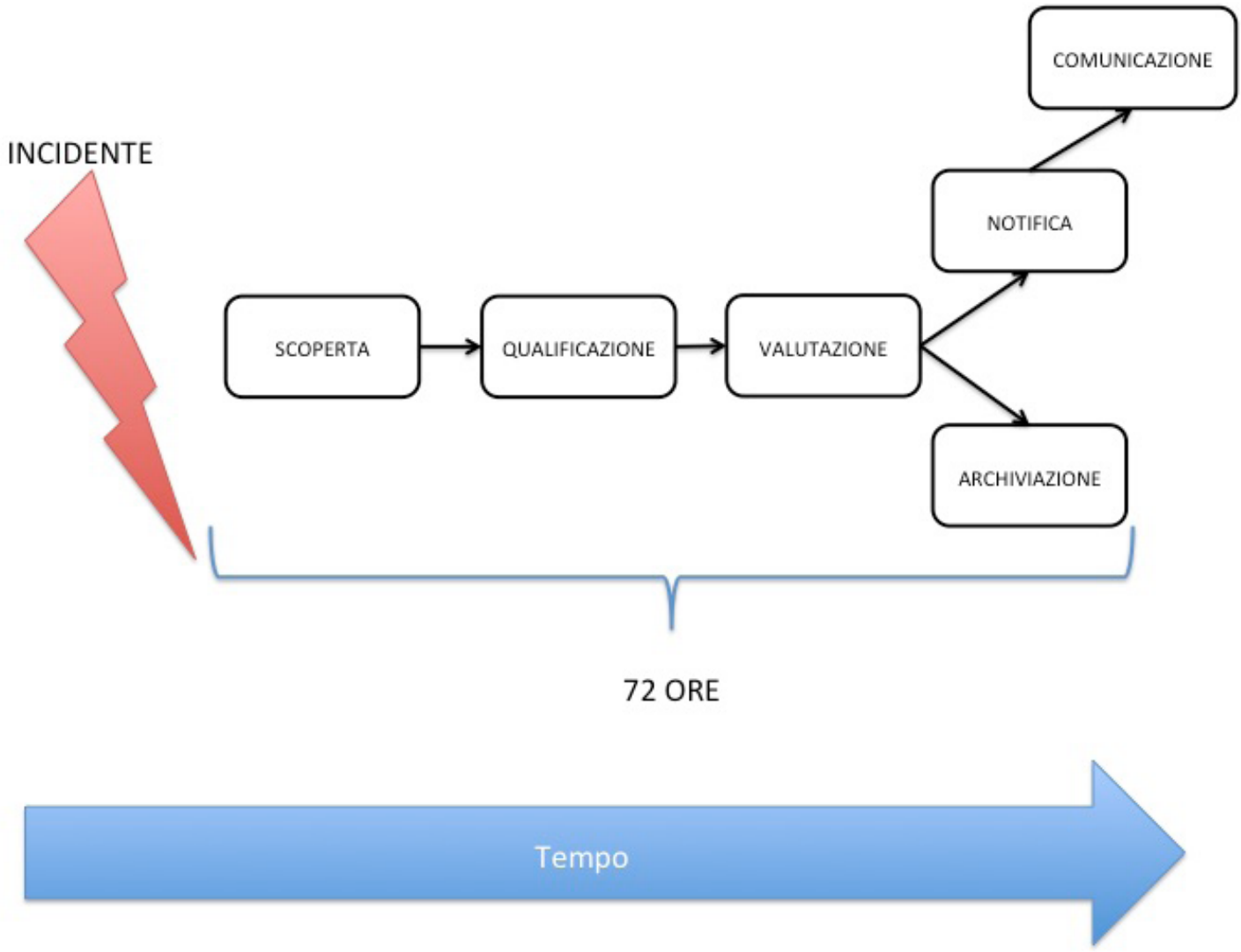
Smartphone e tablet sono terreno di caccia per lo spam.

Attenzione ai link presenti in e-mail, sms e messaggistica istantanea, perché, in alcuni casi, cliccandoli, potresti inconsapevolmente accettare di ricevere comunicazioni indesiderate, divenendo bersaglio di messaggi pubblicitari non richiesti da cui, poi, può anche essere abbastanza difficile liberarsi.

Vuoi sempre far sapere dove sei?

Smartphone e tablet hanno **funzioni di geolocalizzazione**, ma sei tu a decidere se, quando e chi può conoscere la tua posizione.
Per **disabilitare la geolocalizzazione**, puoi disattivare - controllando le impostazioni dello smartphone o tablet - il GPS o la connessione wi-fi quando non usi questi servizi o altri ad essi collegati.

E' bene, inoltre, controllare anche le **impostazioni di geolocalizzazione dei servizi di social network** che eventualmente utilizzi su smartphone o tablet. La scelta finale di far sapere o meno dove sei, in fin dei conti, è sempre la tua.


INCIDENTE
SCOPERTA
QUALIFICAZIONE
VALUTAZIONE
NOTIFICA
COMUNICAZIONE
ARCHIVIAZIONE
72 ORE
Tempo

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Scheda aggiornata in base alla versione delle Linee guida del WP29 emendata e adottata il 5 aprile 2017

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. Non sono richieste attestazioni formali o l'iscrizione ad appositi albi professionali, anche se la partecipazione a master e corsi di studio/professionali può rappresentare un utile strumento per valutare il possesso di un livello adeguato di conoscenze.
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** .

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: www.garanteprivacy.it/rpd

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

PRIVACY SHIELD
Lo Scudo per la privacy fra Ue e USA

L'accordo detto *Privacy Shield* fra Ue e USA **impone alle imprese americane obblighi più stringenti** di tutela dei dati personali degli europei. E' in linea con quanto chiesto dalla Corte di giustizia dell'Ue, che aveva invalidato il precedente accordo detto «Safe Harbor», ossia «Porto sicuro». Il *Privacy Shield* prevede che le autorità americane **vigilino e assicurino con più forza** sul rispetto dell'accordo e che collaborino in misura maggiore con le Autorità europee per la protezione dei dati. L'accordo contiene - ed è la prima volta - dichiarazioni e impegni assunti formalmente per quanto riguarda **l'accesso ai dati da parte di soggetti dell'Amministrazione americana**.

Gli elementi fondamentali del nuovo accordo

SETTORE COMMERCIALE
Obblighi stringenti per le imprese e rigide misure di attuazione
- Più trasparenza
- Meccanismi di controllo del rispetto delle regole da parte delle imprese
- Sanzioni o esclusione dai benefici dell'accordo per le imprese che non lo rispettano
- Condizioni più rigide per trasferire i dati a destinatari ulteriori

ACCESSO AI DATI DA PARTE DELL'AMMINISTRAZIONE USA
Precise garanzie e obblighi di trasparenza
- Per la prima volta, l'Amministrazione USA ha garantito formalmente che l'accesso delle autorità pubbliche ai dati personali sarà soggetto a limiti, garanzie e meccanismi di controllo specifici e definiti
- Le Autorità USA affermano che non vi saranno attività di sorveglianza indiscriminata o massiva
- Le imprese potranno dichiarare il numero approssimativo di richieste di accesso ricevute
- Disponibile un nuovo strumento di tutela giuridica attraverso il cosiddetto «difensore civico» (*Ombudsperson)* creato per il *Privacy Shield* : un soggetto indipendente incaricato di ricevere e decidere i reclami presentati dagli interessati

STRUMENTI DI TUTELA GIURIDICA
Vi sono diverse possibilità per far valere i propri diritti
- **Rivolgersi direttamente all'impresa**, che deve rispondere, in caso di reclamo da parte di un interessato, entro 45 giorni
- **Utilizzare un meccanismo di ADR** (Risoluzione alternativa delle controversie), gratuito
- **Rivolgersi all'Autorità di protezione dati**, che collaborerà con il *Department of Commerce* e la *Federal Trade Commission* degli USA per garantire accertamenti sui reclami ancora pendenti presentati da cittadini Ue e giungere rapidamente alla loro definizione
- **Rivolgersi al Privacy Shield Panel** (Collegio arbitrale del *Privacy Shield*) per ottenere, se nessun'altra soluzione si è rivelata praticabile, una decisione esecutiva attraverso un meccanismo di arbitrato

MONITORAGGIO
Revisione annuale congiunta del funzionamento dell'Accordo
- Monitoraggio del funzionamento del *Privacy Shield* e del rispetto degli impegni assunti dagli USA anche con riguardo all'accesso ai dati per finalità di polizia e giustizia o di sicurezza nazionale
- La revisione sarà condotta dalla Commissione europea e dal *Department of Commerce* USA con il coinvolgimento di esperti dei servizi di sicurezza americani e delle Autorità europee per la protezione dei dati
- Previsto un vertice annuale, con la partecipazione di ONG e altri soggetti interessati, dedicato agli sviluppi nel settore della normativa privacy negli USA e al relativo impatto sugli europei
- La Commissione europea presenterà una relazione pubblica al Parlamento e al Consiglio, basandosi sui risultati della revisione annuale congiunta e su altre informazioni pertinenti (ad esempio, le relazioni sulla trasparenza presentate dalle imprese)

IN PRATICA

Le imprese americane
- Autocertificheranno su base annuale il rispetto degli obblighi
- Dovranno pubblicare una *privacy policy* (informativa privacy) sul loro sito
- Dovranno rispondere tempestivamente ai reclami
- Dovranno collaborare con le Autorità europee per la protezione dei dati e dare seguito alle loro richieste (se trattano dati relativi al personale/alle risorse umane)

Gli interessati in Europa
- Godranno di più trasparenza rispetto ai trasferimenti di dati personali negli USA e di una tutela rafforzata per questi dati
- Avranno a disposizione strumenti di tutela giuridica più facili da utilizzare e meno costosi in caso di reclami, che potranno gestire da soli oppure con l'aiuto dell'Autorità nazionale di protezione dei dati

FONTE: traduzione italiana di un *factsheet* della Commissione Europea DG Giustizia - anno 2016

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Scheda aggiornata in base alla versione delle Linee guida del WP29 emendata e adottata il 5 aprile 2017

Il diritto alla portabilità dei dati

La scheda presenta il diritto alla portabilità dai dati in relazione a quanto previsto dal Regolamento (UE) 2016/679 e dalle Linee-guida del WP29

COSA È?

È un diritto innovativo previsto dall'articolo 20 del regolamento (Ue) 2016/679 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 a un altro titolare** del trattamento senza impedimenti.

QUALI VANTAGGI PUO' OFFRIRE?

- **facilitare il passaggi**o da un fornitore di servizi all'altro;
- consentire la **creazione di nuovi servizi** nel quadro della strategia dell'Ue 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 o un *cloud* privato in vista di un utilizzo ulteriore per scopi personali, senza trasmetterli necessariamente a un altro titolare *(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 *(es.: un diverso fornitore di servizi).*

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

- **continuare a fruire del servizio** offerto dal titolare anche dopo un'operazione di portabilità;
- **esercitare il diritto di cancellazione** *(o «diritto all'oblio»)* ai sensi dell'art. 17 del regolamento.

QUANDO TROVA APPLICAZIONE?

Per essere portabili i dati devono:

- essere **dati personali chiaramente riferibili all'interessato**. Sono quindi ad esempio esclusi i dati anonimi;
- essere **trattati sulla base del consenso preventivo** dell'interessato o di un **contratto** di cui è parte l'interessato;
- essere **trattati attraverso strumenti automatizzati**. Sono quindi esclusi gli archivi e registri cartacei;
- essere stati **forniti consapevolmente** e in modo attivo dall'interessato *(ad es., i dati di registrazione inseriti compilando un modulo online, come indirizzo postale, nome utente, età, ecc.*).
- Sono compresi anche i **dati osservati forniti dall'interessato attraverso la fruizione di un servizio o l'utilizzo di un dispositivo** *(es.: la cronologia delle ricerche effettuate dall'interessato, i dati relativi al traffico, i dati relativi all'ubicazione, dati grezzi come la frequenza cardiaca registrata da dispositivi sanitari o di fitness.)*

Il diritto alla portabilità **non si applica** invece ai «dati inferenziali» né ai «dati derivati» *(es.: l'esito di una valutazione concernente la salute di un utente o il profilo creato al fine di attribuire uno score creditizio o di ottemperare a normativa antiriciclaggio).*

L'esercizio del diritto alla portabilità **non deve ledere i diritti e le libertà altrui**.

I dati portabili **devono essere forniti in un formato «interoperabile»**, ossia in un formato che ne consenta il riutilizzo. I titolari potranno utilizzare formati di impiego comune, se già esistenti, oppure utilizzare formati aperti (es. XML), ovvero sviluppare formati interoperabili e strumenti informatici che consentano di estrarre i dati pertinenti.

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

Codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato a fini di informazione commerciale

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

La scheda illustra in sintesi le regole più rilevanti fissate dal nuovo Codice di deontologia [doc. web n. 4298343], che entrerà in vigore il 1° ottobre 2016 ed è rivolto alle società che raccolgono e offrono informazioni sull'affidabilità commerciale di imprenditori e manager.

UTILIZZO DEI DATI

Sono utilizzabili **senza il consenso** degli interessati:

- **i dati provenienti da "fonti pubbliche"**, come pubblici registri, elenchi, documenti conoscibili da chiunque: bilanci, informazioni contenute nel registro delle imprese presso le Camere di commercio, atti immobiliari e altri atti c.d. pregiudizievoli, come l'iscrizione di ipoteche o la trascrizione di pignoramenti, decreti ingiuntivi o altri atti giudiziari;
- **i dati estratti da "fonti pubblicamente e generalmente accessibili da chiunque"**, come le testate giornalistiche cartacee o digitali, le informazioni attinte da elenchi telefonici, da siti web di enti pubblici o di altre autorità di vigilanza e controllo.

Sono inoltre utilizzabili **i dati personali** che il soggetto ha **liberamente** deciso di comunicare al fornitore di informazioni commerciali.

Gli operatori dovranno

- utilizzare **solo** dati **pertinenti, non eccedenti** l'attività di informazione commerciale e **sempre aggiornati**;
- **annotare sempre la fonte** da cui hanno tratto i dati personali sulla persona censita.

I **dati giudiziari** della persona censita potranno essere trattati solo se già disponibili in **archivi pubblici** o in altre **fonti pubblicamente accessibili**.
Se tali informazioni sono tratte da un **una testata giornalistica,** non possono risalire a più **di 6 mesi prima**.

INFORMATIVA E RISCONTRO AGLI INTERESSATI

Tutte le società del settore dovranno fornire una informativa completa sul proprio sito web.

Inoltre, le società di informazioni commerciali di maggiori dimensioni hanno provveduto alla costituzione di un portale unico (https://www.informativaprivacyancic.it) nel quale saranno inserite tutte informazioni per verificare i dati relativi agli interessati.

E' previsto l'**obbligo** per gli operatori del settore di garantire un riscontro telematico, tempestivo e completo, alle richieste di **accesso ai dati personali** avanzate dalle persone censite.

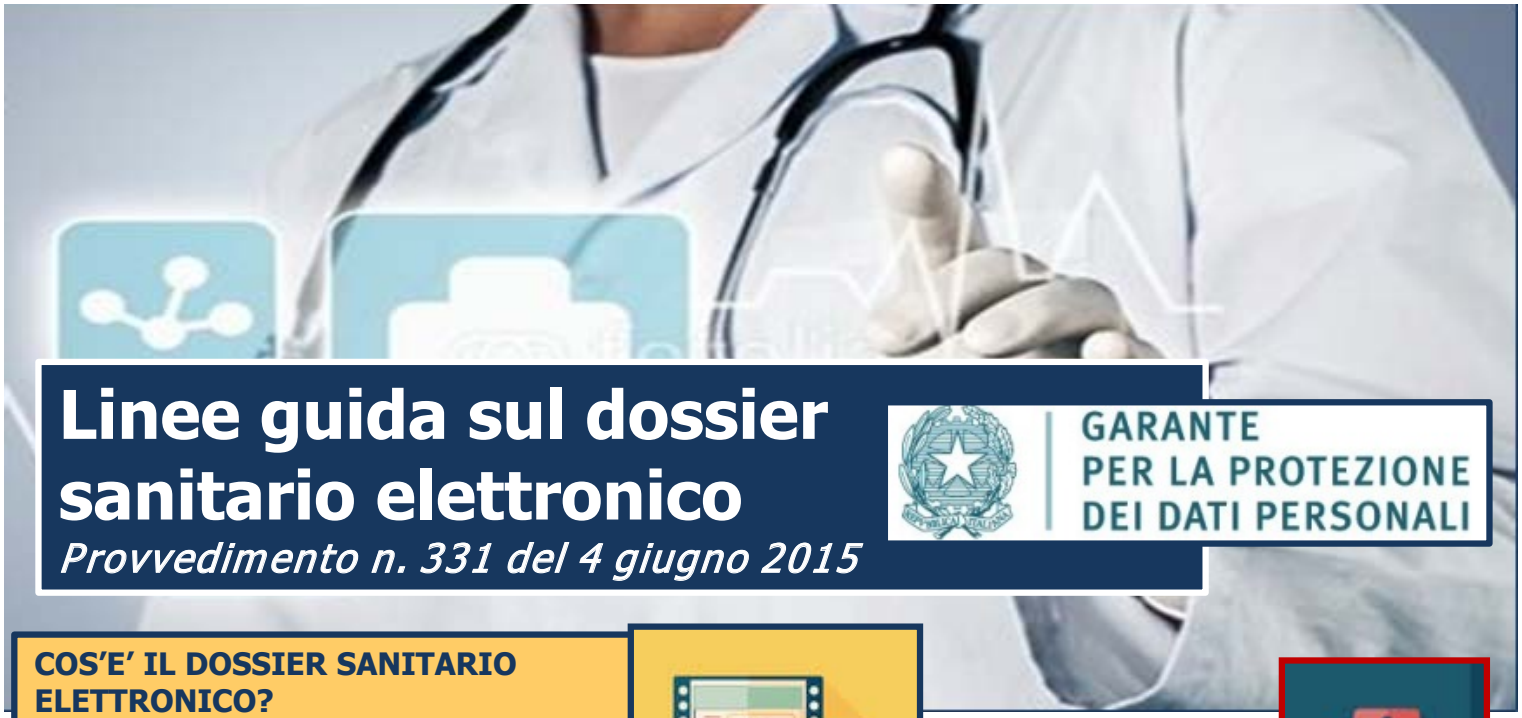
CONSERVAZIONE DEI DATI

I dati potranno essere conservati solo per **periodi di tempo ben definiti** e nei limiti della conoscibilità, dell'utilizzabilità e della pubblicità degli stessi, previsti dalle normative di riferimento.

In particolare, le informazioni relative ai fallimenti e alle altre procedure concorsuali possono essere conservate per un periodo di tempo **non superiore a 10 anni** dalla data di apertura della procedura di fallimento.

Le società dovranno adottare **misure per garantire la sicurezza, l'integrità e la riservatezza** delle informazioni commerciali.

La scheda ha mere finalità divulgative
Per ulteriori informazioni, consultare il sito: www.garanteprivacy.it



Linee guida sul dossier sanitario elettronico

Provvedimento n. 331 del 4 giugno 2015

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

COS'E' IL DOSSIER SANITARIO ELETTRONICO?

Il **dossier sanitario elettronico** è lo strumento costituito presso un'unica struttura sanitaria (ospedale, azienda sanitaria, casa di cura) che raccoglie informazioni sulla salute di un paziente al fine di documentarne la **storia clinica** presso quella **singola struttura** e offrirgli un migliore processo di cura.
Si differenzia dal **fascicolo sanitario elettronico** in cui invece confluisce l'intera storia clinica di una persona generata **da più strutture sanitarie**.

LE LINEE GUIDA

Con il **provvedimento del 4 giugno 2015**, il Garante per la protezione dei dati personali ha varato le nuove **Linee guida** che puntano a definire un quadro di riferimento unitario per il corretto trattamento dei dati raccolti nei dossier, già istituiti o che si intendono istituire, da parte di strutture sanitarie pubbliche e private.

LE PRINCIPALI INDICAZIONI A TUTELA DEI PAZIENTI

- ai pazienti deve essere consentito di **scegliere**, in piena libertà, se **far costituire o meno il dossier sanitario**
- in **assenza del consenso** il medico avrà a disposizione solo le informazioni rese in quel momento dal paziente o in precedenti prestazioni fornite dallo stesso professionista
- la mancanza del consenso **non** deve incidere minimamente sulla **possibilità di accedere** alle cure richieste
- per poter inserire nel dossier **informazioni particolarmente delicate** (infezioni Hiv, interventi di interruzione volontaria della gravidanza, dati relativi ad atti di violenza sessuale o pedofilia) sarà necessario un **consenso specifico**
- per consentire al paziente di scegliere in maniera libera e consapevole, la struttura sanitaria dovrà informarlo in modo chiaro, indicando in particolare, chi avrà accesso ai suoi dati e che tipo di operazioni potrà compiere.

LE PRINCIPALI PRESCRIZIONI PER I TITOLARI DEL TRATTAMENTO

La struttura sanitaria deve

- garantire al paziente **l'esercizio dei diritti riconosciuti dal Codice privacy** (accesso ai dati, integrazione, rettifica, etc.) e la possibilità di conoscere il reparto, la data e l'orario in cui è avvenuta la consultazione del suo dossier
- garantire al paziente la possibilità di **"oscurare"** alcuni dati o documenti sanitari che non intende far confluire nel dossier
- adottare **elevate misure di sicurezza**. I dati sulla salute dovranno essere separati dagli altri dati personali, e dovranno essere individuati criteri per la cifratura dei dati sensibili. L'accesso al dossier sarà consentito solo al personale sanitario coinvolto nella cura. Ogni accesso e ogni operazione effettuata, anche la semplice consultazione, saranno tracciati e registrati automaticamente in appositi file di log che la struttura dovrà conservare per almeno 24 mesi.
- **comunicare al Garante eventuali violazioni di dati o incidenti informatici (*data breach*)** entro quarantotto ore dalla conoscenza del fatto.

Per ulteriori informazioni, consultare il provvedimento del Garante del 4 giugno 2015 [doc. web n. 4084632] oppure contattare l'URP del Garante: www.garanteprivacy.it/home/urp

Consigli per rispettare la privacy se si usa un DRONE a fini ricreativi

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI
A TUTELA DI UN DIRITTO FONDAMENTALE

1. SEGUI SEMPRE LE REGOLE

Usare i droni per scopi ricreativi è lecito e divertente, ma occorre sempre **rispettare la privacy degli altri** e informarsi bene sulle **regole previste dall'ENAC** per far volare i Sistemi Aeromobili a Pilotaggio Remoto *(www.enac.gov.it)*.

2. FAI ATTENZIONE ALLE RIPRESE

Se si fa volare a fini ricreativi un drone munito di fotocamera in un **luogo pubblico** (parchi, strade, spiagge) è meglio **evitare di invadere gli spazi personali e l'intimità delle persone**. La diffusione di riprese realizzate con il drone (sul web, sui social media, in chat) può avvenire **solo con il consenso** dei soggetti ripresi, fatti salvi particolari usi connessi alla libera manifestazione del pensiero, come quelli a fini giornalistici. Negli altri casi, quando è eccessivamente difficile raccogliere il consenso degli interessati, è possibile diffondere le immagini **SOLO se i soggetti ripresi non sono riconoscibili**, o perché **ripresi da lontano**, o perché si sono utilizzati appositi software per oscurare i loro volti. Occorre poi **evitare** di riprendere e diffondere immagini che contengono **dati personali come targhe di macchine, indirizzi di casa, ecc**. Le riprese che violano gli **spazi privati altrui** (casa, giardino domestico) sono invece **SEMPRE da evitare**, anche perché si potrebbero violare norme penali.

3. RISPETTA GLI ALTRI

La presenza di un drone che effettua riprese nelle vicinanze può dare la **sensazione di essere osservati**, inducendo disagio e influenzando il normale comportamento delle persone. E' quindi buona regola usare questi strumenti **senza invadere la sfera personale degli altri**, magari anche comunicando preventivamente le proprie intenzioni. Ad esempio, se si vuole far volare un drone per riprendere una festa nel proprio giardino di casa, sarebbe bene prima avvisare i vicini, che hanno il diritto di chiedere di **non** essere - anche **solo inavvertitamente** - ripresi nel loro privato. Un'altra buona pratica da seguire è quella di fare in modo che il **pilota** del drone sia **sempre ben visibile,** così da non suscitare sospetti o allarme negli altri.

4. NON DIVENTARE UN «ORECCHIO INDISCRETO»

Non si possono usare droni per captare **volontariamente** conversazioni altrui. Eventuali **frammenti di conversazione** registrati in modo **accidentale** possono essere utilizzati (ad esempio, per pubblicare un video online) **SOLO** se **NON** rendono riconoscibile il contesto, cioè il contenuto dei discorsi e le persone coinvolte.

5. A PROVA DI PRIVACY

In base a quanto previsto dal nuovo Regolamento europeo in materia di protezione dei dati personali (Regolamento UE 2016/679), i droni, come tutti i dispositivi elettronici, devono rispettare i principi di **privacy by design** e **privacy by default**. Cioè devono essere costruiti e configurati per raccogliere meno dati possibile.

6. COME TUTELARE LA TUA PRIVACY

Se è possibile individuare il pilota del drone, si possono chiedere a lui informazioni su come intende utilizzare le riprese ed eventualmente **negare il consenso** al trattamento dei dati raccolti, specie se sono previste forme di diffusione delle immagini. **E nel caso si ritenesse di essere stati vittime di violazioni della propria privacy**, ci si può rivolgere al Garante per la protezione dei dati personali o, in alternativa, all'Autorità giudiziaria.

La scheda ha finalità meramente divulgative e sarà aggiornata in base agli sviluppi tecnologici e normativi

2016 General Data Protection Regulation

Prepararsi all'arrivo del nuovo Regolamento Europeo sulla Data Protection in 9 passi

01 Consapevolezza

Le figure chiave all'interno dell'azienda dovranno essere pronte a recepire i cambiamenti.

02 Informazioni

Controllare le tipologie e la qualità delle informazioni e le modalità di condivisione dei dati.

03 Informative

Verificare i contenuti e la struttura delle informative fornite agli interessati.

04 Diritti dell'interessato

Verificare il rispetto dei diritti degli interessati: cancellazione/modifica dei dati, accesso, portabilità e formati dicondivisione.

05 Fondamento Giuridico

Gestione in linea con le nuove normative e senza eccedere le finalità di raccolta che dovranno essere adeguatamente documentate.

06 Consenso

Rivedere le modalità di richiesta del consenso e di verifica dell'età dell'interessato.

07 Data Breach

Implementare i processi necessari per individuare, comunicare e investigare gli illeciti.

08 Privacy by design e valutazione di impatto

Familiarizzare con la valutazione di impatto e progettare i nuovi processi nell'ottica della privacy by design.

09 Data Protection Officer

Adottare se necessario la figura del data protection officer e capire se questa figura dovrà essere interna o esterna all'impresa.

PHARMONY
empower your sales!

info@pharmony.it pharmonyservices.com

COME ADEGUARSI AL GDPR IN 9 PUNTI

1

Valutazione della compliance

Raccolta e analisi delle informazioni sull'organizzazione aziendale

2

Creazione del registro dei trattamenti

Un registro delle attività di trattamento svolte sotto la responsabilità del titolare del trattamento.

3

Stesura/Modifica della documentazione

Tutta la documentazione deve necessariamente essere aggiornata e completa

4

Individuazione dei ruoli e delle responsabilità

5

Definizione delle politiche di sicurezza e valutazione dei rischi

Espressione del concetto di accountability

6

Processo di Data Breach

Al fine di assicurarsi di aver adottato tutte le procedure idonee a scoprire eventuali violazioni

7

Valutazione d'impatto sulla protezione dei dati personali

Consente di valutare gli aspetti relativi alla protezione dei dati, prima che questi vengano trattati

8

Implementazione dei processi per l'esercizio dei diritti dell'interessato

Al fine di assicurarsi di aver adottato tutte le procedure idonee a scoprire eventuali violazioni

9

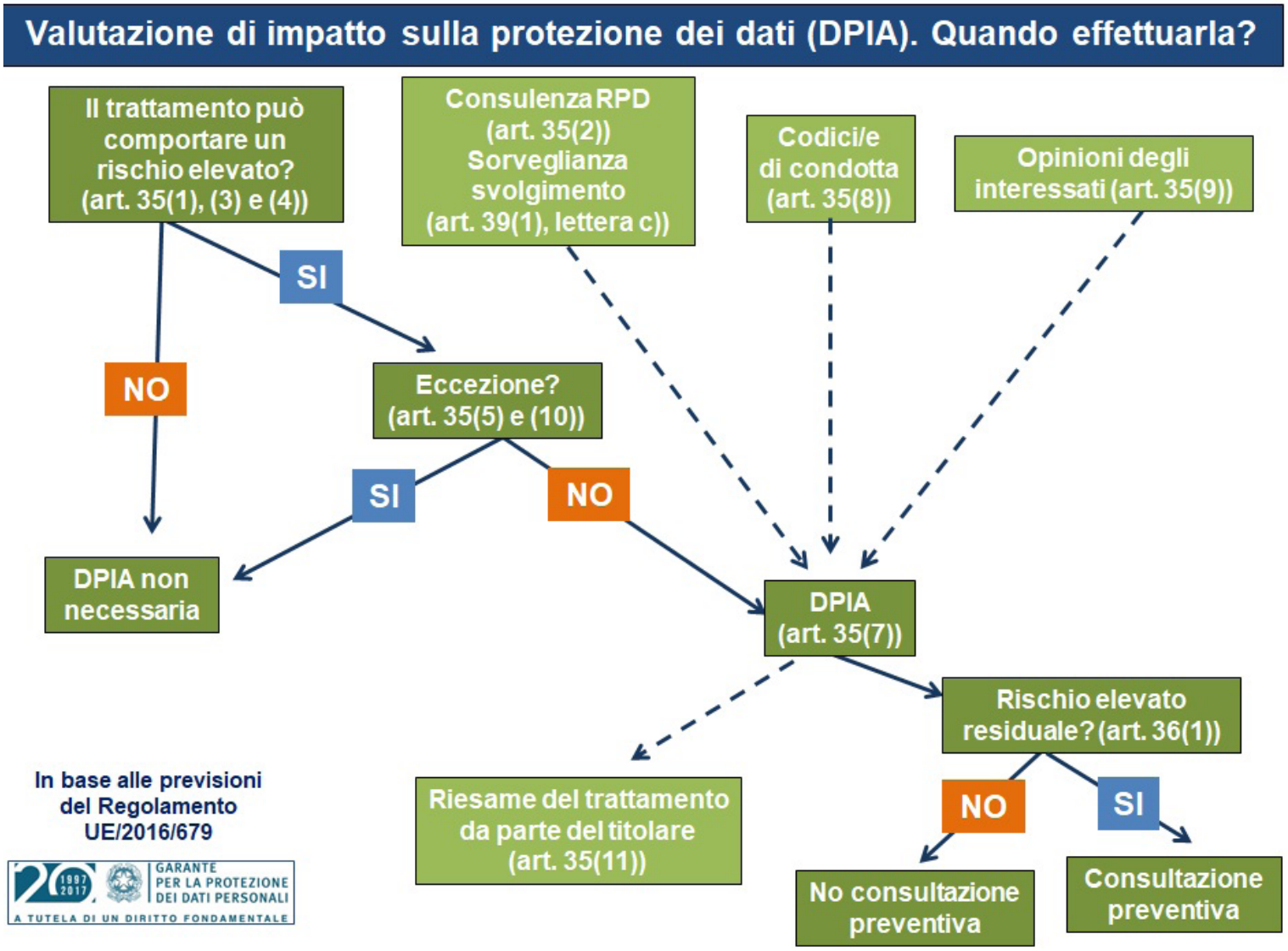
Individuazione e nomina di un Data Protection Officer

La sua responsabilità principale è quella di osservare, valutare e organizzare la gestione del trattamento di dati personali.

Informazioni da www.agendadigitale.eu

AD CONSULTING

Valutazione di impatto sulla protezione dei dati (DPIA). Quando effettuarla?



In base alle previsioni del Regolamento UE/2016/679

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI
A TUTELA DI UN DIRITTO FONDAMENTALE

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Il tuo sito/blog installa cookie? Cosa devi fare

IMPORTANTE: per una corretta interpretazione degli adempimenti previsti, si raccomanda la consultazione del **Provvedimento del Garante dell'8 maggio 2014** e dei **«Chiarimenti in merito all'attuazione della normativa in materia di cookie»**. I documenti sono disponibili su www.garanteprivacy.it/cookie

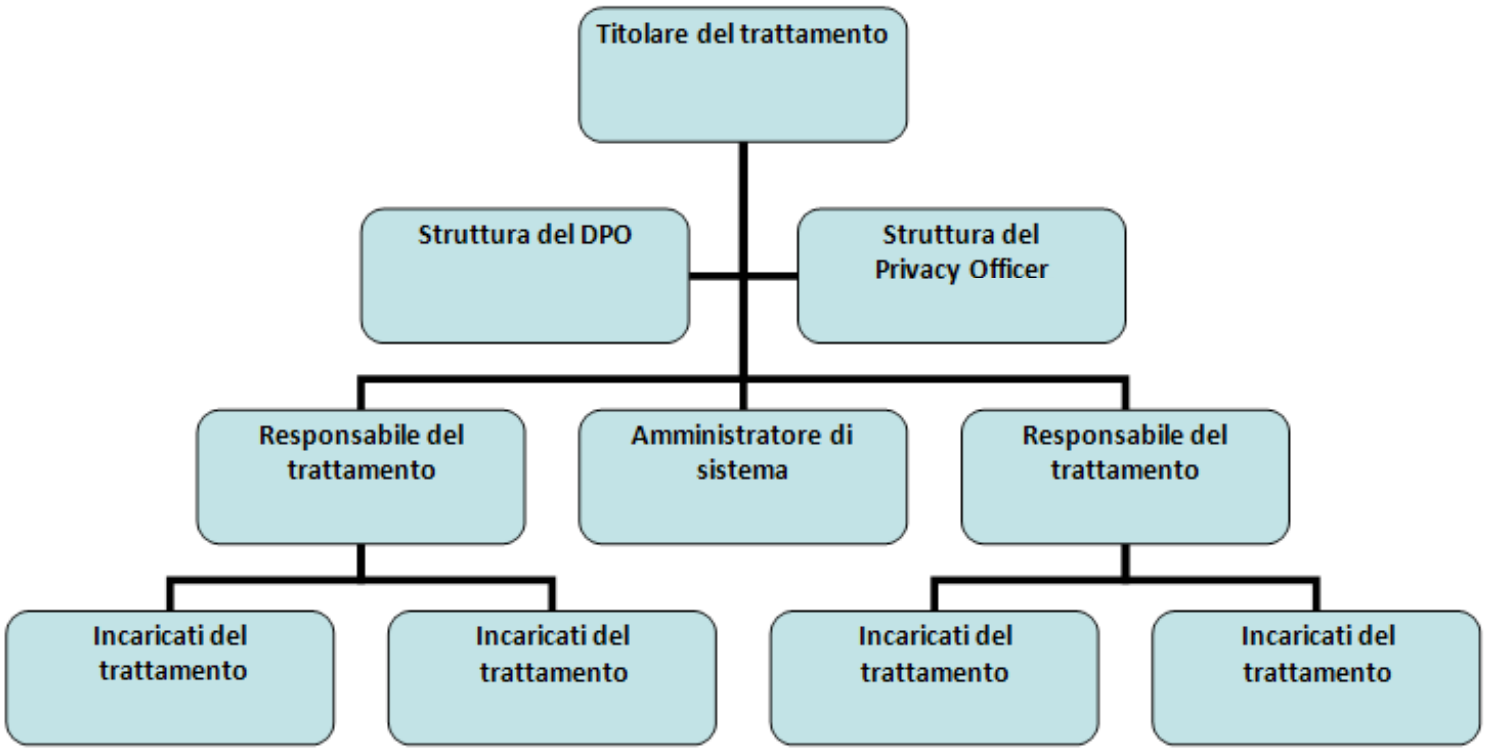
CHE TIPO DI COOKIE INSTALLI?	Segnalarli nell'informativa Art .2, par. 5, Direttiva 2009/136/CE e art. 122, comma 1, Codice privacy	Inserire il banner e richiedere il consenso ai visitatori Art .2, par. 5, Direttiva 2009/136/CE e art. 122, comma 1, Codice privacy	Notificare al Garante Art. 37, comma 1, lett. d), Codice privacy
Nessun cookie	✗	✗	✗
Tecnici o analitici prima parte	✓	✗	✗
Analitici terze parti (se sono adottati strumenti che riducono il potere identificativo dei cookie e la terza parte non incrocia le informazioni raccolte con altre di cui già dispone) – vedi punto 2 dei «Chiarimenti in merito all'attuazione della normativa in materia di cookie»	✓	✗	✗
Analitici terze parti (se **NON** sono adottati strumenti che riducono il potere identificativo dei cookie e la terza parte non incrocia le informazioni raccolte con altre di cui già dispone) – vedi punto 2 dei «Chiarimenti in merito all'attuazione della normativa in materia di cookie»	✓	✓	✓
Di profilazione prima parte	✓	✓	✓
Di profilazione terze parti	✓	✓	✗

LEGENDA: ✓ adempimento previsto ✗ adempimento non previsto

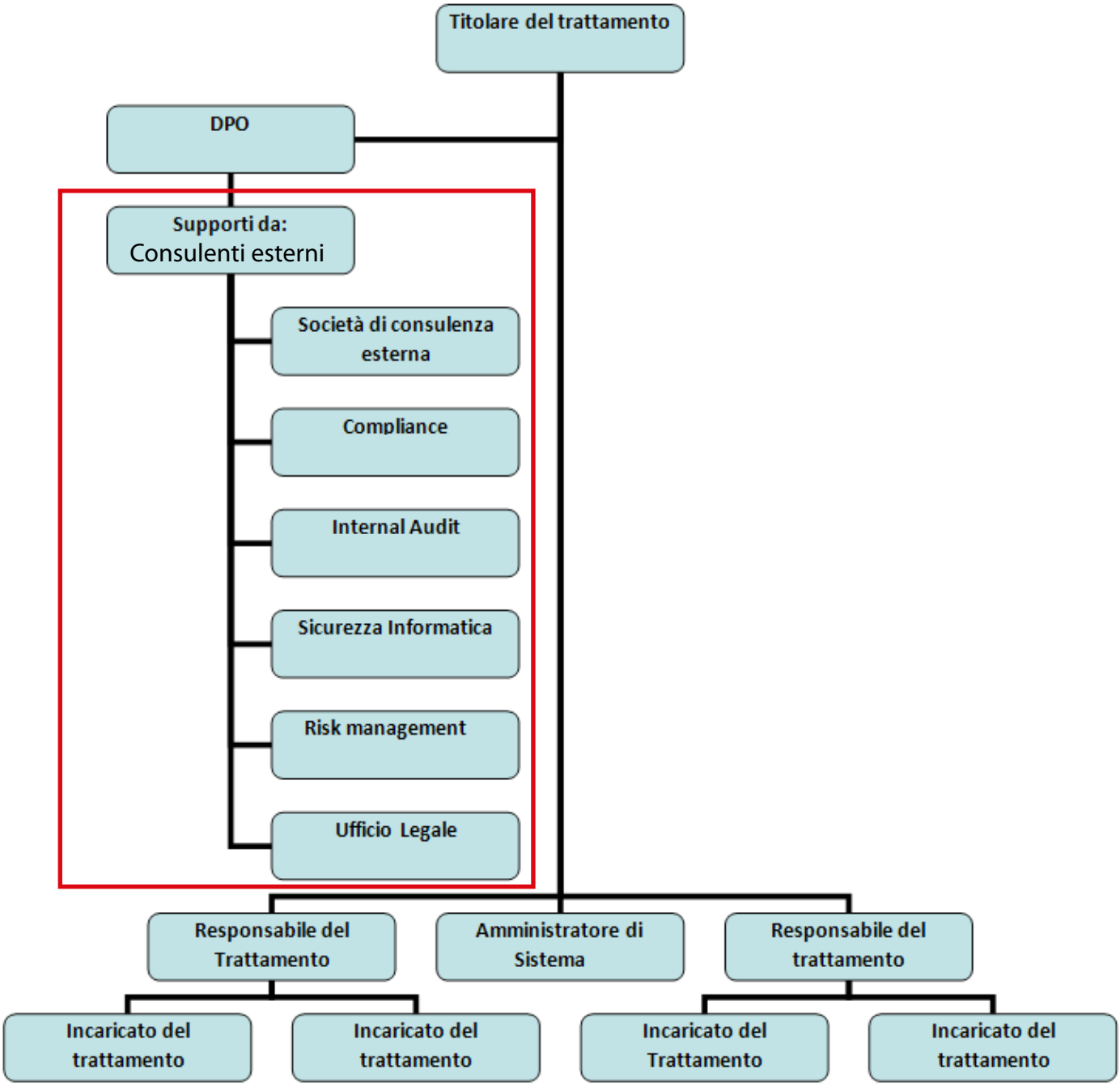
ⓘ La notificazione è a carico del soggetto terza parte che svolge l'attività di profilazione

Esempi di organigramma aziendale

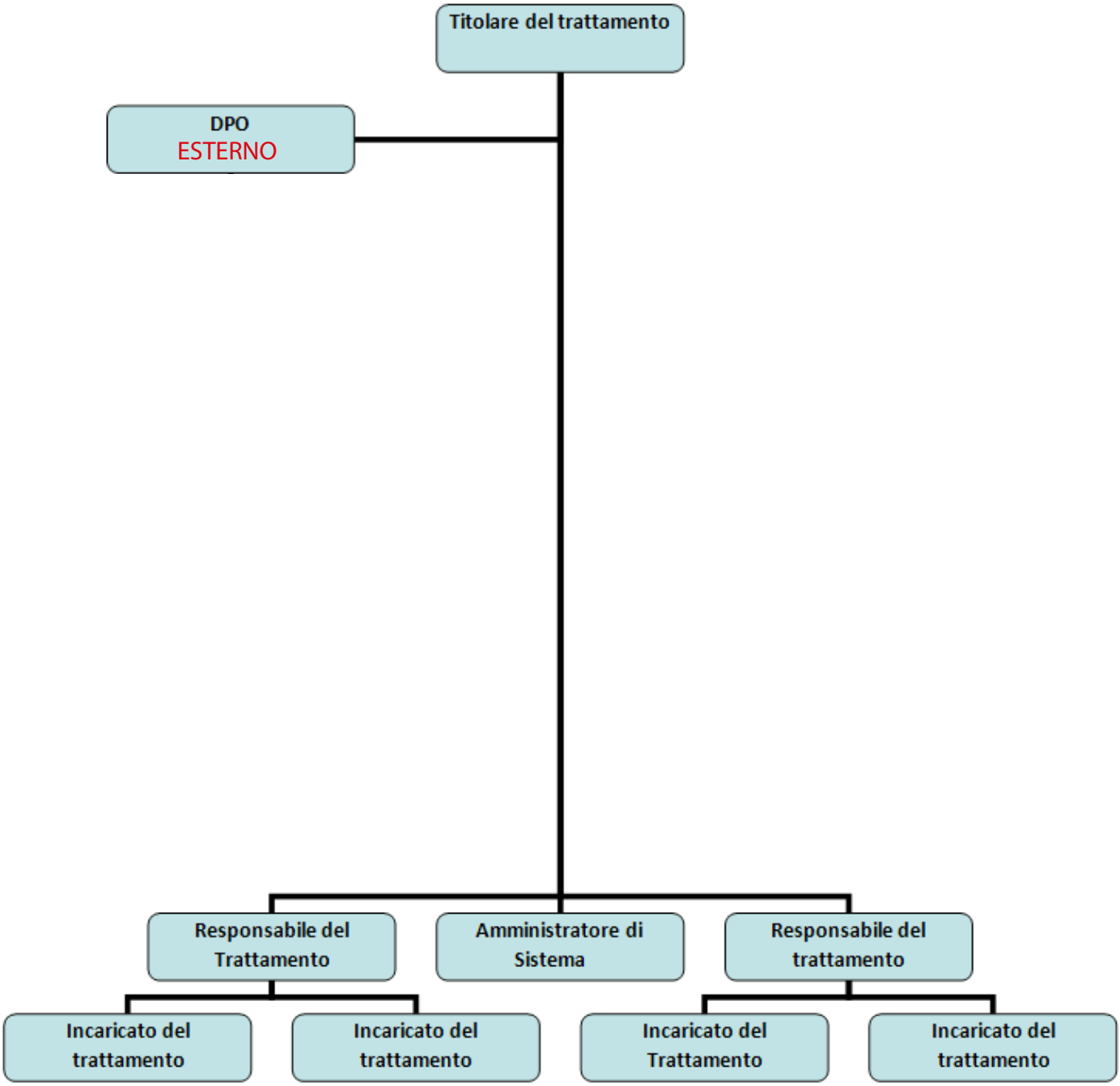
Organigramma con DPO di una "grande impresa"



Organigramma con DPO in aziende medio /grandi



Organigramma con DPO esterno



Vuoi un **aiuto**
per la compliance al

Contattaci!!

Omega Computer srl

Home Page: http://www.omegacomputer.it
E-mail: **info@omegacomputer.it**
Tel. +39 348 3226888

Servizi offerti
alla nostra clientela

- Consulenza Informatica Aziendale
- Assistenza Hardware e Software
- Archiviazione Documentale
- Compliance GDPR

- Servizi IT
- Progetti Web
- Posizionamento siti