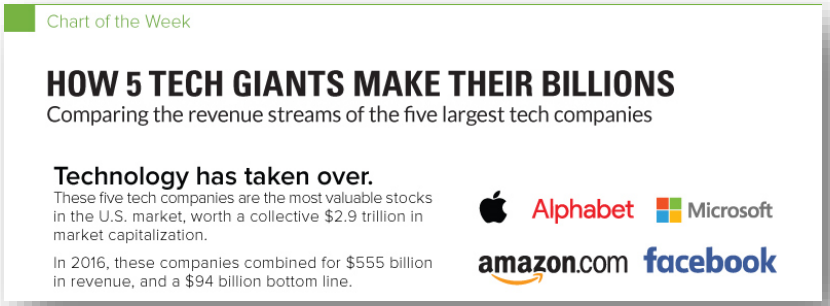
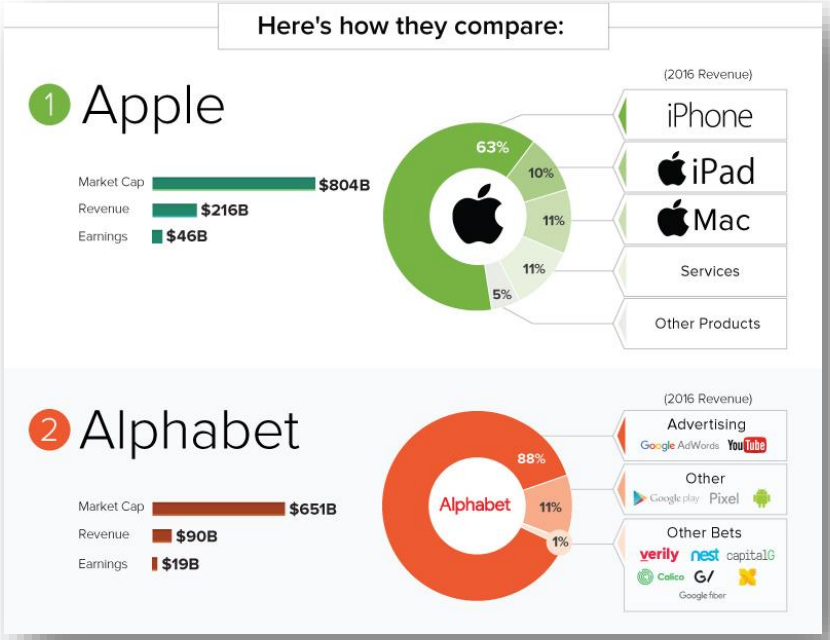
Regolamento Europeo 2016/679

27 OTTOBRE 2018





Privacy = **The right to be let alone**

Diritto al rispetto della propria vita privata e familiare

Privacy = **Data Protection**

Diritto alla protezione dei dati personali

Direttiva UE 95/46

«Tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati»

Legge n. 675 del 31 dicembre 1996

"Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali»

Decreto Legislativo n. 196/2003

"Codice della protezione dei dati personali", entrato in vigore il 1 gennaio 2004, con ss.mm.

Decreto Legislativo n.101/2018

"Disposizioni per l'adeguamento delle normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento Europeo [...]!, entrato in vigore il 19 settembre 2018

Applicazione:
25 maggio 2018

2016 2017 2018 2019 2020

Entrata in vigore:
27 aprile 2016

Prima relazione:
20 maggio 2020

A decorrere dal 25 maggio 2018 :

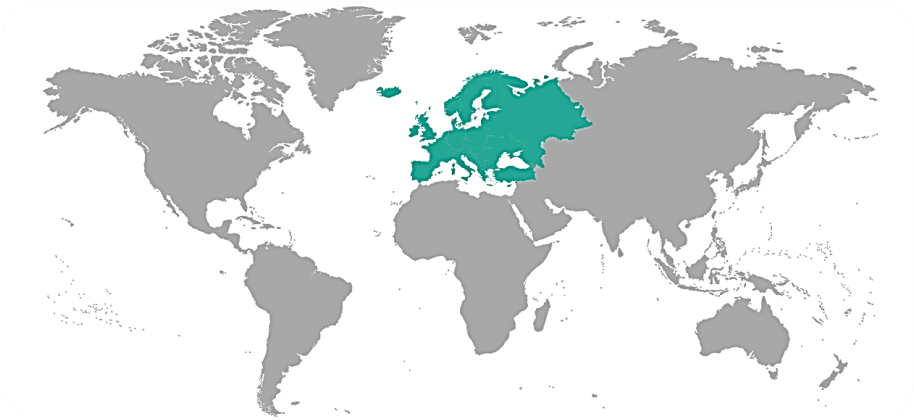
- il GDPR è **obbligatorio** in tutti i suoi elementi nonché direttamente applicabile in ciascuno degli Stati Membri dell'Unione Europea.
- Dalla stessa data è **abrogata la Direttiva 95/46/CE** che disciplinava a livello comunitario il trattamento dei dati.
- Pertanto, le disposizioni precedentemente in vigore contenute nel Codice della Privacy D. lgs. 196/2003 che si pongano in **contrasto** con il Regolamento Europeo devono essere disapplicate.
- L'articolo 13 della legge di delegazione europea, legge 163/2017 entrata in vigore il 21 novembr e 2017, ha **delegato il governo** ad emanare le norme di dettaglio.
- Il **D. Lgs. n. 101 del 10 agosto 2018, in vigore dal 19 settembre 2018**, ha modificato il Codice al fine di adeguarlo alle disposizioni introdotte dal GDPR.

Il regolamento si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali di persone fisiche contenuti in un archivio o destinati a figurarvi.

Sono esclusi i trattamenti effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico.

Ambito Territoriale di applicazione:

- il titolare o il responsabile è stabilito nell'UE, anche se il trattamento avviene in territorio extra UE
- se l'interessato si trova in territorio UE



DATO PERSONALE (art. 4):

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

TRATTAMENTO (art. 4):

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

TITOLARE del TRATTAMENTO (art. 4) (7):

la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, **determina le finalità e i mezzi del trattamento di dati personali**; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

RESPONSABILE del TRATTAMENTO (art. 4) (8):

la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che **tratta dati personali per conto del titolare del trattamento**

INTERESSATO del TRATTAMENTO (art. 4) (1):

- La persona fisica identificata o identificabile cui si riferiscono i dati personali

- d.lgs. 196/2003: il Garante ha chiarito (Registro dei provvedimenti n. 262 del 20 settembre 2012) che, a seguito delle modifiche al Codice apportate nel 2012, tutte le disposizioni del Codice che riguardano gli interessati ovvero il trattamento di dati personali è stata limitata in via esclusiva alle persone fisiche ed ai trattamenti di informazioni personali che vi si riferiscono

- Considerando 27: **Il regolamento non si applica ai dati personali delle persone decedute.** Gli Stati membri possono prevedere norme riguardanti il trattamento dei dati personali delle persone decedute

PERSONA AUTORIZZATA AL TRATTAMENTO

La figura dell' *incaricato* (prevista dall'art. 30 Codice Privacy (D. lgs. 196/2003) non è espressamente prevista dal GDPR 2016/679, ma è compatibile con il medesimo in quanto fa riferimento a «**persone autorizzate al trattamento** dei dati sotto l'autorità diretta del titolare o del responsabile» (art. 4, n. 10, GDPR)

RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI (RPD)
o DATA PROTECTION OFFICER (DPO) (artt. 37-39):

Nuova figura introdotta dal GDPR 2016/679

È un soggetto indipendente avente funzione di garanzia della conformità al Regolamento della circolazione e della protezione dei dati.

Devono designare obbligatoriamente un **DPO**:

- 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 DPO

Il DPO può essere costituito attraverso un contratto di servizio esterno all'azienda.

Deve essere competente nei tre ambiti richiesti dal GDPR:

- Ambito Tecnico
- Ambito Organizzativo
- Ambito Giuridico

NOVITÀ RISPETTO ALLA DISCIPLINA DEL CODICE DELLA PRIVACY (D. LGS. 196/2003)

La normativa non prevede specifici adempimenti necessari e sufficienti per ritenersi in linea con le prescrizioni previste.
Il GDPR indica le finalità da raggiungere, lasciando al titolare del trattamento il compito di definire in concreto le attività da porre in essere.

Accountability, ossia «*responsabilità*» di titolari e responsabili (accountable), sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento.

Viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali , nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel regolamento.

Responsabilità del titolare del trattamento

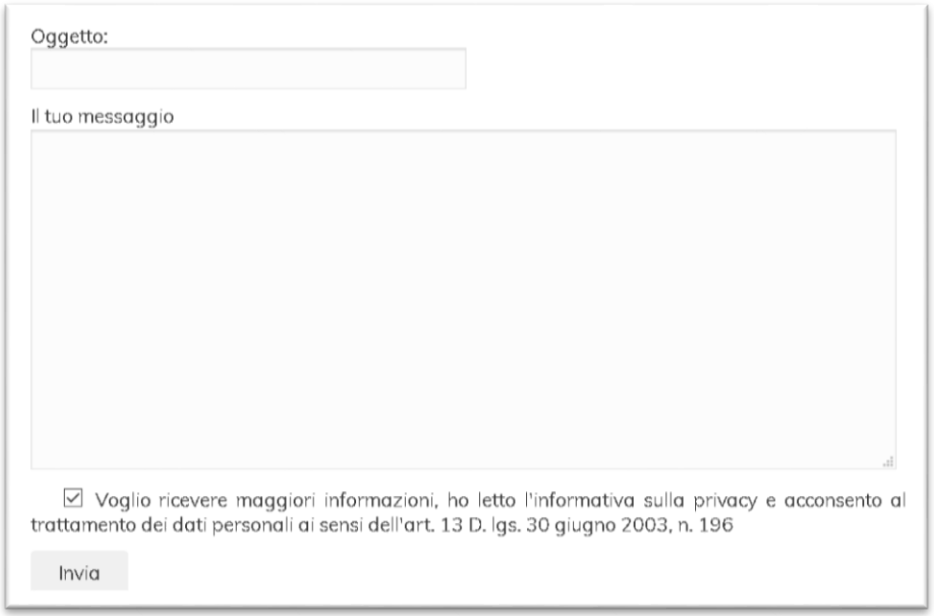
1. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.

Data Protection by Design, ossia la gestione del trattamento dei dati a partire dalla fase di «*progettazione*» in conformita` al GDPR, compresa la scelta dei mezzi per effettuare il trattamento (software), oltre che alle modalità di trattamento in sè.

Data Protection by Default, ossia la gestione del trattamento dei dati in conformita` al GDPR per impostazione predefinita, in modo che sia gestito solo il numero di informazioni necessarie per ogni specifica finalità di trattamento.

Esempio:

«La nostra società si dotata di tutti gli strumenti software e delle competenze necessarie allo svolgimento di tutti gli adempimenti obbligatori»



SICUREZZA DEI DATI (art. 32 GDPR)

Per garantire la **Sicurezza del Trattamento** dei dati, «il titolare del trattamento e il responsabile del trattamento mettono in atto **misure tecniche e organizzative** adeguate per garantire un livello di sicurezza adeguato al rischio»

Pertanto le «adozione di '**misure minime**' di sicurezza» (ex art. 33 Codice) non valgono più al fine di dimostrare l'adempimento richiesto in termini di sicurezza del trattamento.

Le misure di sicurezza sia tecniche che organizzative, devono essere adeguate al rischio della specifica realtà aziendale.

Codice in materia di protezione dei dati personali
B. Disciplinare tecnico in materia di misure minime di sicurezza
(Artt. da 33 a 36 del Codice)

La sicurezza dei dati consegue a:

- una adeguata **valutazione del rischio**

  Es.: eventualità di distruzione accidentale o illegale, perdita, modifica, rivelazione o accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati.
  Valutare gravità del rischio ed interessi coinvolti

- **alla realizzazione di misure per limitare tali rischi**

  Es.: pseudonimizzazione e cifratura; sistemi per assicurare integrità e resilienza dei sistemi; procedure per testare periodicamente efficacia delle misure di sicurezza adottate.

Valutazione del rischio ed adozione di misure adeguate tengono conto di:

- stato dell'arte
- costi di attuazione,
- natura, oggetto, contesto e finalità del trattamento,

-rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

Art. 32 § 3 l'adesione a un **codice di condotta** o a un **meccanismo di certificazione** approvato può essere utilizzata come elemento per dimostrare la conformità ai requisiti di sicurezza

Art. 32 VALUTAZIONE DEI RISCHI DEL TRATTAMENTO

Obbligatoria per tutti i titolari ed i responsabili del trattamento.

Art. 35 VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI (Data Protection Impact Assessment – DPIA)

Obbligatoria quando il trattamento può comportare un **rischio elevato per i diritti e le libertà delle persone interessate, prima di procedere al trattamento**

Valutazione del rischio → Rischio elevato → Valutazione d'impatto sulla protezione dei dati - DPIA

Registri delle attività di Trattamento:

- **Registro del Titolare**
- **Registro del Responsabile**

da tenere in forma scritta (anche in formato elettronico) contenenti la mappatura dei trattamenti operati sui dati.

Alcune informazioni da tracciare:

- Riferimenti dei titolari e responsabili
- Misure di sicurezza tecniche ed organizzative
- Finalità di trattamento
- Categoria dei dati
- Categoria degli interessati
- Categoria dei destinatari
- Termini di retention del dato per ogni categoria
- Categorie di attività di trattamento

Gli **obblighi** di tenuta dei registri **non si applicano** alle imprese o organizzazioni con meno di 250 dipendenti, a meno che:

- il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato
- il trattamento non sia occasionale
- Il trattamento includa categorie particolari di dati di cui all'art. 9, par. 1 - e cioè dati sensibili e biometrici - o i dati personali relativi a condanne penali e a reati.

Formazione del personale

Art. 29 e art. 32 § 4 GDPR

Il responsabile del trattamento e chiunque agisca sotto l'autorità del titolare e/o del responsabile del trattamento **non può trattare dati se non è istruito in tal senso** (salvo eccezioni di legge).

ART. 39 § 1.B: il RPD/DPO controlla che siano adempiuti i doveri di formazione in capo al titolare del trattamento.

Basi Giuridiche

1) Consenso
2) Adempimento di obblighi contrattuali
3) Obblighi di legge cui è soggetto il titolare del trattamento
4) Interessi vitali della persona interessata
5) Legittimo interesse prevalente del titolare
6) Interesse pubblico o esercizio di pubblici poteri

App fake

Android, l'invasione delle app maligne: ne fioccano 350 all'ora, 3,5 milioni all'anno

I dati di una ricerca G Data mettono sull'allerta gli utenti di dispositivi che montano il sistema operativo di Big G, quasi 9 su 10 al mondo: i software fasulli servono solo come cavalli di Troia per diffondere malware o prendere il controllo del telefono

App fake

R.it Social Network

Home | News | Speciali | Mobile | Social Network | Sicurezza | Prodotti | Interattivi | Video

WhatsApp, occhio al fake: un milione di download per la finta app

Pretexting

Sempre più cyberspioni: si fa largo la minaccia del 'pretexting'

Lo dimostra il rapporto annuale dell'azienda americana Verizon Enterprise Solutions. In aumento soprattutto i ransomware, ossia richieste di riscatto per sbloccare dispositivi infettati da virus

Software fake

WIRED.IT Sezioni | Wired Next Fest | Gallery | Video

HOT TOPIC MOLESTIE CATALOGNA INFLUENZA LUCCA COMICS & GAMES FINTECH GOOGLE STRANGER THINGS SMARTPHONE... VEDI TUTTI

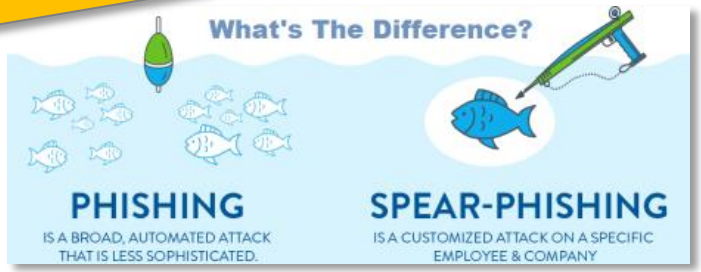
Windows Movie Maker, il programma fake è una truffa

di Alessio Caprodossi
Giornalista
10 NOV, 2017

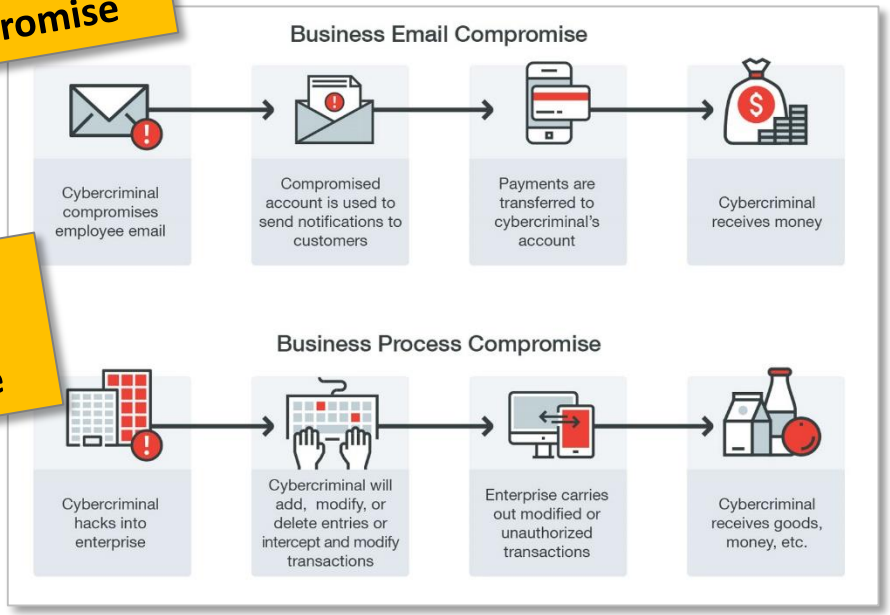
L'applicazione per realizzare videoclip è stata rimossa dallo store ufficiale ma rilanciata da truffatori che chiedono trenta dollari per il download. Tanti gli utenti caduti nel tranello, grazie anche all'ottima indicizzazione su Google

Ransomware

Spear - Phishing



Business Email Compromise



Phishing

Business Process Compromise

Data Breach colpisce Wind Tre. Garante Privacy 'L'azienda deve avvertire tutti i 5mila clienti coinvolti'

Il Garante Privacy ha ordinato a Wind Tre di informare tutte le oltre 5mila potenziali vittime di furto dati personali del data breach che ha colpito l'azienda.

Data Breach a Facebook, 90 milioni di utenti coinvolti. Cosa è successo

1 ottobre 2018 | Europa

Per l'attacco hacker più grande della sua storia e peggiore di Cambridge Analytica, **Facebook** rischia una multa di 1,4 miliardi di euro dall'Unione europea. È la sanziona massima a cui potrebbe andare incontro il social network per il "security breach" comunicato venerdì scorso, qualora il regolatore europeo accertasse una violazione da parte della compagnia guidata da **Mark Zuckerberg** del Regolamento generale in materia di protezione dei dati.

NAVIGA HOME RICERCA — 24 ORE TECNOLOGIA — ABBONATI ACCEDI

PRODOTTI BUSINESS STARTUP WEB SOCIAL SICUREZZA & PRIVACY APP VIDEOGIOCHI SCIENZA INFODATA NÒVA

Il dato è mio e lo controllo sempre io | Banche, piano Npl in quattro mosse | Amazon ci prova: Alexa sugli occhiali intelligenti? | Oltre tre milioni di euro (da UniCredit e altre banche) per...

SICUREZZA & PRIVACY

Il caso Unicredit e l'obbligo a denunciare gli attacchi hacker (con la nuova normativa)

–di Alessandro Curioni * | 26 luglio 2017

VIDEO

18 maggio 2017
Pagare con il telefonino: come cambieranno le abitudini degli italiani dopo #ApplePay

Yahoo hack: 1bn accounts compromised by biggest data breach in history

The latest incident to emerge – which happened in 2013 – is probably distinct from the breach of 500m user accounts in 2014

A laptop computer bearing the LinkedIn logo. Photograph by David Paul Morris—Bloomberg via Getty Images

CHANGING FACE OF SECURITY

LinkedIn Lost 167 Million Account Credentials in Data Breach

Robert Hackett
May 18, 2016

PRIMA DEL GDPR

Art. 32-bis Codice Privacy

Provvedimento del Garante n. 161 del 04/04/2013
Regolamento UE 611/13

- Comunicazione al Garante entro 24 ore dalla scoperta dell'evento
- Informazione a ciascun utente coinvolto entro 3 giorni dalla scoperta dell'evento (a meno che vi sia cifratura e anonimizzazione)

- ❑ **SOCIETÀ TELEFONICHE ED INTERNET PROVIDER**
- ❑ **BIOMETRIA** (Provv. Garante n. 513 del 12/11/2014)
- ❑ **DOSSIER SANITARIO ELETTRONICO** (Provv. Garante n. 331 del 04/06/2015)
- ❑ **AMMINISTRAZIONI PUBBLICHE** (Provv. Garante n. 392 del 02/07/2015)

COSA CAMBIA CON IL GDPR

Il Regolamento generalizza l'obbligo di notificazione del DataBreach estendendolo a tutti i titolari di trattamento (artt. 33-34 GDPR)

A partire dal 25 maggio 2018, TUTTI i titolari devono:

- **notificare al Garante** le violazioni di dati personali di cui vengano a conoscenza **entro 72 ore** e comunque "senza ingiustificato ritardo", ma soltanto se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati

- comunicare all'interessato la violazione dei dati personali senza indebito ritardo, in caso di **rischio elevato per i diritti e le libertà** della persona fisica, al fine di consentirgli di prendere le precauzioni necessari

In tutti i casi, occorre tenere una documentazione su qualsiasi violazione dei dati personali, le sue conseguenze e i provvedimenti adottati per porvi rimedio.

Tutela dei diritto dell'interessato

- Reclamo al Garante della Privacy
- Ricorso dinanzi all'autorità giurisdizionale

Risarcimento

Art. 82, paragrafo 1:

"Chiunque subisca un danno materiale o immateriale causato da una violazione del presente Regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento»

Non è esclusa responsabilità ex art. 2050 c.c. dell'incaricato o dell'autorizzato al trattamento

Sanzioni amministrative

Il Garante della Privacy ha il potere di imporre sanzioni amministrative a seguito del riscontro di violazioni alla disciplina normativa di tutela della privacy.
L'ammontare massimo di tali sanzioni, a seconda della disposizione violata, varia da € 10.000.000,00 ad € 20.000.000,00, ovvero in percentuale, dal 2 al 4% del fatturato mondiale totale annuo dell'esercizio precedente.

Sanzioni penali

Gli Stati membri possono stabilire disposizioni relative a sanzioni penali per violazioni del Regolamento, comprese violazioni di norme nazionali adottate in virtù ed entro i limiti del Regolamento.

BBC Sign in News Sport Weather Shop Reel Travel

NEWS

Home Video World UK Business Tech Science Stories Entertainment & Arts

World Africa Asia Australia Europe Latin America Middle East US & Canada

GDPR: US news sites unavailable to EU users under new rules

25 May 2018 Share

c|net BEST PRODUCTS REVIEWS NEWS VIDEO HOW TO SMART HOME CARS DEALS JOIN / SIGN IN

INTERNET SERVICES

Hundreds of US news sites unavailable in Europe two months after GDPR

European visitors are still blocked from viewing many US outlets.

BY SEAN KEANE | AUGUST 8, 2018 5:44 AM PDT

News > Over 1,000 US news sites still unavailable in EU following GDPR

Over 1,000 US news sites still unavailable in EU following GDPR

By Mike Moore August 08, 2018 Internet

Don't worry though, EU users, Instapaper is back

art. 615 ter Codice Penale

il reato di accesso abusivo ad un sistema informatico o telematico

art. 615 quater Codice Penale

il reato di detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici

Fattispecie di reato previste dal D. Lgs. 196/2003 (Codice Privacy), come modificato dal D. Lgs. 101/2018:

- Art. 167 Trattamento illecito di dati
- Art. 167 bis Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala
- Art. 167 ter Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala
- Art. 168 Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione di compiti o dell'esercizio di poteri del Garante
- Art. 170 Inosservanza di provvedimenti del Garante

Per un corretto utilizzo dei dispositivi aziendali (pc, notebook, smartphone, ...)

- Non lasciare dispositivi mobili incustoditi
- Custodire le credenziali di accesso in posti sicuri (no a bigliettini con la password attaccati alla postazione) e non divulgarle
- Non lasciare accessibile il sistema operativo in caso di allontanamento, anche temporaneo, dalla postazione di lavoro
- Non lasciare incustoditi dispositivi mobili di archiviazione di dati (hard disk, pendrive ecc....)
- Evitare di visualizzare o trasmettere documenti riservati utilizzando collegamenti wireless in luoghi pubblici.
- Comunicare immediatamente al titolare eventuali incidenti di sicurezza

Indicazioni generali per un corretto trattamento dei dati da parte del personale:

- svolgere, in ogni caso, il trattamento dei dati personali per le finalità e secondo le modalità stabilite dal titolare del trattamento e, comunque, in modo lecito e secondo correttezza;
- trattare i soli dati per i quali ha ricevuto autorizzazione e la cui conoscenza sia necessaria e sufficiente per lo svolgimento delle operazioni da effettuare
- non lasciare documenti o supporti informatici sulla scrivania, ma custodirli in armadi e cassetti appositi;
- non lasciare documenti incustoditi presso le stampanti o fax;
- evitare di visualizzare o trasmettere documenti riservati utilizzando collegamenti wireless in luoghi pubblici.
- mantenere la riservatezza sui dati personali dei quali viene a conoscenza, anche in modo fortuito, anche successivamente al termine del rapporto di lavoro con il titolare del trattamento.

In generale, nelle comunicazioni:

- Prima di condividere verbalmente o per iscritto dati, documenti o informazioni di lavoro, accertarsi che il destinatario sia autorizzato a venirne a conoscenza;
- Non trasferire a terzi informazioni aziendali non espressamente destinate alla diffusione.

GRAZIE per l'ATTENZIONE

Relatore: Francesco cilona
f.cilona@athlantic.it