
Unione Province d'Italia
UPI
Emilia-Romagna

CORSO DI PREPARAZIONE

PER IL CONCORSO

A SEGRETARIO COMUNALE E PROVINCIALE

E DI AGGIORNAMENTO PER DIRIGENTI

N. 25 giornate
27 settembre - 27 novembre 2019

Sede:
Sala Formazione UPI
viale Silvani 6 Bologna

UPI Emilia-Romagna
Organizzazione e coordinamento: Dott.ssa Luana Plessi
Segreteria Organizzativa: Dott.ssa Irene De Giorgi - Elettra Bergamini – Tel. 051/6492491 – Fax 051/6494321
http://www.upi.emilia-romagna.it/

1

PRIVACY!

NEL GDPR E NEL "NUOVO" CODICE PRIVACY ITALIANO

AVV. STEFANO ORLANDI

FOUNDER ORLANDI&PARTNERS STUDIO LEGALE, BOLOGNA - WWW.ORLANDI.MOBI

FOUNDER E VICE DIRETTORE CENTRO STUDI PNT, ROMA - WWW.CENTROSTUDIPNT.ORG

Unione Province d'Italia
UPI
Emilia-Romagna

CENTRO STUDI PRIVACY E NUOVE TECNOLOGIE

LE FONTI AWARDS WINNER 2018

ORLANDI&PARTNERS STUDIOLEGALE

BOUTIQUE DI ECCELLENZA 2018

Unione Province d'Italia
UPI
Emilia-Romagna

CORSO DI PREPARAZIONE

PER IL CONCORSO

A SEGRETARIO COMUNALE E PROVINCIALE

E DI AGGIORNAMENTO PER DIRIGENTI

N. 25 giornate
27 settembre - 27 novembre 2019

Sede:
Sala Formazione UPI
viale Silvani 6 Bologna

UPI Emilia-Romagna
Organizzazione e coordinamento: Dott.ssa Luana Plessi
Segreteria Organizzativa: Dott.ssa Irene De Giorgi - Elettra Bergamini – Tel. 051/6492491 – Fax 051/6494321
http://www.upi.emilia-romagna.it/

1

PRIVACY!

- VENTICINQUE ANNI DI PROTEZIONE DATI IN EUROPA E IN ITALIA (CENNI)
- LA NORMATIVA DI RIFORMA: IL GDPR E LA DISCIPLINA ITALIANA DI ADEGUAMENTO
- I NUOVI PRINCIPI (ACCOUNTABILITY; PRIVACY BY DESIGN E BY DEFAULT)
- LE FIGURE ORGANIZZATIVE (TITOLARI, CONTITOLARI, RESPONSABILI, DESIGNATI)
- I DIRITTI DEGLI INTERESSATI (CENNI)
- IL DATA PROTECTION OFFICER
- IL REGISTRO DEI TRATTAMENTI
- LA DPIA E LA CONSULTAZIONE PREVENTIVA DEL GARANTE (CENNI)
- MISURE DI SICUREZZA INFORMATICHE, FISICHE ED ORGANIZZATIVE
- DATA BREACH: COS'È E COME GESTIRLO
- TRASPARENZA E PRIVACY: ACCESSO CIVICO, OBBLIGHI DI PUBBLICAZIONE
- RESPONSABILITÀ E SANZIONI

PRIVACY MATTERS!

“LA PRIVACY? PER ME È UNA QUESTIONE INUTILE, IO NON HO NIENTE DA NASCONDERE...”

“Negli ultimi 16 mesi, discutendo di questa questione in giro per il mondo, ogni volta che qualcuno mi ha detto "*Non mi preoccupano le invasioni della privacy perché non ho niente da nascondere*” rispondo sempre la stessa cosa. Tiro fuori una penna, scrivo il mio indirizzo email. Dico: "*Ecco il mio indirizzo email. Quello che voglio che tu faccia quando arrivi a casa è mandarmi le password di tutti i tuoi account, non solo quella elegante e rispettabile che usi al lavoro, ma tutte quante, perché voglio essere in grado di scandagliare quello che fai online, leggere quello che voglio e pubblicare tutto quello che trovo interessante. Dopo tutto, se non sei una persona cattiva, se non fai niente di sbagliato, non dovresti avere niente da nascondere. Dicevi proprio Tu che uno nasconde solo ciò che è male…o sbaglio?*”

Glenn Greenwald

Giornalista ed avvocato di Edward Snowden


NO TRESPASSING

Unione Province d'Italia
UPI
Emilia-Romagna

CENTRO STUDI PRIVACY E NUOVE TECNOLOGIE

LE FONTI AWARDS
WINNER 2018

ORLANDI&PARTNERS
STUDIOLEGALE
BOUTIQUE DI ECCELLENZA 2018


X
Downloading Future
Please Wait...
Cancel

Il problema dei nostri giorni è che
il ***futuro*** *non è più quello di una volta*
(Paul Valery)


di 26 settembre 1994

MISS
Il sorriso di Micaela incanta Canale 5

«Perché ho vinto? Probabilmente grazie alla mia spontaneità». Micaela Grandi, diciannovenne bolognese che abita in via dell'Incisore (zona Roveri) giustifica così la sua vittoria venerdì sera durante il gran finale del concorso «Ragazza Sorrisi» grazie alla quale affiancherà Maurizio Seymandi alla guida della trasmissione di Canale 5 Superclassifica Show. Bion-
capelli corti, un fisico
un metro e
altezza,

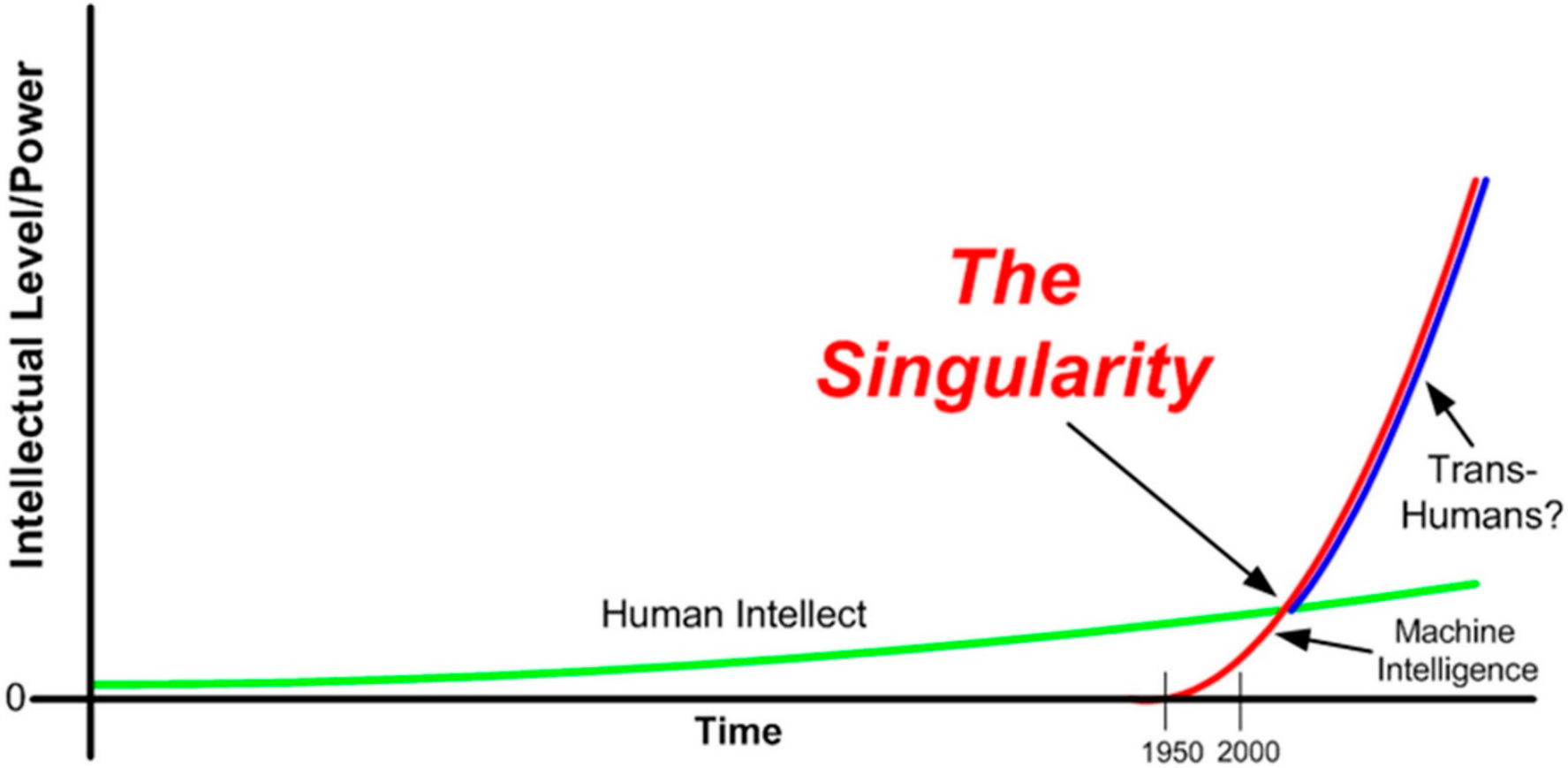
il **futuro** *(…) di una volta*

Unione Province d'Italia
UPI
Emilia-Romagna

CENTRO STUDI PRIVACY E NUOVE TECNOLOGIE

LE FONTI AWARDS
WINNER 2018

ORLANDI&PARTNERS
STUDIOLEGALE
BOUTIQUE DI ECCELLENZA 2018


Intellectual Level/Power
The Singularity
Trans-Humans?
Human Intellect
Machine Intelligence
0
Time
1950
2000

"L'evoluzione della tecnologia è un ***processo a crescita esponenziale*** *e non lineare. Nel 21° secolo non assisteremo a 100 anni di progresso, ma a* ***20.000 anni di progresso****. Lo scenario del futuro è quello in cui il ritmo del cambiamento* ***sarà così rapido e il suo impatto così profondo che la vita umana ne sarà trasformata in modo irreversibile****"*

Ray Kurzweil

"Si può dire che oggi ***non viviamo un'epoca di cambiamento quanto un cambiamento d'epoca****. Le situazioni che viviamo oggi pongono dunque* ***sfide nuove*** *che per noi a volte sono* ***persino difficili da comprendere****. Questo nostro tempo richiede di vivere i* ***problemi come sfide*** *e non come ostacoli." (****Firenze****, 10 novembre 2015)*

Francisc us

sfide nuove *che*

per noi a volte sono ***persino difficili da comprendere***.

wired - le parole del 2019

Christopher Wiley

"In pochi altri momenti della storia ***le persone sono diventate prodotti****: abbiamo avuto la tratta degli schiavi, abbiamo la prostituzione e abbiamo il mercato dei dati. Il comportamento delle persone sta diventando* ***una merce****, l'identità può trasformarsi in un prodotto da vendere o da sfruttare.* ***I dati sono come gli atomi di uranio****: puoi costruire o distruggere una città, o una società. Per questo* ***dobbiamo trattarli seriamente e mettere persone responsabili nelle posizioni cruciali****, affinché garantiscano che vengano gestiti* ***in maniera sicura****"*

www.corriere.it 18/1/2019

Collection #1, il «più grande» furto di dati online: rubati 730 milioni di mail e password. Cambiate gli account

Il numero mostruoso di indirizzi mail e di password trafugati dalla Rete e raccolti in un unico file da 87 Gigabyte in barba a tutti i sistemi di cybersecurity

di Redazione Tecnologia

I NOSTRI DATI CI SEGUONO

The New York Times

July 21, 2010

The Web Means the End of Forgetting

By JEFFREY ROSEN

(…) In the meantime, as all of us stumble over the challenges of **living in a world without forgetting,** we need to learn **new forms of empathy**, **new ways of defining ourselves without reference to what others say about** us and **new ways of forgiving one another** for the digital trails that will follow us forever.

I NOSTRI DATI CI SEGUONO

STEVE BANNON – EX CAPO STRATEGA DONALD TRUMP
Io vi posso aiutare focalizzando le prossime europee per vincere vi possiamo fornire e far realizzare sondaggi, analisi di big data, preparare cabine di regia, tutto quello di cui si ha bisogno per vincere le elezioni. Vi aiutiamo in modo gratuito.

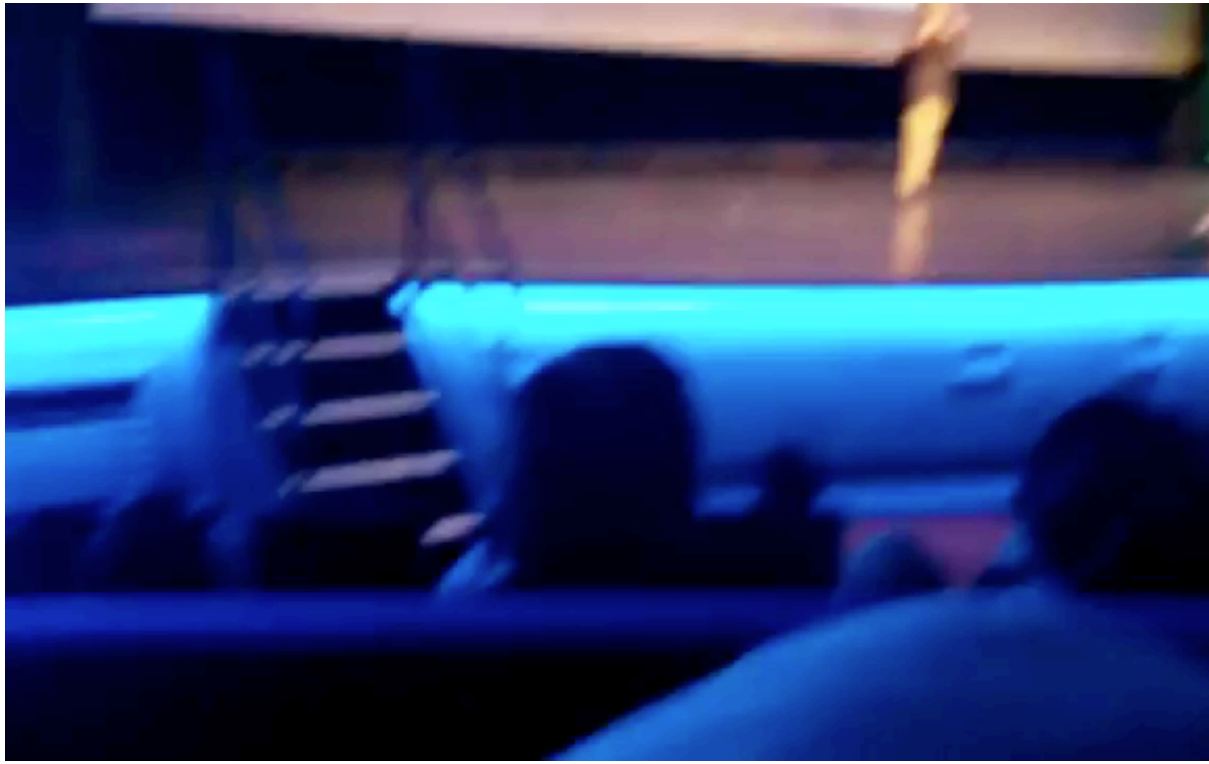
GIORGIO MOTTOLA FUORI CAMPO
Steve Bannon è il fondatore di Cambridge Analytica, la società che ha violato illegalmente 50 milioni di profili su Facebook, ma come dimostra questo fuori onda del documentario "The Brink" il vizio della profilazione a scopo elettorale Bannon non sembra averlo perso.

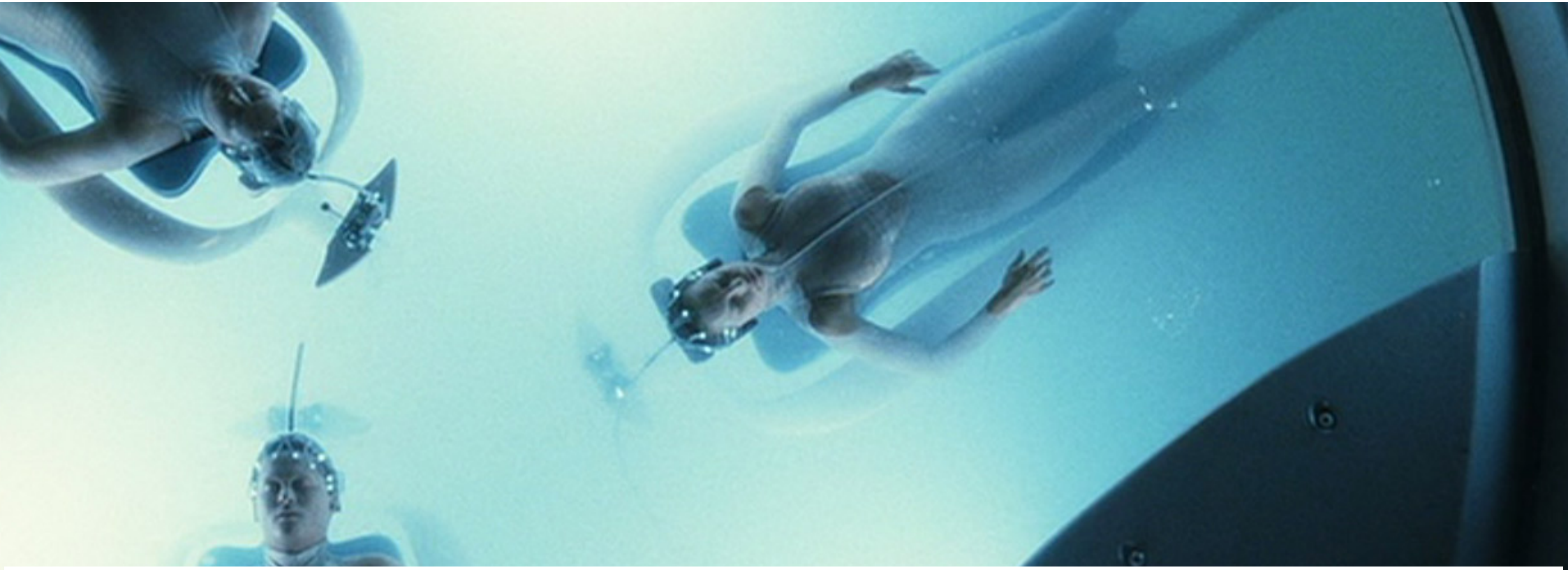
STEVE BANNON – EX CAPO STRATEGA DONALD TRUMP
Questi tizi stanno cercando di profilare il volto cattolico: se il tuo telefono è entrato in una chiesa cattolica è straordinario impossessarsi di quei dati. Possono dirti davvero chi è stato in una chiesa cattolica e quanto spesso. Te li possono profilare. Le compagnie telefoniche, poi i dati te li vende un tizio e così io posso rivolgermi direttamente al tuo telefono. Domani in Iowa ad esempio, faremo mandare un messaggio ai cattolici non daremo indicazioni di voto per una persona specifica, ma diremo che tutti i cattolici devono andare a votare e fare il loro dovere sostenendo il presidente Trump. Tutte le compagnie telefoniche raccolgono i dati, poi c'è qualcuno che decide di guadagnarci sopra e le vende.

DA "REPORT", RAI 3, 28/10/2019

BIG DATA!... (OK, OK, OK... Ma come "gestirli"?)

"Se noi mettiamo insieme ***l'Internet of Things, i big data e l'intelligenza artificiale*** *…* ***è lì che tutto in qualche modo esplode. (…)***
Stiamo parlando di macchine talmente efficienti che non solo sono in grado di svolgere al meglio i compiti che noi affidiamo loro, ma che sono anche ***in grado di apprendere e di individuare le falle nel sistema****, in questo caso videogiochi e di perseguire l'obiettivo che è stato dato loro, anche* ***al di là della stessa comprensione e conoscenza di chi ha messo in piedi questi algoritmi.*** *Come dicono i ricercatori: "it ruthlessly exploits the weaknesses of the system"*
Massimo Russo-"Wired Italia"





Nel 2054 la città di Washington ha cancellato gli omicidi da ormai 6 anni grazie a un sistema chiamato Precrimine. Basandosi sulle premonizioni di tre individui dotati di poteri extrasensoriali di precognizione amplificati, detti Precog, la polizia riesce a impedire gli omicidi prima che essi avvengano e ad arrestare i "colpevoli". In questo modo non viene punito il fatto (che non avviene), bensì l'intenzione di compierlo e che porterebbe a concretizzarlo

BIG DATA + A.I. = PREVEDERE IL FUTURO?

Amazon sempre avanti: arrivano le consegne predittive

Minimizzare i tempi di consegna: è ormai questo il mantra di Amazon, big internazionale dell'eCommerce, seriamente intenzionato a stravolgere quello che è il mercato online dei giorni nostri poggiandosi su tecniche sempre più innovative per soddisfare i suoi utenti.

La chiamano **"Consegna Predittiva" – "Anticipatory Shopping"** in lingua originale ed il concetto, tanto semplice quanto d'effetto, è far arrivare un prodotto all'utente **prima ancora che questi abbia pensato di ordinarlo.**

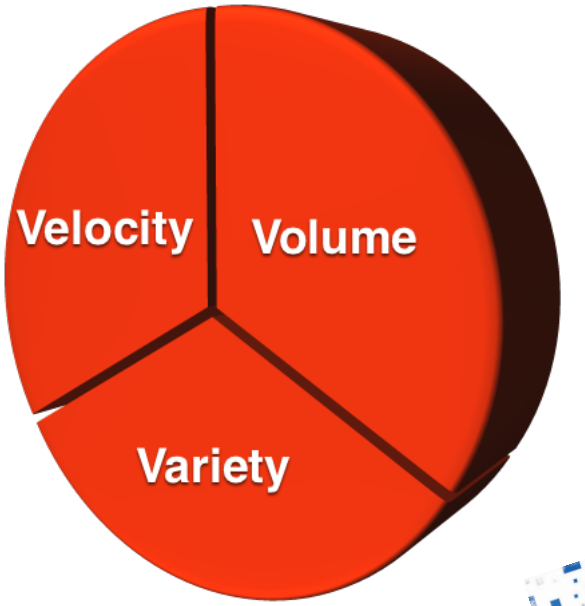
Il brevetto depositato dal big statunitense illustra tale metodologia come una maniera per ridurre i tempi d'attesa tra l'ordine e la consegna, in quanto ciò "potrebbe dissuadere i clienti dall'acquistare dai mercati online".

In poche parole, Amazon prevede – e prevede di farlo a breve termine – di gestire le consegne nel modo seguente: **anziché far partire l'oggetto soltanto ad ordine avvenuto, grazie ad un'accurata analisi (di cui parleremo tra poco) i prodotti potrebbero essere "consegnati a priori" ad uno o più utenti prima ancora che questi abbiano eseguito l'ordine.**

In effetti tutto si basa su un **sofisticato algoritmo di selezione**, in grado di ottenere risultati accurati a partire dall'incrocio di dati ben precisi: per ogni utente, l'algoritmo esaminerà le ricerche e gli ordini precedenti, le wishlist, i carrelli, i resi e **addirittura il tempo in cui tale utente tiene fermo il mouse su un determinato oggetto.**

NOI SIAMO I NOSTRI DATI ???!

“come dice? non mi assicura perché sono un soggetto ad alto rischio?!?!?!?! ma come fa a saperlo?!?!?!”



“Aviva, a large insurance firm, has studied the idea of **using credit reports and consumer-marketing data as proxies for the analysis of blood and urine samples for certain applicants**. The intent is to identify those who may be at higher risk of **illnesses like high blood pressure, diabetes, or depression.** The method uses lifestyle data that includes hundreds of variables such as **hobbies, the websites people visit, and the amount of television they watch, as well as estimates of their income.**
Aviva’s **predictive model** was considered successful at identifying health risks.”

tratto da: *Kenneth Cukier,* ***“Big Data”***

La storia *A Venezia l'ultimo arresto grazie alla nuova tecnologia*

L'algoritmo che mette le manette ai ladri

PIERO COLAPRICO

Detective del futuro contro ladri che sono rimasti nel passato. Si può leggere anche in questo modo l'ultimo arresto, avvenuto a Mestre, vicino Venezia. E per leggerlo meglio, bisogna partire da un verbo greco che ha messo in crisi generazioni di studenti del classico: Eurisco, trovare. L'altra notte, il computer della questura, nel quale è inserito il programma X-law, ha lanciato una previsione: «Tra le 3 e le 4 del mattino commissione di un reato predatorio presso esercizio».
Le volanti si piazzano in zona e, in effetti, intorno alle ore 3.45 il portiere di notte di un hotel chiama il 112. Ha sorpreso un ladro, voleva razziare i soldi della cassa e, scoperto, sta scappando: abiti scuri, grande e grosso, in ciabatte, va dove crede di far sparire le sue tracce, verso il posteggio dei taxi e, purtroppo per lui, si trova a dover salire su un altro tipo di auto. Non gialla, ma azzurrina. Senza tassametro e tassista, ma con due agenti.
«X-law – spiega Vittorio Rizzi, direttore centrale dell'Anticrimine – opera da diversi anni ed è nata a Napoli, grazie a un ispettore, Elia Lombardo. Prima l'abbiamo sperimentata in Campania, poi a Prato, adesso a Venezia. Nel corso del tempo ci sono stati progressivi affinamenti, il programma si basa su un algoritmo euristico». Cioè intuitivo, sperimentale, che trova. È considerato un sistema «previsionale».
Più che di controllo del territorio, forse è un caso di «protezione» del territorio, ma in ogni caso questa tecnologia si aggiunge alle intercettazioni, alle telecamere, alle microspie e colpisce quella che viene definita «microcriminalità», la criminalità che fa razzie in strada, al pianoterra, o cerca di truffare i più fragili, gli anziani.
Al momento, la polizia sta usando alcuni sistemi diversi. A Milano, molti anni fa, grazie all'assistente Mario Venturi (che ora lavora con aziende Usa), si dette vita al modello Key-crime. Colpisce i criminali seriali, specialmente i rapinatori di farmacie e supermercati. C'erano alcuni sconosciuti. Per esempio, "Keep Calm", che dopo le rapine veniva inquadrato a pedalare su una vecchia bici. O "Photo Finish", che in ogni filmato proteggeva i lineamenti sotto il casco integrale con la bandiera dello start della Formula Uno. Key-crime studia come e quando i seriali agiscono, la zona preferita, le armi usate e, da quello che le pattuglie ricavano dall'interrogatorio delle vittime, il computer «deduce» la prossima mossa del criminale.
«Infatti, Key-crime è più utile alla polizia giudiziaria – continua il dirigente Anticrimine Rizzi – mentre X-law annuncia qualunque, letteralmente qualunque tipo di reato, orienta le pattuglie sul territorio e sugli orari». E cosa dice Elia Lombardo, l'ispettore che l'ha studiato e realizzato a Napoli? «Studio in verità da vent'anni i reati predatori e sono riuscito a dimostrare che hanno alcune caratteristiche. Sono ciclici e stanziali, spesso sono commessi da persone modestamente organizzate. La loro strategia tende a scegliere zone del territorio dove una ricchezza c'è, si percepisce, ma c'è anche bisogno di vie di fuga e di coperture. Le ho chiamate "riserve di caccia", gli autori tendono a ripetersi e il mio logaritmo riconosce le " riserve"».
Quindi funziona? «A Napoli i reati sono stati abbattuti del 27 per cento e gli arresti o le denunce sono aumentati del 24; a Prato i reati sono stati abbattuti del 32 per cento e denunce e arresti aumentati del 54; a Venezia non ho gli ultimi numeri, ma siamo in linea con Prato, e due università, Federico II e Partenope, avallano i nostri dati».

Leda con le figlie Silvia e Cecilia, i nipoti Giacomo, Cosimo e Livia piangono la scomparsa dell'amatissimo marito, padre, nonno

Massimo Violati

I funerali si svolgeranno a Roma oggi alle ore 15 presso la Chiesa di Santa Maria in Portico in Campitelli.

Roma, 17 novembre 2018

Il Consiglio Direttivo e i Soci di Studio Arti Floreali si stringono con affetto alla Presidente Leda Violati e alla sua famiglia per la scomparsa del caro marito

DOTT.

Massimo Violati

Roma, 17 novembre 2018

17 novembre 2010 17 novembre 2018

ANNIVERSARIO

Nicola Rossi

Maria Vittoria, Barbara e Alessandro ti ricordano con amore e infinito rimpianto.

Una Messa di suffragio sarà celebrata oggi, presso la chiesa dei Padri Barnabiti in via Ulisse Seni, alle ore 18.

Roma, 17 novembre 2018

17-11-2009 17-11-2018

Claudia Bianchi

Oggi, come ieri, come sempre, sei qui con noi che ti vogliamo bene.

La tua famiglia.

Milano, 17 novembre 2018

*il **futuro** non è più quello di una volta*

Unione Province d'Italia
UPI
Emilia-Romagna

CENTRO STUDI PRIVACY E NUOVE TECNOLOGIE

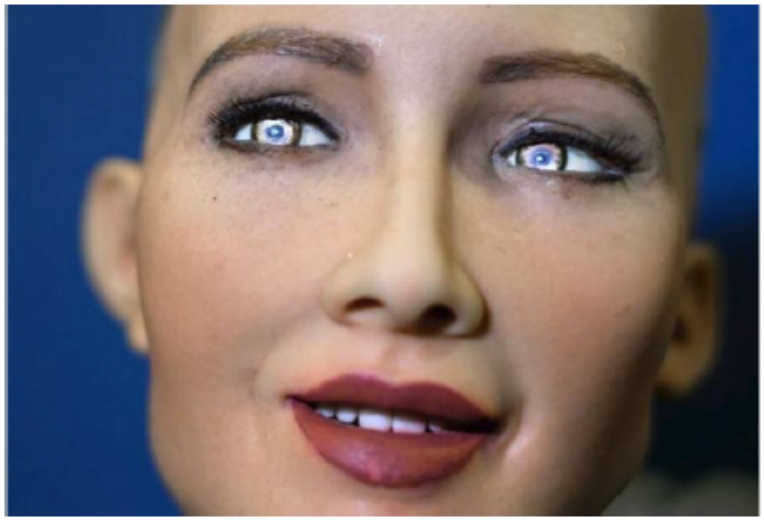
LE FONTI AWARDS
WINNER 2018

ORLANDI&PARTNERS
STUDIOLEGALE
BOUTIQUE DI ECCELLENZA 2018

[La storia] Ecco Sophia, la prima donna robot della storia diventata cittadina

Il diritto le è stato riconosciuto dall'Arabia Saudita. Grazie alla sua intelligenza artificiale può conversare con gli uomini riuscendo perfino ad essere ironica

30 ottobre 2017



IL GARANTE EUROPEO:
"CAMBIERÀ LA NOZIONE DI DATO PERSONALE E INTANTO SERVE UNA POLITICA PROATTIVA A TUTELA DEI DIRITTI DI TUTTI"

WWW.ABOUTPHARMA.COM - I SETTEMBRE 2017 I N. 151

"Del resto, ***la nozione stessa di dati personali, mi spiace dirlo, sparirà entro qualche anno****...*
Che succederà?
Saremo tutti più facilmente identificabili
e ***i dati anonimi saranno una categoria soggetta a continua erosione."***

Unione Province d'Italia
UPI
Emilia-Romagna

il ***futuro*** *non è più quello di una volta*

CENTRO STUDI PRIVACY E NUOVE TECNOLOGIE

LE FONTI AWARDS
WINNER 2018

ORLANDI&PARTNERS
STUDIOLEGALE
BOUTIQUE DI ECCELLENZA 2018

GDPR

Gazzetta ufficiale L 119

dell'Unione europea

Edizione in lingua italiana

Legislazione

59° anno

4 maggio 2016

Sommario

I *Atti legislativi*

REGOLAMENTI

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

Unione Province d'Italia
UPI
Emilia-Romagna

CENTRO STUDI PRIVACY E NUOVE TECNOLOGIE

LE FONTI AWARDS
WINNER 2018

ORLANDI&PARTNERS
STUDIOLEGALE
BOUTIQUE DI ECCELLENZA 2018

Il completamento (?) del quadro normativo

Gazzetta ufficiale L 119

dell'Unione europea

Edizione in lingua italiana — Legislazione — 59° anno — 4 maggio 2016

Sommario

1 Atti legislativi

REGOLAMENTI

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

+

Supplemento ordinario alla "Gazzetta Ufficiale", n. 174 del 29 luglio 2003 - Serie generale

Spediz. abb. post. 45% - art. 2, comma 20/b Legge 23-12-1996, n. 662 - Filiale di Roma

GAZZETTA UFFICIALE DELLA REPUBBLICA ITALIANA

PARTE PRIMA Roma - Martedì, 29 luglio 2003 — SI PUBBLICA TUTTI I GIORNI NON FESTIVI

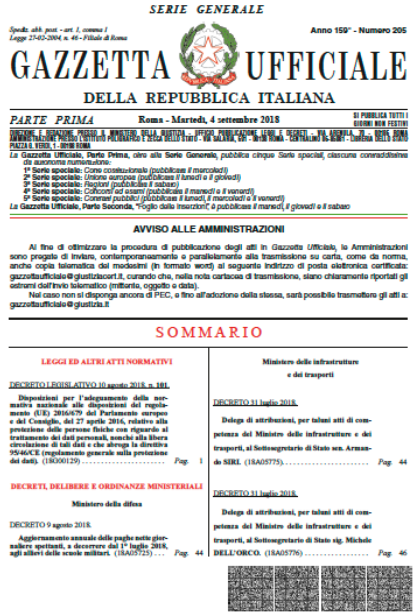
DIREZIONE E REDAZIONE PRESSO IL MINISTERO DELLA GIUSTIZIA - UFFICIO PUBBLICAZIONE LEGGI E DECRETI - VIA ARENULA 70 - 00100 ROMA
AMMINISTRAZIONE PRESSO L'ISTITUTO POLIGRAFICO E ZECCA DELLO STATO - LIBRERIA DELLO STATO - PIAZZA G. VERDI 10 - 00100 ROMA - CENTRALINO 06.85.081

N. 123/L

DECRETO LEGISLATIVO 30 giugno 2003, n. **196.**

Codice in materia di protezione dei dati personali.

+



SERIE GENERALE

Spediz. abb. post. - art. 1, comma 1 Legge 27-02-2004 n. 46 - Filiale di Roma — Anno 159° - Numero 205

GAZZETTA UFFICIALE DELLA REPUBBLICA ITALIANA

PARTE PRIMA Roma - Martedì, 4 settembre 2018 — SI PUBBLICA TUTTI I GIORNI NON FESTIVI

AMMINISTRAZIONE PRESSO L'ISTITUTO POLIGRAFICO E ZECCA DELLO STATO - VIA SALARIA, 691 - 00138 ROMA - CENTRALINO 06 85081 - Gazzetta Ufficiale

PIAZZA G. VERDI, 1 - 00100 ROMA

La Gazzetta Ufficiale, Parte Prima, cioè alla Serie Generale, pubblica cinque Serie speciali, ciascuna contraddistinta da autonoma numerazione:

- *1ª Serie speciale: Corte costituzionale (pubblicata il mercoledì)*
- *2ª Serie speciale: Unione europea (pubblicata il lunedì e il giovedì)*
- *3ª Serie speciale: Regioni (pubblicata il sabato)*
- *4ª Serie speciale: Concorsi ed esami (pubblicata il martedì e il venerdì)*
- *5ª Serie speciale: Contratti pubblici (pubblicata il lunedì, il mercoledì e il venerdì)*

La Gazzetta Ufficiale, Parte Seconda, "Foglio delle inserzioni", è pubblicata il martedì, il giovedì e il sabato

AVVISO ALLE AMMINISTRAZIONI

Al fine di ottimizzare la procedura di pubblicazione degli atti in Gazzetta Ufficiale, le Amministrazioni sono pregate di inviare, contemporaneamente e parallelamente alla trasmissione su carta, come da norma, anche copia telematica del medesimi (in formato word) al seguente indirizzo di posta elettronica certificata: gazzettaufficiale@giustiziacert.it, curando che, nella nota cartacea di trasmissione, siano chiaramente riportati gli estremi dell'invio telematico (mittente, oggetto e data).

Nel caso non si disponga ancora di PEC, a fino all'adozione della stessa, sarà possibile trasmettere gli atti a: gazzettaufficiale@giustizia.it

SOMMARIO

LEGGI ED ALTRI ATTI NORMATIVI

DECRETO LEGISLATIVO 10 agosto 2018, n. 101.

Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). (18G00129) ..... Pag. 1

DECRETI, DELIBERE E ORDINANZE MINISTERIALI

Ministero della difesa

DECRETO 9 agosto 2018.

Aggiornamento annuale delle paghe nette giornaliere spettanti, a decorrere dal 1° luglio 2018, agli allievi delle scuole militari. (18A05725) ..... Pag. 44

Ministero delle infrastrutture e dei trasporti

DECRETO 31 luglio 2018.

Delega di attribuzioni, per talune atti di competenza del Ministro delle infrastrutture e dei trasporti, al Sottosegretario di Stato sen. Armando SIRI. (18A05775) ..... Pag. 44

DECRETO 31 luglio 2018.

Delega di attribuzioni, per talune atti di competenza del Ministro delle infrastrutture e dei trasporti, al Sottosegretario di Stato sig. Michele DELL'ORCO. (18A05776) ..... Pag. 46

Unione Province d'Italia UPI Emilia-Romagna

CENTRO STUDI PRIVACY E NUOVE TECNOLOGIE

LE FONTI AWARDS WINNER 2018

ORLANDI&PARTNERS STUDIOLEGALE

BOUTIQUE DI ECCELLENZA 2018

SERIE GENERALE

Spediz. abb. post. - art. 1, comma 1
Legge 27-02-2004, n. 46 - Filiale di Roma

Anno 159° - Numero 205

GAZZETTA UFFICIALE

DELLA REPUBBLICA ITALIANA

PARTE PRIMA — Roma - Martedì, 4 settembre 2018 — SI PUBBLICA TUTTI I GIORNI NON FESTIVI

DECRETO LEGISLATIVO 10 agosto 2018, n. 101.

Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). (18G00129) . . . . . .

SERIE GENERALE

Spediz. abb. post. - art. 1, comma 1
Legge 27-02-2004, n. 46 - Filiale di Roma

Anno 159° - Numero 205

GAZZETTA UFFICIALE

DELLA REPUBBLICA ITALIANA

PARTE PRIMA — Roma - Martedì, 4 settembre 2018 — SI PUBBLICA TUTTI I GIORNI NON FESTIVI

DECRETO LEGISLATIVO 10 agosto 2018, n. 101.

Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). (18G00129) . . . . . .

Highlights

Comunicato stampa del Consiglio dei Ministri n. 14 dell' 8 agosto 2018

Il decreto legislativo, in attuazione dell'art. 13 della legge di delegazione europea 2016-2017 (legge 25 ottobre 2017, n. 163), introduce disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento europeo relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati. Dopo l'esame di una commissione appositamente costituita si è deciso, al fine di semplificare l'applicazione della norma, **di agire novellando il codice della privacy esistente**, nonostante il regolamento abbia di fatto cambiato la prospettiva dell'approccio alla tutela della privacy rispetto al codice introducendo il principio di dell'accountability.

Si è scelto di **garantire la continuità facendo salvi per un periodo transitorio i provvedimenti del Garante e le autorizzazioni, che saranno oggetto di successivo riesame, nonché i Codici deontologici vigenti.** Essi restano fermi nell'attuale configurazione nelle materie di competenza degli Stati membri, mentre possono essere riassunti e modificati su iniziativa delle categorie interessate quali codici di settore.

In considerazione delle esigenze di semplificazione delle micro, piccole e medie imprese, si è previsto che il Garante promuova modalità semplificate di adempimento degli obblighi del titolare del trattamento.

SERIE GENERALE

Spediz. abb. post. - art. 1, comma 1
Legge 27-02-2004, n. 46 - Filiale di Roma

Anno 159° - Numero 205

GAZZETTA UFFICIALE

DELLA REPUBBLICA ITALIANA

PARTE PRIMA — Roma - Martedì, 4 settembre 2018 — SI PUBBLICA TUTTI I GIORNI NON FESTIVI

DECRETO LEGISLATIVO 10 agosto 2018, n. 101.

Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). (18G00129) . . . . . .

Highlights

Nonostante questi risultati delle cennate verifiche, e le indubbie difficoltà di natura squisitamente tecnico-redazionale, si è deciso di operare essenzialmente all'interno del Codice vigente, in chiave, quindi, di sua novellazione. Pur dovendosi ribadire che quest'ultimo testo normativo, come profondamente innovato, ha senz'altro perso la sua centralità.

RELAZIONE ILLUSTRATIVA

Passando dall'illustrazione della tecnica normativa al merito delle scelte effettuate, si è ritenuto, perseguendo l'obiettivo della chiarezza e della semplificazione, di evitare di duplicare alcune disposizioni, molto simili ma non coincidenti, presenti e nel regolamento e nel codice, operando così una scelta chiara.

Conseguentemente dovevano essere abrogate le corrispondenti disposizioni del codice ove la materia fosse già disciplinata da disposizioni del regolamento europeo.

SERIE GENERALE

Spediz. abb. post. - art. 1, comma 1
Legge 27-02-2004, n. 46 - Filiale di Roma

Anno 159° - Numero 205

GAZZETTA UFFICIALE

DELLA REPUBBLICA ITALIANA

PARTE PRIMA — Roma - Martedì, 4 settembre 2018 — SI PUBBLICA TUTTI I GIORNI NON FESTIVI

DECRETO LEGISLATIVO 10 agosto 2018, n. 101.

Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). (18G00129) . . . . . .

Highlights

Titolo, Artt. 1 e 2

Modifiche al **titolo**

Modifiche all'**oggetto**

Modifiche alle **finalità**

*tutte le norme dell'ordinamento italiano relative alla protezione dei dati personali, o che possono incidere su questa materia, devono essere interpretate alla luce del **GDPR***

GDPR *rules*!

Art. 22 Dlgs n. 101/2018
Altre disposizioni transitorie e finali
1. Il presente decreto e le disposizioni dell'ordinamento nazionale si interpretano e si applicano alla luce della disciplina dell'Unione europea in materia di protezione dei dati personali e assicurano la libera circolazione dei dati personali tra Stati membri ai sensi dell'articolo 1, paragrafo 3, del Regolamento (UE) 2016/679.

Unione Province d'Italia
UPI
Emilia-Romagna

CENTRO STUDI PRIVACY E NUOVE TECNOLOGIE

LE FONTI AWARDS
WINNER 2018

ORLANDI&PARTNERS
STUDIOLEGALE
BOUTIQUE DI ECCELLENZA 2018

SERIE GENERALE

Spediz. abb. post. - art. 1, comma 1
Legge 27-02-2004, n. 46 - Filiale di Roma

Anno 159° - Numero 205

GAZZETTA UFFICIALE

DELLA REPUBBLICA ITALIANA

PARTE PRIMA — Roma - Martedì, 4 settembre 2018 — SI PUBBLICA TUTTI I GIORNI NON FESTIVI

DECRETO LEGISLATIVO 10 agosto 2018, n. 101.

Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). (18G00129) . . . . . .

Highlights

RELAZIONE ILLUSTRATIVA

L'art. 2 del Codice, come sostituito, sotto la rubrica "*Finalità*", è volto semplicemente a chiarire che il Codice ora è deputato ad adeguare l'ordinamento nazionale al suddetto Regolamento; cosa che, peraltro, si è inteso chiarire sin dal titolo del medesimo Codice, come modificato, ai sensi dell'art. 1, comma 1, lett. a), dello schema di decreto legislativo.

Come già esplicitato, infatti, il Codice, come qui modificato, è finalizzato all'adeguamento dell'ordinamento nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). Alla luce della tecnica legislativa adottata, quindi, le sue disposizioni dovranno quindi essere lette in "combinato disposto" con le disposizioni previste dal regolamento.

SERIE GENERALE

Spediz. abb. post. - art. 1, comma 1
Legge 27-02-2004, n. 46 - Filiale di Roma

Anno 159° - Numero 205

GAZZETTA UFFICIALE

DELLA REPUBBLICA ITALIANA

PARTE PRIMA — Roma - Martedì, 4 settembre 2018 — SI PUBBLICA TUTTI I GIORNI NON FESTIVI

DECRETO LEGISLATIVO 10 agosto 2018, n. 101.

Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). (18G00129) . . . . . .

Highlights

Art. 2-quater

obblighi legali,
interesse pubblico

dati genetici, dati biometrici
o dati relativi alla salute

CAPO IX - Disposizioni relative a specifiche situazioni di trattamento

libertà d'espressione e di informazione
accesso del pubblico ai documenti ufficiali
rapporti di lavoro
protezione dei dati vigenti presso chiese
e associazioni religiose
.....

Regole deontologiche

Il rispetto delle disposizioni contenute nelle regole deontologiche di cui al comma 1 costituisce condizione essenziale per la liceita' e la correttezza del trattamento dei dati personali.

cd. "soft law"

Unione Province d'Italia
UPI
Emilia-Romagna

CENTRO STUDI PRIVACY E NUOVE TECNOLOGIE

LE FONTI AWARDS
WINNER 2018

ORLANDI&PARTNERS
STUDIOLEGALE
BOUTIQUE DI ECCELLENZA 2018

Regole deontologiche

AGGIORNAMENTO DEL 16 GENNAIO 2019

Si fa presente che

- nella G.U. del 4 gennaio 2019, n. 3, sono state pubblicate le **"Regole deontologiche relative al trattamento dei dati personali nell'esercizio dell'attività giornalistica"**

- nella G.U. del 14 gennaio 2019, n. 11, sono state pubblicate le **"Regole deontologiche per trattamenti a fini statistici o di ricerca scientific** e le **"Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica effettuati nell'ambito del Sistema statistico nazionale"**

- nella G.U. del 15 gennaio 2019, n. 12, sono state pubblicate le **Regole deontologiche relative ai trattamenti di dati personali effettuati per svolgere investigazioni difensive o per fare valere o difendere un diritto in sede giudiziaria** e le **Regole deontologiche per il trattamento fini di archiviazione nel pubblico interesse o per scopi di ricerca storica**

VEDI ANCHE: comunicato stampa del 14 dicembre 20

GDPR: verificata dal Garante la conformità dei Codici deontologici

Le "Regole deontologiche" pubblicate sulla Gazzetta Ufficiale

Il Garante per la protezione dei dati personali ha verificato la conformità dei Codici di deontologia e di buona condotta per i trattamenti di dati personali p scopi storici, statistici, scientifici e investigazioni difensive al Regolamento Ue 2016/679 sulla protezione dei dati personali.

La verifica - demandata all'Autorità dal **decreto legislativo 101/2018** di adeguamento della normativa nazionale al Regolamento Ue - oltre ad aggiornamento formale dei riferimenti al nuovo quadro normativo europeo ha comportato la soppressione o la ridefinizione di talune previsioni alla lu del diverso approccio richiesto ai titolari del trattamento dal Regolamento Ue in omaggio ai principi di accountability, privacy by default e by design.

Le disposizioni ritenute conformi, ridenominate "regole deontologiche" integreranno, in base al decreto legislativo 101/2018, le condizioni di liceità correttezza dei trattamenti per scopi statistici e scientifici, per quelli a fini statistici e di ricerca scientifica nell'ambito del SISTAN, per quelli a fini archiviazione nel pubblico interesse o di ricerca storica e per quelli effettuati per svolgere investigazioni difensive o per far valere o difendere un diritto sede giudiziaria.

Giova precisare che in sede di prima applicazione l'art. 20 del decreto legislativo 101/2018 stabilisce che entro 90 giorni il Garante ripubblichi i vec codici, emendati dalle disposizioni incompatibili, senza prevedere alcuna consultazione pubblica. Consultazione prevista invece - per una durata minir di 60 giorni - per le regole deontologiche a regime (art. 2-quater del Codice), ossia per quelle che verranno scritte da oggi in poi o per le modifiche c saranno approvate rispetto a quelle appena pubblicate.

I testi aggiornati, in corso di pubblicazione nella Gazzetta ufficiale **(ora pubblicati)**, sono stati trasmessi al Ministero della giustizia per essere riportati c decreto nell'Allegato A) del **Codice in materia di protezione dei dati personali**.

Nei giorni scorsi il Garante aveva già verificato la conformità del Codice dei giornalisti. Anche questo testo denominato "Regole deontologic relative al trattamento dei dati personali nell'esercizio dell'attività giornalistica", è in corso di pubblicazione nella Gazzetta Ufficiale **(ora pubblicato)**.

Roma, 24 dicembre 2018

SERIE GENERALE

Spediz. abb. post. - art. 1, comma 1
Legge 27-02-2004, n. 46 - Filiale di Roma

Anno 159° - Numero 205

GAZZETTA UFFICIALE

DELLA REPUBBLICA ITALIANA

PARTE PRIMA — Roma - Martedì, 4 settembre 2018 — SI PUBBLICA TUTTI I GIORNI NON FESTIVI

DECRETO LEGISLATIVO 10 agosto 2018, n. 101.

Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). (18G00129) . . . . . .

Highlights

RELAZIONE ILLUSTRATIVA

Tale disposizione trova in parte la propria *ratio* nella scelta di conservare le regole stabilite nei "Codici di deontologia e di buona condotta", previsti all'articolo 12 del previgente codice in materia di protezione dei dati personali, che sino ad oggi hanno costituito una rilevante fonte di riferimento per i settori a cui sono diretti. Sebbene si sia dunque preferito far sopravvivere tali *corpus* settoriali, non si è optato per una loro integrale trasposizione nel nuovo testo normativo, ritenendo piuttosto necessario un loro aggiornamento ed adeguamento alla luce del nuovo impianto normativo e dei progressi tecnico-scientifici. Per tale motivo, l'articolo in esame prevede che lo schema di regole deontologiche sia sottoposto ad una previa consultazione pubblica. Il dialogo con le parti, gli *stakeholders* e i settori direttamente interessati è essenziale al fine di elaborare regole condivisibili e stabilire modalità di attuazione che non risultino eccessivamente onerose ovvero inefficaci agli occhi degli operatori.

SERIE GENERALE

Spediz. abb. post. - art. 1, comma 1
Legge 27-02-2004, n. 46 - Filiale di Roma

Anno 159° - Numero 205

GAZZETTA UFFICIALE

DELLA REPUBBLICA ITALIANA

PARTE PRIMA — Roma - Martedì, 4 settembre 2018 — SI PUBBLICA TUTTI I GIORNI NON FESTIVI

DECRETO LEGISLATIVO 10 agosto 2018, n. 101.

Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). (18G00129) . . . . . .

Highlights

Art. 2-septies

dati genetici, dati biometrici
o dati relativi alla salute

Misure di garanzia

stabilite dal Garante e aggiornate con cadenza almeno biennale

cd. "soft law"

Unione Province d'Italia
UPI
Emilia-Romagna

CENTRO STUDI PRIVACY E NUOVE TECNOLOGIE

LE FONTI AWARDS
WINNER 2018

ORLANDI&PARTNERS
STUDIOLEGALE
BOUTIQUE DI ECCELLENZA 2018

SERIE GENERALE

Spediz. abb. post. - art. 1, comma 1
Legge 27-02-2004, n. 46 - Filiale di Roma

Anno 159° - Numero 205

GAZZETTA UFFICIALE

DELLA REPUBBLICA ITALIANA

PARTE PRIMA — Roma - Martedì, 4 settembre 2018 — SI PUBBLICA TUTTI I GIORNI NON FESTIVI

DECRETO LEGISLATIVO 10 agosto 2018, n. 101.

Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). (18G00129) . . . . . .

Highlights

RELAZIONE ILLUSTRATIVA

Le misure di garanzia disciplinate dal presente articolo dovrebbero presentare soprattutto un contenuto tecnico ed organizzativo, e dettare misure di sicurezza.

Unione Province d'Italia
UPI
Emilia-Romagna

CENTRO STUDI PRIVACY E NUOVE TECNOLOGIE

LE FONTI AWARDS
WINNER 2018

ORLANDI&PARTNERS
STUDIOLEGALE
BOUTIQUE DI ECCELLENZA 2018

SERIE GENERALE

Spediz. abb. post. - art. 1, comma 1
Legge 27-02-2004, n. 46 - Filiale di Roma

Anno 159° - Numero 205

GAZZETTA UFFICIALE

DELLA REPUBBLICA ITALIANA

PARTE PRIMA — Roma - Martedì, 4 settembre 2018 — SI PUBBLICA TUTTI I GIORNI NON FESTIVI

DECRETO LEGISLATIVO 10 agosto 2018, n. 101.

Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). (18G00129) . . . . . .

Highlights

Art. 2-ter

Concetti centrali

Comunicazione

il dare conoscenza dei dati personali a uno o piu' soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate, ai sensi dell'articolo 2-quaterdecies, al trattamento dei dati personali sotto l'autorita' diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione

Diffusione

il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Unione Province d'Italia
UPI
Emilia-Romagna

CENTRO STUDI PRIVACY E NUOVE TECNOLOGIE

LE FONTI AWARDS
WINNER 2018

ORLANDI&PARTNERS
STUDIOLEGALE
BOUTIQUE DI ECCELLENZA 2018

SERIE GENERALE

Spediz. abb. post. - art. 1, comma 1
Legge 27-02-2004, n. 46 - Filiale di Roma

Anno 159° - Numero 205

GAZZETTA UFFICIALE

DELLA REPUBBLICA ITALIANA

PARTE PRIMA — Roma - Martedì, 4 settembre 2018 — SI PUBBLICA TUTTI I GIORNI NON FESTIVI

DECRETO LEGISLATIVO 10 agosto 2018, n. 101.

Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). (18G00129) . . . . . .

Highlights

Art. 2-septies

dati genetici, dati biometrici
o dati relativi alla salute

}

Divieto di diffusione

Unione Province d'Italia
UPI
Emilia-Romagna

CENTRO STUDI PRIVACY E NUOVE TECNOLOGIE

LE FONTI AWARDS
WINNER 2018

ORLANDI&PARTNERS
STUDIOLEGALE
BOUTIQUE DI ECCELLENZA 2018

SERIE GENERALE

Spediz. abb. post. - art. 1, comma 1
Legge 27-02-2004, n. 46 - Filiale di Roma

Anno 159° - Numero 205

GAZZETTA UFFICIALE

DELLA REPUBBLICA ITALIANA

PARTE PRIMA — Roma - Martedì, 4 settembre 2018 — SI PUBBLICA TUTTI I GIORNI NON FESTIVI

DECRETO LEGISLATIVO 10 agosto 2018, n. 101.

Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). (18G00129) . . . . . .

Highlights
Art. 2-ter

Base giuridica per trattamento di **DATI PERSONALI "COMUNI"** effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri

Legge e regolamento >
per il trattamento

Legge/regol. o Garante >
solo per la comunicazione per finalità pubbliche

(?)

Legge e regolamento >
per comunicazione/diffusione a soggetti per altri fini

Unione Province d'Italia
UPI
Emilia-Romagna

CENTRO STUDI PRIVACY E NUOVE TECNOLOGIE

LEGAL BUSINESS AWARDS
WINNER 2018

ORLANDI&PARTNERS
STUDIOLEGALE
BOUTIQUE DI ECCELLENZA 2018

SERIE GENERALE

Spediz. abb. post. - art. 1, comma 1
Legge 27-02-2004, n. 46 - Filiale di Roma

Anno 159° - Numero 205

GAZZETTA UFFICIALE

DELLA REPUBBLICA ITALIANA

PARTE PRIMA — Roma - Martedì, 4 settembre 2018 — SI PUBBLICA TUTTI I GIORNI NON FESTIVI

DECRETO LEGISLATIVO 10 agosto 2018, n. 101.

Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). (18G00129) . . . . . .

Highlights

Art. 2-ter

Art. 19 VECCHIO CODICE PRIVACY

(Principi applicabili al trattamento di dati diversi da quelli sensibili e giudiziari)

1. Il trattamento da parte di un soggetto pubblico riguardante dati diversi da quelli sensibili e giudiziari è consentito, fermo restando quanto previsto dall'articolo 18, comma 2, anche in mancanza di una norma di legge o di regolamento che lo preveda espressamente.

2. La comunicazione da parte di un soggetto pubblico ad altri soggetti pubblici è ammessa quando è prevista da una norma di legge o di regolamento. In mancanza di tale norma la comunicazione è ammessa

quando è comunque necessaria per lo svolgimento di funzioni istituzionali e può essere iniziata se è decorso il termine di cui all'articolo 39, comma 2, e non è stata adottata la diversa determinazione ivi indicata.

3. La comunicazione da parte di un soggetto pubblico a privati o a enti pubblici economici e la diffusione da parte di un soggetto pubblico sono ammesse unicamente quando sono previste da una norma di legge o di regolamento

(?)

Unione Province d'Italia
UPI
Emilia-Romagna

CENTRO STUDI PRIVACY E NUOVE TECNOLOGIE

LE FONTI AWARDS
WINNER 2018

ORLANDI&PARTNERS
STUDIOLEGALE
BOUTIQUE DI ECCELLENZA 2018

SERIE GENERALE

Spediz. abb. post. - art. 1, comma 1
Legge 27-02-2004, n. 46 - Filiale di Roma

Anno 159° - Numero 205

GAZZETTA UFFICIALE

DELLA REPUBBLICA ITALIANA

PARTE PRIMA — Roma - Martedì, 4 settembre 2018 — SI PUBBLICA TUTTI I GIORNI NON FESTIVI

DECRETO LEGISLATIVO 10 agosto 2018, n. 101.

Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). (18G00129) . . . . . .

Highlights

Art. 2-sexies

Base giuridica per il trattamento di **CATEGORIE PARTICOLARI DI DATI PERSONALI** necessario per motivi di interesse pubblico rilevante

disposizioni di legge o, nei casi previsti dalla legge, di regolamento che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato > **"NORME RINFORZATE"**

elenco di materie di "interesse pubblico rilevante"

Unione Province d'Italia
UPI
Emilia-Romagna

CENTRO STUDI PRIVACY E NUOVE TECNOLOGIE

LEFONTI AWARDS WINNER 2018

ORLANDI&PARTNERS STUDIOLEGALE
BOUTIQUE DI ECCELLENZA 2018

SERIE GENERALE

Spediz. abb. post. - art. 1, comma 1
Legge 27-02-2004, n. 46 - Filiale di Roma

Anno 159° - Numero 205

GAZZETTA UFFICIALE

DELLA REPUBBLICA ITALIANA

PARTE PRIMA — Roma - Martedì, 4 settembre 2018 — SI PUBBLICA TUTTI I GIORNI NON FESTIVI

DECRETO LEGISLATIVO 10 agosto 2018, n. 101.

Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). (18G00129) . . . . . .

Highlights

Art. 2-quinquiesdecies

Trattamento che presenta **rischi elevati** per l'esecuzione di un **compito di interesse pubblico**

il Garante puo', **con provvedimenti di carattere generale adottati d'ufficio**, prescrivere misure e accorgimenti a garanzia dell'interessato, che il titolare del trattamento e' tenuto ad adottare.

Unione Province d'Italia
UPI
Emilia-Romagna

CENTRO STUDI PRIVACY E NUOVE TECNOLOGIE

LE FONTI AWARDS
WINNER 2018

ORLANDI&PARTNERS
STUDIOLEGALE
BOUTIQUE DI ECCELLENZA 2018

SERIE GENERALE

Spediz. abb. post. - art. 1, comma 1
Legge 27-02-2004, n. 46 - Filiale di Roma

Anno 159° - Numero 205

GAZZETTA UFFICIALE

DELLA REPUBBLICA ITALIANA

PARTE PRIMA — Roma - Martedì, 4 settembre 2018 — SI PUBBLICA TUTTI I GIORNI NON FESTIVI

DECRETO LEGISLATIVO 10 agosto 2018, n. 101.

Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). (18G00129) . . . . . .

Highlights

Art. 154-bis

Linee Guida per PMI

In considerazione delle esigenze di semplificazione delle micro, piccole e medie imprese, il Garante promuove **linee guida** recanti **modalita' semplificate** di adempimento degli obblighi del titolare del trattamento

Comunicato stampa del Consiglio dei Ministri n. 14 dell' 8 agosto 2018

In considerazione delle esigenze di semplificazione delle micro, piccole e medie imprese, si è previsto che il Garante promuova modalità semplificate di adempimento degli obblighi del titolare del trattamento.

Unione Province d'Italia
UPI
Emilia-Romagna

CENTRO STUDI PRIVACY E NUOVE TECNOLOGIE

LE FONTI AWARDS
WINNER 2018

ORLANDI&PARTNERS
STUDIOLEGALE
BOUTIQUE DI ECCELLENZA 2018

SERIE GENERALE

Spediz. abb. post. - art. 1, comma 1
Legge 27-02-2004, n. 46 - Filiale di Roma

Anno 159° - Numero 205

GAZZETTA UFFICIALE

DELLA REPUBBLICA ITALIANA

PARTE PRIMA — Roma - Martedì, 4 settembre 2018 — SI PUBBLICA TUTTI I GIORNI NON FESTIVI

DECRETO LEGISLATIVO 10 agosto 2018, n. 101.

Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). (18G00129) . . . . . .

Highlights

Art. 2-quinquies

14 anni

Consenso del minore

servizi della **societa' dell'informazione**

linguaggio particolarmente chiaro e semplice, conciso ed esaustivo, facilmente accessibile e comprensibile dal minore, al fine di rendere significativo il consenso prestato da quest'ultimo

Unione Province d'Italia
UPI
Emilia-Romagna

CENTRO STUDI PRIVACY E NUOVE TECNOLOGIE

LE FONTI AWARDS WINNER 2018

ORLANDI&PARTNERS STUDIOLEGALE
BOUTIQUE DI ECCELLENZA 2018

SERIE GENERALE

Spediz. abb. post. - art. 1, comma 1
Legge 27-02-2004, n. 46 - Filiale di Roma

Anno 159° - Numero 205

GAZZETTA UFFICIALE

DELLA REPUBBLICA ITALIANA

PARTE PRIMA — Roma - Martedì, 4 settembre 2018 — SI PUBBLICA TUTTI I GIORNI NON FESTIVI

DECRETO LEGISLATIVO 10 agosto 2018, n. 101.

Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). (18G00129) . . . . . .

Highlights

RELAZIONE ILLUSTRATIVA

Vengono poi delineate, all'art. 2-quinquies, talune regole per il *"Consenso del minore in relazione ai servizi della società dell'informazione"*. L'articolo rappresenta un esercizio di delega in materia riservata da parte del legislatore statale, chiamato a fissare la soglia minima di età ai fini della validità del consenso espresso dal minore. Si è comunque stabilito che il minore debba avere almeno sedici anni al fine di prestare un valido consenso al trattamento dei propri dati in tale ambito, come, di norma, previsto dal Regolamento. Tale disposizione è circoscritta ai trattamenti che vengono effettuati nell'ambito dei servizi della società dell'informazione, vale a dire quei servizi prestati normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario. Si tratta ad esempio dei trattamenti di dati conseguenti all'iscrizione a *social network* o a servizi di messaggistica. La norma è dunque volta a tutelare il minore in quei contesti virtuali ove risulta maggiormente esposto a causa di una minore consapevolezza dei rischi insiti nella "rete". La disposizione, infatti, rende l'operatore consapevole del fatto che minori possono accedere ai servizi, e quindi richiede di apprestare le relative misure. All'infuori dell'ambito dei servizi della società dell'informazione, permane in ogni caso il limite dei diciotto anni per la prestazione di un valido consenso al trattamento dei dati personali.

SERIE GENERALE

Spediz. abb. post. - art. 1, comma 1
Legge 27-02-2004, n. 46 - Filiale di Roma

Anno 159° - Numero 205

GAZZETTA UFFICIALE

DELLA REPUBBLICA ITALIANA

PARTE PRIMA — Roma - Martedì, 4 settembre 2018 — SI PUBBLICA TUTTI I GIORNI NON FESTIVI

DECRETO LEGISLATIVO 10 agosto 2018, n. 101.

Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). (18G00129) . . . . . .

Highlights

Art. 2-undecies e duodecies

Limitazioni ai diritti dell'interessato

riciclaggio
sostegno alle vittime di richieste estorsive
Commissioni parlamentari d'inchiesta
politica monetaria e valutaria, al sistema dei pagamenti, al controllo degli intermediari e dei mercati creditizi e finanziari, nonche' alla tutela della loro stabilita'
svolgimento delle investigazioni difensive esercizio di un diritto in sede giudiziaria
riservatezza dell'identita' del dipendente (whistleblowing)

Unione Province d'Italia
UPI
Emilia-Romagna

CENTRO STUDI PRIVACY E NUOVE TECNOLOGIE

LE FONTI AWARDS
WINNER 2018

ORLANDI&PARTNERS
STUDIOLEGALE
BOUTIQUE DI ECCELLENZA 2018

SERIE GENERALE

Spediz. abb. post. - art. 1, comma 1
Legge 27-02-2004, n. 46 - Filiale di Roma

Anno 159° - Numero 205

GAZZETTA UFFICIALE

DELLA REPUBBLICA ITALIANA

PARTE PRIMA — Roma - Martedì, 4 settembre 2018 — SI PUBBLICA TUTTI I GIORNI NON FESTIVI

DECRETO LEGISLATIVO 10 agosto 2018, n. 101.

Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). (18G00129) . . . . . .

Highlights

Art. 2-terdecies

Dati relativi a persone decedute

diritti esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato, in qualita' di suo mandatario, o per ragioni familiari meritevoli di protezione

"testamento digitale" per i servizi della società dell'informazione, non equivoco, specifico, libero e informato

Unione Province d'Italia
UPI
Emilia-Romagna

CENTRO STUDI PRIVACY E NUOVE TECNOLOGIE

LE FONTI AWARDS
WINNER 2018

ORLANDI&PARTNERS
STUDIOLEGALE
BOUTIQUE DI ECCELLENZA 2018

GDPR=

Unione Province d'Italia
UPI
Emilia-Romagna

CENTRO STUDI
PRIVACY E NUOVE
TECNOLOGIE

LE FONTI
AWARDS
WINNER 2018

ORLANDI&PARTNERS
STUDIOLEGALE
BOUTIQUE DI ECCELLENZA 2018

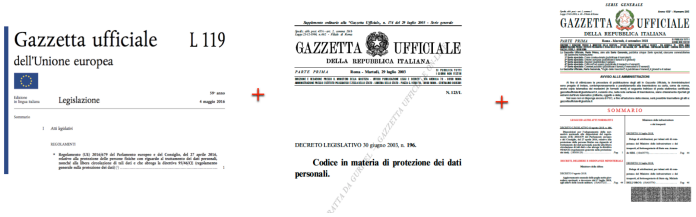
Il completamento (?)
del quadro normativo

Provvedimenti attuativi definiti o in «lavorazione»

- Provvedimento contenente le prescrizioni contenute nelle «vecchie» autorizzazioni generali ritenute compatibili con il nuovo Regolamento (provv. 5 giugno 2019, doc. web 9124510)

- Decreto del Ministro della Giustizia in materia di trattamento dei dati giudiziari (vedi art. 2-octies del Codice e art. 22, comma 12, d.lgs. n. 101/2018)

Il completamento (?)
del quadro normativo



- Le nuove regole deontologiche

- I 2 Codici di deontologia trasformati in Codici di condotta:

  1. Codice di condotta per il trattamento dei dati personali in materia di informazioni commerciali (provv. del 12 giugno 2019)

  2. Codice di condotta per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti (provv. 12 settembre 2019)

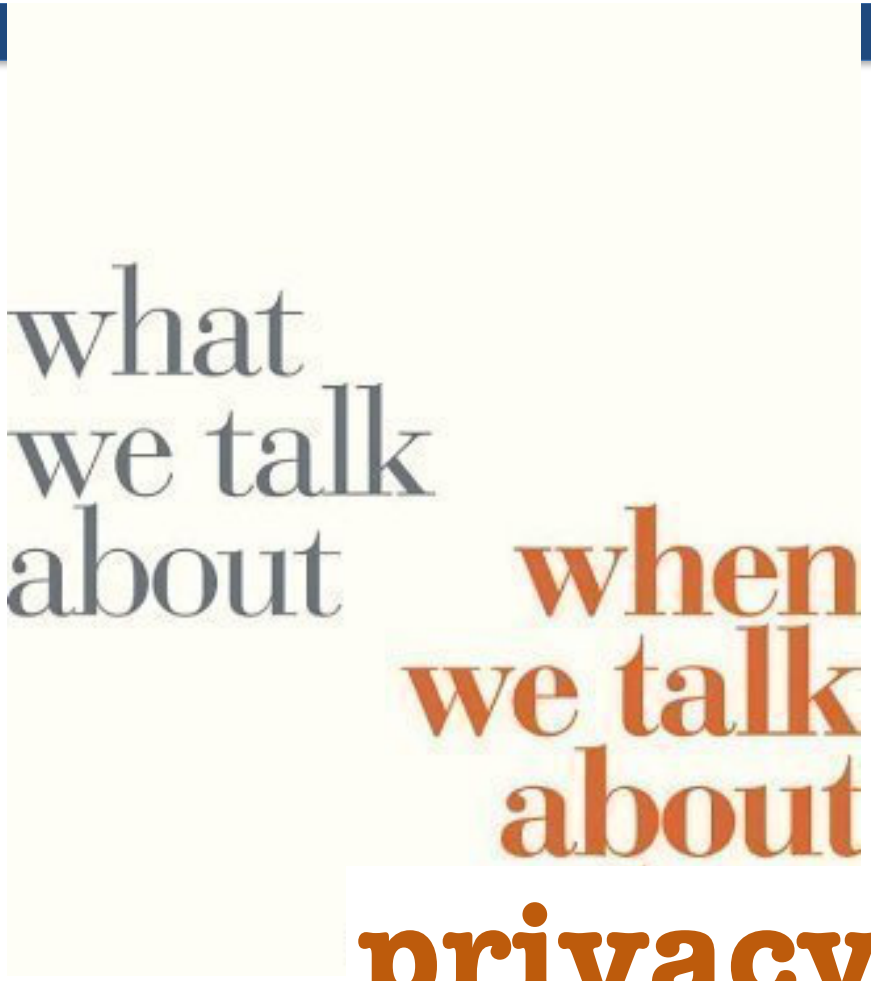
Il completamento (?) del quadro normativo

- Nuovi Codici di condotta attualmente in gestazione e prospettive di sviluppo di questo strumento di «*accountability*»

- Il provvedimento contenente le «misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute (in lavorazione)

- I nuovi regolamenti n° 1/2019 e n° 2/2019 sui procedimenti dinanzi al Garante e la relativa tempistica (v. Gazz. Uff. 8 maggio 2019)

(parafrasando Carver…)



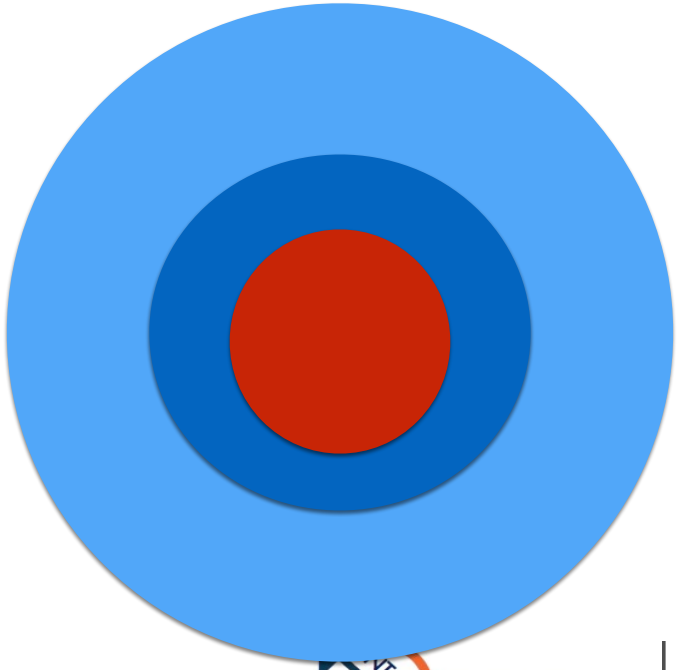
“*LA VITA DEGLI ALTRI*”:
IL BENE DA PROTEGGERE

NO PRIVACY

Informazioni su **soggetti <u>diversi</u> da persone fisiche** quali persone giuridiche; enti; IA **(!!!!)**

Dati anonimi

SI' PRIVACY



Unione Province d'Italia
UPI
Emilia-Romagna

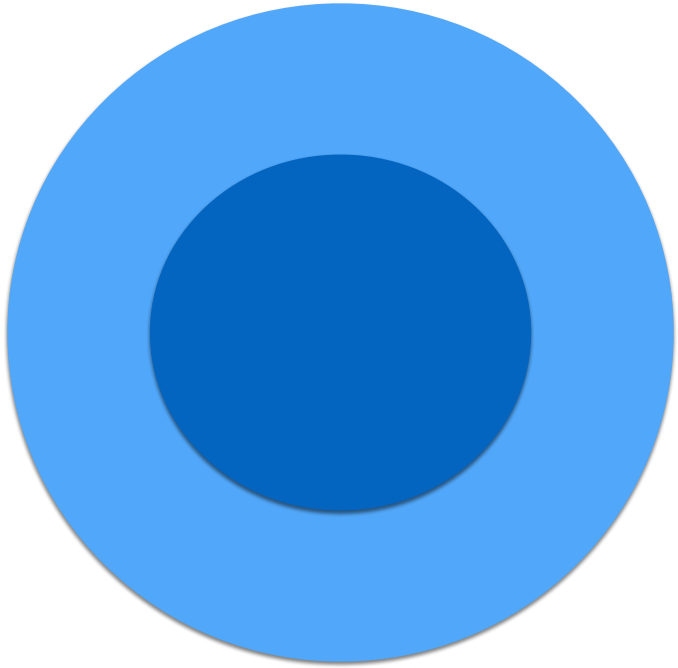
CENTRO STUDI
PRIVACY E NUOVE
TECNOLOGIE

LE FONTI
AWARDS
WINNER 2018

ORLANDI&PARTNERS
STUDIOLEGALE
BOUTIQUE DI ECCELLENZA 2018

dati personali: qualsiasi informazione concernente una persona fisica identificata o identificabile; inclusi i dati oggetto di **pseudonimizzazione**, ossia trattati in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile

categorie particolari di dati personali: dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, come pure trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona o dati relativi alla salute o alla vita sessuale e all'orientamento sessuale.



dati relativi alla salute: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute

dati biometrici: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici

dati genetici: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione

Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del d.lgs. 10 agosto 2018, n. 101

(In corso di pubblicazione sulla Gazzetta Ufficiale)

Registro dei provvedimenti n. 146 del 5 giugno 2019

1. Prescrizioni relative al trattamento di categorie particolari di dati nei rapporti di lavoro (aut. gen. n. 1/2016);
2. Prescrizioni relative al trattamento di categorie particolari di dati da parte degli organismi di tipo associativo, delle fondazioni, delle chiese e associazioni o comunit. religiose (aut. gen. n. 3/2016);
3. Prescrizioni relative al trattamento di categorie particolari di dati da parte degli investigatori privati (aut. gen. n. 6/2016);
4. Prescrizioni relative al trattamento dei dati genetici (aut. gen. n. 8/2016);
5. Prescrizioni relative al trattamento dei dati personali effettuato per scopi di ricerca scientifica (aut. gen. n. 9/2016).

I CUSTODI
DELLA "*VITA DEGLI ALTRI*"

Unione Province d'Italia
UPI
Emilia-Romagna

CENTRO STUDI
PRIVACY E NUOVE
TECNOLOGIE

LE FONTI
AWARDS
WINNER 2018

ORLANDI&PARTNERS
STUDIOLEGALE
BOUTIQUE DI ECCELLENZA 2018

196	GDPR	RGPD
Titolare del trattamento	Data controller	Titolare del trattamento
Responsabile del trattamento	Data processor	Responsabile del trattamento
	Data protection officer	Responsabile della protezione dei dati
Incaricato del trattamento	Any person acting under the authority of the controller or of the processor	Chiunque agisca sotto la sua autorità o sotto quella del responsabile del trattamento
Amministratore di sistema		

IL *CORE* DEL GDPR:
L' "ALGORITMO SPIDERMAN"

Unione Province d'Italia
UPI
Emilia-Romagna

CENTRO STUDI PRIVACY E NUOVE TECNOLOGIE

LE FONTI AWARDS
WINNER 2018

ORLANDI&PARTNERS
STUDIOLEGALE
BOUTIQUE DI ECCELLENZA 2018

ACCOUNTABILITY

ACCOUNTABILITY

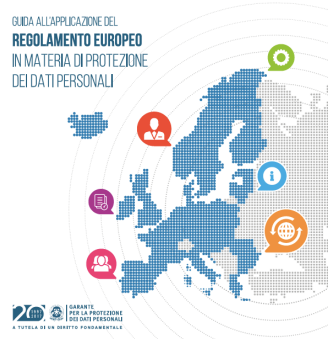
Il **titolare** del trattamento
è GREAT POWER
per il rispetto dei **PRINCIPI**
e in grado di **comprovarlo**

ACCOUNTABILITY

ossia, adozione di **comportamenti proattivi** e tali da **dimostrare la concreta adozione di misure** finalizzate ad assicurare l'applicazione (dei **PRINCIPI**) del regolamento.

Si tratta di una **grande novità** per la protezione dei dati in quanto **viene affidato ai titolari** il compito di **decidere autonomamente** le modalità, le garanzie e i limiti del trattamento dei dati personali

ACCOUNTABILITY  PRINCIPI



PRINCIPI APPLICABILI AL TRATTAMENTO DI DATI PERSONALI

I dati personali sono:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato **(«liceità, correttezza e trasparenza»)**

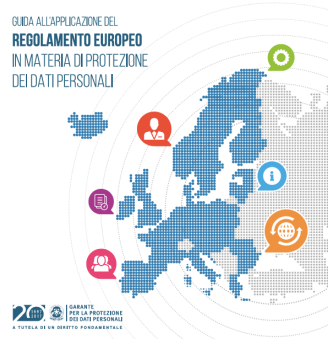
b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità (…); **(«limitazione della finalità»)**

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati **(«minimizzazione dei dati»)**

d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati **(«esattezza»)**

e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati **(«limitazione della conservazione»)**

f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («**integrità e riservatezza**»)



RESPONSABILITA' GENERALE DEL TITOLARE

Unione Province d'Italia
UPI
Emilia-Romagna

CENTRO STUDI PRIVACY E NUOVE TECNOLOGIE

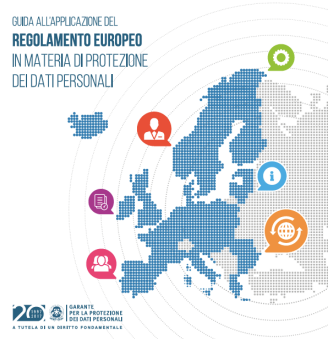
LE FONTI AWARDS
WINNER 2018

ORLANDI&PARTNERS
STUDIOLEGALE
BOUTIQUE DI ECCELLENZA 2018

ACCOUNTABILITY

Responsabilità del titolare del trattamento **(art. 24 GDPR)**

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.



PRIVACY BY DEFAULT & BY DESIGN

PBD

Proactive not reactive, Preventative not remedial
(Proattivo non reattivo, preventivo non correttivo).
Privacy as the Default Setting
(Privacy come impostazione predefinita).
Privacy Embedded into design
(Privacy incorporata nella progettazione).
Full functionality – Positive-sum, Not zero-sum
(Massima funzionalità, valore positivo e non valore zero).
End-to-end security – full lifecycle protection
(Sicurezza fino alla fine, durante tutto il ciclo del prodotto o servizio).
Visibility and transparency – keep it Open
(Visibilità e trasparenza).
Respect for User Privacy – keep it User-Centric
(Rispetto per la privacy dell'utente, centralità dell'utente).

PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE

(Privacy by design)

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati

Tali misure potrebbero consistere, tra l'altro, nel ridurre al minimo il trattamento dei dati personali, pseudonimizzare i dati personali il più presto possibile, offrire trasparenza per quanto riguarda le funzioni e il trattamento di dati personali, consentire all'interessato di controllare il trattamento dei dati e consentire al titolare del trattamento di creare e migliorare caratteristiche di sicurezza **(considerando n. 78 GDPR)**

PROTEZIONE PER IMPOSTAZIONE PREDEFINITA

(Privacy by default)

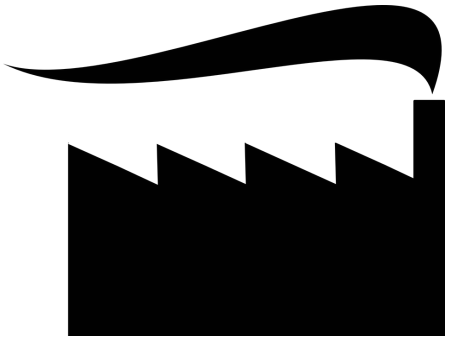
Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica

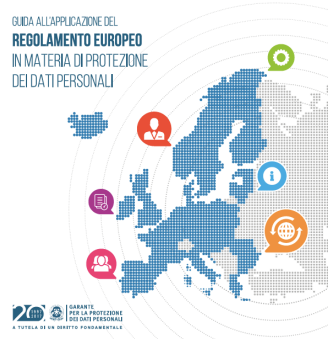
In fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, a far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati **(considerando n. 78 GDPR)**

PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE

(Privacy by design)

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento **mette in atto misure tecniche e organizzative adeguate**, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati





SICUREZZA DEI DATI

Unione Province d'Italia
UPI
Emilia-Romagna

CENTRO STUDI
PRIVACY E NUOVE
TECNOLOGIE

LE FONTI
AWARDS
WINNER 2018

ORLANDI&PARTNERS
STUDIOLEGALE
BOUTIQUE DI ECCELLENZA 2018

SICUREZZA > DATA BREACH

SICUREZZA DEL TRATTAMENTO

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, 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.

Nel valutare l'adeguato livello di sicurezza, **si tiene conto in special modo** dei **rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.**

ACCOUNTABILITY: CHE COSA IMPLICA?

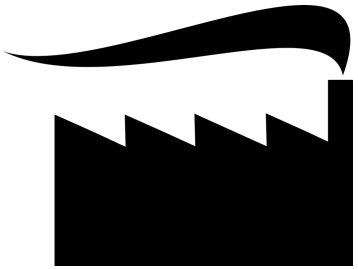
SICUREZZA ADEGUATA (E NON PIU' MINIMA..)

SICUREZZA DEL TRATTAMENTO

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, 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.

Nel valutare l'adeguato livello di sicurezza, **si tiene conto in special modo** dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

MISURE TECNICHE E ORGANIZZATIVE "TIPICHE" *("SE DEL CASO")*



la pseudonimizzazione *

la **cifratura** dei dati personali

la capacità di **assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza** dei sistemi e dei servizi di trattamento

la capacità di **ripristinare tempestivamente la disponibilità e l'accesso dei dati** in caso di incidente fisico o tecnico

una **procedura** per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento

ACCOUNTABILITY: CHE COSA IMPLICA?

SICUREZZA ADEGUATA (E NON PIU' MINIMA..)

Le misure di sicurezza devono "garantire un livello di sicurezza adeguato al rischio" del trattamento; **la lista di cui al paragrafo 1 dell'art. 32 è una lista aperta e non esaustiva ("tra le altre, se del caso").**
Per lo stesso motivo, **non potranno sussistere dopo il 25 maggio 2018 obblighi generalizzati di adozione di misure "minime" di sicurezza** poiché **tale valutazione sarà rimessa, caso per caso, al titolare e al responsabile.**

Art. 31 Codice Privacy

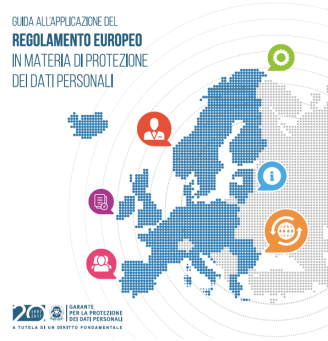
Obblighi di sicurezza

1. I dati personali oggetto di trattamento sono custoditi e controllati, **anche in relazione alle conoscenze acquisite** in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di **idonee e preventive** misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

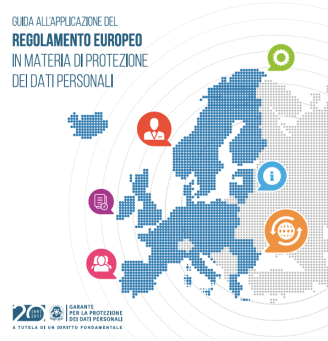
UNO *SWITCH* CULTURALE!

*"**Più armonizzazione, più adattamento alla realtà tecnologica che oggi a distanza di vent'anni è completamente diversa.** Il nuovo regolamento introduce maggiori garanzie per gli interessati e anche **maggiori responsabilità per chi tratta i dati.***

*La **novità dell'accountability** significa che potremmo esigere dai titolari del trattamento **maggiore proattività** nella **definizione della loro policy interna, nella distribuzione di ruoli, nella valutazione dei rischi**. Al tempo stesso, le autorità regolatore dovranno essere **ragionevolmente più selettive** e anche accettare di più ciò che è sostenibile giuridicamente, ma non condivisibile al 100%"*



ACCOUNTABILITY: CHE COSA IMPLICA?



TITOLARI, CONTITOLARI, RESPONSABILI

ACCOUNTABILITY: CHE COSA IMPLICA?

CONTRATTI/ACCORDI PIU' CHIARI (E NUOVI…)

CONTITOLARI DEL TRATTAMENTO

Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento dei dati personali, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito al rispetto degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni.Tale accordo può designare un punto di contatto per gli interessati.

L'accordo riflette adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.

Indipendentemente dalle disposizioni dell'accordo, l'interessato può esercitare i propri diritti nei confronti di e contro ciascun titolare del trattamento

RESPONSABILI DEL TRATTAMENTO

I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento.

Il contratto o altro atto giuridico è stipulato in forma scritta, anche in formato elettronico.

ACCOUNTABILITY: CHE COSA IMPLICA?

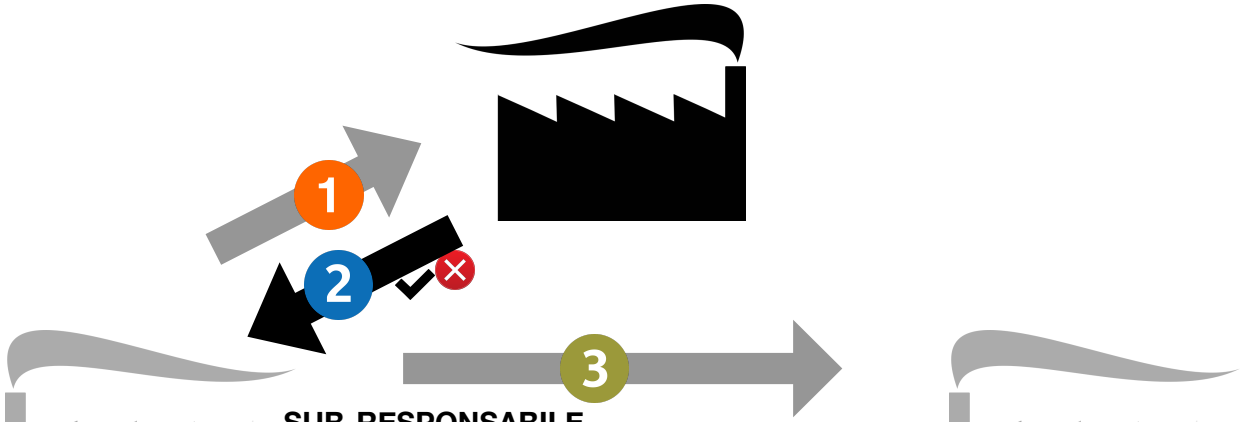
CONTRATTI/ACCORDI PIU' CHIARI (E NUOVI…)

CONTENUTI MINIMI
materia disciplinata
durata del trattamento
natura e finalità del trattamento
tipo di dati personali
categorie di interessati
obblighi e diritti del responsabile del trattamento

Il **contratto tra titolare e responsabile** deve prevedere che il responsabile:
a) tratti i dati personali **soltanto su istruzione documentata** del titolare del trattamento (…)
b) garantisca che l**e persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo statutario di riservatezza**;
c) adotti **tutte le misure (di sicurezza) richieste** ai sensi dell'articolo 32;
d) rispetti **le condizioni per ricorrere a un altro responsabile** del trattamento
e) **assista** il titolare del trattamento con misure tecniche ed organizzative adeguate al fine di soddisfare l'obbligo del titolare del trattamento di **dare seguito alle richieste per l'esercizio dei diritti dell'interessato**;
f) **assista** il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 (**sicurezza; data breaches; DPIA; prior checking**), tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
g) su scelta del titolare del trattamento, **cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione** dei servizi di trattamento di dati e cancelli le copie esistenti
h) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e **contribuisca agli audit, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato**.

ACCOUNTABILITY: CHE COSA IMPLICA?

CONTRATTI/ACCORDI PIU' CHIARI (E NUOVI…)



SUB-RESPONSABILE

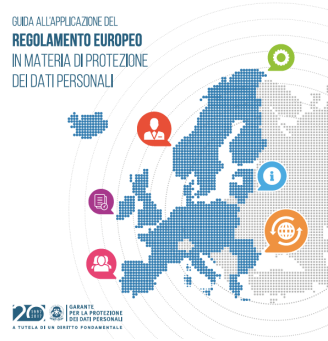
Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.

CONTRATTO TRA RESPONSABILE E SUB-RESPONSABILE

Il contratto è stipulato in forma scritta, anche in formato elettronico.

Al sub-responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento.

Qualora l'altro responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile.



REGISTRO DEI TRATTAMENTI

Unione Province d'Italia
UPI
Emilia-Romagna

CENTRO STUDI
PRIVACY E NUOVE
TECNOLOGIE

LE FONTI
AWARDS
WINNER 2018

ORLANDI&PARTNERS
STUDIOLEGALE
BOUTIQUE DI ECCELLENZA 2018

NOTIFICAZIONE BYE BYE (E BENVENUTO REGISTRO!)

ACCOUNTABILITY

CONSIDERANDO 82 GDPR:
Per dimostrare che si conforma al presente regolamento, il titolare del trattamento o il responsabile del trattamento dovrebbe tenere un registro delle attività di trattamento effettuate sotto la sua responsabilità. Sarebbe necessario obbligare tutti i titolari del trattamento e i responsabili del trattamento a cooperare con l'autorità di controllo e a mettere, su richiesta, detti registri a sua disposizione affinché possano servire per monitorare detti trattamenti.

SERIE GENERALE

Spediz. abb. post. - art. 1, comma 1
Legge 27-02-2004, n. 46 - Filiale di Roma

Anno 159° - Numero 205

GAZZETTA UFFICIALE

DELLA REPUBBLICA ITALIANA

PARTE PRIMA — Roma - Martedì, 4 settembre 2018 — SI PUBBLICA TUTTI I GIORNI NON FESTIVI

DECRETO LEGISLATIVO 10 agosto 2018, n. 101.

Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). (18G00129) . . . . . .

Highlights

Il "vecchio" Registro

Art. 22 Dlgs n. 101/2018

Altre disposizioni transitorie e finali

8. Il registro dei trattamenti di cui all'articolo 37, comma 4, del codice in materia di protezione dei dati personali, di cui al decreto legislativo n. 196 del 2003, cessa di essere alimentato a far data dal 25 maggio 2018. Da tale data e fino al 31 dicembre 2019, il registro resta accessibile a chiunque secondo le modalita' stabilite nel suddetto articolo 37, comma 4, del decreto legislativo n. 196 del 2003.

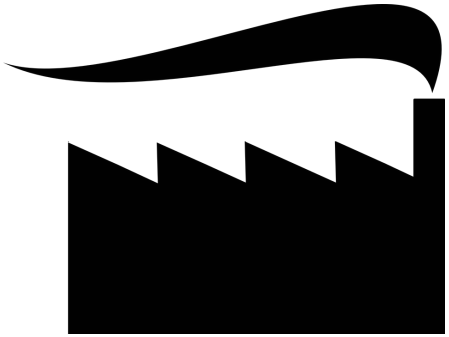
Unione Province d'Italia
UPI
Emilia-Romagna

CENTRO STUDI PRIVACY E NUOVE TECNOLOGIE

LE FONTI AWARDS
WINNER 2018

ORLANDI&PARTNERS
STUDIOLEGALE
BOUTIQUE DI ECCELLENZA 2018

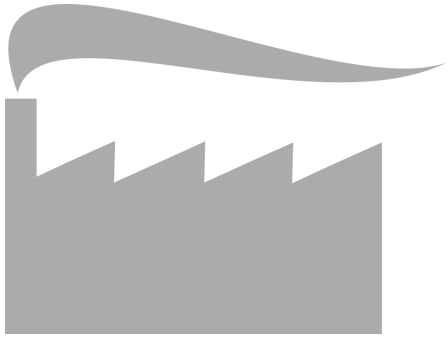
NOTIFICAZIONE BYE BYE (E BENVENUTO REGISTRO!)



REGISTRI DELLE ATTIVITA' DI TRATTAMENTO

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

Su richiesta, il titolare del trattamento, il responsabile del trattamento e l'eventuale rappresentante del titolare del trattamento o del responsabile del trattamento mettono il registro a disposizione dell'autorità di controllo.



ACCOUNTABILITY

FORMA SCRITTA
ANCHE IN FORMATO ELETTRONICO

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Unione Province d'Italia
UPI
Emilia-Romagna

CENTRO STUDI PRIVACY E NUOVE TECNOLOGIE

[redacted]AND|&PARTNERS

WINNER 2018 || BOUTIQUE DI ECCELLENZA 2018

NOTIFICAZIONE BYE BYE (E BENVENUTO REGISTRO!)

Art. 30, c. 5 GDPR:
Gli obblighi di cui ai paragrafi 1 e 2 **non** si applicano alle imprese o organizzazioni **con meno di 250 dipendenti, a meno che** il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10.

Tutti i titolari e i responsabili di trattamento, **eccettuati gli organismi con meno di 250 dipendenti ma solo se non effettuano trattamenti a rischio** (si veda art. 30, paragrafo 5), devono tenere un registro delle operazioni di trattamento i cui contenuti sono indicati all'art. 30. **Si tratta di uno strumento fondamentale** non soltanto ai fini dell'eventuale supervisione da parte del Garante, ma anche allo scopo di **disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda o di un soggetto pubblico – indispensabile per ogni valutazione e analisi del rischio**. Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.

ACCOUNTABILITY: CHE COSA IMPLICA?

NOTIFICAZIONE BYE BYE (E BENVENUTO REGISTRO!)

Art. 30, c. 5 GDPR:
Gli obblighi di cui ai paragrafi 1 e 2 **non** si applicano alle imprese o organizzazioni **con meno di 250 dipendenti, a meno che** il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10.

La tenuta del registro dei trattamenti **non costituisce un adempimento formale bensì parte integrante di un sistema di corretta gestione** dei dati personali. Per tale motivo, si invitano tutti i titolari di trattamento e i responsabili, **a prescindere dalle dimensioni dell'organizzazione**, a compiere i passi necessari per dotarsi di tale registro e, in ogni caso, a compiere un'accurata ricognizione dei trattamenti svolti e delle rispettive caratteristiche – ove già non condotta. I contenuti del registro sono fissati, come detto, nell'art. 30; tuttavia, niente vieta a un titolare o responsabile di **inserire ulteriori informazioni se lo si riterrà opportuno proprio nell'ottica della complessiva valutazione di impatto dei trattamenti svolti**.

ACCOUNTABILITY: CHE COSA IMPLICA?

NOTIFICAZIONE BYE BYE (E BENVENUTO REGISTRO!)

Nello specifico, si richiama l'attenzione sulla **sostanziale coincidenza** fra i contenuti della notifica dei trattamenti di cui all' a**rt. 38 del Codice** e quelli che devono costituire il registro dei trattamenti **ex art. 30 regolamento**; l'Autorità sta valutando di mettere a disposizione un modello di registro dei trattamenti sul proprio sito, che i singoli titolari potranno integrare nei modi opportuni.

Art. 38 (Modalità di notificazione)

1. La notificazione del trattamento è presentata al Garante prima dell'inizio del trattamento ed una sola volta, a prescindere dal numero delle operazioni e della durata del trattamento da effettuare, e può anche riguardare uno o più trattamenti con finalità correlate.

2. La notificazione è validamente effettuata solo se è trasmessa attraverso il sito del Garante, utilizzando l'apposito modello, che contiene la richiesta di fornire tutte e soltanto le seguenti informazioni:

a) le coordinate identificative del titolare del trattamento e, eventualmente, del suo rappresentante, nonché le modalità per individuare il responsabile del trattamento se designato;

b) la o le finalità del trattamento;

c) una descrizione della o delle categorie di persone interessate e dei dati o delle categorie di dati relativi alle medesime;

d) i destinatari o le categorie di destinatari a cui i dati possono essere comunicati;

e) i trasferimenti di dati previsti verso Paesi terzi;

f) una descrizione generale che permetta di valutare in via preliminare l'adeguatezza delle misure adottate per garantire la sicurezza del trattamento.

NOTIFICAZIONE BYE BYE (E BENVENUTO REGISTRO!)

REGISTRO DELLE ATTIVITA' DI TRATTAMENTO (art. 30 GDPR)

Il **registro del titolare del trattamento** contiene:

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

b) le finalità del trattamento;

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

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

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

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

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

Art. 38 CODICE PRIVACY (Modalità di notificazione)

(…)

2. La **notificazione** è validamente effettuata solo se è trasmessa attraverso il sito del Garante, utilizzando l'apposito modello, che contiene la richiesta di fornire tutte e soltanto le seguenti informazioni:

a) le coordinate identificative del titolare del trattamento e, eventualmente, del suo rappresentante, nonché le modalità per individuare **il responsabile del trattamento** se designato;

b) la o le finalità del trattamento;

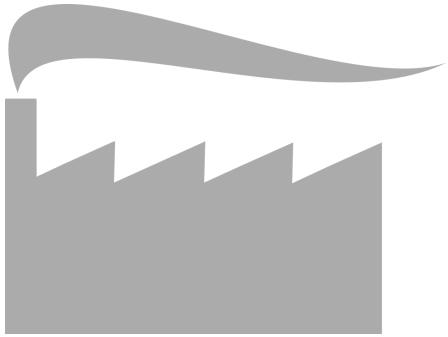
c) una descrizione della o delle categorie di persone interessate e dei dati o delle categorie di dati relativi alle medesime;

d) i destinatari o le categorie di destinatari a cui i dati possono essere comunicati;

e) i trasferimenti di dati previsti verso Paesi terzi;

f) una descrizione generale che permetta di valutare in via preliminare l'adeguatezza delle misure adottate per garantire la sicurezza del trattamento.

NOTIFICAZIONE BYE BYE (E BENVENUTO REGISTRO!)



REGISTRI DELLE ATTIVITA' DI TRATTAMENTO

Ogni responsabile del trattamento e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente:

a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;

b) le categorie dei **trattamenti effettuati per conto di ogni titolare del trattamento;**

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

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

FAQ GARANTE su REGISTRO - 8 ottobre 2018

Regolamento Ue: le istruzioni del Garante privacy sul registro dei trattamenti

Il Garante per la protezione dei dati personali ha messo a disposizione sul proprio sito le istruzioni sul **Registro delle attività di trattamento**, previsto dal Regolamento (EU) n. 679/2016 (di seguito "RGPD").

Il Registro, che deve essere predisposto dal titolare e del responsabile del trattamento, è un documento contenente le principali informazioni (specificatamente individuate dall'art. 30 del Regolamento) relative alle operazioni di trattamento svolte da una impresa, un'associazione, un esercizio commerciale, un libero professionista.

L'obbligo di redigere il Registro costituisce uno dei principali elementi di accountability del titolare, poiché rappresenta uno strumento idoneo a fornire un quadro aggiornato dei trattamenti in essere all'interno della propria organizzazione, indispensabile ai fini della valutazione o analisi del rischio e dunque preliminare rispetto a tale attività.

Il Registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.

Come specificato nelle FAQ del Garante, sono tenuti a redigere il Registro le imprese o le organizzazioni con almeno 250 dipendenti e - al di sotto dei 250 dipendenti - qualunque titolare o responsabile che effettui trattamenti che possano presentare rischi, anche non elevati, per i diritti e le libertà delle persone o che effettui trattamenti non occasionali di dati oppure trattamenti di particolari categorie di dati (come i dati biometrici, dati genetici, quelli sulla salute, sulle convinzioni religiose, sull'origine etnica etc.), o anche di dati relativi a condanne penali e a reati.

Nelle FAQ vengono indicate, tra l'altro, quali informazioni deve contenere il Registro e le modalità per la sua conservazione e il suo aggiornamento.

Roma, 8 ottobre 2018

FAQ GARANTE su REGISTRO - 8 ottobre 2018

FAQ n. 2

Chi è tenuto a redigerlo?

Tutti i titolari e i responsabili del trattamento sono tenuti a redigere il Registro delle attività di trattamento (v. art. 30, par. 1 e 2 del RGPD).

In particolare, in ambito privato, i soggetti obbligati sono così individuabili:

- imprese o organizzazioni con almeno 250 dipendenti;
- qualunque titolare o responsabile (incluse imprese o organizzazioni con meno di 250 dipendenti) che effettui trattamenti che possano presentare un rischio – anche non elevato – per i diritti e le libertà dell'interessato;
- qualunque titolare o responsabile (incluse imprese o organizzazioni con meno di 250 dipendenti) che effettui trattamenti non occasionali;
- qualunque titolare o responsabile (incluse imprese o organizzazioni con meno di 250 dipendenti) che effettui trattamenti delle categorie particolari di dati di cui all'articolo 9, paragrafo 1 RGPD, o di dati personali relativi a condanne penali e a reati di cui all'articolo 10 RGPD.

Rientrano nella categoria delle "organizzazioni" di cui all'art. 30, par. 5 anche le associazioni, fondazioni e i comitati.

FAQ GARANTE su REGISTRO - 8 ottobre 2018

FAQ n. 2

Chi è tenuto a redigerlo?

In particolare, in ambito privato, i soggetti obbligati sono così individuabili:

- esercizi commerciali, esercizi pubblici o artigiani con almeno un dipendente (bar, ristoranti, officine,negozi, piccola distribuzione, ecc.) e/o che trattino dati sanitari dei clienti (es. parrucchieri, estetisti, ottici, odontotecnici, tatuatori ecc.);
- liberi professionisti con almeno un dipendente e/o che trattino dati sanitari e/o dati relativi a condanne penali o reati (es. commercialisti, notai, avvocati, osteopati, fisioterapisti, farmacisti, medici in generale);
- **associazioni, fondazioni e comitati ove trattino "categorie particolari di dati" e/o dati relativi a condanne penali o reati** (i.e. organizzazioni di tendenza; associazioni a tutela di soggetti c.d. "vulnerabili" quali ad esempio malati, persone con disabilità, ex detenuti ecc.; associazioni che perseguono finalità di prevenzione e contrasto delle discriminazioni di genere, razziali, basate sull'orientamento sessuale, politico o religioso ecc.; associazioni sportive con riferimento ai dati sanitari trattati; partiti e movimenti politici; sindacati; associazioni e movimenti a carattere religioso);
- **il condominio ove tratti "categorie particolari di dati" (es. delibere per interventi volti al superamento e all'abbattimento delle barriere architettoniche ai sensi della L. n. 13/1989; richieste di risarcimento danni comprensive di spese mediche relativi a sinistri avvenuti all'interno dei locali condominiali).**

FAQ GARANTE su REGISTRO - 8 ottobre 2018

MISURA DI SEMPLIFICAZIONE

SOTTO I 250 dipendenti, l'obbligo di redazione del registro può essere circoscritto alle sole specifiche attività di trattamento sopra individuate (es. ove il trattamento delle categorie particolari di dati si riferisca a quelli inerenti un solo lavoratore dipendente, il registro potrà essere predisposto e mantenuto esclusivamente con riferimento a tale limitata tipologia di trattamento).

FAQ GARANTE su REGISTRO - 8 ottobre 2018

FAQ n. 4

Può contenere informazioni ulteriori?

Può essere riportata nel registro **qualsiasi altra informazione** che il titolare o il responsabile ritengano utile indicare (ad es. le modalità di raccolta del consenso, le eventuali valutazioni di impatto effettuate, l'indicazione di **eventuali "referenti interni"** individuati dal titolare in merito ad alcune tipologie di trattamento ecc.).

FAQ GARANTE su REGISTRO - 8 ottobre 2018

FAQ n. 5

Quali sono le modalità di conservazione e di aggiornamento?

Il Registro dei trattamenti è un documento di censimento e analisi dei trattamenti effettuati dal titolare o responsabile.

In quanto tale, il registro deve essere **mantenuto costantemente aggiornato** poiché il suo contenuto deve sempre corrispondere all'effettività dei trattamenti posti in essere. Qualsiasi cambiamento, in particolare in ordine alle modalità, finalità, categorie di dati, categorie di interessati, deve essere immediatamente inserito nel Registro, dando conto delle modifiche sopravvenute.

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

"- scheda creata in data XY"

"- ultimo aggiornamento avvenuto in data XY"

FAQ GARANTE su REGISTRO - 8 ottobre 2018

Modello di “registro semplificato” delle attività di trattamento del titolare per PMI (ALLEGATO 1)

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

SCHEDA REGISTRO DEI TRATTAMENTI *[per i contenuti vedi Faq sul registro delle attività di trattamento: https://www.garanteprivacy.it/regolamentoue/registro]*							
TITOLARE/CONTITOLARE/RAPPRESENTANTE DEL TITOLARE *[inserire la denominazione e i dati di contatto]*							
RESPONSABILE DELLA PROTEZIONE DEI DATI *[inserire la denominazione e i dati di contatto]*							
TIPOLOGIA DI TRATTAMENTO	**FINALITA' E BASI LEGALI DEL TRATTAMENTO**	**CATEGORIE DI INTERSSATI**	**CATEGORIE DI DATI PERSONALI**	**CATEGORIE DI DESTINATARI** *[indicare eventuali responsabili del trattamento o altri titolari cui i dati siano comunicati]*	**TRASFERIMENTO DATI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI** *[indicare il Paese terzo o l'organizzazione internazionale cui i dati sono trasferiti e le “garanzie” adottate ai sensi del capo V del RGPD]*	**TERMINI ULTIMI DI CANCELLAZIONE PREVISTI**	**MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE**

FAQ GARANTE su REGISTRO - 8 ottobre 2018

Modello di “registro semplificato” delle attività di trattamento del titolare per PMI (ALLEGATO 1)

TIPOLOGIA DI TRATTAMENTO	FINALITA' E BASI LEGALI DEL TRATTAMENTO

nel campo **“finalità del trattamento”** oltre alla precipua indicazione delle stesse, **distinta per tipologie di trattamento** (es. trattamento dei dati dei dipendenti per la gestione del rapporto di lavoro; trattamento dei dati di contatto dei fornitori per la gestione degli ordini), sarebbe opportuno indicare anche **la base giuridica** dello stesso (v. art. 6 del RGPD; in merito, con particolare riferimento al **“legittimo interesse”**, si rappresenta che il registro potrebbe riportare la descrizione del legittimo interesse concretamente perseguito, le “garanzie adeguate” eventualmente approntate, nonché, ove effettuata, la preventiva valutazione d’impatto posta in essere dal titolare (v. provv. del Garante del 22 febbraio 2018 – [doc web n. 8080493]).

Sempre con riferimento alla base giuridica, sarebbe parimenti opportuno: in caso di **trattamenti di “categorie particolari di dati”**, indicare una delle condizioni di cui all’art. 9, par. 2 del RGPD; in caso di **trattamenti di dati relativi a condanne penali e reati**, riportare la specifica normativa (nazionale o dell’Unione europea) che ne autorizza il trattamento ai sensi dell’art. 10 del RGPD

FAQ GARANTE su REGISTRO - 8 ottobre 2018

Modello di "registro semplificato" delle attività di trattamento del titolare per PMI (ALLEGATO 1)

nel campo "**descrizione delle categorie di interessati e delle categorie di dati personali**" andranno specificate **sia le tipologie di interessati** (es. clienti, fornitori, dipendenti) sia **quelle di dati personali oggetto di trattamento** (es. dati anagrafici, dati sanitari, dati biometrici, dati genetici, dati relativi a condanne penali o reati, ecc.);

FAQ GARANTE su REGISTRO - 8 ottobre 2018

Modello di "registro semplificato" delle attività di trattamento del titolare per PMI (ALLEGATO 1)

nel campo **"categorie di destinatari a cui i dati sono stati o saranno comunicati"** andranno riportati, anche semplicemente per categoria di appartenenza, **gli altri titolari** cui siano comunicati i dati (es. enti previdenziali cui debbano essere trasmessi i dati dei dipendenti per adempiere agli obblighi contributivi). Inoltre, si ritiene **opportuno che siano indicati anche gli eventuali altri soggetti ai quali – in qualità di responsabili e sub-responsabili del trattamento– siano trasmessi i dati da parte del titolare** (es. soggetto esterno cui sia affidato dal titolare il servizio di elaborazione delle buste paga dei dipendenti o altri soggetti esterni cui siano affidate in tutto o in parte le attività di trattamento). Ciò al fine di consentire al titolare medesimo di avere effettiva contezza del novero e della tipologia dei soggetti esterni cui sono affidate le operazioni di trattamento dei dati personali

FAQ GARANTE su REGISTRO - 8 ottobre 2018

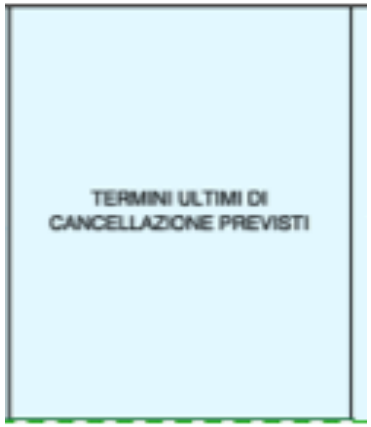
Modello di "registro semplificato" delle attività di trattamento del titolare per PMI (ALLEGATO 1)


TRASFERIMENTO
DATI VERSO PAESI
TERZI O ORGANIZZAZIONI
INTERNAZIONALI *[indicare il Paese terzo o l'organizzazione internazionale cui i dati sono trasferiti e le "garanzie" adottate ai sensi del capo V del RGPD]*

nel campo **"trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale"** andrà riportata l'informazione relativa ai **suddetti trasferimenti** unitamente all'indicazione relativa al **Paese/i terzo/i cui i dati sono trasferiti** e alle **"garanzie" adottate** ai sensi del capo V del RGPD (es. decisioni di adeguatezza, norme vincolanti d'impresa, clausole contrattuali tipo, ecc.);

FAQ GARANTE su REGISTRO - 8 ottobre 2018

Modello di "registro semplificato" delle attività di trattamento del titolare per PMI (ALLEGATO 1)



nel campo **"termini ultimi previsti per la cancellazione delle diverse categorie di dati"** dovranno essere individuati i **tempi di cancellazione per tipologia e finalità di trattamento** (ad es. "in caso di rapporto contrattuale, i dati saranno conservati per 10 anni dall'ultima registrazione – v. art. 2220 del codice civile").

Ad ogni modo, ove non sia possibile stabilire a priori un termine massimo, i tempi di conservazione potranno essere specificati mediante il riferimento a **criteri** (es. norme di legge, prassi settoriali) indicativi degli stessi (es. "in caso di contenzioso, i dati saranno cancellati al termine dello stesso")

FAQ GARANTE su REGISTRO - 8 ottobre 2018

Modello di "registro semplificato" delle attività di trattamento del titolare per PMI (ALLEGATO 1)

nel campo **"descrizione generale delle misure di sicurezza"** andranno indicate le misure tecnico-organizzative adottate dal titolare ai sensi dell'art. 32 del RGDP tenendo presente che l'elenco ivi riportato costituisce **una lista aperta e non esaustiva,** essendo rimessa al titolare la valutazione finale relativa al livello di sicurezza adeguato, caso per caso, ai rischi presentati dalle attività di trattamento concretamente poste in essere.

Tale lista ha di per sé un **carattere dinamico** (e non più statico come è stato per l'Allegato B del d. lgs. 196/2003) dovendosi continuamente confrontare con gli sviluppi della tecnologia e l'insorgere di nuovi rischi. Le misure di sicurezza possono essere descritte **in forma riassuntiva e sintetica, o comunque idonea** a dare un quadro generale e complessivo di tali misure in relazione alle attività di trattamento svolte, con possibilità di fare rinvio per una valutazione più dettagliata a documenti esterni di carattere generale (es. procedure organizzative interne; security policy ecc.).

FAQ GARANTE su REGISTRO - 8 ottobre 2018

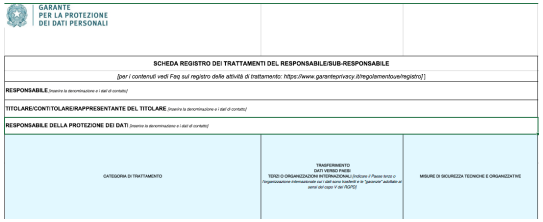
Modello di “registro semplificato” delle attività di trattamento del responsabile per PMI (ALLEGATO 2)

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

SCHEDA REGISTRO DEI TRATTAMENTI DEL RESPONSABILE/SUB-RESPONSABILE		
[per i contenuti vedi Faq sul registro delle attività di trattamento: https://www.garanteprivacy.it/regolamentoue/registro]]		
RESPONSABILE *[inserire la denominazione e i dati di contatto]*		
TITOLARE/CONTITOLARE/RAPPRESENTANTE DEL TITOLARE *[inserire la denominazione e i dati di contatto]*		
RESPONSABILE DELLA PROTEZIONE DEI DATI *[inserire la denominazione e i dati di contatto]*		
CATEGORIA DI TRATTAMENTO	TRASFERIMENTO DATI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI *[indicare il Paese terzo o l'organizzazione internazionale cui i dati sono trasferiti e le "garanzie" adottate ai sensi del capo V del RGPD]*	MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE

FAQ GARANTE su REGISTRO - 8 ottobre 2018

Modello di “registro semplificato” delle attività di trattamento del responsabile per PMI (ALLEGATO 2)


GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

SCHEDA REGISTRO DEI TRATTAMENTI DEL RESPONSABILE/SUB-RESPONSABILE

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

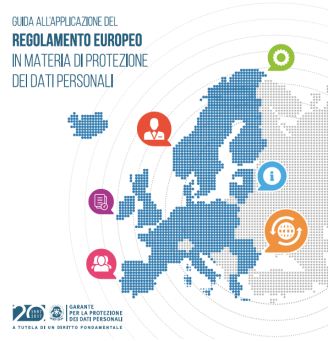
RESPONSABILE (inserire la denominazione e i dati di contatto)

TITOLARE/CONTITOLARE/RAPPRESENTANTE DEL TITOLARE (inserire la denominazione e i dati di contatto)

RESPONSABILE DELLA PROTEZIONE DEI DATI (inserire la denominazione e i dati di contatto)

CATEGORIA DI TRATTAMENTO	TRASFERIMENTO DATI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI (indicare il Paese terzo o l'organizzazione internazionale cui i dati sono trasferiti e le "garanzie" adottate ai sensi del capo V del RGPD)	MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE

- nel caso in cui uno stesso soggetto agisca in qualità di responsabile del trattamento per conto di più clienti quali autonomi e distinti titolari (es. società di software house), l**e informazioni di cui all’art. 30, par. 2 del RGPD dovranno essere riportate nel registro con riferimento a ciascuno dei suddetti titolari**. In questi casi **il responsabile dovrà suddividere il registro in tante sezioni** quanti sono i titolari per conto dei quali agisce; ove, a causa dell’ingente numero di titolari per cui si operi, l’attività di puntuale indicazione e di continuo aggiornamento dei nominativi degli stessi nonché di correlazione delle categorie di trattamenti svolti per ognuno di essi risulti eccessivamente difficoltosa, il registro del responsabile potrebbe riportare il rinvio, ad es., a schede o banche dati anagrafiche dei clienti (titolari del trattamento), contenenti la descrizione dei servizi forniti agli stessi, ferma restando la necessità che comunque tali schede riportino tutte le indicazioni richieste dall’art. 30, par. 2 del RGPD;
- con riferimento alla **“descrizione delle categorie di trattamenti effettuati”** (art. 30, par. 2, lett. b) del RGPD) è possibile **far riferimento a quanto contenuto nel contratto di designazione a responsabile** che, ai sensi dell’art. 28 del RGPD, deve individuare, in particolare, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati oggetto del trattamento, nonché la durata di quest’ultimo;
- in caso di **sub-responsabile**, parimenti, il registro delle attività di trattamento svolte da quest’ultimo potrà specificatamente far riferimento ai contenuti del contratto stipulato tra lo stesso e il responsabile ai sensi dell’art. 28, paragrafi 2 e 4 del RGPD.



DPIA: VALUTAZIONE DI IMPATTO

ACCOUNTABILITY: CHE COSA IMPLICA?

DAL PRIOR CHECKING AL DPIA (DA "EX ANTE" A "EX POST")

DPIA - DATA PROTECTION IMPACT ASSESSMENT

Quando un tipo di trattamento, **allorché prevede in particolare l'uso di nuove tecnologie**, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, **il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali**

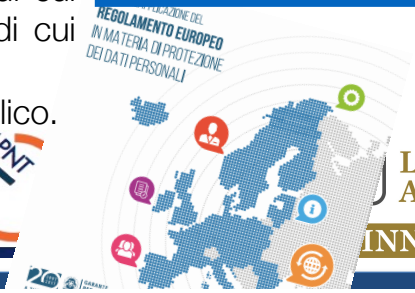
La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta **in particolare** nei casi seguenti:

a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;

b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o

c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Tali impatti dovranno essere analizzati attraverso un **apposito processo di valutazione**, tenendo conto dei **rischi noti o evidenziabili** e delle **misure tecniche e organizzative (anche di sicurezza)** che il titolare ritiene di dover adottare per mitigare tali rischi. All'esito di questa valutazione di impatto **il titolare potrà decidere in autonomia se** iniziare il trattamento (avendo adottato le misure idonee a mitigare sufficientemente il rischio) **ovvero** consultare l'autorità di controllo competente per ottenere indicazioni su come gestire il rischio residuale; **l'autorità non avrà il compito di "autorizzare" il trattamento, bensì di indicare le misure ulteriori eventualmente da implementare a cura del titolare**.



CAPO IV TITOLARE E RESPONSABILE

DPIA - DATA PROTECTION IMPACT ASSESSMENT

Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali

La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta **in particolare** nei casi seguenti:

a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;

b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o

c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

DPIA

UPI Emilia-Romagna

CENTRO STUDI PRIVACY E NUOVE TECNOLOGIE

WINNER 2018

STUDIOLEGALE

BOUTIQUE DI ECCELLENZA 2018

ACCOUNTABILITY: CHE COSA IMPLICA?

DAL PRIOR CHECKING AL DPIA (DA "EX ANTE" A "EX POST")

Dall'approccio orientato ai diritti deriva anche il **passaggio da una tutela in chiave prevalentemente remediale, dunque successiva, a una di tipo essenzialmente preventivo.**
Fondata, come tale, sulla minimizzazione del rischio di violazione attraverso tecniche di protezione fin dalla progettazione e con impostazioni predefinite ma anche mediante la complessiva responsabilizzazione dei titolari del trattamento, nella prevenzione del rischio "sociale" derivante da banche dati poco protette.

Trattamento 1	**Trattamento 4**
Trattamento 2	**Trattamento 5**
Trattamento 3	**Trattamento 6**

L'autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto.
L'autorità di controllo può inoltre redigere e rendere pubblico **un elenco delle tipologie di trattamenti per le quali non è richiesta** una valutazione d'impatto sulla protezione dei dati.

Unione Province d'Italia
UPI
Emilia-Romagna

CENTRO STUDI PRIVACY E NUOVE TECNOLOGIE

LE FONTI AWARDS
WINNER 2018

ORLANDI&PARTNERS
STUDIOLEGALE
BOUTIQUE DI ECCELLENZA 2018

ACCOUNTABILITY: CHE COSA IMPLICA?

DAL PRIOR CHECKING AL DPIA (DA "EX ANTE" A "EX POST")

GARANTE BELGA

1. trattamenti che utilizzano dati biometrici per l'identificazione univoca di persone in un luogo pubblico o in un luogo privato accessibile al pubblico;
2. quando i dati personali vengono raccolti da terzi per essere successivamente utilizzati ai fini della decisione di rifiutare o risolvere un determinato contratto di servizi con una persona fisica;
3. quando il trattamento riguarda categorie particolari di dati personali, ai sensi dell'art. 9 GDPR, che sono (ri)utilizzati per uno scopo diverso da quello per il quale sono stati raccolti, tranne nel caso in cui il trattamento sia basato sul consenso dell'interessato o se è necessario per adempiere ad un obbligo legale a cui è sottoposto il titolare;
4. quando il trattamento viene eseguito utilizzando un apparato ed una violazione dei dati personali potrebbe compromettere la salute fisica dell'interessato;
5. nel caso di trattamento su larga scala di dati personali di soggetti vulnerabili, compresi i bambini, per uno o più scopi diversi da quelli per i quali i dati sono stati raccolti;
6. quando i dati vengono raccolti su larga scala da terze parti per analizzare o prevedere la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, la posizione o il movimento di persone fisiche;
7. quando particolari categorie di dati personali ai sensi dell'articolo 9 GDPR o dati di natura molto personale (come i dati sulla povertà, disoccupazione, partecipazione al lavoro giovanile o lavoro sociale, dati di attività domestiche e private, dati di localizzazione) sono sistematicamente scambiati tra diversi titolari;
8. quando si tratta di elaborazione su larga scala di dati generati da dispositivi dotato di sensori che inviano dati via Internet o altri mezzi (**Internet of Things**, come smartTV, elettrodomestici intelligenti, giocattoli, smart cities, contatori intelligenti di energia, ecc.) e tale trattamento viene utilizzato per analizzare o prevedere la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, la posizione o il movimento delle persone fisiche;
9. quando si tratta di elaborazione su larga scala e/o sistematica di dati di telefonia, Internet o altri dati di comunicazione, metadati o dati di localizzazione di persone fisiche o che consentano di condurre a persone fisiche (ad es. tracciamento wifi o elaborazione dei dati sulla posizione dei viaggiatori nel trasporto pubblico) quando il trattamento non è strettamente necessario per l'esecuzione di un servizio richiesto dall'interessato;
10. in caso di elaborazione automatizzata e sistematica di dati personali su larga scala in cui il comportamento delle persone fisiche è monitorato, raccolto, stabilito o influenzato, inclusi i trattamenti per scopi pubblicitari.

ACCOUNTABILITY: CHE COSA IMPLICA?

DAL PRIOR CHECKING AL DPIA (DA "EX ANTE" A "EX POST")

GARANTE BELGA

1 i trattamenti effettuati da privati necessari ad adempiere ad un obbligo normativo, e per i quali la legge abbia indicato gli scopi dell'elaborazione, le categorie di dati personali e le garanzie per prevenire abusi o accessi o trasferimenti illegittimi;

2 il trattamento relativo esclusivamente ai dati necessari per l'amministrazione degli stipendi dei dipendenti del Titolare, quando i dati sono utilizzati unicamente per tale finalità, sono comunicati solo ai destinatari autorizzati a tale scopo e non vengono conservati più a lungo del tempo necessario per conseguire la finalità del trattamento;

3 il trattamento relativo esclusivamente all'amministrazione dei dipendenti del Titolare, nella misura in cui tale trattamento non coinvolge i dati relativi alla salute degli interessati o altre particolari categorie di dati di cui all'art. 9 GDPR o dati di cui all'art. 10 GDPR, ed i dati personali non vengono conservati più a lungo del tempo richiesto per la finalità di amministrazione del personale e sono comunicati a terzi solo se previsto da una disposizione di legge o regolamentare o per la realizzazione delle finalità del trattamento;

4 trattamenti di dati personali che riguardano esclusivamente la contabilità del Titolare, quando i dati vengono utilizzati esclusivamente per tale finalità, e purché i dati personali non sono conservati più a lungo del tempo necessario al conseguimento delle finalità del trattamento ed i dati personali trattati sono comunicati a terzi in base ad una previsione di legge o la comunicazione è necessaria per la contabilità;

5 il trattamento di dati personali relativi all'amministrazione di azionisti e soci quando il trattamento riguarda solo i dati necessari per tale amministrazione, e sono comunicati a terzi esclusivamente in base ad una previsione di legge o regolamentare e non vengono conservati oltre il tempo necessario per raggiungere gli scopi del trattamento;

6 il trattamento di dati personali da parte di una fondazione, associazione o qualsiasi altra istituzione senza scopo di lucro in occasione delle sue attività abituali, a condizione che il trattamento riguardi esclusivamente i dati personali relativi ai propri membri, alle persone con cui il Titolare mantiene contatti regolari quali beneficiari, purché non vi siano dati ottenuti da terzi, e che i dati non vengano conservati più a lungo del tempo richiesto per l'amministrazione e siano comunicati a terzi solo in presenza di una disposizione di legge o regolamentare;

7 il trattamento di dati personali relativo alla registrazione dei visitatori per il controllo accessi, quando i dati elaborati sono limitati al nome ed indirizzo professionale del visitatore, all'identificazione del suo datore di lavoro, all'identificazione del veicolo, al nome, la sezione e la funzione della persona visitata ed al momento della visita, ed i dati non sono conservati oltre il tempo necessario alla finalità di controllo accessi;

8 il trattamento di dati personali da parte di istituti di formazione per la gestione dei loro rapporti con gli alunni e studenti, purché il trattamento si riferisca solo a studenti attuali e potenziali o ad ex studenti e non vengano trattati dati ottenuti da terzi, e la comunicazione avvenga unicamente sulla base di una disposizione normativa o regolamentare ed il dato non sia conservato per un periodo superiore a quello necessario a mantenere la comunicazione tra lo studente e l'istituto;

9 il trattamento di dati personali relativi esclusivamente alla gestione dei clienti e fornitori del Titolare, purché il trattamento riguardi solo clienti e fornitori attuali o precedenti e non siano ricomprese particolari categorie di dati, ex art. 9 GDPR o dati di cui all'art. 10 GDPR, e per quanto riguarda l'amministrazione della clientela, non vengano registrati dati forniti da terzi, ed i dati siano conservati per il periodo necessario alla normale gestione della clientela del Titolare e siano comunicati a terzi solamente in base ad una norma di legge o di regolamento o nel quadro della normale gestione aziendale.

REGOLE PER I DATA BREACH

ACCOUNTABILITY: CHE COSA IMPLICA?

DATA BREACH

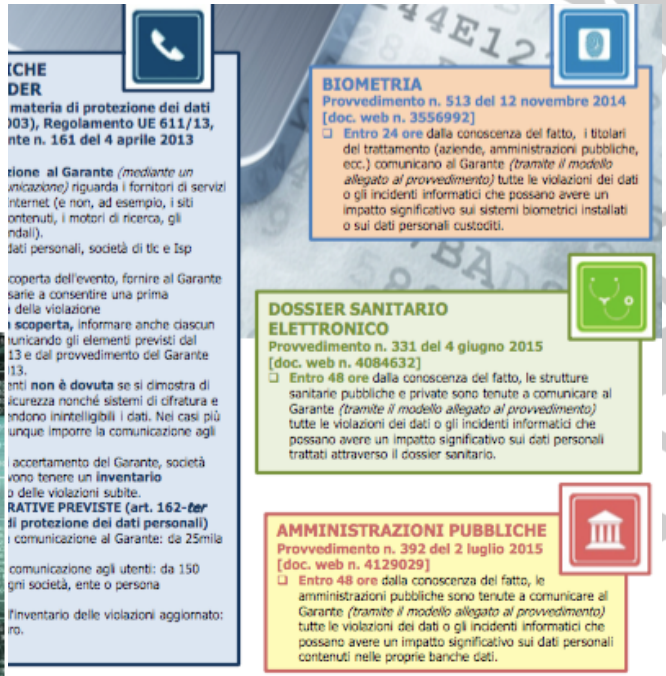
In un caso recente, relativo ad altro operatore, un attacco informatico effettuato sfruttando una vulnerabilità dei sistemi, ha consentito l'accesso, con successiva copia, alle credenziali di autenticazione di oltre 5.000 clienti, utilizzate per accedere all'area riservata delle proprie utenze.
La sola acquisizione delle credenziali di accesso, infatti, è da considerare, già di per sé, fonte di potenziale pregiudizio per gli interessati, con particolare riferimento al rischio di furto d'identità, indipendentemente dal fatto che vi sia un loro effettivo utilizzo nel medesimo contesto, giacché spesso gli utenti adoperano le credenziali per accedere a diversi servizi web.

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 del data breach che ha colpito l'azienda.

5 giugno 2017, ore 11:38

Wind Tre dovrà comunicare per iscritto a oltre 5mila clienti di aver subito un attacco informatico lo scorso 20 marzo, che ha consentito di visualizzare e acquisire in chiaro le user id e le password necessarie per l'accesso al loro profilo online e al rischio di furto dati fra cui nominativo,



Unione Province d'Italia
UPI
Emilia-Romagna

LE FONTI AWARDS
WINNER 2018

ORLAND&PARTNERS
STUDIOLEGALE
BOUTIQUE DI ECCELLENZA 2018

Ashley Madison, una taglia da 500mila dollari sugli hacker

Furto sul Playstation Network: 70 milioni di utenze!

"Abbiamo scoperto che **tra il 17 e il 19 aprile** determinate **informazioni** degli account utente dei servizi Playstation Network e Qriocity sono state compromesse a causa di **un'intrusione illegale e non autorizzata** nella nostra rete". Con queste parole Sony ha ammesso che gli hacker (o cracker, per meglio dire) hanno fatto breccia nei propri servizi, **sottraendo i dati sensibili di tutti gli utenti registrati. Si parla di oltre 70 milioni di persone.**

"In risposta a questo evento abbiamo temporaneamente spento i servizi PSN e Qriocity. In seguito abbiamo **ingaggiato un'azienda di sicurezza esterna** per condurre un'indagine completa su quanto avvenuto e compiuto i passi necessari per migliorare la sicurezza e rafforzare l'infrastruttura di rete, ricostruendo il nostro sistema per offrire maggiore protezione ai vostri dati personali. Faremo quanto necessario per risolvere questi problemi nel modo più rapido ed efficiente possibile".

Secondo Sony chi ha eseguito l'attacco - gli Anonymous si sono chiamati fuori - potrebbe essere **entrato in possesso delle seguenti informazioni**: nome, indirizzo (città, stato, codice postale), paese, email, data di nascita, password e login di PSN/Qriocity e PSN online ID. "Potrebbe aver ottenuto anche i dati del vostro profilo - inclusa la cronologia degli acquisti - l'indirizzo di fatturazione e le risposte di sicurezza per il recupero della password di PlayStation Network/Qriocity. Se avete autorizzato un sotto-account per un vostro dipendente, potrebbero essere stati sottratti gli stessi dati".

pena la pubblicazione dei dati trafugati. Detto, fatto. L'azienda ha continuato sulla sua

Web: impennata del traffico illecito di dati personali in Gran Bretagna

Rubate oltre 5 milioni di impronte digitali di dipendenti Usa

Ascolta

Cosa ci può essere di peggio per un governo del furto dei dati personali di 21,5 milioni di suoi attuali o passati dipendenti? Ad esempio, scoprire dopo qualche tempo che ad essere sottratte sono state anche le impronte digitali di 5,6 milioni di suoi impiegati e contractor .In quello che sembra essere uno scorcio di distopico futuro, ieri il governo statunitense ha comunicato proprio questa amara scoperta.

Quasi 6 milioni di dati biometrici non modificabili di cittadini americani sono ora in mano a degli hacker stranieri, forse al soldo della Cina, almeno secondo l'ipotesi non ufficiale delle autorità americane. O comunque in mano a un gruppo organizzato, vista l'entità e profondità dell'attacco, possibilmente collegato a qualche Stato straniero. È una notizia senza precedenti, specie considerata la scala e i soggetti coinvolti. E le cui implicazioni saranno a lungo termine e ancora imprevedibili.

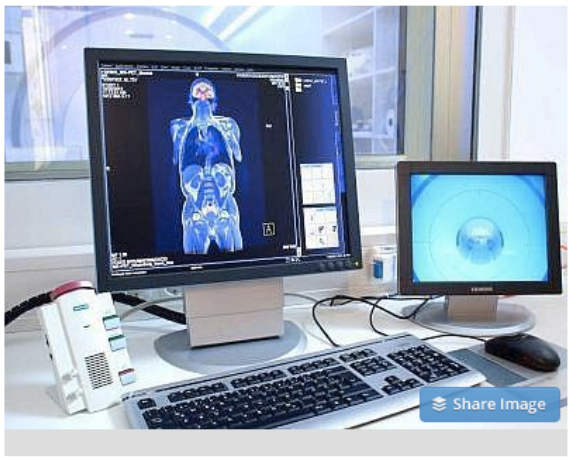
permettono di compiere furti di identità. Relativamente contenuti (3,5%) gli altri casi, fra i quali però sono anche quelli di traffico di dati sulle carte di credito: dal numero alla data di scadenza ai codici di sicurezza, quelli a tre cifre sul retro della carta, che servono per i pagamenti on line.

DATA BREACH

Esperta cyber-attacchi: ospedali appetibili per furto dati

SANITÀ

Tweet Condividi



Pubblicato il: 31/10/2017 16:12

Quanto può costare a un'azienda italiana ogni 'furto' di dati tramite cyber-attacco? In media 2,6 milioni di euro, e circa 119 euro per record di dati perso o rubato. E le violazioni sanitarie sono le più onerose: per il settimo anno consecutivo, l'healthcare risulta a livello mondiale il settore d'industria più costoso, con 380 dollari per ogni record violato, oltre 2,5 volte la media globale di tutti i comparti. E' quanto emerge dal recente rapporto '2017 Cost of Data Breach' di Ibm Security e Ponemon Institute. "Fra il 2014 e il 2016 le aziende sanitarie sono balzate al primo posto come realtà prese di mira dai cyber-attacchi - spiega all'Adnkronos Salute Marzia D'Argenio, Security Services Sales Ibm Italia - perché il dato sanitario è appetibile, anche a lungo termine".

L'esperta di cyber-security spiega: "Il furto del numero di una carta di credito si usa una sola volta, perché ormai tutti hanno alert attivi, al limite un'operazione può andare a buon fine, ma poi interviene il blocco. **Mentre con i dati sanitari è diverso, essere un'altra persona è estremamente utile per una serie di attività illecite**".

DATA BREACH

DATA BREACH *aka* **”violazione dei dati personali"**: la violazione di sicurezza che comporta **accidentalmente o in modo illecito** la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati

ACCOUNTABILITY: CHE COSA IMPLICA?

DATA BREACH

DATA BREACH *aka* "violazione dei dati personali": la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati

A partire dal 25 maggio 2018, tutti i titolari – e non soltanto i fornitori di servizi di comunicazione elettronica accessibili al pubblico, come avviene oggi – dovranno notificare all'autorità di controllo le violazioni di dati personali (…) ma **soltanto se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati**. Pertanto, l**a notifica all'autorità dell'avvenuta violazione non è obbligatoria, essendo subordinata alla valutazione del rischio per gli interessati che spetta, ancora una volta, al titolare.** Se la probabilità di tale rischio è elevata, si dovrà informare delle violazione anche gli interessati, sempre "senza ingiustificato ritardo".

Tutti i titolari di trattamento dovranno i**n ogni caso documentare le violazioni di dati personali subite, anche se non notificate all'autorità di controllo e non comunicate agli interessati.**
Si raccomanda, pertanto, ai titolari di trattamento di adottare le misure necessarie a documentare eventuali violazioni, essendo peraltro tenuti a fornire tale documentazione, su richiesta, al Garante in caso di accertamenti.

DATA BREACH

DATA BREACH *aka* "violazione dei dati personali": la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati

Articolo 33
Notifica di una violazione dei dati personali all'autorità di controllo

1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, **a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.**

Considerando 85: "Una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata. **Pertanto, non appena viene a conoscenza di un'avvenuta violazione dei dati personali, il titolare del trattamento dovrebbe notificare la violazione dei dati personali all'autorità di controllo competente, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che il titolare del trattamento non sia in grado di dimostrare che, conformemente al principio di responsabilizzazione, è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.**
Oltre il termine di 72 ore, tale notifica dovrebbe essere corredata delle ragioni del ritardo e le informazioni potrebbero essere fornite in fasi successive senza ulteriore ingiustificato ritardo".

DATA BREACH

DATA BREACH *aka* ”violazione dei dati personali": la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati

Notificazione di una violazione dei dati personali all'autorità di controllo

senza ingiustificato ritardo, ove possibile entro 72 ore dal momento in cui ne è venuto a conoscenza

Comunicazione di una violazione dei dati personali all'interessato

senza ingiustificato ritardo

Registro dei data breach

Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto di quanto sopra.

ACCOUNTABILITY: CHE COSA IMPLICA?

DATA BREACH

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Notificazione di una violazione dei dati personali all'autorità di controllo

senza ingiustificato ritardo, ove possibile entro 72 ore dal momento in cui ne è venuto a conoscenza

VIOLAZIONE DI DATI PERSONALI – MODELLO DI NOTIFICA AL GARANTE

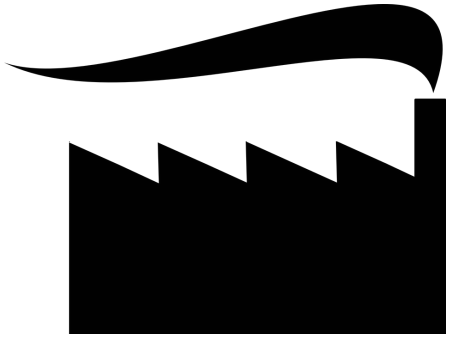
I titolari di trattamento di dati personali sono tenuti a notificare al Garante le violazioni dei dati personali (*data breach*) che comportano accidentalmente o in modo illecito la distruzione, la perdita, la modificazione, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati, anche nell'ambito delle comunicazioni elettroniche, a meno che sia improbabile che la violazione presenti un rischio per i diritti e le libertà degli interessati.

La notifica non deve includere i dati personali oggetto di violazione (es. non fornire i nomi dei soggetti interessati dalla violazione).

[doc. web n. 9126951]
Provvedimento del Garante sulla notifica delle violazioni dei dati personali (data breach)
Registro dei provvedimenti
n. 157 del 30 luglio 2019

DATA BREACH

DATA BREACH *aka* "violazione dei dati personali": la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati



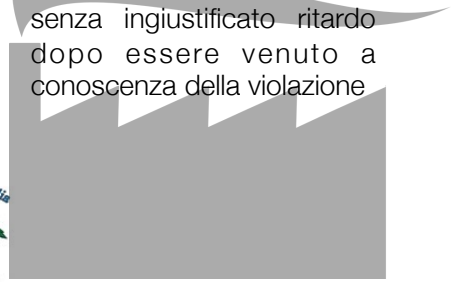
Notificazione di una violazione dei dati personali all'autorità di controllo

senza ingiustificato ritardo, ove possibile entro 72 ore dal momento in cui ne è venuto a conoscenza

La notifica deve almeno:

a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
c) descrivere le probabili conseguenze della violazione dei dati personali;
d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Il responsabile del trattamento **informa** il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione



ACCOUNTABILITY

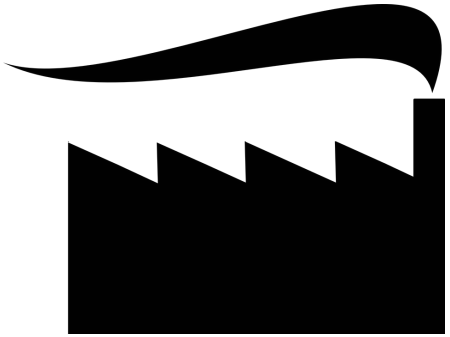
Unione Province d'Italia
UPI
Emilia-Romagna

CENTRO STUDI PRIVACY E NUOVE TECNOLOGIE

LE FONTI AWARDS
WINNER 2018

ORLANDI&PARTNERS
STUDIOLEGALE
BOUTIQUE DI ECCELLENZA 2018

DATA BREACH *aka* "violazione dei dati personali": violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati o comunque trattati;



Comunicazione di una violazione dei dati personali all'interessato

senza ingiustificato ritardo

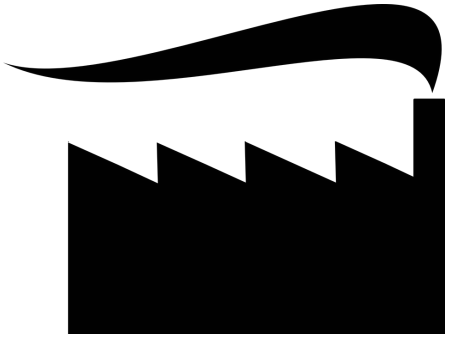
descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le raccomandazioni

La comunicazione deve come minimo:

b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
c) descrivere le probabili conseguenze della violazione dei dati personali;
d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

DATA BREACH

DATA BREACH *aka* "violazione dei dati personali": violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati o comunque trattati;



Non è richiesta la comunicazione all'interessato se è soddisfatta una delle seguenti condizioni:

A. il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
B. il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
C. detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

L'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni è soddisfatta.

GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI

18/IT

WP250rev.01

Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679

adottate il 3 ottobre 2017

Versione emendata e adottata in data 6 febbraio 2018

Violazioni di dati personali (Data Breach)

Violazioni di dati personali (data breach), in base alle previsioni del Regolamento (UE) 2016/679

La pagina contiene link alla normativa e a documenti interpretativi, schede informative e pagine tematiche,
ed è in continuo aggiornamento.

Ultimo aggiornamento 14 dicembre 2018

DATA BREACH

Unione Province d'Italia
UPI
Emilia-Romagna

CENTRO STUDI PRIVACY E NUOVE TECNOLOGIE

LE FONTI AWARDS
WINNER 2018

ORLANDI&PARTNERS
STUDIOLEGALE
BOUTIQUE DI ECCELLENZA 2018

About 60,000 EU data breaches filed under GDPR

Valentina Spiridonova 06.02.19

06 February, 2019

La percezione di ciò che costituisce data breach e di quando deve essere notificato alle Autorità Garanti varia significativamente da Stato a Stato!!

Paesi Bassi: 15.400
Germania: 12.600
UK: 10.600
Irlanda: 3.800
Danimarca: 3.100

e in Italia….?

RGPD
REGOLAMENTO (UE) 2016/679

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Il bilancio dei primi 4 mesi di applicazione

Un primo bilancio sull'applicazione in Italia, a partire dal 25 maggio, del **Regolamento europeo in materia di protezione dei dati personali** mostra come pubbliche amministrazioni, mondo delle imprese e cittadini abbiano colto l'importanza del nuovo quadro giuridico e le opportunità che esso offre in termini di tutela e garanzie per le persone.

Comunicazioni dei dati di contatto degli RPD **40.738**

Reclami e segnalazioni **2.547**
(1.795 nello stesso periodo 2017)

Notificazioni di Data Breach **305**

Contatti con l'URP circa **7.200**
(circa 4.400 nello stesso periodo 2017)

Dati aggiornati al 28 settembre 2018 www.garanteprivacy.it

Unione Province d'Italia
UPI
Emilia-Romagna

RGPD
REGOLAMENTO (UE) 2016/679

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Il bilancio del 2018

(Periodo: 25 maggio - 31 dicembre 2018)

Comunicazioni dei dati di contatto degli RPD **43.269**

Reclami e segnalazioni **4.704**
(3.378 nello stesso periodo 2017)

Notificazioni di Data Breach **630**

Contatti con l'URP **13.835**
(8.331 nello stesso periodo 2017)

www.garanteprivacy.it

CENTRO STUDI PRIVACY E NUOVE TECNOLOGIE

LE FONTI AWARDS WINNER 2018

ORLANDI&PARTNERS STUDIOLEGALE
BOUTIQUE DI ECCELLENZA 2018

RGPD
REGOLAMENTO (UE) 2016/679

Il bilancio dell'applicazione

(Periodo: 25 maggio 2018 – 31 marzo 2019)

Comunicazioni dei dati di contatto degli RPD **48.591**

Reclami e segnalazioni **7.219**

Notifiche di Data Breach **946**

Contatti con l'URP **18.557**

www.garanteprivacy.it

Unione Province d'
UPI
Emilia-Romagna

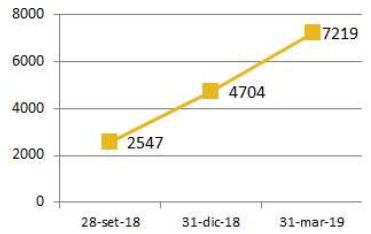
RGPD
REGOLAMENTO (UE) 2016/679

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

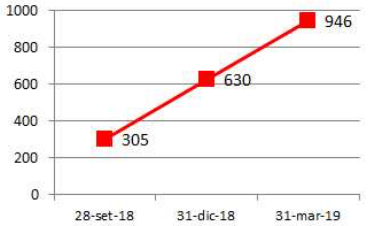
Il bilancio dell'applicazione

I grafici mostrano l'andamento nel periodo compreso tra il 28 settembre 2018 (data del primo bilancio applicativo diffuso sul sito del Garante) e il 31 marzo 2019.

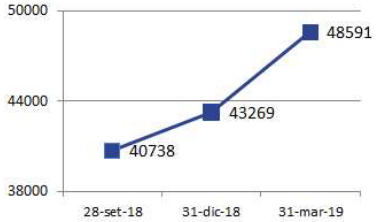
Reclami e segnalazioni



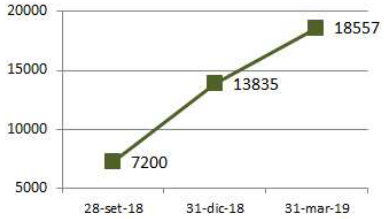
Notifiche di data breach



Comunicazioni dei dati di contatto degli RPD



Contatti con l'URP



www.garanteprivacy.it

CENTRO STUDI PRIVACY E NUOVE TECNOLOGIE

LE FONTI AWARDS WINNER 2018

ORLANDI&PARTNERS STUDIOLEGALE

BOUTIQUE DI ECCELLENZA 2018

RGPD
REGOLAMENTO (UE) 2016/679

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Il bilancio dell'applicazione

(Periodo: 25 maggio 2018 – 30 settembre 2019)

Comunicazioni dei dati di contatto degli RPD — **52.659**

Reclami e segnalazioni — **12.063**

Notifiche di Data Breach — **1.520**

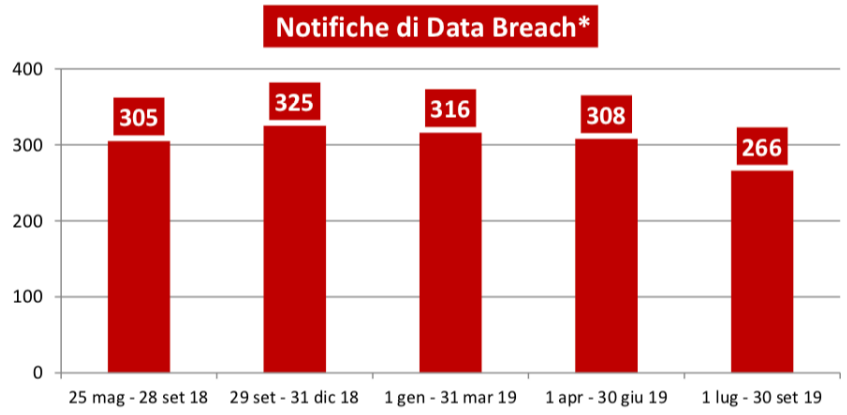
Contatti con l'URP — **26.247**

www.garanteprivacy.it

RGPD
REGOLAMENTO (UE) 2016/679

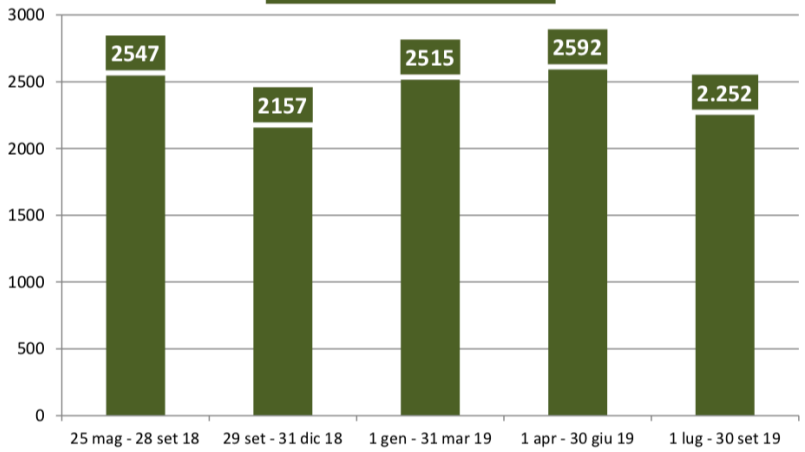
GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Il bilancio dell'applicazione



**Il grafico mostra le notifiche di data breach in vari periodo temporali. Il primo periodo considerato copre un arco di 4 mesi (25 maggio-28 settembre 2018), mentre gli altri periodi coprono archi temporali trimestrali*

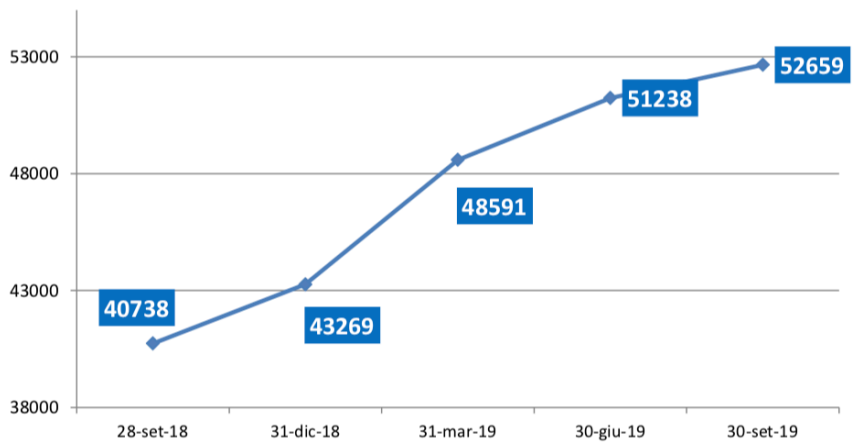
Reclami e segnalazioni*



**Il grafico mostra i reclami e segnalazioni al Garante in vari periodo temporali. Il primo periodo considerato copre un arco di 4 mesi (25 maggio-28 settembre 2018), mentre gli altri periodi coprono archi temporali trimestrali*

RGPD REGOLAMENTO (UE) 2016/679
GARANTE PER LA PROTEZIONE DEI DATI PERSONALI
Il bilancio dell'applicazione

Comunicazioni dei dati di contatto degli RPD*



La tabella illustra l'andamento del numero totale delle **comunicazioni attive. Ciascun valore indicato nel grafico comprende quelli dei periodi precedenti **al netto** di modifiche e revoche intervenute nel corso del tempo.*

IL CASO ITALIAONLINE

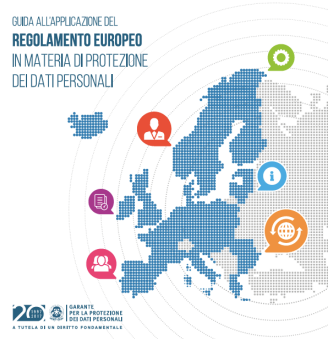
Provvedimento su data breach - 30 aprile 2019
Registro dei provvedimenti n. 106 del 30 aprile 2019

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

circa **1.5 milioni di account** (credenziali) violati
fattori da considerare nella valutazione del rischio per i diritti e le libertà delle persone fisiche: tipo di violazione; natura, carattere sensibile e volume dei dati personali; facilità di identificazione delle persone fisiche; gravità delle conseguenze per le persone fisiche; caratteristiche particolari dell'interessato; caratteristiche particolari del titolare del trattamento dei dati; numero di persone fisiche interessate; altri aspetti generali

Nel caso di specie:
elevato numero di persone fisiche
la **facilità con cui è possibile identificare specifiche persone fisiche** direttamente dai dati personali oggetto di violazione, senza che sia necessaria alcuna speciale ricerca per scoprire l'identità degli interessati;
potenziale pregiudizio per gli interessati in considerazione della probabilità che le medesime credenziali possano essere utilizzate per accedere anche ad altri servizi online>> **rischio di furto o usurpazione di identità**

DECISIONE: necessità di effettuare una nuova comunicazione della violazione dei dati personali agli interessati contenente una descrizione della natura della violazione e delle possibili conseguenze della stessa, nonché indicazioni specifiche sulle misure che gli interessati possono adottare per proteggersi da eventuali conseguenze negative della violazione, quale la raccomandazione di non utilizzare più le credenziali compromesse, modificando la password utilizzata per l'accesso a qualsiasi altro servizio online qualora coincidente o simile a quella oggetto di violazione



DPO-DATA PROTECTION OFFICER

Unione Province d'Italia
UPI
Emilia-Romagna

CENTRO STUDI
PRIVACY E NUOVE
TECNOLOGIE

LE FONTI
AWARDS
WINNER 2018

ORLANDI&PARTNERS
STUDIOLEGALE
BOUTIQUE DI ECCELLENZA 2018

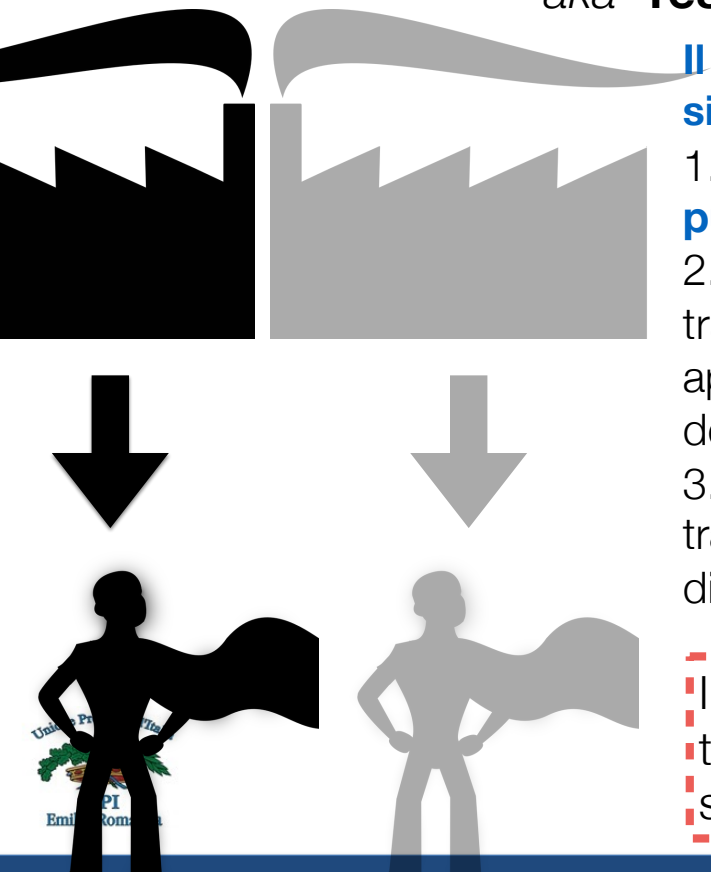
UNA NUOVA FIGURA: IL DPO

Anche la designazione di un "responsabile della protezione dati" (RPD, ovvero DPO se si utilizza l'acronimo inglese: Data Protection Officer) riflette **l'approccio responsabilizzante** che è proprio del regolamento essendo finalizzata a facilitare l'attuazione del regolamento da parte del titolare/del responsabile. Non è un caso, infatti, che fra i compiti del RPD rientrino "la sensibilizzazione e la formazione del personale" e la sorveglianza sullo svolgimento della valutazione di impatto di cui all'art. 35

ACCOUNTABILITY: CHE COSA IMPLICA?

UNA NUOVA FIGURA: IL DPO

aka "**responsabile della protezione dei dati - RPD"**

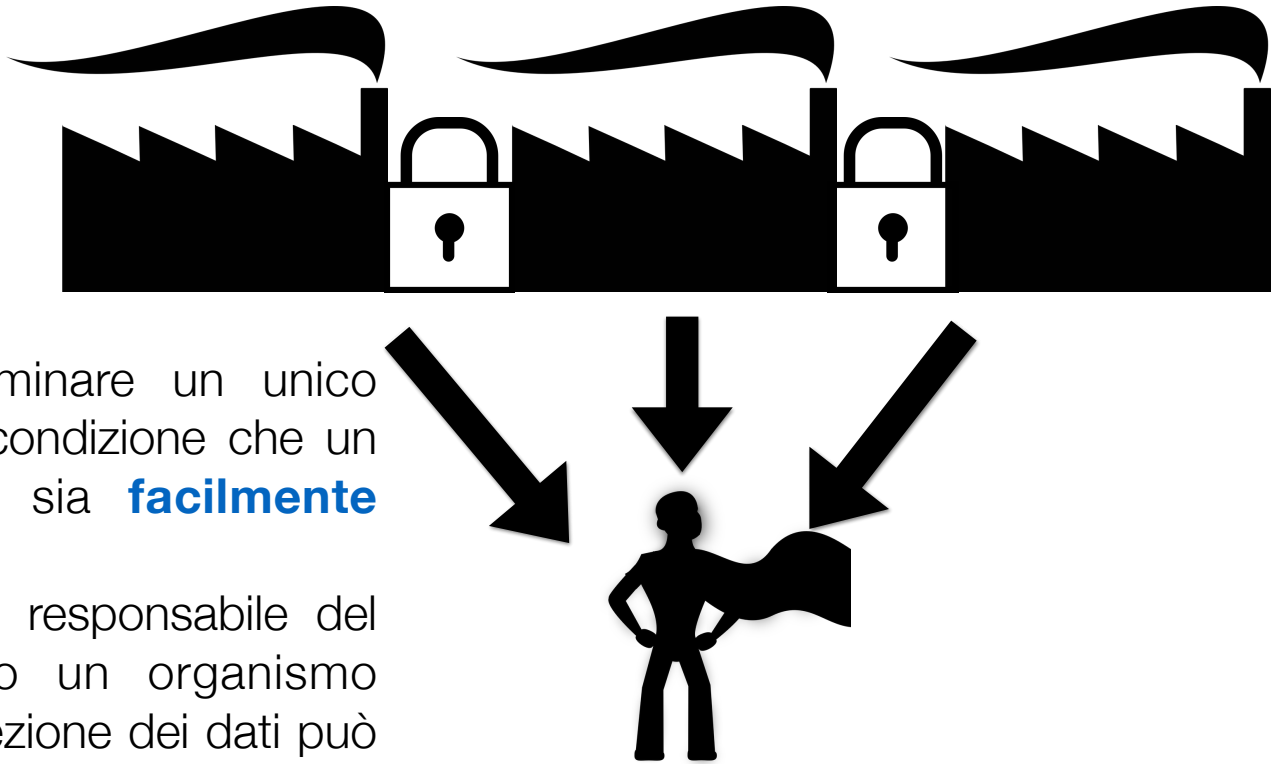


Il titolare del trattamento e il responsabile del trattamento designano sistematicamente (cioè: **obbligatoriamente!)** un DPO:

1. se il trattamento è effettuato **da un'autorità pubblica o da un organismo pubblico**
2. se le **attività principal**i del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, campo di applicazione e/o finalità, richiedono il **monitoraggio regolare e sistematico** degli interessati **su larga scala**
3. se le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, **su larga scala,** di categorie particolari di dati o di dati relativi a condanne penali e a reati

Il responsabile della protezione dei dati può essere **un dipendente** del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un **contratto di servizi.**

Articolo 37
Designazione del responsabile della protezione dei dati

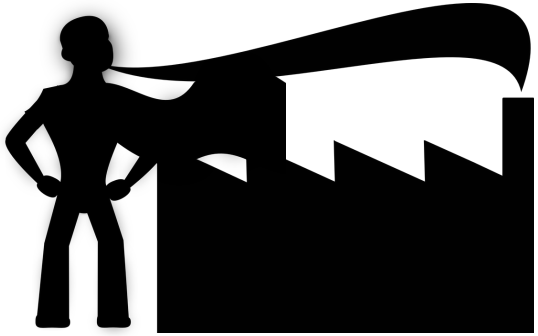


2. Un gruppo imprenditoriale può nominare un unico responsabile della protezione dei dati, a condizione che un responsabile della protezione dei dati sia **facilmente raggiungibile** da ciascuno stabilimento.

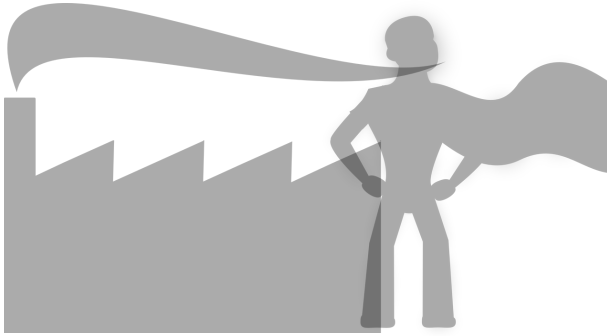
3. Qualora il titolare del trattamento o il responsabile del trattamento sia un'autorità pubblica o un organismo pubblico, un unico responsabile della protezione dei dati può essere designato per più autorità pubbliche o organismi pubblici, **tenuto conto della loro struttura organizzativa e dimensione.**

Sezione 4
Responsabile della protezione dei dati

Articolo 37
Designazione del responsabile della protezione dei dati



Il titolare del trattamento o il responsabile del trattamento **pubblica** i dati di contatto del responsabile della protezione dei dati e **li comunica all'autorità di controllo**



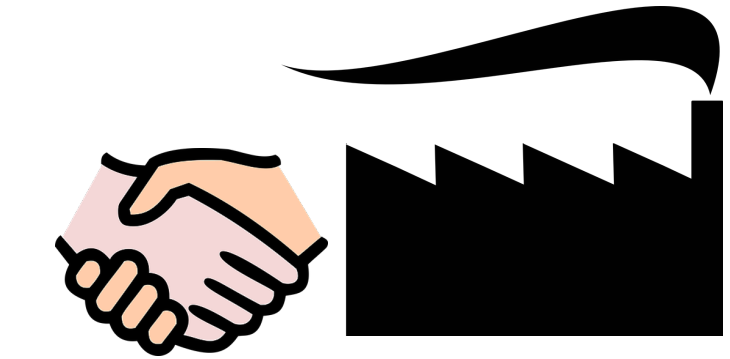
Articolo 37
Designazione del responsabile della protezione dei dati

Il responsabile della protezione dei dati può essere **un dipendente** del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un **contratto di servizi.**

REQUISITI
qualità professionali

in particolare **conoscenza specialistica** della normativa e delle pratiche in materia di protezione dei dati

capacità di adempiere ai compiti propri del DPO



CONTRATTO DI SERVIZI

COMPITI

Il responsabile della protezione dei dati è incaricato **almeno dei seguenti compiti**:

a) **informare e fornire consulenza** al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
b) **sorvegliare l'osservanza del GDPR** e di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
c) **fornire, se richiesto, un parere in merito alla DPIA e sorvegliarne lo svolgimento** ai sensi dell'articolo 35;
d) cooperare con l'autorità di controllo; e
e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

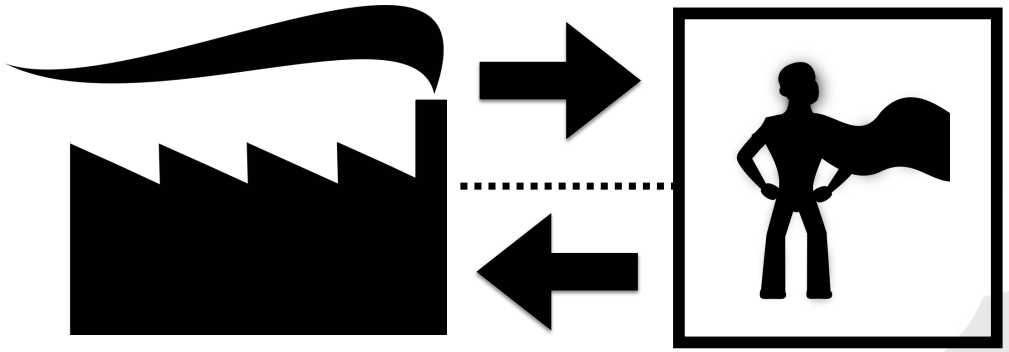
Nell'eseguire i propri compiti il responsabile della protezione dei dati **considera debitamente i rischi** inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

NB: Art. 38 Il responsabile della protezione dei dati può svolgere **altri compiti e funzioni.** Il titolare del trattamento o il responsabile del trattamento si assicura che tali compiti e funzioni non diano adito a un **conflitto di interessi.**

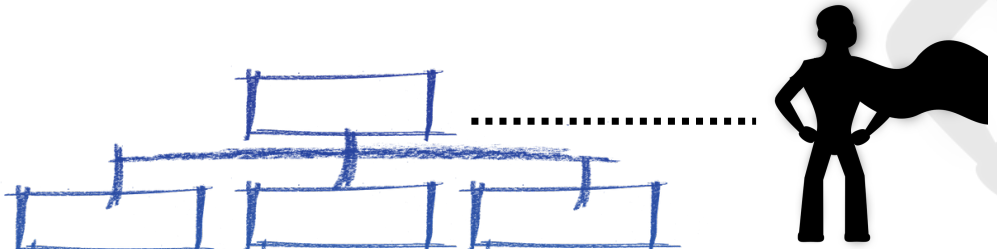
Sezione 4
Responsabile della protezione dei dati

Articolo 38
Posizione del responsabile della protezione dei dati

Il titolare del trattamento o il responsabile del trattamento:
- si assicurano che il DPO sia **prontamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali**
- sostengono il DPO nell'esecuzione dei propri compiti fornendogli le **risorse necessarie** per adempiere a tali compiti nonché l'accesso ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica.



Il responsabile della protezione dei dati **riferisce direttamente ai massimi superiori gerarchici** del titolare del trattamento o del responsabile del trattamento.



Sezione 4
Responsabile della protezione dei dati

Art. 29 DLgs n. 196/2003
(Responsabile del trattamento)
I compiti affidati al responsabile sono analiticamente specificati per iscritto dal titolare. Il responsabile effettua il trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle proprie istruzioni.

≠

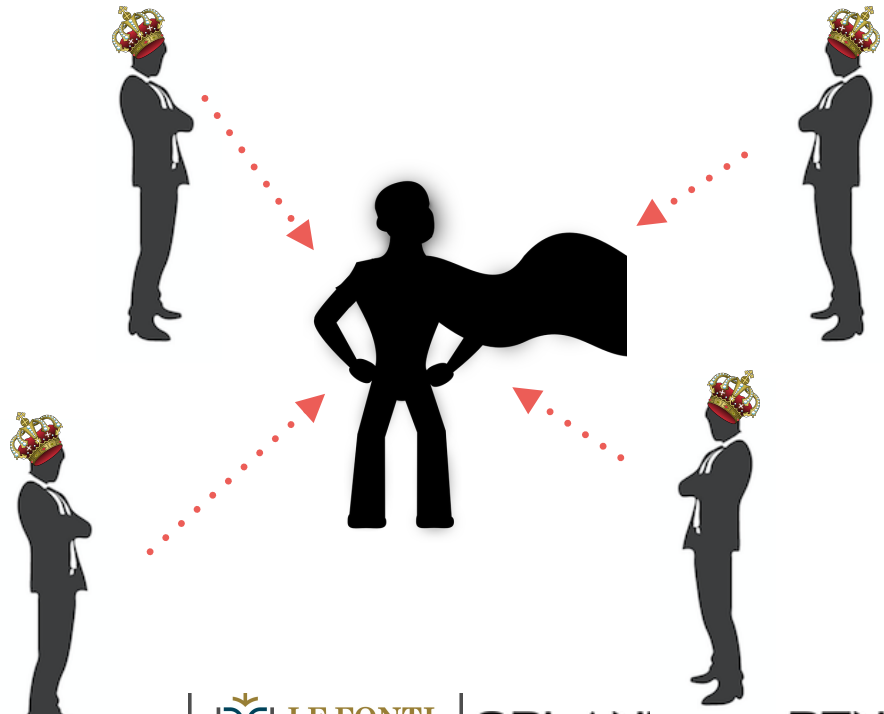
Il titolare del trattamento o il responsabile del trattamento si assicurano che il responsabile della protezione dei dati **non riceva alcuna istruzione** per quanto riguarda l'esecuzione dei propri compiti.

Il responsabile della protezione dei dati **non è rimosso o penalizzato** dal titolare del trattamento o dal responsabile del trattamento **per l'adempimento dei propri compiti**

Unione Province d'Italia
UPI
Emilia-Romagna

Articolo 38
Posizione del responsabile della protezione dei dati

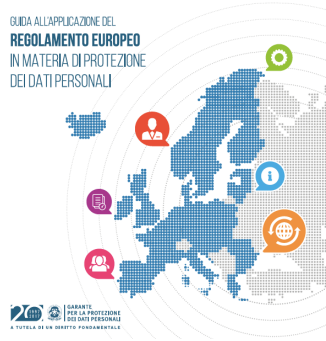
Gli interessati possono contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento.



PNT
CE PRIVACY E NUOVE TECNOLOGIE

LE FONTI AWARDS
WINNER 2018

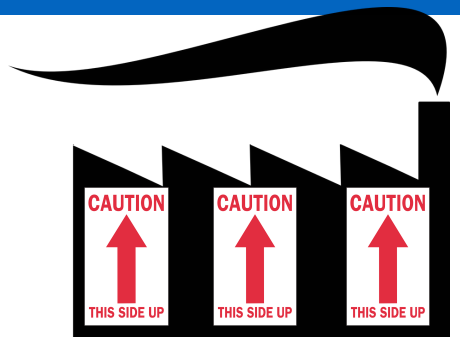
ORLANDI PARTNERS
STUDIOLEGALE
BOUTIQUE DI ECCELLENZA 2018


GUIDA ALL'APPLICAZIONE DEL
REGOLAMENTO EUROPEO
IN MATERIA DI PROTEZIONE
DEI DATI PERSONALI

FORMAZIONE

ACCOUNTABILITY: CHE COSA IMPLICA?

TRAINING, TRAINING, TRAINING…

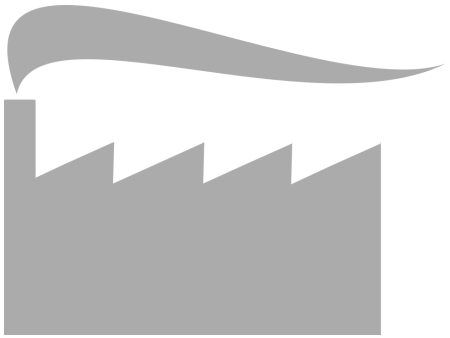


Trattamento sotto l'autorità del titolare del trattamento e del responsabile del trattamento

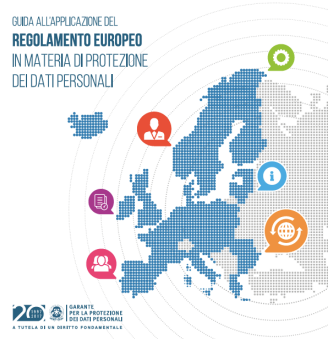
Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati **se non è istruito in tal senso dal titolare del trattamento,** salvo che lo richieda il diritto dell'Unione o degli Stati membri.

Sicurezza del trattamento

Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati **se non è istruito in tal senso dal titolare del trattamento**, salvo che lo richieda il diritto dell'Unione o degli Stati membri.



il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il presente regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.



DIRITTI DELL'INTERESSATO

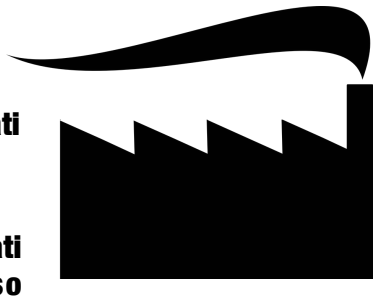
+ DIRITTI PER L'INTERESSATO

Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato

Informazioni da fornire qualora i dati siano raccolti presso l'interessato

Informazioni da fornire qualora i dati non siano stati ottenuti presso l'interessato

Obbligo di notifica in caso di rettifica, cancellazione o limitazione dei dati



VS.

Diritto di accesso

Diritto di rettifica

Diritto alla cancellazione ("diritto all'oblio")

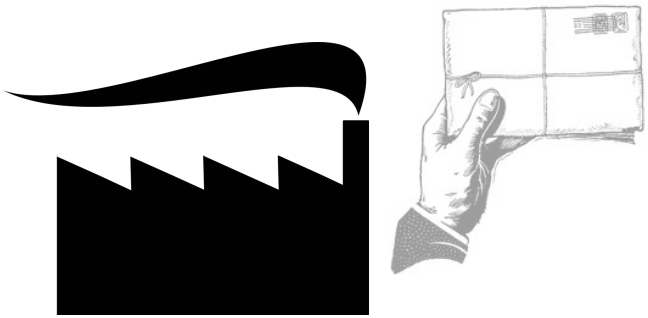
Diritto di limitazione di trattamento

Diritto alla portabilità dei dati

Diritto di opposizione

Diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato

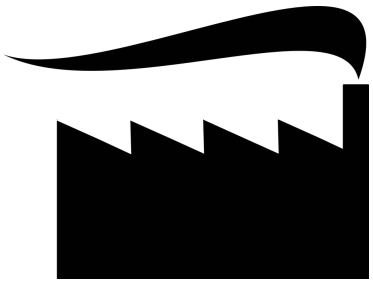
+ DIRITTI PER L'INTERESSATO



Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato

Il titolare del trattamento adotta **misure appropriate per fornire all'interessato tutte le informazioni e le comunicazioni** relative al trattamento dei dati personali in **forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro**, in particolare nel caso di informazioni destinate specificamente ai minori. Le informazioni sono fornite **per iscritto o con altri mezzi, se del caso in formato elettronico**. Se richiesto dall'interessato, le informazioni possono essere **fornite oralmente**, purché sia comprovata con altri mezzi l'identità dell'interessato.

necessario, tenuto conto della complessità della richiesta e [illegible] mesi, se



Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato

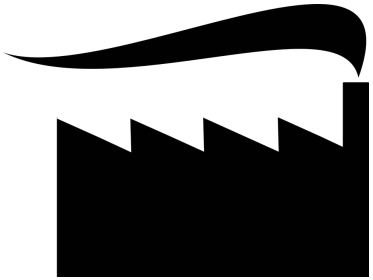
UN MESE + FINO A DUE MESI

Il titolare del trattamento **agevola** l'esercizio dei diritti dell'interessato.

Il titolare del trattamento fornisce all'interessato le informazioni **senza ingiustificato ritardo e al più tardi entro un mese** dal ricevimento della richiesta stessa. Tale termine può essere **prorogato di due mesi**, se necessario, tenuto conto della complessità della richiesta e del numero di richieste.

Il titolare del trattamento informa l'interessato di tale proroga, e dei motivi del ritardo, entro un mese dal ricevimento della richiesta.

Se l'interessato presenta la richiesta in formato elettronico, le informazioni sono fornite, ove possibile, in formato elettronico



Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato

GRATIS! MA NON ESAGERIAMC

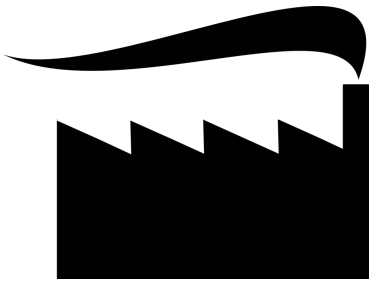
Le informazioni e le comunicazioni sono **gratuite**. Se le richieste dell'interessato sono manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo, il titolare del trattamento può:

a) addebitare un contributo spese ragionevole tenendo conto dei costi amministrativi sostenuti per fornire le informazioni o la comunicazione o intraprendere l'azione richiesta; oppure

b) rifiutare di soddisfare la richiesta.

Incombe al titolare del trattamento l'onere di dimostrare il carattere manifestamente infondato o eccessivo della richiesta.

+ DIRITTI PER L'INTERESSATO

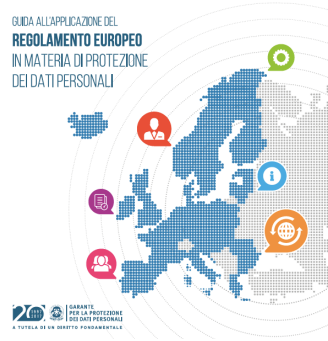


Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato

ICONA	INFORMAZIONI ESSENZIALI	SÌ/NO
	La **raccolta** di dati personali è limitata al minimo necessario per ogni specifica finalità del trattamento	
	La **memorizzazione** di dati personali è limitata al minimo necessario per ogni specifica finalità del trattamento	
	Il **trattamento** di dati personali è limitato alle finalità per le quali sono stati raccolti	
	Non sono **forniti** dati personali a terze parti commerciali	
	Non sono effettuati **la vendita o l'affitto** di dati personali	
	I dati personali non sono memorizzati in forma **non cifrata**	

IL RISPETTO DELLE RIGHE 1-3 È RICHIESTO AI SENSI DEL DIRITTO UE

Le informazioni da fornire agli interessati possono essere fornite in combinazione con **icone standardizzate**



INFORMATIVA & CONSENSO

ACCOUNTABILITY: CHE COSA IMPLICA?

INFORMATIVE PIU' CHIARE E "RICCHE"

CONTENUTI DELL'INFORMATIVA

I contenuti dell'informativa **sono più ampi** rispetto al Codice privacy.

In particolare, il titolare deve sempre:

1 specificare **i dati di contatto del DPO** (cioè il Data Protection Officer, nuova figura introdotta proprio dal GDPR) ove esistente

2 **dettagliare la base giuridica del trattamento** e, nel caso, chiarire qual è il suo **interesse legittimo** se quest'ultimo costituisce la base giuridica del trattamento

3 precisare **se trasferisce i dati personali in Paesi terzi e, in caso affermativo, attraverso quali strumenti**

4 specificare **il periodo di conservazione dei dati o i criteri seguiti** per stabilire tale periodo di conservazione

5 **informare sul diritto di presentare un reclamo all'autorità di controllo**

6 Indicare se il trattamento comporta **processi decisionali automatizzati (anche la profilazione),** altresì illustrando, in tal caso, la logica di tali processi decisionali e le conseguenze previste per l'interessato.

CARATTERISTICHE DELL'INFORMATIVA

Forma concisa, trasparente, intelligibile per l'interessato e facilmente accessibile

Linguaggio chiaro e semplice

Informative idonee per i minori

Scritta (e preferibilmente in formato elettronico)

Anche **orale**

Anche mediante **"icone"** (di prossima definizione)

GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI

17/IT

WP260 rev.01

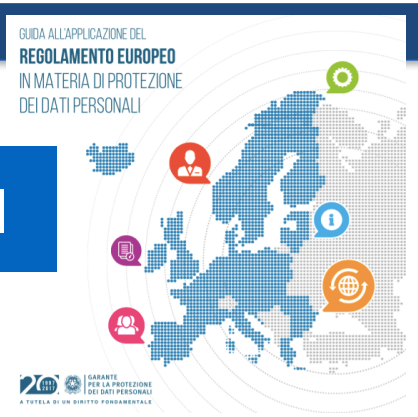
Gruppo di lavoro articolo 29

Linee guida sulla trasparenza ai sensi del regolamento 2016/679

adottate il 29 novembre 2017

Versione emendata adottata l'11 aprile 2018

ACCOUNTABILITY: CHE COSA IMPLICA?



CONSENSI PIU' AGILI, MA CERTI E DOCUMENTABILI

Per i **dati "sensibili" il consenso DEVE essere "esplicito"**; lo stesso dicasi per il consenso a decisioni basate su trattamenti automatizzati (compresa la profilazione)

NON deve essere necessariamente "documentato per iscritto", né è richiesta la "forma scritta"

il titolare DEVE essere in grado di dimostrare che l'interessato ha prestato il consenso a uno specifico trattamento

Il consenso dei minori è valido a partire dai 16 anni; prima di tale età occorre raccogliere il consenso dei genitori o di chi ne fa le veci.

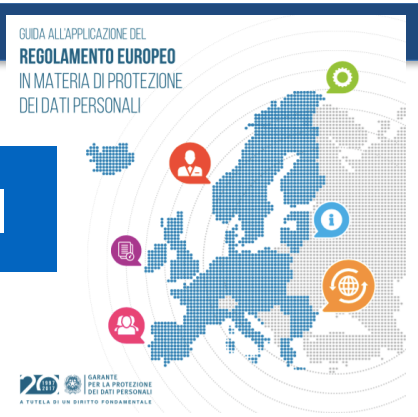
il consenso DEVE (continuare ad) essere, in tutti i casi, **libero, specifico, informato e inequivocabile**

NON è ammesso il consenso tacito o presunto (no a caselle pre-spuntate su un modulo).

DEVE essere manifestato **attraverso "dichiarazione o azione positiva inequivocabile"**

Si intravede l'opportunità di **valorizzare più la sostanza che la forma del consenso**, superando finalmente –si spera!- una certa … rigidità imposta, oggi, dalle norme vigenti.

CONSENSI PIU' AGILI, MA CERTI E DOCUMENTABILI

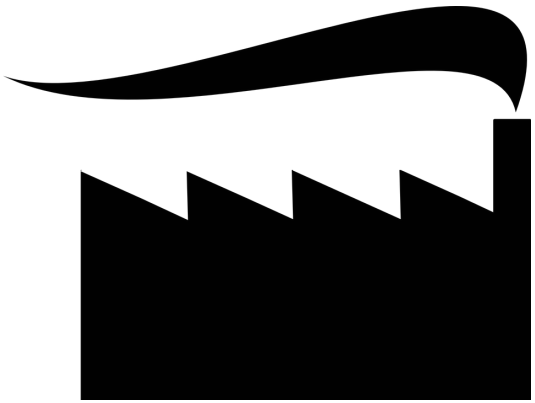


I CONSENSI GIA' RACCOLTI PRIMA DEL 25 MAGGIO 2018: QUID?

Il consenso raccolto precedentemente al 25 maggio 2018 **resta valido se ha tutte le caratteristiche sopra individuate.**

In caso contrario, è opportuno adoperarsi prima di tale data per **raccogliere nuovamente il consenso degli interessati** secondo quanto prescrive il Regolamento, se si vuole continuare a fare ricorso a tale base giuridica.

+ DIRITTI PER L'INTERESSATO



Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato

Informazioni da fornire qualora i dati siano raccolti presso l'interessato

Informazioni da fornire qualora i dati non siano stati ottenuti presso l'interessato

Diritto di accesso

+ DIRITTI PER L'INTERESSATO

L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo.

Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa

Diritto di rettifica

SENTENZA

sul ricorso 14392-2010 proposto da:

L.C. (c.f. **(omissis)**),

Da ultimo va chiarito che l'omessa pubblicazione dei dati personali della ricorrente all'interno dell'organigramma comunale va apprezzata quale violazione del principio di completezza dei dati personali trattati dall'amministrazione.

+ DIRITTI PER L'INTERESSATO

L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali (…)

Corte di Giustizia UE, Grande Sezione, sentenza 13 maggio 2014, causa C- 131/12

(…) l'attività di un motore di ricerca consistente nel trovare informazioni pubblicate o inserite da terzi su Internet, nell'indicizzarle in modo automatico, nel memorizzarle temporaneamente e, infine, nel metterle a disposizione degli utenti di Internet secondo un determinato ordine di preferenza, deve essere qualificata come «trattamento di dati personali», ai sensi del citato articolo 2, lettera b), qualora tali informazioni contengano dati personali, e che, dall'altro lato, il gestore di detto motore di ricerca deve essere considerato come il «responsabile» del trattamento summenzionato, ai sensi dell'articolo 2, lettera d), di cui sopra

(…)il gestore di un motore di ricerca è obbligato a sopprimere, dall'elenco di risultati che appare a seguito di una ricerca effettuata a partire dal nome di una persona, dei link verso pagine web pubblicate da terzi e contenenti informazioni relative a questa persona, anche nel caso in cui tale nome o tali informazioni non vengano previamente o simultaneamente cancellati dalle pagine web di cui trattasi, e ciò eventualmente anche quando la loro pubblicazione su tali pagine web sia di per sé lecita.

(…) si deve verificare in particolare **se l'interessato abbia diritto a che l'informazione in questione riguardante la sua persona non venga più, allo stato attuale, collegata al suo nome da un elenco di risultati che appare a seguito di una ricerca effettuata a partire dal suo nome,** senza per questo che la constatazione di un diritto siffatto presupponga che l'inclusione dell'informazione in questione in tale elenco arrechi un pregiudizio a detto interessato (…) i diritti fondamentali di cui sopra prevalgono, in linea di principio, non soltanto sull'interesse economico del gestore del motore di ricerca, ma anche sull'interesse di tale pubblico ad accedere all'informazione suddetta in occasione di una ricerca concernente il nome di questa persona. Tuttavia, così non sarebbe qualora risultasse, per ragioni particolari, come il ruolo ricoperto da tale persona nella vita pubblica, che l'ingerenza nei suoi diritti fondamentali è giustificata dall'interesse preponderante del pubblico suddetto ad avere accesso, in virtù dell'inclusione summenzionata, all'informazione di cui trattasi.

Diritto alla cancellazione ("diritto all'oblio")

L'interessato ha il diritto

+ DIRITTI PER L'INTERESSATO

SE

a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento;
c) l'interessato si oppone al trattamento ai sensi dell'articolo 21 ("opposizione"), paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2;
d) i dati personali sono stati trattati illecitamente;
e) i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;
f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1 ("servizi offerti a minori")

Diritto alla cancellazione ("diritto all'oblio")

+ DIRITTI PER L'INTERESSATO

L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento quando ricorre una delle seguenti ipotesi:

a) l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali;

b) il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;

c) benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;

d) l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

2. Se il trattamento dei dati personali è limitato a norma del paragrafo 1, **tali dati possono essere trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.**

Diritto di limitazione di trattamento

limitazione di trattamento: contrassegno dei dati personali memorizzati con l'obiettivo di limitarne il trattamento in futuro

NB > DLgs 193: "blocco" = la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento

+ DIRITTI PER L'INTERESSATO

Diritto alla portabilità dei dati

L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora:
a) il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o dell'articolo 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b); **e**
b) il trattamento sia effettuato con mezzi automatizzati.

L'interessato ha il diritto di ottenere la trasmissione diretta dei dati da un responsabile del trattamento all'altro, se tecnicamente fattibile.

+ DIRITTI PER L'INTERESSATO

Diritto di opposizione "bilanciato"

L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f), compresa la profilazione sulla base di tali disposizioni.

E CIOE' SE:

il trattamento è necessario per **l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri** di cui è investito il responsabile del trattamento

OPPURE

il trattamento è necessario per il **perseguimento del legittimo interesse del responsabile del trattamento o di terzi,** a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore

Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

+ DIRITTI PER L'INTERESSATO

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

Diritto di opposizione "assoluto"

Qualora i dati personali siano trattati per finalità di **marketing diretto**, l'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali finalità, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto.

Qualora l'interessato si opponga al trattamento per finalità di marketing diretto, i dati personali non sono più oggetto di trattamento per tali finalità.

+ DIRITTI PER L'INTERESSATO

Garanzia per il diritto di opposizione sia "bilanciato" che "assoluto"

Il diritto di opposizione è esplicitamente portato all'attenzione dell'interessato ed è presentato chiaramente e separatamente da qualsiasi altra informazione al più tardi al momento della prima comunicazione con l'interessato.

+ DIRITTI PER L'INTERESSATO

Diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato

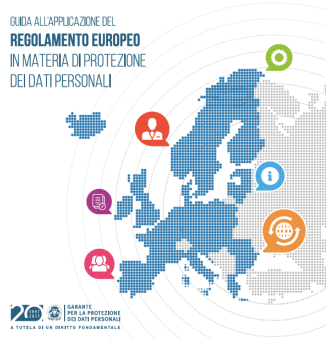
L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida allo stesso modo significativamente sulla sua persona.

… a meno che la decisione:
a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento, oppure
b) sia autorizzata dal diritto dell'Unione o degli Stati membri cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato, oppure
c) si basi sul consenso esplicito dell'interessato.

In via generale, le decisioni in esame non si basano sulle categorie particolari di dati personali

Grazie!

www.orlandi.mobi

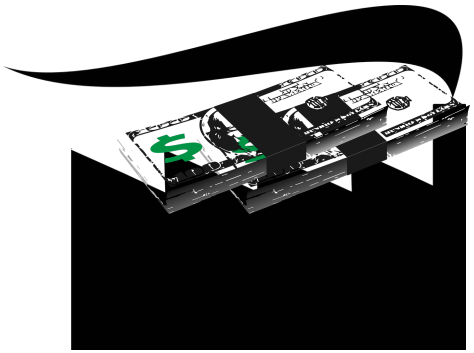


SANZIONI & RESPONSABILITA'

Diritto al risarcimento e responsabilità

Chiunque subisca un danno materiale o immateriale cagionato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno **dal titolare del trattamento o dal responsabile del trattamento.**

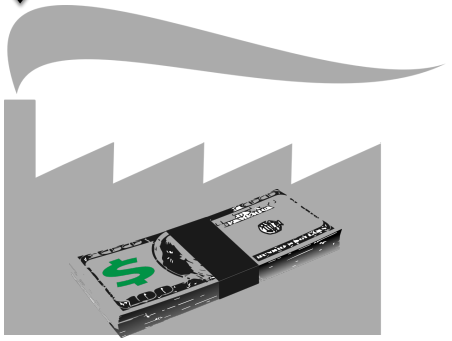
Ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato.



Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento non conforme al presente regolamento

"RECLAMO"
(rectius: "RIVALSA")

salvo che dimostri che l'evento dannoso non gli è in alcun modo imputabile.



Un responsabile del trattamento risponde per il danno cagionato dal trattamento **solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo esterno o contrario alle legittime istruzioni del titolare del trattamento.**

Il concetto di danno dovrebbe essere interpretato **in senso lato** alla luce della giurisprudenza della Corte di giustizia dell'Unione europea in modo tale da rispecchiare pienamente gli obiettivi del presente regolamento **(considerando n. 146 GDPR)**

Sanzioni pecuniarie e altre sanzioni

Ogni autorità di controllo garantisce che le sanzioni amministrative pecuniarie inflitte ai sensi in relazione alle violazioni del regolamento siano **in ogni singolo caso effettive, proporzionate e dissuasive.**
Le sanzioni amministrative pecuniarie sono irrogate, in funzione delle circostanze di ogni singolo caso, **oltre alle misure correttive o in luogo di tali misure.**

NB: ogni Stato membro può prevedere norme che dispongano **se e in quale misura** possono essere irrogate sanzioni amministrative pecuniarie **ad autorità pubbliche e organismi pubblici.**

Sanzioni pecuniarie e altre sanzioni

MISURE CORRETTIVE

fra le quali

avvertimenti al titolare del trattamento o al responsabile del trattamento sul fatto che i trattamenti previsti possono verosimilmente violare le disposizioni del regolamento;

ammonimenti al titolare del trattamento o al responsabile del trattamento ove trattamenti abbiano violato le disposizioni del presente regolamento;

ingiunzioni a al titolare del trattamento o al responsabile del trattamento di **soddisfare le richieste dell'interessato** di esercitare i diritti derivantigli dal regolamento;

ingiunzioni al al titolare del trattamento o al responsabile del trattamento di **conformare i trattamenti alle disposizioni del regolamento**, se del caso, in una determinata maniera ed entro un determinato termine;

ingiunzioni al titolare del trattamento di **comunicare all'interessato una violazione dei dati personali**;

imposizione di una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento;

ordine di rettifica, limitazione o cancellazione di dati nonché di notificazione di tali misure ai destinatari cui sono stati trasmessi

ritiro della certificazione o ingiunzione all'organismo di certificazione di ritirare la certificazione oppure ingiunzione all'organismo di certificazione di non rilasciare la certificazione

ordine di sospensione dei flussi di dati verso un destinatario in un paese terzo o un'organizzazione internazionale.

Sanzioni pecuniarie e altre sanzioni

SANZIONI PECUNIARIE - CRITERI DI IRROGAZIONE

a) la natura, la gravità e la durata della violazione tenendo in considerazione la natura, l'oggetto o a finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito;
b) il carattere doloso o colposo della violazione;
c) le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati;
d) il grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli articoli 25 e 32;
e) eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento;
f) il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;
g) le categorie di dati personali interessate dalla violazione;
h) la maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione;
i) qualora siano stati precedentemente disposti provvedimenti di cui all'articolo 58, paragrafo 2, nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti;
j) l'adesione ai codici di condotta approvati ai sensi dell'articolo 40 o ai meccanismi di certificazione approvati ai sensi dell'articolo 42; e
k) eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione.

Sanzioni pecuniarie e altre sanzioni

ENTITA' DELLE SANZIONI PECUNIARIE
fino a **€ 10.000.000, o per le imprese, fino al 2% del fatturato mondiale totale annuo** dell'esercizio precedente, se superiore, per violazione di

obblighi del titolare del trattamento e del responsabile del trattamento

8 Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione
11 Trattamento che non richiede l'identificazione
25 Protezione dei dati fin dalla progettazione e protezione di default
26 Contitolari del trattamento
27 Rappresentanti di responsabili del trattamento non stabiliti nell'Unione
28 Responsabile del trattamento
29 Trattamento sotto l'autorità del titolare del trattamento e del responsabile del trattamento
30 Registri delle attività di trattamento
31 Cooperazione con l'autorità di controllo
32 Sicurezza del trattamento
33 Notificazione di una violazione dei dati personali all'autorità di controllo
34 Comunicazione di una violazione dei dati personali all'interessato
35 Valutazione d'impatto sulla protezione dei dati
36 Consultazione preventiva
37, 38, 39 Designazione (e posizione e compiti…) del responsabile della protezione dei dati

obblighi dell'organismo di certificazione
obblighi dell'organismo di controllo

Sanzioni pecuniarie e altre sanzioni

ENTITA' DELLE SANZIONI PECUNIARIE
fino a **€ 20.000.000, o per le imprese, fino al 4% del fatturato mondiale totale annuo** dell'esercizio precedente, se superiore, per violazione di:

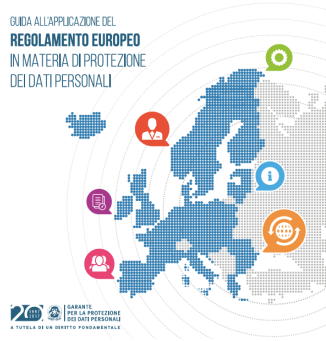
principi di base del trattamento, comprese le condizioni relative al consenso, a norma degli articoli 5, 6, 7 e 9 (Principi applicabili al trattamento di dati personali; Liceità del trattamento; Condizioni per il consenso; Trattamento di categorie particolari di dati personali)

diritti degli interessati (artt. da 12 a 22)

trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale a norma degli articoli da 44 a 49;

qualsiasi obbligo ai sensi delle legislazioni degli Stati membri adottate a norma del capo IX (DISPOSIZIONI RELATIVE A SPECIFICHE SITUAZIONI DI TRATTAMENTO DEI DATI)

mancata osservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo ai sensi dell'articolo 58, paragrafo 2, o il negato accesso in violazione dell'articolo 58, paragrafo 1


GUIDA ALL'APPLICAZIONE DEL
REGOLAMENTO EUROPEO
IN MATERIA DI PROTEZIONE
DEI DATI PERSONALI

CASISTICA

Sanzioni pecuniarie: casistica

GOOGLE: € 50.000.000

Una delle più alte sanzioni del 2019 èstata comminata dal Garante privacy francese - CNIL nei confronti di Google LLC. La sanzione di 50 milioni di euro è stata determinata dai reclami provenienti dall'associazione austriaca None Of Your Business e dall'associazione francese La Quadrature du Net, che promuovono i diritti digitali e le libertà dei cittadini. Le denunce sono state presentate rispettivamente il 25 maggio 2018 e il 28 maggio 2018, immediatamente dopo l'inizio del periodo di piena applicazione del GDPR. Le contestazioni riguardavano principalmente l**a mancanza di una valida base giuridica per trattare i dati personali degli utenti, nello specifico per finalità di pubblicità mirata.**

Sanzioni pecuniarie: casistica

SOCIETA' POLACCA: € 219.000

La prima sanzione ai sensi del GDPR comminata dal Garante privacy polacco è stata di 219.538 euro: il titolare sanzionato è stata una società che non ha rispettato l'obbligo di informativa. Molti interessati, circa 6 milioni, non erano consapevoli del fatto che la società trattasse i loro dati personali e quindi non erano in grado di esercitare i loro diritti. La società nello specifico **trattava dati personali provenienti da fonti pubbliche per finalità commerciali senza fornire l'informativa ai sensi dell'art. 14 del GDPR**.

Sanzioni pecuniarie: casistica

COMUNE DI BERGEN: € 170.000

Una sanzione di una certa rilevanza è stata inflitta dal Garante privacy norvegese: in questo caso il comune di Bergen ha ricevuto la sanzione di 170.000 euro per **mancanza di misure di sicurezza adeguate a protezione del sistema informatico comunale**, ma nello specifico delle credenziali di accesso degli studenti e dei dipendenti delle scuole primarie. La mancanza di adeguate misure di sicurezza, in violazione degli artt. 5, comma 1, lett. f) e 32 del GDPR, rendeva possibile a chiunque l'accesso ai vari sistemi informatici delle scuole con la possibilità di accedere a diverse categorie di dati personali relativi a circa 35 mila utenti, di cui **la maggior parte era costituita da minori. Questo fatto ha costituito un aggravante in virt. della particolare categoria di interessati coinvolta, meritevole di una specifica protezione.**

Sanzioni pecuniarie: casistica

ROUSSEAU: € 50.000

Con il Provvedimento del 4 aprile 2019 il Garante per la protezione dei dati personali ha comminato la sanzione di 50 mila euro all'Associazione Rousseau per la **mancanza di adeguate misure di sicurezza a protezione dei dati personali degli iscritti alla piattaforma Rousseau, in violazione quindi dell'art. 32 del GDPR**. La sanzione, inflitta nel "periodo di tolleranza" conclusosi il 19 maggio 2019.

Sanzioni pecuniarie: casistica

SERGIC: € 400.000

Il Garante privacy francese ha sanzionato SERGIC, società specializzata nell'acquisto, nella vendita, nell'affitto e nella gestione di proprietà immobiliari, per 400 mila euro in virtù della **mancanza di adeguate misure di sicurezza**, in violazione dell'art. 32 del GDPR, e per **un eccessivo periodo di conservazione dei dati degli utenti, configurandosi la violazione del principio di limitazione della conservazione di cui all'art. 5, comma 1, lett. e) del GDPR**. In merito alla mancanza di misure di sicurezza, i dati personali degli utenti, tra cui i documenti trasmessi dai richiedenti affitto contenenti anche copie di carte di identità, erano accessibili online senza una procedura di autenticazione. Inoltre, la società conservava la documentazione inoltrata dagli utenti per un periodo di tempo superiore alle effettive necessità, mantenendo nei database una grande quantità di dati obsoleti e non aggiornati.

Sanzioni pecuniarie: casistica

IDDesign: € 200.000

Il Garante privacy danese ha sanzionato la società produttrice di mobili IDdesign per 200.850 euro **per aver conservato i dati di un elevato numero di clienti per un periodo superiore al necessario. Non erano stati definiti e rispettati specifici periodi di conservazione**. Infatti, alcuni negozi di vendita al dettaglio della società utilizzavano un sistema informatico obsoleto, sostituito da un sistema nuovo solo in alcuni negozi della catena. Nei negozi forniti del vecchio sistema informatico erano conservati, senza essere stati mai cancellati, nomi, indirizzi, numeri di telefono, indirizzi e-mail e cronologia degli acquisti di circa 385 mila clienti. Tutto ciò ha determinato la **violazione del principio di limitazione della conservazione di cui all'art. 5, comma 1, lett. e)**

Sanzioni pecuniarie: casistica

Ospedale di HAGA: € 460.000

Un'elevata sanzione, pari a 460 mila euro, è stata comminata dal Garante privacy olandese all'ospedale di Haga, situato a L'Aia, per **un'insufficiente protezione dei file dei pazienti**. La violazione dell'art. 32 del GDPR è stata rilevata quando è emerso che decine di membri del personale ospedaliero avevano controllato le cartelle cliniche di un noto personaggio olandese, star di un reality televisivo, senza necessità, in quanto non coinvolti nella terapia del paziente

Sanzioni pecuniarie: casistica

MORELE.NET: € 660.000

L'autorità polacca per la protezione dei dati personali ha annunciato l'imposizione più alta fino ad oggi per violazione delle norme sulla protezione dei dati personali: 660.000 euro di multa alla società Morele.net, accusata di **non aver rispettato il principio di integrità e riservatezza definito nel GDPR.** La multa è stata stabilita il 19 settembre 2019.

Sanzioni pecuniarie: casistica

DSK BANK: OLTRE € 500.000

La DSK Bank, una banca del gruppo ungherese OTP operante in Bulgaria, è stata sanzionata per più di mezzo milione di euro a causa di una **violazione di dati riferiti a circa 33.000 suoi clienti**. L'Autorità bulgara per la protezione dei dati ha evidenziato che tra le informazioni divulgate e rese accessibili a terzi non espressamente autorizzati, vi erano nominativi dei clienti, carte d'identità e numeri di conto corrente, includendo anche indirizzi e dati riconducibili ad atti di clienti che avevano acceso prestiti dall'istituto bancario stesso, inoltre sono stati violati i dati delle persone che avevano prestato garanzia sulla restituzione dei prestiti stessi, dei coniugi, per un complessivo di oltre 23.000 pratiche.

Sanzioni pecuniarie: casistica

VUELING: € 18.000

Vueling Airlines multata per inadeguatezza al regolamento europeo. La decisione dell'Autorità spagnola per la protezione dei dati arriva dopo la decisione della Corte di giustizia dell'Unione europea, che aveva stabilito l'obbligo dal primo ottobre 2019 del consenso attivo sull'uso dei cookie. A seguito della decisione presa il 10 settembre 2019 dalla Corte di giustizia dell'Unione europea (CGUE) sui requisiti di consenso per l'uso dei cookie, l'autorità spagnola per la protezione dei dati – AEPD ha multato Vueling Airlines per 30.000 euro (ridotto a 18.000 euro per il pagamento in un unica soluzione) **per non aver fornito un consenso sui cookie conforme ai sensi del GDPR (casella consenso preselezionata)**

Sanzioni pecuniarie: casistica

(in itinere) **BRITISH AIRWAYS: 205.000.000**

Il Garante privacy inglese ha intenzione di sanzionare la compagnia aerea British Airways per 204.6 milioni di euro). La sanzione, riconducibile alla violazione dell'art. 32 del GDPR, è relativa ad un i**ncidente di sicurezza notificato all'ICO a settembre 2018**.

L'incidente ha comportato la parziale deviazione del traffico degli utenti del sito della società verso un sito fraudolento, attraverso cui gli hacker hanno ottenuto i dati personali, tra cui credenziali di accesso, numeri di carte di pagamento, dettagli di prenotazioni, indirizzi, etc., di circa 500 mila clienti

Sanzioni pecuniarie: casistica

(in itinere) **MARRIOTT: 110.000.000**

Il Garante privacy inglese ha intenzione di sanzionare la catena di hotel Marriott International. In tal caso la sanzione si riferisce ad un **incidente informatico notificato all'ICO a novembre 2018**. Sono stati esposti i dati contenuti in circa 339 milioni di registri informatici degli ospiti a livello globale, di cui circa 30 milioni relativi a residenti in 31 paesi dello Spazio Economico Europeo (SEE) e circa 7 milioni legati ai residenti nel Regno Unito

Sanzioni pecuniarie: casistica

Deutsche Wohen: 14.500.000

L'Autorità di controllo della protezione dei dati per lo stato di Berlino (Die Berliner Beauftragte für Datenschutz und Informationsfreiheit) ha sanzionato la seconda più grande società immobiliare tedesca Deutsche Wohnen per **le violazioni del GDPR per la conservazione di dati personali senza giustificazione legale.**

La sanzione è stata emessa per violazioni verificatesi tra maggio 2018 e marzo 2019 del principio dell'art. 5 e di quello di "privacy by design" dell'art. 25. La Deutsche Wohnen ha utilizzato **un sistema di archiviazione dei dati personali dei suoi inquilini che non prevedeva un'opzione per eliminare i dati non più necessari.** I dati sono stati quindi a**rchiviati senza valutare se la loro conservazione è lecita o addirittura necessaria. In alcuni dei casi valutati, l'autorità di vigilanza ha rilevato dati personali di inquilini che non erano più pertinenti allo scopo per il quale erano stati originariamente raccolti.**

Tra i dati rilevati dall'autorità di vigilanza c'erano dichiarazioni salariali, moduli di auto-divulgazione, dati fiscali, previdenziali e di assicurazione sanitaria e altri dati personali relativi alla situazione personale e finanziaria degli inquilini di DW. **Tale sistema viola i principi di protezione dei dati relativi alla minimizzazione dei dati, alla limitazione della conservazione e alla liceità sanciti dall'art. 5 (1) (a), (c), (e) GDPR e la protezione dei dati secondo il principio di progettazione di cui all'art. 25 (1) GDPR.** Oltre all'ammenda di 14,5 milioni di euro, l'autorità di controllo ha emesso ammende supplementari nei confronti di DW con importi compresi tra 6.000 e 17000 euro per l'archiviazione illegale dei dati personali degli inquilini in 15 casi individuali.di imporre un'ammenda.