Convegno **Associazione ICT Dottori Commercialisti**

NUCLEO SPECIALE TUTELA PRIVACY E FRODI TECNOLOGICHE

GDPR: MODALITA' E CONTENUTO DELLE ATTIVITA' ISPETTIVE DI QUESTI MESI

Col. Marco Menegazzo

Politecnico di Torino, 20 novembre 2020

TaxLawPlanet *Webinar*

NUCLEO SPECIALE TUTELA PRIVACY E FRODI TECNOLOGICHE

LA CONSAPEVOLEZZA E L'OPPORTUNITA'

NUCLEO SPECIALE TUTELA PRIVACY E FRODI TECNOLOGICHE

IL QUADRO

Attacchi cyber a tema covid, è boom: ecco i più pericolosi

Phishing che sfrutta l'attesa del vaccino covid. Dati a rischio negli apparecchi di monitoraggio pazienti. Videoconferenze sempre nel mirino del cyber crime. Ecco una rassegna degli allarmi più gravi, alla luce di numerosi studi e rapporti

IL CASO

Donna morta per colpa di ransomware: la Sanità non cyber-sicura uccide

Succede in Germania, per il blocco informatico dell'ospedale universitario di Duesseldorf. Bloccati 30 server interni, il 10 settembre, sfruttando una vulnerabilità del gateway Citrix, denominata CVE-2019-19871. Già Wannacry aveva aumentato il tasso di mortalità connessa. Ecco perché avere ospedali cyber sicuri è vitale

L'ANALISI TECNICA

Alien, il malware che infetta le app Android e svuota i conti correnti delle vittime

Si chiama Alien un nuovo banking trojan per Android molto insidioso che consente di sottrarre le credenziali da 226 app e agire da remoto sui device della vittima in modo del tutto indisturbato. Ecco tutti i dettagli

Glupteba: il malware che ruba dati pubblici a organizzazioni governative

Un cyber attacco ha violato il parlamento della Norvegia

Violate le caselle di posta elettronica dei dipendenti e di alcuni parlamentari. Anche una delle principali aziende pubbliche ha avuto disservizi con le email. Indagini in corso

NUCLEO SPECIALE TUTELA PRIVACY E FRODI TECNOLOGICHE

ENISA: 10 principali trend del cybercrime

1. L'area o meglio la superficie di potenziali cyberattacchi continua ad espandersi con l'avvicinarsi di una nuova fase della trasformazione digitale
2. Ci sarà una nuova normalità sociale ed economica dopo la pandemia COVID-19 ancora più dipendente da un cyberspazio sicuro e affidabile
3. L'utilizzo di piattaforme di social media in attacchi mirati è una tendenza seria e raggiunge diversi domini e tipi di minacce
4. Attacchi mirati e persistenti su dati di alto valore (ad es. Proprietà intellettuale e segreti di stato) vengono pianificati ed eseguiti meticolosamente da attori sponsorizzati dallo stato
5. Gli attacchi distribuiti in modo massiccio con una breve durata e un ampio impatto vengono utilizzati con molteplici obiettivi come il furto di credenziali
6. La motivazione alla base della maggior parte degli attacchi informatici resta ancora quella finanziaria
7. Il ransomware rimane sempre diffuso con conseguenze costose per molte organizzazioni
8. Ancora molti incidenti di sicurezza informatica passano inosservati o richiedono molto tempo per essere rilevati
9. Con una maggiore automazione della sicurezza, le organizzazioni investiranno di più nella preparazione utilizzando la Cyber Threat Intelligence
10. Il numero di vittime di phishing continua a crescere poiché sfrutta la dimensione umana che è l'anello più debole

NUCLEO SPECIALE TUTELA PRIVACY E FRODI TECNOLOGICHE

NUCLEO SPECIALE TUTELA PRIVACY E FRODI TECNOLOGICHE

Credenziali, follower e informazioni sanitarie mercificati nell'area oscura della rete

Dati sotto assedio nel dark web Con danni per 6 mila mld $

Pagine a cura
DI ANTONIO CICCIA MESSINA

Nel web bazar si vendono e si comprano carte di credito, credenziali bancarie, passaporti. E non solo. Se si vuole commissionare un attacco internet si può scegliere il livello di efficacia distruttiva: il listino contempla aree geografiche preferite e ci sono opzioni per i vari portafogli.

Però qualcuno può essere interessato a dati sanitari e anche in questo caso non è un problema: nel web oscuro si trova anche questo. Oppure, ancora, si può desiderare di avere un pacchetto completo di una identità da spendere nelle relazioni sul web e c'è solo l'imbarazzo della scelta.

Tutto questo si trova nel «dark web» (per distinguerlo dal

Come scoprire se sono stato hackerato

Controlli	Strumenti utili
Attivare un alert sul proprio nome, sul proprio cellulare, sulla propria email, in modo che non appena dovesse comparire uno dei tre elementi online nel clear web saremmo i primi a esserne informati	Google Alert TalkWalker Alert (molto veloce per trovare informazioni sui social network) https://pastebin.com (necessario autenticarsi)
Controlli sul dark web	https://ahmia.fi/
Verificare se il tuo account mail è mai stato vittima di un breach	https://haveibeenpwned.com/
Verificare se siamo vittime di attacco cyber, eseguire la ricerca tramite indicazione della mail, nome e cognome e addirittura indirizzo fisico	https://dehashed.com/
In caso rilevi il breach del tuo account segnala anche parte della password ad esso associata	https://ghostproject.fr

del trattamento di rispettare i principi generali del trattamento e di osservare la privacy quale impostazione predefinita dei propri strumenti (privacy by default) e di porsi il problema del rispetto della privacy fin dalla progettazione della sua attività (privacy by design). Quanto ai principi, l'articolo 5 del Gdpr stabilisce che il trattamento deve essere corretto, oltre che lecito. Questo significa che bisogna rispettare anche requisiti di etica e moralità delle operazioni che si compiono. Sono canoni che assumono un particolare rilievo quando si parla di dati estratti a mezzo di tecniche in grado di rilevare l'impronta del cervello. Il medesimo articolo 5 impone che i trattamenti rispondano a criteri di sicurezza.

È indispensabile che imprese e pubbliche amministrazioni esaminino questi

NUCLEO SPECIALE TUTELA PRIVACY E FRODI TECNOLOGICHE

CLEAR E DARK WEB

NUCLEO SPECIALE TUTELA PRIVACY E FRODI TECNOLOGICHE

Dark Web, diventare italiani costa 750 euro

Nella rete osura si acquistano droghe, si commissionano omicidi e si ottengono documenti falsi di qualsiasi nazionalità. Il pacchetto-Italia comprende passaporto, patente e carta d'identità

Passaporti e patenti

Ma non siamo certo limitati al Paese dello Zio Sam. FakeID, infatti, ha un listino che comprende la fornitura di passaporti, patenti di guida e documenti di identità fasulli per molte nazioni.

Country	Price for Passport	Price for Passport + Driving license	Price for Passport + ID card	Price for Passport + Driving license + ID card
Australia	600 Euro	700 Euro	700 Euro	800 Euro
Belgium	500 Euro	600 Euro	600 Euro	700 Euro
Brazil	400 Euro	-	-	-
Canada	600 Euro	700 Euro	700 Euro	800 Euro
Ireland	500 Euro	600 Euro	600 Euro	700 Euro
Italia	550 Euro	650 Euro	650 Euro	750 Euro
Finland	500 Euro	600 Euro	600 Euro	700 Euro
France	600 Euro	700 Euro	700 Euro	800 Euro
Germany	600 Euro	700 Euro	700 Euro	800 Euro
Malaysia	450 Euro	550 Euro	550 Euro	650 Euro
Netherlands	600 Euro	700 Euro	700 Euro	800 Euro
Norway	650 Euro	750 Euro	750 Euro	850 Euro

Se il Paese che ci interessa non è nella lista, si può parlare con un operatore per verificare la fattibilità e il prezzo della prestazione particolare.

Falsa cittadinanza

Ormai abbiamo appurato che nel Dark Web esiste un surrogato di qualsiasi attività criminale di spicco e non poteva mancare quella della falsificazione di documenti, realizzata con la solita professionalità che contraddistingue i cybercriminali.

Con 5.900 dollari ci viene garantito tutto il necessario per diventare cittadino americano: passaporto, numero di sicurezza sociale (il nostro codice fiscale), patente di guida e addirittura un certificato di nascita. Si può anche scegliere a che nome intestare tutto e via, iniziare una nuova vita Oltreoceano.

NUCLEO SPECIALE TUTELA PRIVACY E FRODI TECNOLOGICHE

ATTIVITÀ ISPETTIVA II SEM. 2020

data breach.

trattamenti dei dati personali effettuati mediante applicativi per la gestione delle segnalazioni di condotte illecite (c.d. whistleblowing);

trattamenti di dati personali effettuati da Enti pubblici in tema di rilascio di certificati anagrafici e di stato civile, attraverso l'accesso ad ANPR;

trattamenti di dati personali effettuati da società private ed Enti pubblici per la gestione e la registrazione delle telefonate nell'ambito del servizio di call center;

trattamenti dei dati personali effettuati da intermediari per la fatturazione elettronica;

trattamenti di dati personali effettuati da società rientranti nel settore denominato "Food Delivery";

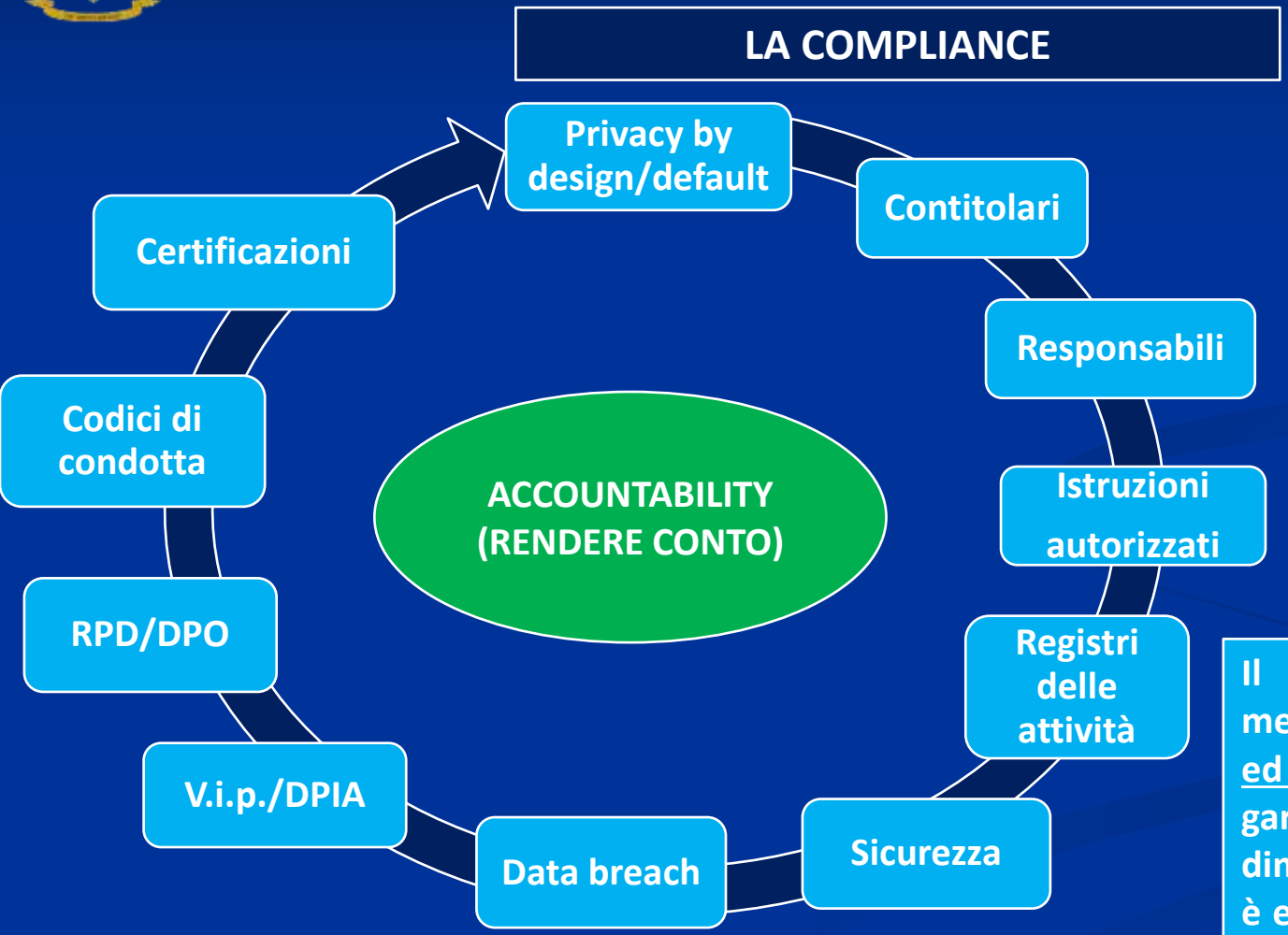
trattamento di dati personali effettuati da società private in tema di banche reputazionali;

NUCLEO SPECIALE TUTELA PRIVACY E FRODI TECNOLOGICHE

ART. 5 - PRINCIPI E DIRITTI

NUCLEO SPECIALE TUTELA PRIVACY E FRODI TECNOLOGICHE

LA COMPLIANCE

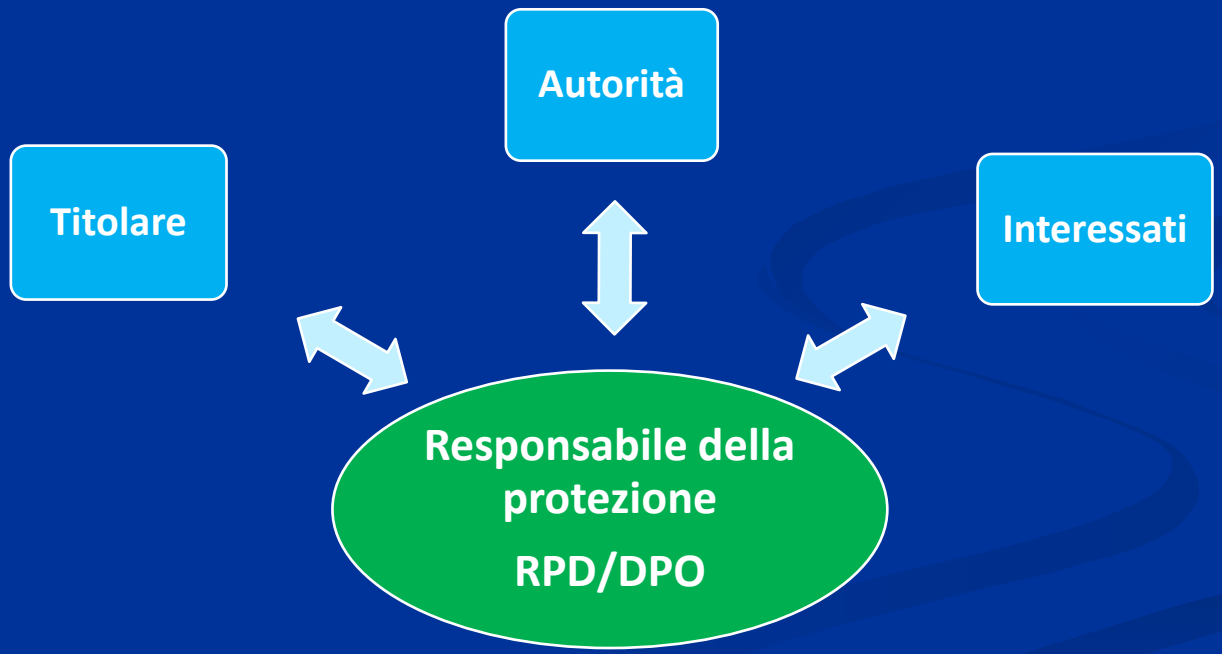


Per il GDPR deve essere dimostrata la sostanza degli adempimenti non il rispetto formale. Non basta aver adempiuto alle richieste normative, ma occorre essere in grado di DIMOSTRARLO.

Il titolare del trattamento mette in atto misure tecniche ed organizzative adeguate per garantire ed essere in grado di dimostrare che il trattamento è effettuato conformemente al presente regolamento (art. 24)

NUCLEO SPECIALE TUTELA PRIVACY E FRODI TECNOLOGICHE

IL RUOLO CHIAVE



NUCLEO SPECIALE TUTELA PRIVACY E FRODI TECNOLOGICHE

ATTIVITA' ISPETTIVA (1)

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

DIPARTIMENTO ATTIVITA' ISPETTIVE

Prot. n.

Roma,

Oggetto: *Richiesta di informazioni ai sensi dell'art. 58, comma 1, lettera a) ed e), del Regolamento generale sulla protezione dei dati (UE) 2016/679 (di seguito Rgdp) e dell'art. 157 e 158 del decreto legislativo n. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali) (di seguito Codice).*

Con riferimento al trattamento di dati personali effettuato
si invita il soggetto in indirizzo, ai sensi dell'art. 58, c. 1, lettera a) ed e), del *Rgdp* e dell'art. 157 e 158 del *Codice*, a comunicare all'organo incaricato di notificare la presente richiesta:

1) struttura ed organizzazione della società;
2) distribuzione delle funzioni in materia di protezione dei dati personali;
3) modalità con la quale viene fornita agli interessati l'informativa di cui agli art. 13 e 14 del *Rgdp* acquisendo copia della relativa documentazione;
4) modalità di acquisizione dei consensi ai sensi degli artt. 7 e 8 del *Rgdp*, per le ulteriori finalità (*marketing* – profilazione – comunicazione dei dati a soggetti terzi) con relativa documentazione;

NUCLEO SPECIALE TUTELA PRIVACY E FRODI TECNOLOGICHE

ATTIVITA' ISPETTIVA (2)

5) eventuale istituzione del registro dei trattamenti mettendone a disposizione copia dello stesso (art. 30 *Rgdp*);
6) eventuale designazione di responsabili esterni (e/o *sub* responsabili) del trattamento con acquisizione del relativo contratto e designazione (art. 28 del *Rgdp*);
7) eventuale nomina del DPO in relazione agli artt. 37 e segg. del *Rgdp*;
8) soggetti autorizzati ad accedere ai dati personali oggetto del trattamento e documentazione relativa all'istruzione ed alla formazione degli incaricati ed eventuale copia delle nomine a incaricati (art. 29 *Rgdp*);
9) tipologia di profilazione effettuata e descrizione dettagliata del suo funzionamento, con particolare riferimento alle modalità di raccolta, di aggregazione e di analisi dei dati personali della clientela;
10) eventuale utilizzo a fini di profilazione di dati particolari dell'interessato (art. 9 *Rgdp*);
11) tipologia di attività di *marketing* effettuato a seguito della profilazione;
12) il periodo di conservazione dei dati di profilazione personali ovvero i criteri utilizzati per determinare tale periodo;
13) valutazione d'impatto eventualmente effettuata in relazione ai trattamenti dei dati oggetto della profilazione tenendo conto di quanto previsto al riguardo nella delibera del Collegio datata 11 ottobre 2018 (*vgs. doc. web.* 9058979) fornendo gli elementi di tale valutazione;

Piazza di Monte Citorio, 121 - 00186 Roma
Tel. +39 06 696772794 - Fax +39 06 696773785
www.garanteprivacy.it
E-mail: dais@gpdp.it
Posta certificata: dais@pec.gpdp.it

ATTIVITA' ISPETTIVA (3)

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

14) presupposti, ambito e modalità di comunicazione a terzi dei dati, anche in riferimento ad eventuali società controllanti, controllate o collegate ed all'eventuale trasferimento dei dati in paesi non appartenenti all'Unione europea;
15) procedure poste in essere per l'esercizio dei diritti degli interessati (artt. 15 a 22 del *Rgdp*);
16) misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio (art. 32 del *Rgdp*) con particolare riferimento a:
- eventuale pseudonimizzazione e cifratura dei dati personali;
- capacità di assicurare la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi del trattamento;
- capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative al fine di garantire la sicurezza del trattamento;
- principali applicazioni utilizzate sui sistemi (*client server/web application*);
- misure idonee per accedere a banche dati (*username* e *password*; *strong authentication*;
- *audit* effettuato sia internamente che presso eventuali responsabili esterni;
- eventuali *alert* implementati su sistemi;
- eventuale *backup* sui dati;

NUCLEO SPECIALE TUTELA PRIVACY E FRODI TECNOLOGICHE

ATTIVITA' ISPETTIVA (4)

Eventuali ulteriori documenti utili all'istruttoria dovranno pervenire, entro e non oltre 15 giorni dalla notifica della presente richiesta di informazioni, all'organo incaricato di notificare la presente richiesta, per il successivo inoltro al Garante.

Nel far presente che per ogni ulteriore informazione è possibile rivolgersi al Dipartimento in intestazione, si ricorda che, in caso di inottemperanza alla presente richiesta, questa Autorità Garante si riserva di valutare i presupposti per l'applicazione delle sanzioni previste dall'art. 166, comma 2, del Codice per la violazione dell'art. 157 (richiesta di informazione o esibizione di documenti) e delle sanzioni previste dall'art 83, comma 5, lettera e), per la violazione dell'art. 58, paragrafo 1, (negato accesso).

Piazza di Monte Citorio, 121 - 00186 Roma
Tel. +39 06 696772794 - Fax +39 06 696773785
www.garanteprivacy.it
E-mail: dais@gpdp.it
Posta certificata: dais@pec.gpdp.it

LE SANZIONI

NUCLEO SPECIALE TUTELA PRIVACY E FRODI TECNOLOGICHE

SANZIONI PREVISTE DAL GDPR

Art. 83, par. 4

(fino a 10.000.000 € o fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore)

Art. 83, par. 5

(fino a 20.000.000 € o fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore)

NUCLEO SPECIALE TUTELA PRIVACY E FRODI TECNOLOGICHE

REGOLAMENTO UE 2016/679

SANZIONI AMMINISTRATIVE E PECUNIARIE

SANZIONI PECUNIARIE FINO A 10.000.000 EURO O, PER LE IMPRESE FINO AL 2% DEL FATTURATO MONDIALE ANNUO DELL'ESERCIZIO PRECEDENTE, SONO PREVISTE IN CASO DI VIOLAZIONE DI:

- OBBLIGHI DEL TITOLARE E DEL RESPONSABILE DEL TRATTAMENTO;
- OBBLIGHI DELL'ORGANISMO DI CERTIFICAZIONE
- OBBLIGHI DELL'ORGANISMO DI CONTROLLO

NUCLEO SPECIALE TUTELA PRIVACY E FRODI TECNOLOGICHE

REGOLAMENTO UE 2016/679

SANZIONI AMMINISTRATIVE E PECUNIARIE

SANZIONI PECUNIARIE FINO A 20.000.000 EURO O, PER LE IMPRESE FINO AL 4% DEL FATTURATO MONDIALE ANNUO DELL'ESERCIZIO PRECEDENTE, SONO PREVISTE IN CASO DI VIOLAZIONE DI:

- PRINCIPI BASE DEL REGOLAMENTO, INCLUSE LE CONDIZIONI RELATIVE AL CONSENSO;
- DIRITTI DEGLI INTERESSATI;
- TRASFERIMENTI DI DATI PERSONALI A UN DESTINATARIO IN UN PAESE TERZO O UN'ORGANIZZAZIONE INTERNAZIONALE ;
- L'INOSSERVANZA 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.

NUCLEO SPECIALE TUTELA PRIVACY E FRODI TECNOLOGICHE

REGOLAMENTO UE 2016/679

ART. 83 – CONDIZIONI GENERALI PER INFLIGGERE SANZIONI AMMINISTRATIVE PECUNIARIE

C148, C150-C152

LE SANZIONI AMMINISTRATIVE PECUNIARIE DEVONO ESSERE:
-EFFETTIVE
-PROPORZIONATE
-DISSUASIVE.

Nucleo Speciale Tutela Privacy e Frodi Tecnologiche

Top 10: multe individuali più alte

#	TITOLARE	NAZIONE	SANZIONE [€]	VIOLAZIONE
1	GOOGLE INC.	FRANCIA	50,000,000	Base giuridica insufficiente per l'elaborazione dei dati
2	H&M HENNES & MAURITZ ONLINE SHOP A.B. & CO. KG	GERMANIA	35,258,708	Base giuridica insufficiente per l'elaborazione dei dati
3	TIM (operatore di telecomunicazioni)	ITALIA	27,800,000	Base giuridica insufficiente per l'elaborazione dei dati
4	BRITISH AIRWAYS	REGNO UNITO	22,046,000	Misure tecniche e organizzative insufficienti per garantire la sicurezza delle informazioni
5	MARRIOTT INTERNATIONAL, INC	REGNO UNITO	110,390,200	Misure tecniche e organizzative insufficienti per garantire la sicurezza delle informazioni
6	POSTE AUSTRIACHE	AUSTRIA	18,000,000	Base giuridica insufficiente per l'elaborazione dei dati
7	WIND TRE S.P.A.	ITALIA	16,700,000	Base giuridica insufficiente per l'elaborazione dei dati
8	DEUTSCHE WOHNEN SE	GERMANIA	14,500,000	Inosservanza dei principi generali di elaborazione dei dati
9	VODAFONE ITALIA S.P.A.	ITALIA	12,250,000	Base giuridica insufficiente per l'elaborazione dei dati Misure tecniche e organizzative insufficienti per garantire la sicurezza delle informazioni
10	ENI GAS E LUCE	ITALIA	8,500,000	Base giuridica insufficiente per l'elaborazione dei dati

NUCLEO SPECIALE TUTELA PRIVACY E FRODI TECNOLOGICHE

GRAZIE PER L'ATTENZIONE