Cybersecurity e Data Protection:

il valore della crittografia.

14 gennaio 2022

Relatore: Col. Marco Menegazzo

NUCLEO SPECIALE TUTELA PRIVACY E FRODI TECNOLOGICHE

N.S.T.P.F.T.

DIPENDENZA GERARCHICA

UNITA' SPECIALI

AUTORITÀ DI RIFERIMENTO

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

PROTOCOLLO D'INTESA TRA AUTORITA' GARANTE E GUARDIA DI FINANZA

31 MARZO 2021

CONSAPEVOLEZZA E OPPORTUNITA'
ART. 1 GDPR – OGGETTO E FINALITA'

IL PRESENTE REGOLAMENTO STABILISCE NORME RELATIVE ALLA PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI, NONCHÉ NORME RELATIVE ALLA LIBERA CIRCOLAZIONE DI TALI DATI

NUCLEO SPECIALE TUTELA PRIVACY E FRODI TECNOLOGICHE

RAPPORTO CLUSIT 2021

Per quanto riguarda la distribuzione geografica delle vittime: nel 1° semestre 2021 rimangono sostanzialmente invariate le vittime di area americana (dal 45% al 46%), gli attacchi verso realtà basate in Europa aumentano sensibilmente (dal 15% al 25%) mentre rimangono percentualmente quasi invariati quelli rilevati contro organizzazioni asiatiche.

Rispetto al secondo semestre 2020, in termini assoluti nel 1° semestre 2021 la crescita maggiore nel numero di attacchi gravi si osserva verso le categorie "Transportation / Storage" (+108,7%), "Professional, Scientific, Technical" (+85,2%) e "News & Multimedia" (+65,2%), seguite da "Wholesale / Retail" (+61,3%) e "Manufacturing" (+46,9%). Aumentano anche gli attacchi verso le categorie "Energy / Utilities" (+46,2%), "Government" (+39,2%), "Arts / Entertainment" (+36,8%) ed "Healthcare" (+18,8%).

clusit.it

NUCLEO SPECIALE TUTELA PRIVACY E FRODI TECNOLOGICHE

DATA BREACH

IL QUADRO

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

Home > Malware e attacchi hacker

Condividi questo articolo

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

26 Ago 2020

Marco Falconi
Site Reliability Engineer

IL CASO

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

Home > Malware e attacchi hacker > Ransomware

Condividi questo articolo

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

18 Set 2020

il Resto del Carlino
VENETO

COVID OGGI AMADORI GREEN PASS NEGOZI OMICIDIO OMICRON GUARIGIONE QUARANTENA TAMPONE GRATIS MARCHE SCUOLA

Padova, attacco hacker alla Ulss 6 Euganea: riunita la task force, 60 tecnici in ospedali

Pubblicato il 5 dicembre 2021

Obiettivo la bonifica e il ripristino dei sistemi informatici; i punti vaccinali funzionano in modalità provvisoria. Allertate Polizia e Garante della privacy

il Fatto Quotidiano

Facebook, rubati e diffusi i dati di 36 milioni di italiani. Garante della Privacy: "Social fornisca un servizio per verificare il furto"

Attacco hacker: da domani attivo nuovo portale Regione Lazio

Da oggi Centro prenotazioni per 10 aziende,per 15/9 Salute Lazio

Redazione ANSA

ROMA

10 agosto 2021
17:19

NEWS

CRONACA | 11 aprile 2021, 15:03

Attacco informatico all'Agenzia territoriale per la casa di Torino: chiesto un riscatto di 700mila dollari

La Atc ha presentato denuncia alla polizia postale, dopo aver risposto alla mail degli hacker per denunciare che il loro è stato un attacco "contro tutte le 30mila famiglie delle case popolari". Il sistema è al momento bloccato

Tecnologia

Hacker bucano Ho Mobile, ecco cosa devono fare i 2 milioni di clienti a rischio

Giuseppe Mauro — 4 Gennaio 2021

Allarme privacy e rischio truffe per 500 milioni di utenti di Linkedin: dati personali dei profili in vendita online su un forum di hacker

Flash News — Martedì, 06 Aprile 2021 21:16

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 pubbbliche ha avuto disservizi con le email. Indagini in corso

Lo Storting, parlamento norvegese è stato vittima di un cyberattacco (Photo by Sigrid Harms/picture alliance via Getty Images)

la Repubblica

San Giovanni, attacco hacker all'ospedale: in tilt il sistema di telecomunicazioni, impossibile leggere le cartelle cliniche

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

IL BUSINESS DEI DATI

24 Tecnologia Cybersicurezza

Cybersicurezza

Record di dati rubati in vendita nel Dark Web, la pandemia spinge il crimine informatico

Oltre un milione di avvisi di furti in dodici mesi, in crescita del 56%. Telegram l'ambiente più utilizzato

29 ottobre 2021

CLEAR E DARK WEB

ATTIVITÀ ISPETTIVA

PROGRAMMAZIONE II SEM. 2021

* Data breach

- trattamenti di dati personali effettuati da società per attività di marketing e profilazione
- trattamenti di dati personali effettuati dai c.d. "data broker"
- trattamenti di dati personali nel settore della c.d. "videosorveglianza domestica" e nel settore dei sistemi audio/video applicati ai giochi (c.d. giocattoli connessi)
- trattamenti di dati biometrici per il riconoscimento facciale anche mediante sistemi di videosorveglianza
- trattamento di dati personali effettuati da società private in tema di banche dati reputazionali
- trattamento di dati relativi alla salute effettuati da Istituti di Ricovero e Cura a carattere scientifico (IRCCS), sia pubblici che privati
- trattamenti di dati personali effettuati da società rientranti nel settore del cd. "Food Delivery"

* Presente anche nelle deliberazioni del I e II sem. 2020 e del I sem. 2021

RECLAMI (ARTT. 77 GDPR 142 Codice) SEGNALAZIONI (ART. 144 Codice)

CITTADINI/UTENTI/CLIENTI/DIPENDENTI

- comunicazioni indesiderate (telemarketing aggressivo)
- videosorveglianza
- controllo a distanza del lavoratore
- mancato adempimento a richieste per l'esercizio dei diritti
- ecc.

ART. 5 - PRINCIPI E DIRITTI

ARTICOLO 4
Definizioni

(…)

12) «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; (C85)

(…)

ARTICOLO 5
Principi applicabili al trattamento dei dati personali

1. I dati personali sono: (C39)

(…)

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»).

(…)

ARTICOLO 25
Protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita (C75-C78)

1. 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.

2. 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.

(...)

ARTICOLO 28
Responsabile del trattamento (C81)

(…)

3. 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 prevede, in particolare, che il responsabile del trattamento:

(…)

c) adotti tutte le misure richieste ai sensi dell'articolo 32;

ARTICOLO 29
Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento (C81)

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.

ARTICOLO 30
Registri delle attività di trattamento (C82)

1. Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:

(…)

g) ove possibile, una descrizione generale delle MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE di cui all'articolo 32, paragrafo 1.

(…)

ARTICOLO 32
Sicurezza del trattamento (C83)

1. 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, che comprendono, tra le altre, se del caso:

a) la pseudonimizzazione e la CIFRATURA dei dati personali;

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

c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle MISURE TECNICHE E ORGANIZZATIVE al fine di garantire la sicurezza del trattamento.

ARTICOLO 32
Sicurezza del trattamento (C83)

2. 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.

4. 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.

ARTICOLO 33
Notifica di una violazione dei dati personali all'autorità di controllo (C85, C87, C88)

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. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

ARTICOLO 34
Comunicazione di una violazione dei dati personali all'interessato (C86-C88)

1. Quando la violazione dei dati personali è suscettibile di PRESENTARE UN RISCHIO ELEVATO PER I DIRITTI E LE LIBERTÀ DELLE PERSONE FISICHE, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.

2. La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d).

3. Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:

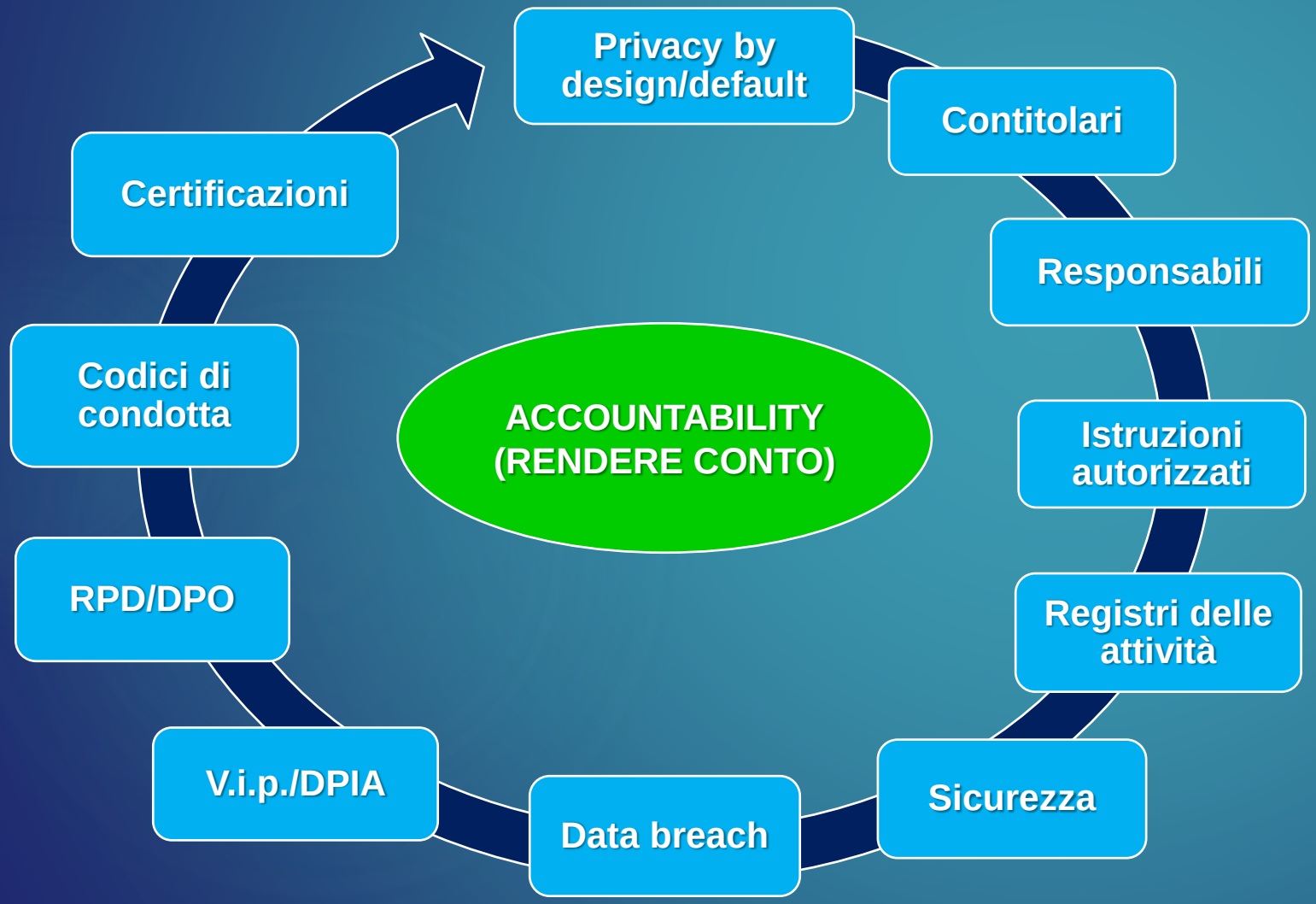
a) il titolare del trattamento ha messo in atto le MISURE TECNICHE E ORGANIZZATIVE adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la CIFRATURA;

(…)

CONSIDERANDO 83 (CIFRATURA DEI DATI)

Per mantenere la sicurezza e prevenire trattamenti in violazione al presente regolamento, il titolare del trattamento o il responsabile del trattamento dovrebbe valutare i rischi inerenti al trattamento e attuare misure per limitare tali rischi, quali la CIFRATURA. Tali misure dovrebbero assicurare un adeguato livello di sicurezza, inclusa la riservatezza, tenuto conto dello stato dell'arte e dei costi di attuazione rispetto ai rischi che presentano i trattamenti e alla natura dei dati personali da proteggere. Nella valutazione del rischio per la sicurezza dei dati è opportuno tenere in considerazione i rischi presentati dal trattamento dei dati personali, come la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati, che potrebbero cagionare in particolare un danno fisico, materiale o immateriale.

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)

IL RUOLO CHIAVE

Autorità

Titolare

Interessati

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;

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;

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

REGOLAMENTO UE 2016/679

ART. 83 – CONDIZIONI GENERALI PER INFLIGGERE SANZIONI AMMINISTRATIVE PECUNIARIE

LE SANZIONI AMMINISTRATIVE PECUNIARIE DEVONO ESSERE:

- **EFFETTIVE**
- **PROPORZIONATE**
- **DISSUASIVE.**

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

REGOLAMENTO UE 2016/679

SANZIONI AMMINISTRATIVE E PECUNIARIE

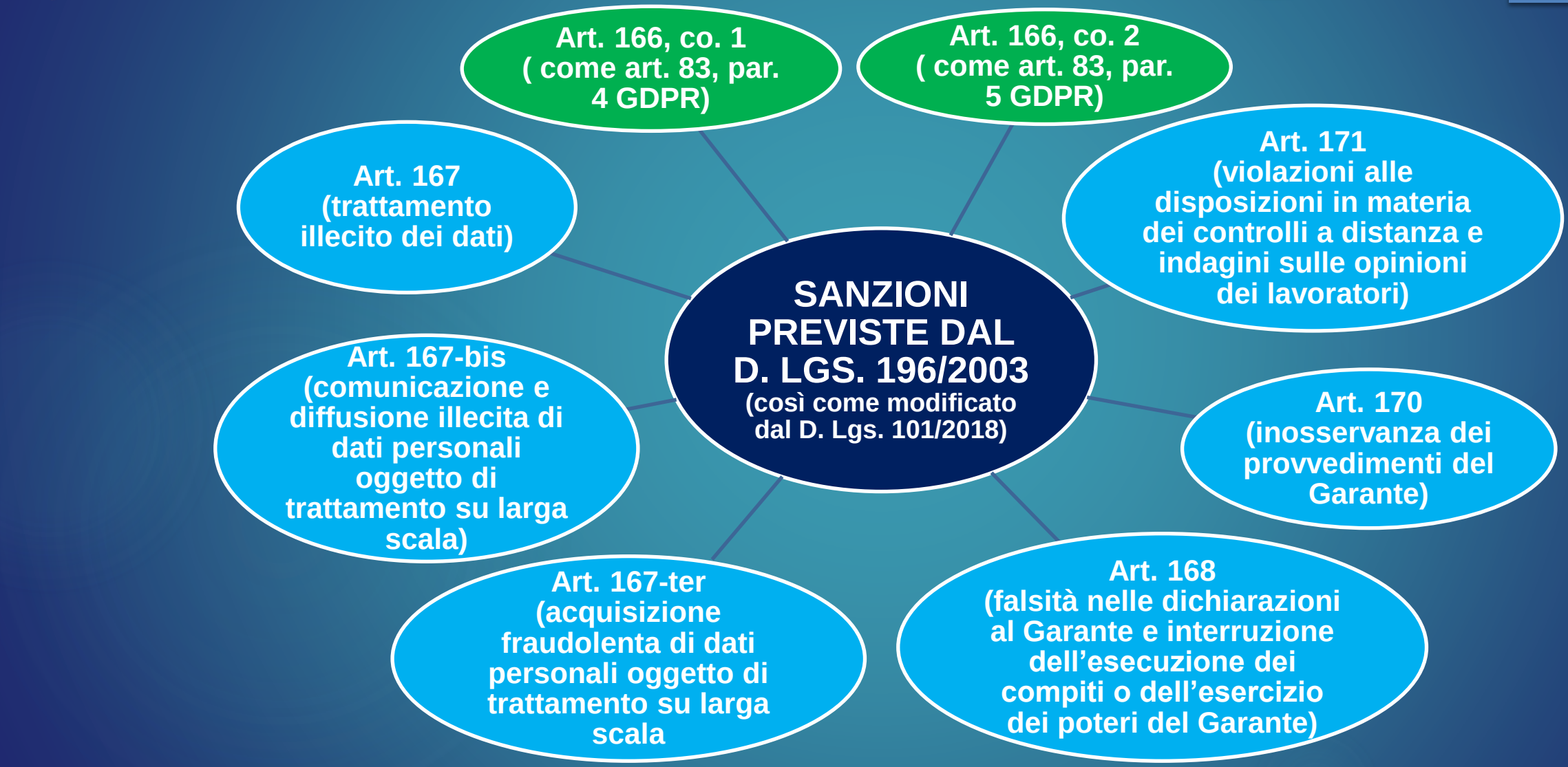
SANZIONI PECUNIARIE FINO A 20.000.000 EURO O, PER LE IMPRESE FINO AL 4% DEL FATTURATO MONDIALE ANNUO DELL'ESERCIZIO PRECEDENTE, SONO PREVISTE IN CASO DI VIOLAZIONE DI:

- 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.

Top 10: multe individuali più alte

TITOLARE	NAZIONE	SANZIONE [€]	VIOLAZIONE
Amazon Europe Core S.à.r.l.	LUSSEMBURGO	746,000,000	Mancato rispetto dei principi generali in materia di trattamento dei dati
WhatsApp Ireland Ltd.	IRLANDA	225,000,000	Insufficiente adempimento degli obblighi di informazione
Google LLC	FRANCIA	90,000,000	Base giuridica insufficiente per l'elaborazione dei dati
Facebook Ireland Ltd.	FRANCIA	60,000,000	Base giuridica insufficiente per l'elaborazione dei dati
Google Ireland Ltd.	FRANCIA	60,000,000	Base giuridica insufficiente per l'elaborazione dei dati
Google LLC	FRANCIA	50,000,000	Base giuridica insufficiente per l'elaborazione dei dati
H&M Hennes & Mauritz Online Shop A.B. & Co. KG	GERMANIA	35,258,708	Base giuridica insufficiente per l'elaborazione dei dati
TIM (operatore di telecomunicazioni)	ITALIA	27,800,000	Base giuridica insufficiente per l'elaborazione dei dati
BRITISH AIRWAYS	REGNO UNITO	22,046,000	Misure tecniche e organizzative insufficienti per garantire la sicurezza delle informazioni
Marriott International, Inc	REGNO UNITO	20,450,000	Misure tecniche e organizzative insufficienti per garantire la sicurezza delle informazioni

NUCLEO SPECIALE TUTELA PRIVACY E FRODI TECNOLOGICHE



NUCLEO SPECIALE TUTELA PRIVACY E FRODI TECNOLOGICHE

"Le tecniche di sicurezza informatica sono parte integrante per soddisfare gli obblighi di protezione dei dati e consentono agli utenti di godere appieno dei loro diritti fondamentali alla protezione dei dati personali e alla privacy".

GRAZIE PER L'ATTENZIONE