CYBER ACT FORUM 2021

La tutela e protezione dei dati personali: ruolo della Guardia di Finanza

Viterbo, 1 ottobre 2021

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

GRUPPO PRIVACY

- Gestione dei rapporti con l'Autorità Garante
- Sviluppo di attività progettuali in sinergia con i Reparti territoriali del Corpo
- Esecuzione di ispezioni su delega dell'Autorità Garante
- Partecipazione ad ispezioni congiunte con l'Autorità Garante nonché con le Autorità di controllo di altri Stati membri (art. 62 GDPR)
- Reperimento di dati e informazioni da segnalare all'Autorità

LA CONSAPEVOLEZZA E L'OPPORTUNITA'

GDPR: ART. 1 – 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

ARTICOLO 58 COMMA 1 GDPR

a) ingiungere al titolare del trattamento e al responsabile del trattamento e, ove applicabile, al rappresentante del titolare del trattamento o del responsabile del trattamento, di fornirle ogni informazione di cui necessiti per l'esecuzione dei suoi compiti

e) ottenere, dal titolare del trattamento o dal responsabile del trattamento, l'accesso a tutti i dati personali e a tutte le informazioni necessarie per l'esecuzione dei suoi compiti

ARTICOLO 157 CODICE PRIVACY

Nell'ambito dei poteri di cui all'articolo 58 del Regolamento, e per l'espletamento dei propri compiti, il Garante puo' richiedere al titolare, al responsabile, al rappresentante del titolare o del responsabile, all'interessato o anche a terzi di fornire informazioni e di esibire documenti anche con riferimento al contenuto di banche di dati.

ARTICOLO 158 CODICE PRIVACY

1. Il Garante puo' disporre accessi a banche di dati, archivi o altre ispezioni e verifiche nei luoghi ove si svolge il trattamento o nei quali occorre effettuare rilevazioni comunque utili al controllo del rispetto della disciplina in materia di trattamento dei dati personali.

2. I controlli di cui al comma 1, nonche' quelli effettuati ai sensi dell'articolo 62 del Regolamento, sono eseguiti da personale dell'Ufficio, con la partecipazione, se del caso, di componenti o personale di autorita' di controllo di altri Stati membri dell'Unione europea.

3. Il Garante si avvale anche, ove necessario, della collaborazione di altri organi dello Stato per lo svolgimento dei suoi compiti istituzionali.

4. Gli accertamenti di cui ai commi 1 e 2, se svolti in un'abitazione o in un altro luogo di privata dimora o nelle relative appartenenze, sono effettuati con l'assenso informato del titolare o del responsabile, oppure previa autorizzazione del presidente del tribunale competente per territorio in relazione al luogo dell'accertamento, il quale provvede con decreto motivato senza ritardo, al piu' tardi entro tre giorni dal ricevimento della richiesta del Garante quando e' documentata l'indifferibilità dell'accertamento.

NUCLEO SPECIALE TUTELA PRIVACY E FRODI TECNOLOGICHE

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

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

SICUREZZA NAZIONALE

ATTIVITA' ISPETTIVA (1)

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

DIPARTIMENTO ATTIVITA' ISPETTIVE

Prot. n.

Roma,

S.r.l.

P.I.

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 attraverso il rilascio di "*fidelity card*", 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) presupposti di liceità del trattamento dei dati personali per il rilascio della "*fidelity card*";
4) modalità con la quale viene fornita agli interessati l'informativa di cui agli art. 13 e 14 del *Rgdp* acquisendo copia della relativa documentazione;
5) 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;
6) eventuale istituzione del registro dei trattamenti mettendone a disposizione copia dello stesso (art. 30 *Rgdp*);
7) eventuale designazione di responsabili esterni (e/o *sub* responsabili) del trattamento con acquisizione del relativo contratto e designazione (art. 28 del *Rgdp*);

ATTIVITA' ISPETTIVA (2)

8) eventuale nomina del DPO in relazione agli artt. 37 e segg. del *Rgdp*;
9) 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*);
10) 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;
11) eventuale utilizzo a fini di profilazione di dati particolari dell'interessato (art. 9 *Rgdp*);
12) tipologia di attività di *marketing* effettuato a seguito della profilazione;
13) numero totale dei soggetti a cui è stata rilasciata la *fidelity card*;
14) il periodo di conservazione dei dati di profilazione personali ovvero i criteri utilizzati per determinare tale periodo;
15) 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;
16) 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;
17) procedure poste in essere per l'esercizio dei diritti degli interessati (artt. 15 a 22 del *Rgdp*);

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

18) 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)

19) eventuali certificazioni (art. 42 del Regolamento).

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).

La presente copia è conforme all'originale
e si compone di n. 2 facciate
Roma, ...

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

DIPARTIMENTO ATTIVITÀ ISPETTIVE E SANZIONI
IL DIRIGENTE

IL SEGRETARIO GENERALE
Avv.

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.

REGOLAMENTO UE 2016/679

ART. 83 – CONDIZIONI GENERALI PER INFLIGGERE SANZIONI AMMINISTRATIVE PECUNIARIE

LE SANZIONI AMMINISTRATIVE PECUNIARIE DEVONO ESSERE:

-EFFETTIVE

-PROPORZIONATE

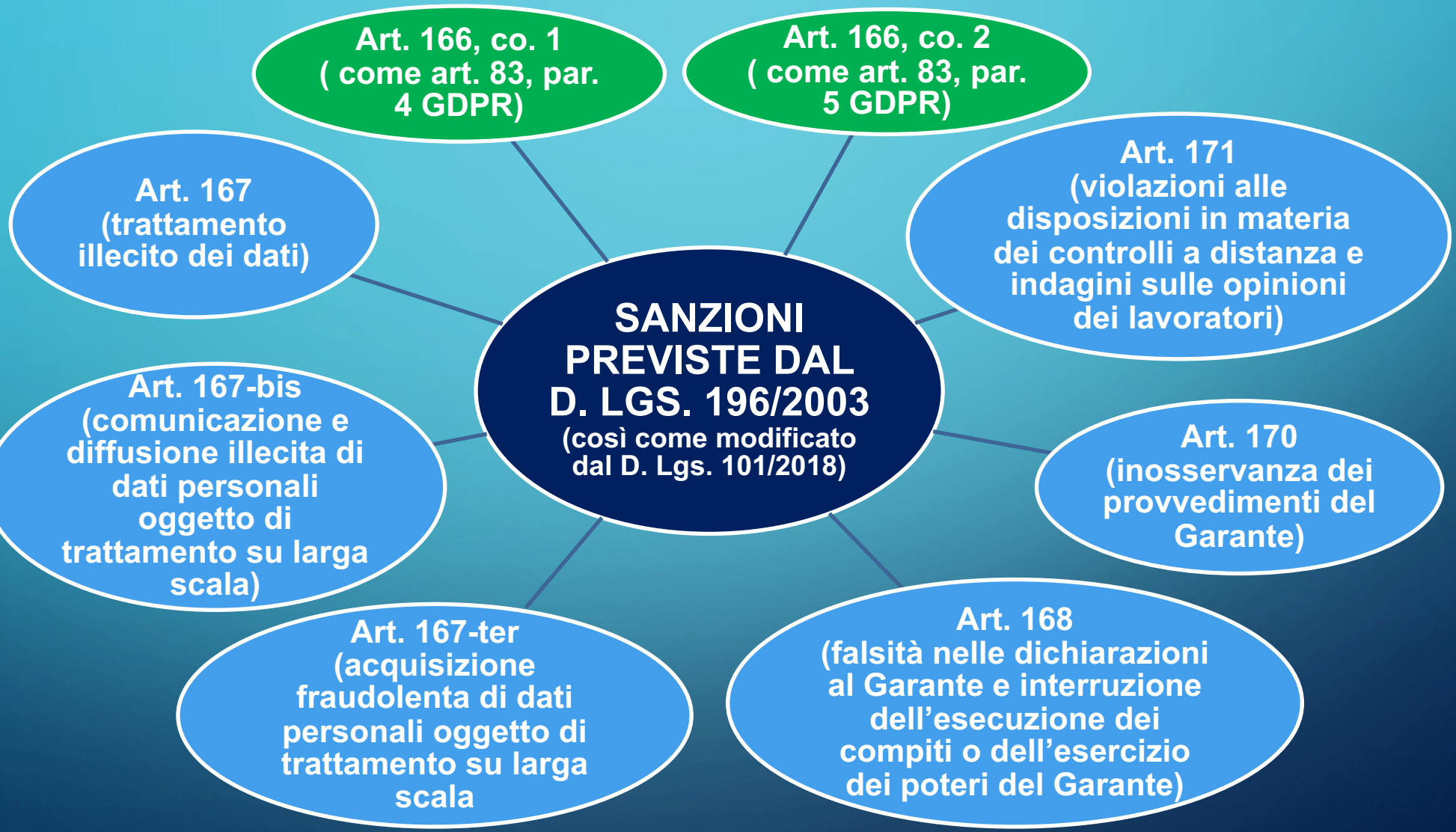
-DISSUASIVE.

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	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
WIND TRE S.P.A.	ITALIA	16,700,000	Base giuridica insufficiente per l'elaborazione dei dati
Vodafone Italia S.p.A.	ITALIA	12,251,601	Mancato rispetto dei principi generali in materia di trattamento dei dati
notebooksbilliger.de	GERMANIA	10,400,000	Base giuridica insufficiente per l'elaborazione dei dati

FONTE: https://www.enforcementtracker.com/

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".

CYBER ACT FORUM 2021

GRAZIE PER L'ATTENZIONE