Scuola Internazionale
Etica&Sicurezza
Milano - L'Aquila

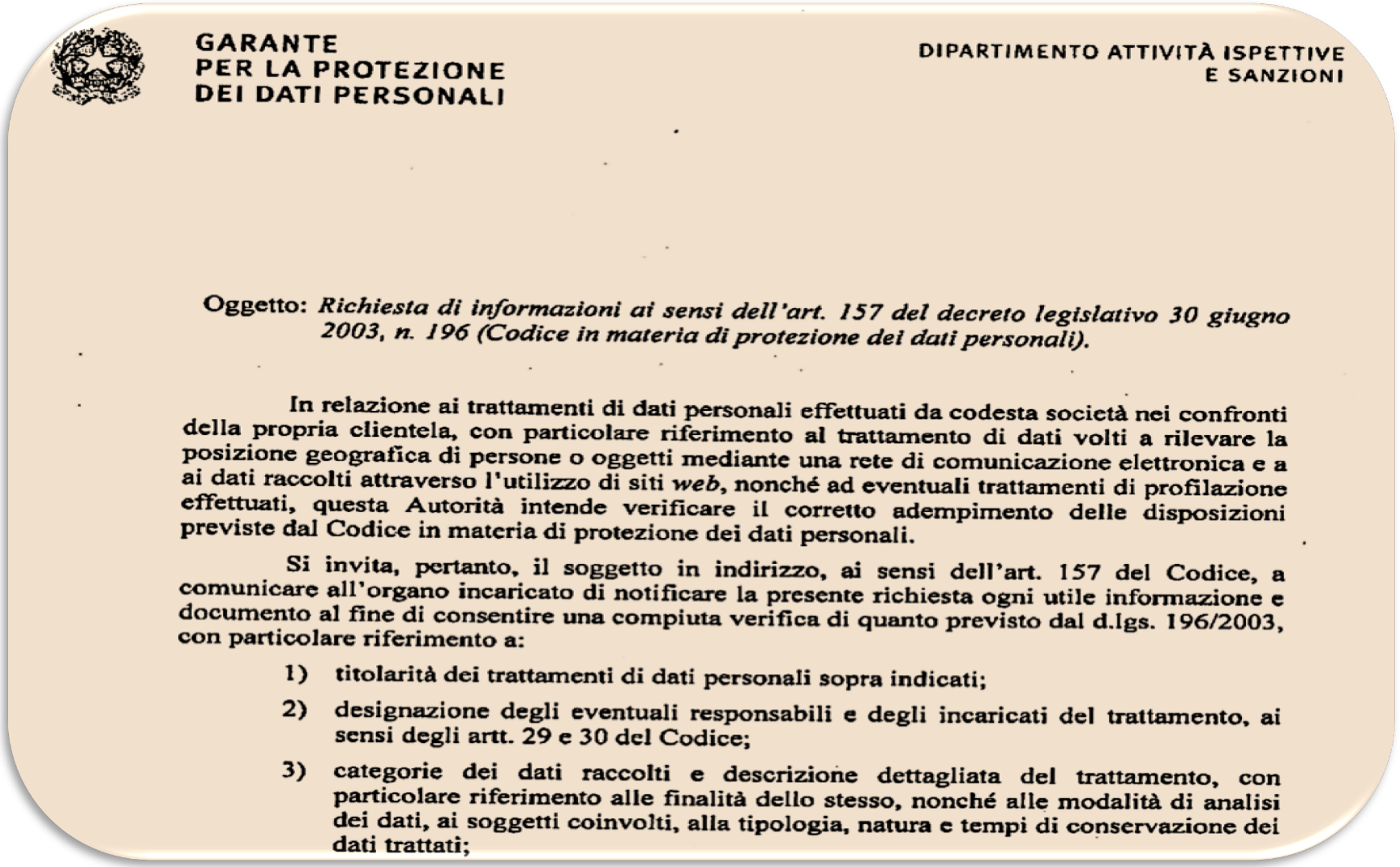
I RUOLI E LE RESPONSABILITA' CONNESSE AL TRATTAMENTO DEI DATI

Dott. Marco Menegazzo

Scuola Internazionale
Etica&Sicurezza
Milano - L'Aquila

ARGOMENTI:

RICHIESTA DI INFORMAZIONI:



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

DIPARTIMENTO ATTIVITÀ ISPETTIVE
E SANZIONI

Oggetto: *Richiesta di informazioni ai sensi dell'art. 157 del decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali).*

In relazione ai trattamenti di dati personali effettuati da codesta società nei confronti della propria clientela, con particolare riferimento al trattamento di dati volti a rilevare la posizione geografica di persone o oggetti mediante una rete di comunicazione elettronica e a ai dati raccolti attraverso l'utilizzo di siti *web*, nonché ad eventuali trattamenti di profilazione effettuati, questa Autorità intende verificare il corretto adempimento delle disposizioni previste dal Codice in materia di protezione dei dati personali.

Si invita, pertanto, il soggetto in indirizzo, ai sensi dell'art. 157 del Codice, a comunicare all'organo incaricato di notificare la presente richiesta ogni utile informazione e documento al fine di consentire una compiuta verifica di quanto previsto dal d.lgs. 196/2003, con particolare riferimento a:

1) titolarità dei trattamenti di dati personali sopra indicati;
2) designazione degli eventuali responsabili e degli incaricati del trattamento, ai sensi degli artt. 29 e 30 del Codice;
3) categorie dei dati raccolti e descrizione dettagliata del trattamento, con particolare riferimento alle finalità dello stesso, nonché alle modalità di analisi dei dati, ai soggetti coinvolti, alla tipologia, natura e tempi di conservazione dei dati trattati;

RICHIESTA DI INFORMAZIONI:

4) in particolare, nel caso del trattamento di dati che rilevino la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica (ad esempio, tramite localizzatori installati sui veicoli o tramite "*app*" per *smartphone*), descrizione dettagliata del trattamento effettuato e delle modalità con le quali si è dato adempimento a quanto disposto dal Codice in ordine all'obbligo di notificazione del trattamento, di cui all'art. 37 del Codice;

5) in particolare, nel caso di profilazione degli interessati, descrizione dettagliata del trattamento, dei dati raccolti e delle finalità, nonché dell'eventuale notificazione dello stesso ai sensi dell'art. 37 del Codice;

6) modalità con le quali si è dato adempimento a quanto disposto dal Codice in ordine all'obbligo di informativa, di cui all'art. 13, ed alla raccolta del consenso, di cui all'art. 23 del Codice;

7) misure di sicurezza, previste dagli artt. 33 e ss. del Codice e dal disciplinare tecnico di cui all'allegato B) del medesimo Codice, in concreto adottate;

8) presupposti, ambito e modalità di eventuale comunicazioni a terzi dei dati, anche in riferimento ad eventuali società controllanti, controllate o collegate ed

Piazza di Monte Citorio, 121 - 00186 Roma
Tel. +39 06 696772794 - Fax +39 06 69677385
www.garanteprivacy.it
E-mail: dais@gpdp.it
Posta certificata: dais@pec.gpdp.it

RICHIESTA DI INFORMAZIONI:

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

all'eventuale trasferimento dei dati in paesi non appartenenti all'Unione europea.

Inoltre, con riferimento ai trattamenti di dati personali eventualmente raccolti attraverso l'utilizzo del sito internet indicato in allegato (ove presente), nonché di altri eventuali siti *web* utilizzati, specificare:

9) titolarità dei trattamenti di dati personali;

10) finalità del trattamento e descrizione delle modalità dello stesso;

11) designazione degli eventuali responsabili e degli incaricati del trattamento ai sensi degli artt. 29 e 30 del Codice;

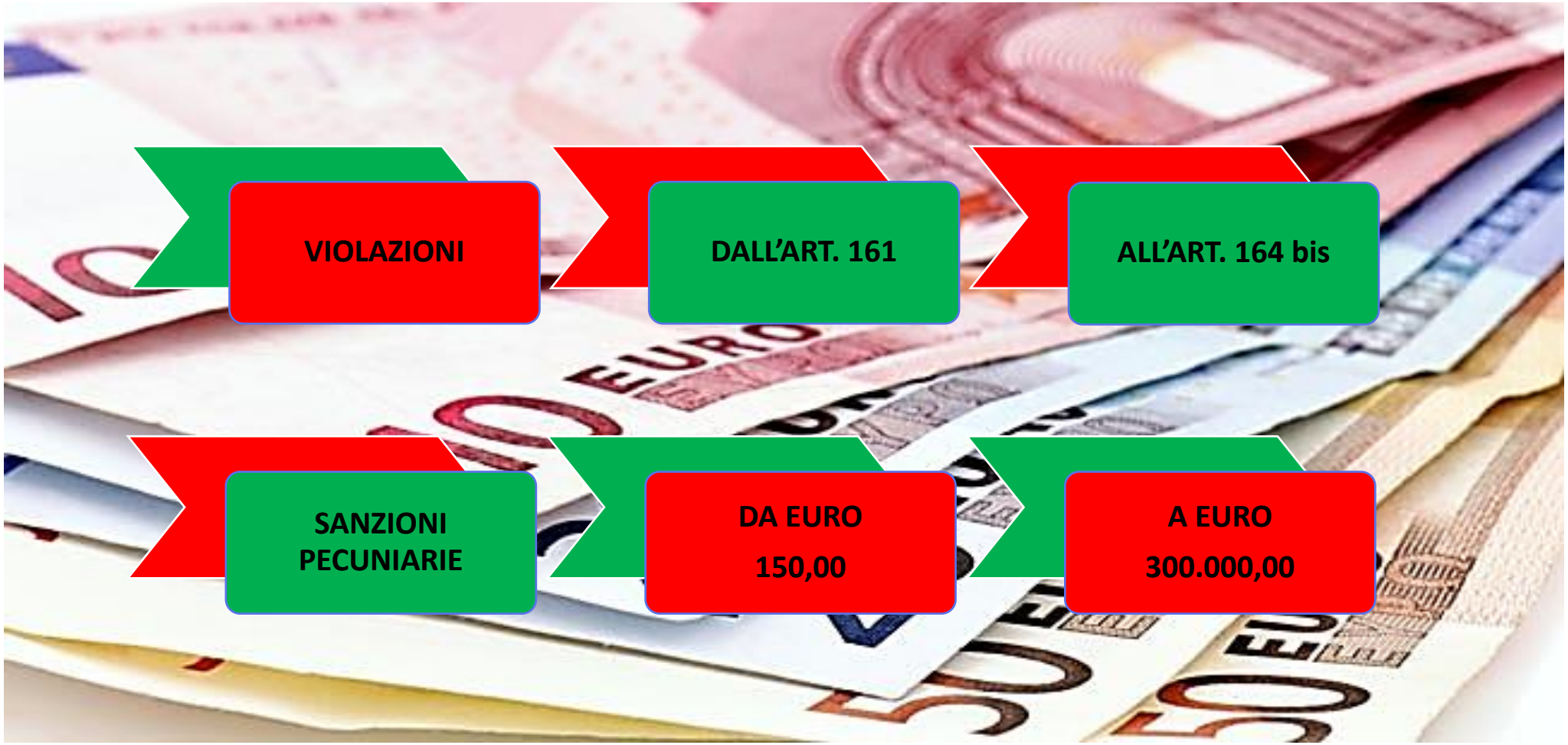
12) tipologia, natura e tempi di conservazione dei dati trattati;

13) modalità con le quali si è dato adempimento a quanto disposto dal Codice in ordine all'obbligo di informativa, di cui all'art. 13, ed alla eventuale raccolta del consenso, di cui all'art. 23, ove previsto.

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, dovrà essere applicata la sanzione amministrativa pecuniaria prevista dall'art. 164 del d.lgs. n. 196/2003.

D.LGS. 196/2003:



LEGGE 689/81 - ART. 11:

CRITERI PER L'APPLICAZIONE DELLE SANZIONI AMMINISTRATIVE PECUNIARIE

NELLA DETERMINAZIONE DELLA SANZIONE AMMINISTRATIVA PECUNIARIA FISSATA DALLA LEGGE TRA UN LIMITE MINIMO ED UN LIMITE MASSIMO E NELL'APPLICAZIONE DELLE SANZIONI ACCESSORIE FACOLTATIVE, SI HA RIGUARDO ALLA:

- **GRAVITÀ DELLA VIOLAZIONE;**
- **OPERA SVOLTA DALL'AGENTE PER LA ELIMINAZIONE O ATTENUAZIONE DELLE CONSEGUENZE DELLA VIOLAZIONE;**
- **PERSONALITÀ DELLO STESSO;**
- **CONDIZIONI ECONOMICHE.**

REGOLAMENTO (UE) 2016/679:

REGOLAMENTO (UE) 2016/679:

ASPETTI TECNICI

IL REGOLAMENTO

- Pubblicato nella Gazzetta Ufficiale dell'Unione Europea il **4 Maggio 2016**.
- Entrato in vigore il ventesimo giorno successivo alla pubblicazione nella Gazzetta Ufficiale.

  (**25 Maggio 2016**).
- Applicabile **a decorrere dal 25 Maggio 2018.**

REGOLAMENTO (UE) 2016/679:

LINEE GUIDA GRUPPO ART. 29 - APPROVATE

Sul diritto alla portabilità dei dati Wp 242	**Sul RPD Wp 243**	**Sull'autorità capofila Wp 244**
Valutazione d'impatto e trattamento considerato ad alto rischio Wp 248	**Sulla notificazione dei data breach Wp 250**	**Processo decisionale automatizzato e profilazione Wp 251**
Sui criteri per l'applicazione delle sanzioni Wp 253	**Sul consenso Wp 259**	**Sulla trasparenza del trattamento Wp 260**

REGOLAMENTO (UE) 2016/679:

EDPB

COMITATO EUROPEO PER LA PROTEZIONE DEI DATI

In consultazione

Sull'accreditamento degli enti di certificazione (Guidelines 1/2018)

Approvato

Sul trasferimento dei dati all'estero (Guidelines 2/2018)

AMBITO DEI POTERI DELLE AUTORITA':

I compiti delle autorità, sul proprio territorio, sono indicati dall'art. 57 del Regolamento e prevedono attività estremamente ramificate e diversificate che pongono, in una fase iniziale, l'autorità fianco a fianco con i titolari del trattamento e dei responsabili

All'autorità di controllo sono conferiti poteri di indagine, correttivi, autorizzativi e consultivi, nonché il potere di infliggere sanzioni amministrative pecuniarie.

AMBITO DEI POTERI DELLE AUTORITA':

Di detti poteri si occupa l'art. 58 del Regolamento fornendo una elencazione degli stessi e ripartendoli in:

- poteri di indagine (art. 58, co.1) anche in collaborazione della Guardia di Finanza;
- poteri correttivi, rivolgere avvertimenti, ammonimenti, imporre limitazioni e infliggere sanzioni (art. 58, co.2);
- poteri autorizzativi e consultivi (art. 58, co.3).

REGOLAMENTO (UE) 2016/679:

IL TITOLARE DEL TRATTAMENTO E':

COMPETENTE PER IL RISPETTO DEI PRINCIPI APPLICABILI AL TRATTAMENTO DI DATI PERSONALI

IN GRADO DI COMPROVARLO (RESPONSABILIZZAZIONE)

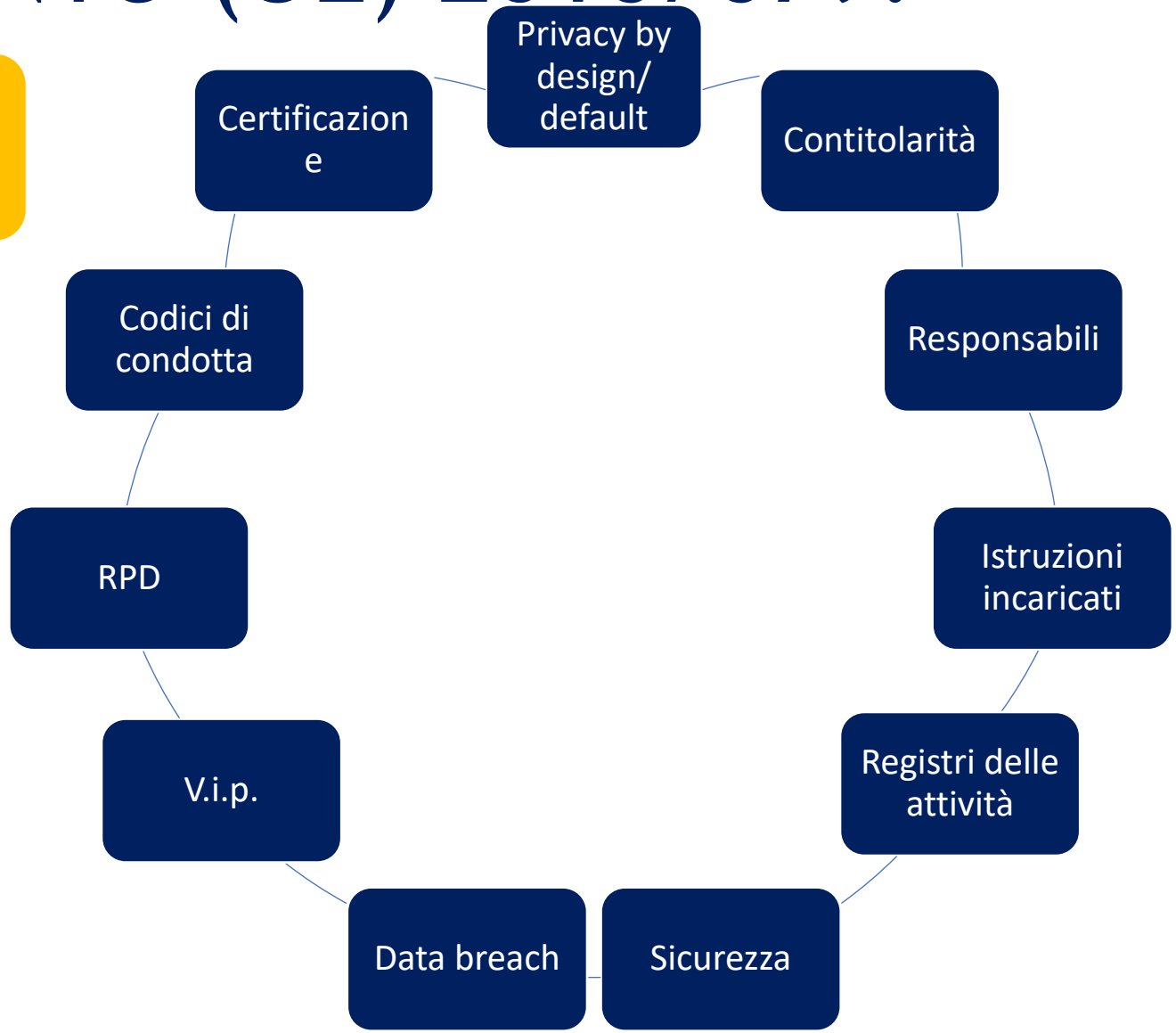
Concetto chiave!

Dimostrare: provare una verità con un ragionamento logico o con prove di fatto

REGOLAMENTO (UE) 2016/679:

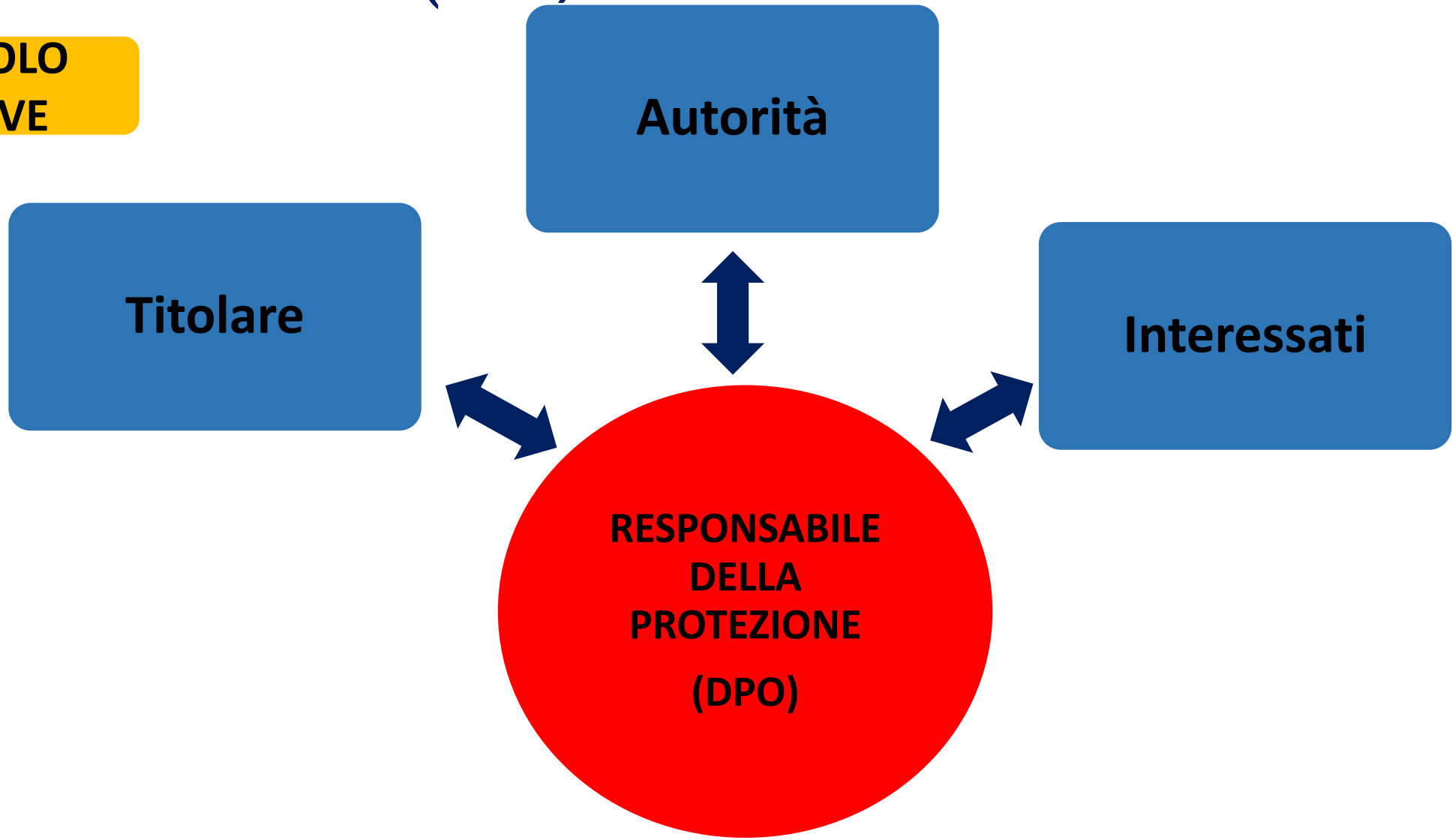
REGOLAMENTO (UE) 2016/679:

L'IMPORTANZA DI UN METODO



REGOLAMENTO (UE) 2016/679:

IL RUOLO CHIAVE



SANZIONI:

ART. 83 – CONDIZIONI GENERALI PER INFLIGGERE SANZIONI AMMINISTRATIVE PECUNIARIE

Le sanzioni amministrative pecuniarie devono essere:

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

SANZIONI:

Al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa si tiene conto di:

- **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;**

SANZIONI:

Al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa si tiene conto di:

- 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;

SANZIONI:

Al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa si tiene conto di:

- 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;

SANZIONI:

Al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa si tiene conto di:

- j) l'adesione ai codici di condotta approvati ai sensi dell'articolo 40 o ai meccanismi di certificazione approvati ai sensi dell'articolo 42;
- 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:

In conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 10.000.000 EUR, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:

- **a) gli obblighi del titolare del trattamento e del responsabile del trattamento a norma degli articoli 8, 11, da 25 a 39, 42 e 43;**
- **b) gli obblighi dell'organismo di certificazione a norma degli articoli 42 e 43;**
- **c) gli obblighi dell'organismo di controllo a norma dell'articolo 41, paragrafo 4;**

SANZIONI:

In conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 20.000.000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:

- **a) i principi di base del trattamento, comprese le condizioni relative al consenso, a norma degli articoli 5, 6, 7 e 9;**
- **b) i diritti degli interessati a norma degli articoli da 12 a 22;**
- **c) i trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale a norma degli articoli da 44 a 49;**
- **d) qualsiasi obbligo ai sensi delle legislazioni degli Stati membri adottate a norma del capo IX;**
- **e) 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 ai sensi dell'articolo 58, paragrafo 2, o il negato accesso in violazione dell'articolo 58, paragrafo 1.**

SANZIONI:

D.LGS. Approvato CDM il 21 marzo 2018 – Atto governo n. 22 - Art. 167 (Trattamento illecito dei dati)

1. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto, operando in violazione di quanto disposto dagli articoli 123, 126 e 13.0 o dal provvedimento di cui all'articolo 129 arreca nocumento all'interessato, è punito con la reclusione da sei mesi a un anno e sei mesi.

2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto, procedendo al trattamento dei dati personali di cui agli articoli 9 e IO del Regolamento in violazione delle disposizioni di cui agli articoli 2-sexiea e 2-octies, o delle misure di ·garanzia ad esso relative ovvero operando in violazione delle misure adottate ai sensi dell'articolo 2-quaterdecies arreca nocumento all'interessato, è punito con la reclusione da uno a tre anni.

SANZIONI:

D.LGS. Approvato CDM il 21 marzo 2018 – Atto governo n. 22 - Art. 167 (Trattamento illecito dei dati)

3. Salvo che il fatto costituisca più grave reato, la pena di cui al comma 2 si applica altresì a chiunque, al fine di trarre per sé o per altri profitto, procedendo al trasferimento dei dati personali verso un paese terzo o un'organizzazione internazionale al di fuori dei casi consentiti ai sensi degli articoli 45,46 o 49 del Regolamento, arreca nocumento all'interessato.

4. Il Pubblico Ministero, quando ha notizia dei reati di cui ai commi l, 2 e 3, ne informa senza ritardo il Garante.

SANZIONI:

D.LGS. Approvato CDM il 21 marzo 2018 – Atto governo n. 22 - Art. 167 (Trattamento illecito dei dati)

5. Il Garante trasmette al Pubblico Ministero, con una relazione motivata, la documentazione raccolta nello svolgimento dell'attività di accertamento nel caso in cui emergano elementi che facciano presumere la esistenza di un reato. La trasmissione degli atti al pubblico ministero avviene al più tardi al termine dell'attività di accertamento delle violazioni delle disposizioni di cui al presente decreto.

6. Quando per lo stesso fatto è stata applicata a norma del presente codice o del Regolamento a carico dell'imputato o dell'ente una sanzione amministrativa pecuniaria dal Galante e questa è stata riscossa, la pena è diminuita.

SANZIONI:

D.LGS. Approvato CDM il 21 marzo 2018 - Atto governo n. 22 - Art. 167-bis
(Comunicazione e diffusione illecita di dati personali riferibili a un rilevante numero di persone)

1. Salvo che il fatto costituisca più grave reato, il titolare o il responsabile del trattamento o la persona designata a norma dell'articolo 2-terdecies che comunica o diffonde, al fine di trarre profitto per sé o altri, dati personali riferibili ad un rilevante numero di persone, in violazione degli articoli 2-ter, 2-sexies e 2-octies, è punito con la reclusione da uno a sei anni.

2. Salvo che il fatto costituisca più grave reato, il titolare o il responsabile del trattamento o la persona designata a norma dell'articolo 2-terdecfes che, al fine trame profitto per sé o altri, comunica o diffonde senza consenso dati personali riferibili a un rilevante numero di persone, è punito con la reclusione da uno a sei anni, quando il consenso dell'interessato è richiesto per le operazioni di comunicazione e di diffusione.

3. Per i reati di cui ai commi l e 2, si applicano i commi 4, 5 e 6 dell'articolo 167.

SANZIONI:

D.LGS. Approvato CDM il 21 marzo 2018 - Atto governo n. 22 -
Art. 167-ter
(Acquisizione fraudolenta di dati personali)

1. Salvo che il fatto costituisca più grave reato, chiunque, al fine trame profitto per sé o altri, acquisisce con mezzi fraudolenti dati personali riferibili a un numero rilevante di persone è punito con la reclusione da uno a quattro anni.

2. Per il reato di cui al comma l si applicano i commi 4, 5 e 6 dell'articolo 167."

SANZIONI:

RISARCIMENTO DEL DANNO

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

…….6. Le azioni legali per l'esercizio del diritto di ottenere il risarcimento del danno sono promosse dinanzi alle autorità giurisdizionali competenti a norma del diritto dello Stato membro di cui all'articolo 79, paragrafo 2.

REGOLAMENTO (UE) 2016/679:

L'aver attuato e verificato le misure influisce sul grado di responsabilità del titolare o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto.

Linee guida Garanti Europei sull'applicazione delle sanzioni amministrative del 03/10/2017 WP253

Il titolare del trattamento ha implementato misure tecniche per implementare il principio di protezione by design o by default (art.25)

Il titolare del trattamento ha implementato misure organizzative per implementare il principio di protezione by design o by default in tutti gli ambiti dell'organizzazione (25)

Il titolare o il responsabile del trattamento hanno implementato un appropriato livello di sicurezza dei dati (art.32)

Le procedure interne sul trattamento dei dati personali (policies/istruzioni) erano conosciute e applicate nell'ambito dell'organizzazione (art.24)

REGOLAMENTO (UE) 2016/679:

74 Lettere

Ministri

Presidenti di autorità indipendenti

Presidenti CSM, Corte dei Conti, Avvocatura dello Stato, Enti centrali e Agenzie

Presidenti di regioni, Conferenza Stato regione,, Conferenza Stato città, Upi e Anci

24 MAGGIO 2017

Priorità:

- RPD
- Registro
- Data Breach

GRAZIE PER L'ATTENZIONE