I DIRITTI dell'interessato: altrettanti OBBLIGHI per il titolare del trattamento

PADOVA, 3 MAGGIO 2018 — CAMERA DI COMMERCIO

I diritti dell'interessato

L'INTERESSATO AL CENTRO DELLA DISCIPLINA

Chi è l'interessato?

È la persona fisica, *identificata* o *identificabile*, a cui si riferiscono i dati personali oggetto di un trattamento.

- Ricordiamo che:
  - il diritto alla protezione dei personali è un diritto fondamentale riconosciuto dalla CEDU, dalla Carta e dal TFUE…
  - … e che *il trattamento dei dati personali dovrebbe essere al servizio dell'uomo*.
  - Il RGPD, per assicurare un'efficace protezione dei d.p. in tutta l'Ue, ha imposto il *rafforzamento* e la disciplina dettagliata dei diritti degli interessati, con i corrispondenti obblighi di coloro che effettuano e determinano il trattamento dei dati personali.

La «identificabilità»

si considera identificabile la persona fisica che può essere identificata, direttamente o *indirettamente*;

- con particolare riferimento a un identificativo
  - come il nome,
  - un numero di identificazione,
  - dati relativi all'ubicazione,
  - un identificativo online
- o a uno o più elementi caratteristici
  - della sua identità fisica, fisiologica,
  - genetica, psichica,
  - economica, culturale o sociale.

Sono tutti dati personali

«Identificazione digitale» dell'interessato

L'identificazione dovrebbe includere l'identificazione digitale di un interessato, ad esempio

mediante un meccanismo di autenticazione

quali le stesse credenziali, utilizzate dall'interessato per l'accesso (*log in*) al servizio on line offerto dal titolare del trattamento.

Dati riferiti alle «persone decedute»

Il regolamento non si applica ai dati personali delle *persone decedute*; nemmeno nel caso di tr. per finalità di archiviazione, di ricerca storica o di ricerca a fini genealogici.

Gli Stati membri possono prevedere norme riguardanti il trattamento dei dati personali delle persone decedute:

- Per es., l'art. 9,3 del Codice della privacy prevede *(va)* che i diritti dell'interessato (art. 7) «*riferiti a dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione*».

• I tre pilastri della protezione dei dati personali

PRINCIPI DI BASE, DIRITTI DELL'INTERESSATO E OBBLIGHI DEL TITOLARE

Struttura di protezione dei dati personali

PRINCIPI DI BASE DEL TR.

- Liceità, correttezza e trasparenza
- Limitazione della finalità del tr.
- Minimizzazione dei dati
- Esattezza dei dati
- Limitazione della conservazione
- Integrità dei d.p. e riservatezza
- Responsabilizzazione (*Accountability*)

(Artt. 5 e 6)

DIRITTI DELL'INTERESSATO

- Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato (Artt. 12, 13, 14)
- Diritto di accesso (Art. 15)
- Diritto di rettifica (Art. 16)
- Diritto alla cancellazione («diritto all'oblio») (Art. 17)
- Diritto di limitazione del tr. (Art. 18)
- Diritto alla portabilità dei dati (Art. 20)
- Diritto di opposizione (Art. 21)

OBBLIGHI DEL TDTR / RDTR

- Garantire il rispetto dei principi
- Soddisfare i diritti dell'interessato
- *Accountability* (Art. 24)
- Privacy *by design* …
- …e *by default* (Art. 24)
- Informativa e consenso
- Registri delle attività di tr.
- Sicurezza dei dati
- Valutazione d'impatto sulla protezione
- Nomina del DPO

I «dati personali»

Qualsiasi informazione può essere ritenuta un dato personale, *a condizione che si riferisca a una persona fisica* (non deceduta, identificabile).

- I dati personali riguardano le informazioni sulla vita privata di una persona
- nonché quelle sulla sua vita professionale o pubblica.

I dati riguardano le persone anche quando sono rivelati indirettamente dal contenuto delle informazioni su tale persona.

I «dati personali»

La forma in cui i dati personali sono conservati o utilizzati non è rilevante:

comunicazioni scritte o orali possono contenere dati personali e lo stesso vale per le immagini, compresi i filmati o i suoni rilevati da impianti televisivi a circuito chiuso (CCTV);

informazioni registrate elettronicamente, come anche le informazioni in formato cartaceo, possono costituire dati personali;

i campioni cellulari di tessuti umani possono costituire dati personali, dal momento che contengono il DNA di una persona.

Dati che richiedono una «speciale protezione»

- Dati personali che rientrano in «*categorie particolari*» (Art. 9, 1)
  - I dati genetici / biometrici / relativi alla salute / alla vita sessuale / all'orientamento sessuale (Art. 9, 2)
- I dati personali relativi a condanne penali e ai reati o a misure di sicurezza (Art. 10)

Il RGPD (Art. 9,1) pone *in via generale*

il <u>divieto</u> di trattare queste tipologie di d.p.

<u>se non a specifiche condizioni</u>

Il trattamento di essi comporta **rischi <u>significativi</u> per i diritti e le libertà fondamentali**:

- il loro utilizzo può condurre a **effetti discriminatori** sulle persone;
- rendono particolarmente pervasiva un'eventuale **profilazione**;
- richiedono un particolare **livello di sicurezza**.

Dati che richiedono una «speciale protezione»

- Dati personali
  «*categ*
  - I d
    all

i dati personali che rivelano

- ✓ l'origine razziale o etnica,
- ✓ le opinioni politiche,
- ✓ le convinzioni religiose o filosofiche,
- ✓ o l'appartenenza sindacale, nonché
- ✓ dati genetici, biometrici, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale

ndizioni

S

I

- rendono pa
- richiedono un particolare **livello di sicurezz**

Dati che richiedono una «speciale protezione»

- Dati per
«*cate*
  - I d

un particolare livello di sicurezza contro pericoli, tra l'altro, di:

- ✓ di un danno fisico, materiale o immateriale,
- ✓ furto o usurpazione d'identità,
- ✓ pregiudizio alla reputazione,
- ✓ perdita di riservatezza in caso di violazione del segreto professionale,
- ✓ pregiudizio ai diritti della persona,
- ✓ etc.

ndizioni

S

I

- rendono pa
- richiedono un particolare **livello di sicurezz**

Il «trattamento» dei dati personali

qualsiasi operazione o **insieme di operazioni**
con o *senza* l'ausilio di processi automatizzati
e **applicate a dati personali** o insiemi di dati personali

Esempi tipici di «operazioni» di trattamento →

- la raccolta,
- la registrazione,
- l'organizzazione,
- la strutturazione,
- la conservazione,
- l'adattamento o la modifica,
- l'estrazione,
- la consultazione,
- l'uso
- la comunicazione, o diffusione
- o qualsiasi altra forma di messa a disposizione,
- il raffronto o l'interconnessione,
- la limitazione,
- la cancellazione o la distruzione

I principi di base

IL TRATTAMENTO DEI DATI PERSONALI DOVREBBE ESSERE AL SERVIZIO DELL'UOMO

I principi «di base» stabiliti dal RGPD

Liceità, correttezza e trasparenza	Art. 5,1,a; art. 6
Condizioni per il consenso	Artt. 7 e 8
Trattamenti di categorie particolari di d.p.	Art. 9
Trattamento di d.p. relativi a condanne penali e reati	Art. 10
Trattamento che non richiede l'identificazione	Art. 11
Limitazione della finalità	Art. 5,1,b
Minimizzazione dei dati	Art. 5,1,c
Esattezza	Art. 5,1,d
Limitazione della conservazione	Art. 5,1,e
Integrità e riservatezza	Art. 5,1,f
Responsabilizzazione (*accountability*)	Art. 5,2

Liceità del trattamento – condizioni

Quando è lecito il trattamento?

Il trattamento è lecito **solo se** *e* **nella misura in cui** ricorre ***almeno una*** delle seguenti **condizioni**:

Il che vuole dire, in pratica, che, *al di fuori di queste condizioni*, il trattamento NON è lecito…

La **prima**, fondamentale, è che **il trattamento è lecito se**

a) l'interessato **ha espresso il consenso** al trattamento dei propri dati personali per *una* o *più* specifiche finalità;

oppure …

Liceità del trattamento – condizioni

oppure … il **trattamento è lecito quando è necessario**:

b) all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;

c) per adempiere un obbligo legale (stabilito dal diritto Ue o dal diritto nazionale) al quale è soggetto il titolare del trattamento;

d) per la salvaguardia degli interessi vitali dell'interessato o *di un'altra persona* fisica;

e) per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri;

Liceità del trattamento – condizioni

…e, infine:

f) per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, *purché* – in questo caso:

> *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.

Non si applica al trattamento di dati effettuato dalle autorità pubbliche *nell'esecuzione dei loro compiti*.

La «trasparenza» del trattamento

Il principio della trasparenza richiede *che le persone fisiche conoscano le modalità* con cui sono raccolti, utilizzati, consultati o altrimenti trattati dati personali che li riguardano nonché *la misura in cui* i dati personali sono o saranno trattati. Esso impone, in generale:

- ✓ che le informazioni e le comunicazioni relative al trattamento dei dati personali siano facilmente accessibili e comprensibili
- ✓ e che sia utilizzato un linguaggio semplice e chiaro.
- ✓ […e] riguarda, in particolare, **l'informazione degli interessati**

Informativa all'interessato (artt. 12, 13, 14)

sull'identità del titolare del trattamento e sulle finalità del trattamento nonché ulteriori informazioni per assicurare un trattamento corretto e trasparente.

Le informazioni da fornire all'interessato

I principi di liceità, correttezza e, in particolare, di trasparenza si concretizzano pertanto nel **diritto dell'interessato** a ricevere (e nel corrispondente **obbligo** del TDTR di fornire) una serie considerevole di

Informazioni che sono funzionali:

- alla prestazione di un consenso libero e consapevole;
- alla conoscenza ed all'esercizio dei diritti riconosciuti all'interessato, *in primis* del diritto di accesso;
- alla conoscenza di rischi, norme e garanzie relativi al trattamento;
- in generale, al controllo sui propri dati personali.

Limitazione delle finalità

I dati personali devono essere raccolti per finalità

- determinate,
- esplicite
- e legittime,
- e successivamente trattati in modo che non sia incompatibile con tali finalità;

Non è considerato incompatibile con le finalità iniziali **un ulteriore trattamento** dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.

Minimizzazione dei dati

I dati personali devono essere:

adeguati,

pertinenti

e limitati a quanto necessario *rispetto alle finalità* per le quali sono trattati.

Da qui l'obbligo, in particolare, di assicurare che il periodo di conservazione dei dati personali sia limitato al minimo necessario.

… è uno dei contenuti della privacy *by design* e *by default* (art. 25)

Onde assicurare che i dati personali non siano conservati più a lungo del necessario, *il titolare del trattamento dovrebbe stabilire un termine per la cancellazione* o *per la verifica periodica*.

Esattezza dei dati

I dati personali devono essere:

- 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.

Onde assicurare che i dati personali non siano conservati più a lungo del necessario, *il titolare del trattamento dovrebbe stabilire un termine per la cancellazione* o *per la verifica periodica*.

Limitazione della conservazione

I dati personali **devono** essere:

- *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 i d.p.);

possono essere *conservati per periodi più lunghi* **a condizione che** siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici

e fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal regolamento a tutela dei diritti e delle libertà dell'interessato.

Integrità dei dati personali e riservatezza

I dati personali devono essere:

trattati in maniera da garantire un'adeguata sicurezza dei dati; compresa la protezione, mediante

misure tecniche *e* organizzative adeguate,

- da trattamenti non autorizzati o illeciti
- e dalla perdita,
- dalla distruzione
- o dal danno accidentali.

Responsabilizzazione del Titolare del trattamento

Il regolamento stabilisce la **responsabilità generale** del titolare (art. 24) del trattamento per qualsiasi trattamento di dati personali

che quest'ultimo abbia effettuato direttamente o che altri abbiano effettuato per suo conto.

Il titolare deve garantire il rispetto dei principi appena visti: di liceità, correttezza e trasparenza, limitazione delle finalità, minimizzazione, esattezza, limitazione della conservazione, integrità e riservatezza.

(accountability)

Trattamenti basati sul consenso

Quando la liceità del trattamento si basa sul consenso dell'interessato,

- il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso;
- il consenso espresso in una dichiarazione scritta, deve essere chiaramente distinguibile da altre questioni;
- deve essere liberamente prestato;
- Il consenso è sempre revocabile (eventuali **clausole limitative** della facoltà di revocare il consenso **non sono valide**).

I diritti dell'interessato

GARANTIRE LA SICUREZZA DEI DATI PERSONALI *TENENDO CONTO DEI RISCHI* PER GLI INTERESSI E I DIRITTI DELL'INTERESSATO

Capo III – Diritti dell'interessato

Art. 12 – Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato
Art. 13 – Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato
Art. 14 – Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato
Art. 15 – Diritto di accesso dell'interessato
Art. 16 – Diritto di rettifica
Art. 17 – Diritto alla cancellazione («diritto all'oblio»)
Art. 18 – Diritto di limitazione di trattamento
Art. 19 – Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento
Art. 20 – Diritto alla portabilità dei dati
Art. 21 – Diritto di opposizione
Art. 22 – Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione
Art. 23 – Limitazioni

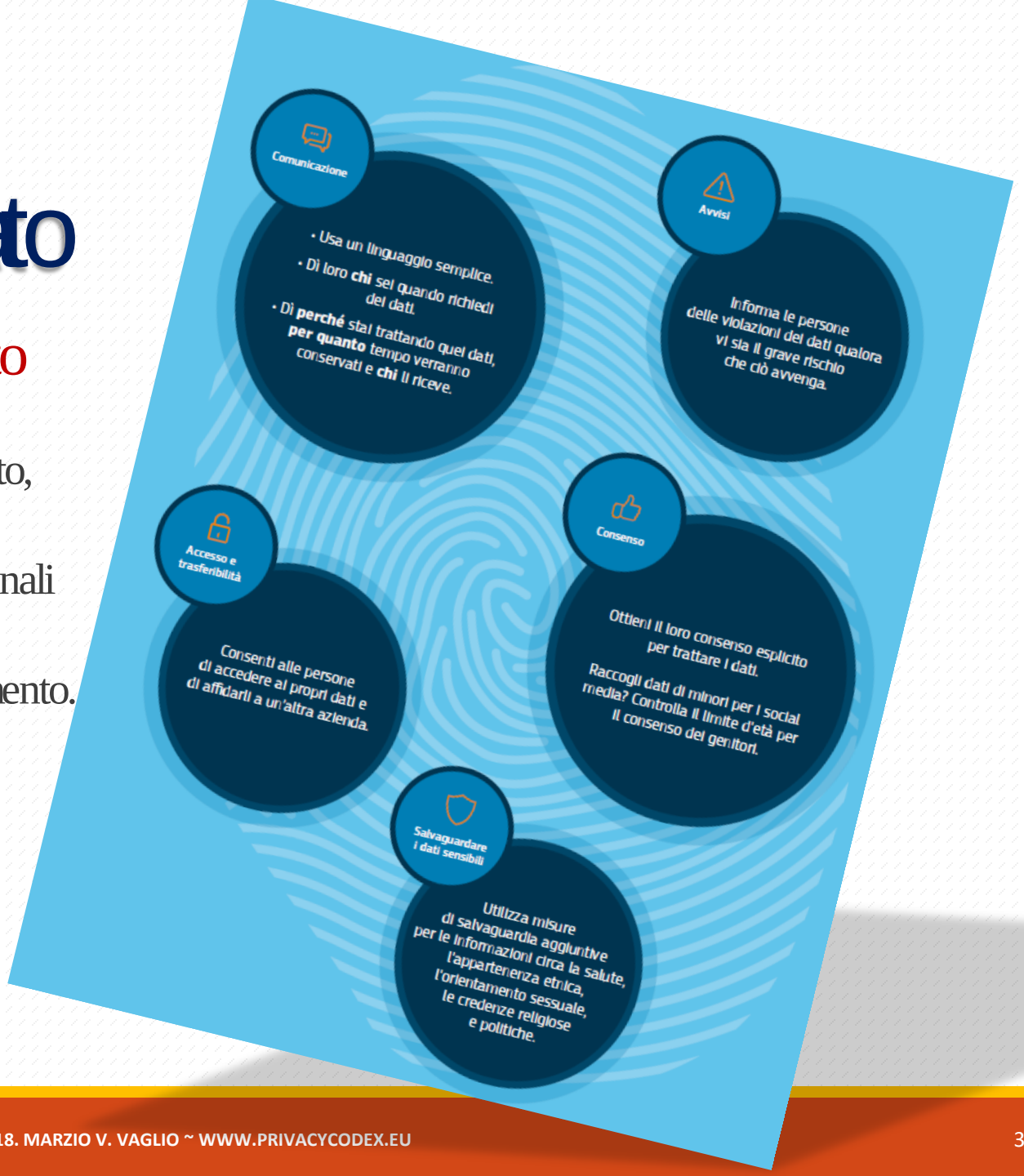
Diritti dell'interessato

Il regolamento ha rafforzato

- il diritto all'informazione
- ed alla trasparenza del trattamento,
- il diritto di accesso ai dati,
- il diritto di rettifica dei dati personali
- e il diritto alla limitazione
- nonché di opposizione al trattamento.

Ha anche codificato:

- Il diritto all'oblio
- il diritto alla portabilità dei dati.



Diritti dell'interessato

Il regolamento ha rafforzato

- il diritto all'informazione
- ed alla trasparenza del trattamento,
- il diritto di accesso ai dati,
- il diritto di rettifica dei dati personali
- e il diritto alla limitazione
- nonché di opposizione al trattamento.

Ha anche codificato:

- Il diritto all'oblio
- il diritto alla portabilità dei dati.

ISBN 978-92-79-65152-6 – doi:10.2838/9836 – DS-04-17-046-IT-N

Informazioni e comunicazioni all'interessato

Il **principio della trasparenza** si concretizza nel **diritto d'informazione** riconosciuto all'interessato dal RGPD.

Alla trasparenza e al diritto d'informazione il RGPD attribuisce *un valore nodale nella disciplina dei diritti e delle garanzie* che devono essere assicurate all'interessato.

Ciò si esprime anche nella *collocazione* di queste norme all'interno della struttura del regolamento: Capo III (*Diritti dell'interessato*), Sezione 1 (*Trasparenza e modalità*), Sezione 2 (*Informazione e accesso ai dati personali*).

Informazioni e comunicazioni all'interessato

- Al diritto di informazione corrisponde l'**obbligo** (art. 12,1), per il titolare del trattamento, **di adottare misure appropriate** per fornire all'interessato:
  - tutte le informazioni di cui agli articoli 13 e 14
  - e le comunicazioni di cui agli articoli da 15 a 22 e all'art. 34,

relative al trattamento.

- A ciò si aggiunge il più generale **obbligo** (art. 12,2) per il titolare **di agevolare l'esercizio dei diritti** dell'interessato (artt. 15-22).

Informazioni e comunicazioni all'interessato

- Dall'obbligo generale di *agevolare l'esercizio dei diritti dell'interessato* (artt. 15-22) discende

il **divieto** al TDTR **di rifiutarsi**

di soddisfare la richiesta dell'interessato al fine
di esercitare i suoi diritti ai sensi degli articoli da 15 a 22

salvo che il titolare dimostri che non è in grado di identificare l'interessato, secondo i principi in tema di trattamenti che non richiedono l'identificazione.

Qualora il TDTR nutra ragionevoli dubbi circa l'identità della persona fisica che richiede di esercitare i propri diritti, *può richiedere ulteriori informazioni* necessarie per confermare l'identità dell'interessato (art. 12,6).

Diritto di accesso

- Il diritto di accedere ai dati personali che lo riguardano garantisce che l'interessato sia consapevole del trattamento e possa verificarne la liceità.
- Ciò deve poter essere fatto (63° Cons.) «*facilmente e a intervalli ragionevoli*» e, se possibile, il TDTR dovrebbe poter fornire l'accesso remoto a un sistema sicuro che consenta all'interessato di consultare direttamente i propri dati personali.
- Il diritto di accesso *non deve* ledere diritti e libertà altrui, compreso il segreto industriale e aziendale e la proprietà intellettuale, segnatamente i diritti d'autore a tutela del sw.

Diritto di rettifica

Conformemente al principio di esattezza dei d.p.,

- l'interessato ha il diritto (art. 16) di ottenere dal titolare del trattamento, senza ingiustificato ritardo

la rettifica dei d.p. inesatti.

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

Quando contesta l'esattezza dei d.p., l'interessato ha anche il diritto di ottenere dal TDTF la limitazione del tr. per il tempo necessario alla verifica (art. 18,1,a).

Diritto «all'oblio» (diritto alla cancellazione)

L'interessato ha il **diritto di ottenere la cancellazione** dei dati personali che lo riguardano (art. 17), senza ingiustificato ritardo

e il TDTF ha l'obbligo di cancellare i d.p.,

in una serie di casi, tassativi, in cui **la conservazione di tali dati viola il regolamento** o il diritto dell'Unione o degli Stati membri cui è soggetto il titolare del trattamento,

in particolare – per es. – quando i d.p. non sono più necessari per le finalità per le quali sono stati raccolti o altrimenti trattati.

Diritto «all'oblio» (diritto alla cancellazione)

1. i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
2. l'interessato revoca il consenso su cui si basa il trattamento (a patto che non sussista altro fondamento giuridico per il trattamento);
3. l'interessato abbia esercitato il diritto di opposizione al trattamento;
4. i dati personali sono stati trattati illecitamente;
5. i dati personali devono essere cancellati per adempiere un obbligo legale;
6. i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione.

Diritto alla limitazione del trattamento

L'interessato ha il diritto di ottenere dal TDTR **la limitazione del trattamento** nelle seguenti ipotesi:

a) l'interessato contesta l'esattezza dei d.p.,

- la limitazione dovrà valere per il periodo necessario al TDTR 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;

Diritto alla limitazione del trattamento

L'interessato ha il diritto di ottenere dal TDTR **la limitazione** del trattamento nelle seguenti ipotesi (segue):

c) i d.p. sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria,

- benché il TDTR non ne abbia più bisogno ai fini del tr.;

d) l'interessato ha esercitato il diritto di opposizione,

- in attesa della verifica in merito all'eventuale *prevalenza di motivi legittimi cogenti del TDTR* rispetto a quelli dell'interessato.

Che cos'è la «limitazione di trattamento»?

- La limitazione di trattamento è una particolare modalità del tr. che consiste nel «*contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro*».
- Il RGPD riconosce all'interessato **il diritto di ottenere dal TDTR la limitazione del tr.** nelle ipotesi di cui all'art. 18.
- Quando si ha un **trattamento soggetto a limitazione**, esso di norma potrà consistere nella *mera conservazione* dei dati personali
  - salvo che vi sia il consenso dell'interessato per ulteriori forme di trattamento; *oppure*
  - per l'esercizio o la difesa di un diritto in sede giudiziaria
  - per tutelare i diritti di un'altra persona (fisica o giuridica)
  - per motivi di interesse pubblico rilevante.

Diritto alla portabilità dei d.p.

- Per rafforzare ulteriormente il controllo sui propri dati il RGPD riconosce all'interessato il diritto alla portabilità dei d.p. (art. 20), ossia il diritto:
  - di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i d.p. che lo riguardano, che abbia fornito a un TDTR, e
  - di trasmettere tali dati a un altro TDTR senza impedimenti da parte del TDTR cui li ha forniti.
- Deve trattarsi di tr. basati sul consenso oppure necessari all'esecuzione di un contratto o di misure precontrattuali.
- In entrambi i casi, deve trattarsi di trattamenti automatizzati.

Diritto di opposizione

- Si è visto come il tr. di d.p. è lecito quando è necessario (art. 6,1,e-f):
  - per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri,
  - per il perseguimento del legittimo interesse del TDTR o di terzi.
- Il RGPD (art. 21) riconosce all'interessato il diritto di opporsi a tali trattamenti, *compresa la profilazione*, in *qualsiasi* momento e per motivi connessi alla sua situazione particolare.
- In caso di opposizione, il TDTR si *deve* astenere dall'ulteriore trattamento.

Diritto di opposizione

- … il TDTR si *deve* astenere dall'ulteriore trattamento, salvo che (art. 21,1) dimostri l'esistenza di motivi legittimi cogenti per procedere comunque al trattamento:
  - deve trattarsi di motivi 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.
- *Obblighi particolari di informazione*: 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* (art. 21,4).

Diritto di opposizione al marketing diretto

- L'interessato ha inoltre il diritto di opporsi (art. 21,2-3) *in qualsiasi momento* e senza oneri («gratuitamente») al tr. dei d.p. effettuato per finalità di marketing diretto, compresa la profilazione (se connessa a tale finalità).
- In caso di opposizione, i d.p. non sono più oggetto di tr. per tali finalità: il TDTR *deve* cessare il trattamento.
- *Obblighi particolari di informazione*: anche in questo caso 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* (art. 21,4).

Altri diritti connessi dell'interessato

- Diritto di revocare il consenso
- Diritto di avere comunicazione di una violazione di d.p. (*data breach*)
- Diritto di proporre reclamo all'autorità di controllo
- Diritto a un ricorso giurisdizionale effettivo
  - nei confronti dell'autorità di controllo
  - nei confronti del titolare o del responsabile del trattamento
- Diritto di essere informato su eventuali limitazioni di legge ai diritti riconosciuti dal RGPD
- Diritto al risarcimento
- … …

Gli obblighi per chi effettua il trattamento

DIRITTI DELL'INTERESSATO = OBBLIGHI DEL TITOLARE

Diritti dell'interessato = obblighi del titolare

I **diritti** riconosciuti all'interessato dal RGPD si traducono in

altrettanti corrispondenti obblighi per il TDTR

- Tali obblighi del TDTR sono inoltre alla **base della responsabilità generale** (*accountability*) prescritta dal regolamento.
- *Accountability* vuol dire anche **documentare** ed essere in grado di **dimostrare** in ogni momento la conformità del tr. al RGPD.

Il **responsabile del trattamento** **assiste** (art. 28,3,e) **il titolare** negli obblighi nascenti dall'esercizio dei diritti dell'interessato.

Obblighi derivanti da principi di base e diritti dell'interessato

- Il TDTR *deve* altresì garantire il rispetto dei principi: di liceità, correttezza e trasparenza, limitazione delle finalità, minimizzazione, esattezza, limitazione della conservazione, integrità e riservatezza…
- … e adempiere gli obblighi nascenti dai diritti dell'interessato:
  - fornire le informazioni e comunicazioni obbligatorie
  - garantire il diritto di accesso dell'interessato
  - assolvere agli obblighi di rettifica e cancellazione
  - procedere alla limitazione del trattamento
  - garantire la portabilità dei dati
  - cessare il tr. in caso di opposizione dell'interessato
  - astenersi da processi decisionali automatizzati /profilazioni nei casi previsti dal RGPD

Adottare misure tecniche *e* organizzative

- È pertanto stabilito (art. 24,1) che il TDTR,

tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del tr., nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche

deve mettere in atto misure tecniche e organizzative adeguate

- per **garantire**,
- ed **essere in grado di dimostrare**

che il tr. è effettuato conformemente al regolamento.

- Dette misure sono riesaminate e aggiornate *qualora necessario*.

Attuare politiche di protezione

- In coerenza con il principio di responsabilizzazione e *tenuto conto delle dimensioni delle attività di trattamento*, le misure tecniche ed organizzative adeguate possono includere (art. 24,2)

«l'attuazione di **politiche** adeguate in materia di protezione dei d.p. da parte del titolare del trattamento».

- Ciò si traduce in un approccio «di sistema», più efficace rispetto a misure eterogenee e non coordinate tra loro.

I TDTF hanno pertanto l'onere di decidere autonomamente modalità, garanzie e limiti del tr., assicurando il rispetto del RGPD, alla luce dei criteri specifici da esso indicati.

Dimostrare il rispetto degli obblighi

- Il TDIR ha l'obbligo di dimostrare e documentare il rispetto degli obblighi imposti da RGPD.

Ciò è funzionale, sul piano generale, non solo sul piano delle responsabilità (tra l'altro, in sede civile) connesse al tr, ma anche all'esercizio dei poteri delle Autorità garanti.

- Uno strumento destinato ad incontrare largo impiego nella pratica sarà l'adesione (art. 24,3):
  - ai codici di condotta di cui all'art. 40
  - o a un meccanismo di certificazione di cui all'art. 42
- che potrà essere utilizzata come elemento per dimostrare il rispetto degli obblighi del TDIR.

Protezione dei dati *by design* e *by default*

- Quale specificazione concreta dell'obbligo di attuare misure tecniche e organizzative adeguate, il RGPD **impone** (Art. 25) ai TDTR un *nuovo approccio* concettuale ed operativo:

1. La protezione dei dati deve essere assicurata fin dalla progettazione (*by design*).
2. La protezione dei dati deve essere un'impostazione predefinita del trattamento (*by default*).

- La conformità (obbligatoria) a tali requisiti può essere dimostrata anche con meccanismi di certificazione approvati (Art. 25,3).

Obbligo di «istruire» (formazione)

- *Coerentemente con la responsabilità di determinare mezzi e finalità del trattamento*, il TDTR ha **l'obbligo di «istruire»** (art. 29)

chiunque abbia accesso ai d.p. e agisca sotto la sua autorità,

- compreso il responsabile del trattamento, se designato
- e chiunque agisca sotto l'autorità di quest'ultimo.

«*istruire*», in questo contesto, vuol dire essenzialmente *dare istruzioni*:

- autorizzare, dare direttive, assicurare una formazione adeguata…

- Ne ricaviamo il **divieto di trattare dati personali** *senza (o al di fuori delle) istruzioni del TDTR*

Obbligo di «istruire» (formazione)

È bene evidenziare che l'inosservanza dell'obbligo formativo si traduce – in concreto – nel consentire indebitamente l'accesso a dati personali a persone *non qualificate*, che per tale ragione non possono essere autorizzate a svolgere attività di trattamento neppure elementari.

- È un obbligo che non deve essere trattato alla stregua di una mera formalità di carattere burocratico…
- … non dovrebbe essere un frettoloso adempimento *una tantum*, bensì costituire oggetto di una pianificazione periodica che tenga conto dei nuovi ingressi nell'organigramma nonché dell'evoluzione delle funzioni e delle procedure connesse.
- La formazione in tale materia è inoltre *una delle componenti chiave di un sistema di politiche di protezione dei dati* personali che tenga conto dei principi di base illustrati.
- La violazione rientra tra quelle previste dall'articolo 83, par. 4, che stabilisce la sanzione amministrativa della pena pecuniaria che vedremo.

Tenuta obbligatoria registri delle attività di trattamento (*Records of processing activities*)

- *Ogni* titolare del trattamento (e, ove applicabile, il suo rappresentante UE) *deve* tenere un **registro delle attività di trattamento** svolte sotto la propria responsabilità (art. 30).

Il registro delle attività di trattamento *non è un mero adempimento formale* ma ha un **ruolo sostanziale**, in quanto *parte integrante di un sistema di corretta gestione* dei d.p.: esso ha la funzione di documentare e dimostrare (82° Cons) la conformità dei trattamenti al RGPD: inoltre è *necessario per il monitoraggio* da parte delle Autorità di controllo ed è presupposto *indispensabile per qualsiasi analisi e valutazione dei rischi*.

Tenuta obbligatoria registri delle attività di trattamento (*Records of processing activities*)

- Anche *ogni* **responsabile del trattamento** (e, ove applicabile, il suo rappresentante) *deve* tenere un **registro *delle categorie di attività* di trattamento *svolte per conto di un titolare*** del trattamento (art. 30,2).

Valgono le stesse considerazioni generali:

Il registro delle attività di trattamento *non è un mero adempimento formale* ma ha un **ruolo sostanziale**, in quanto *parte integrante di un sistema di corretta gestione* dei d.p.: esso ha la funzione di documentare e dimostrare (82° Cons) la conformità dei trattamenti al RGPD: inoltre è *necessario per il monitoraggio* da parte delle Autorità di controllo ed è presupposto *indispensabile per qualsiasi analisi e valutazione dei rischi*.

Obbligo di cooperazione con le Autorità di controllo

- È un obbligo generale stabilito dall'art. 31:
  - Il titolare del trattamento,
  - il responsabile del trattamento

  cooperano, *su richiesta*, con l'autorità di controllo nell'esecuzione dei suoi compiti.

- Abbiamo, per esempio, appena visto, a proposito dei registri, l'obbligo di metterli, su richiesta, a disposizione dell'Autorità di controllo (art. 30,4).

Pur nella sua apparente genericità, l'obbligo di cooperazione è un elemento cruciale per la responsabilità: come vedremo, «*il grado di cooperazione con l'Autorità di controllo*» è uno degli elementi valutati per stabilire l'ammontare delle sanzioni amministrative pecuniarie (art. 83,2,f).

Obblighi inerenti la 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 TDTR e il RDTR *devono* mettere in atto (art. 32)

misure tecniche
e organizzative adeguate

per **garantire**

un **livello di sicurezza adeguato al rischio.**

Misure tecniche ed organizzative di sicurezza

a) la pseudonimizzazione e la cifratura dei d.p.;

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 d.p. 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.

La sicurezza del trattamento

- Coerentemente con il principio di *accountability*, in tema di sicurezza il *focus* si sposta dalla prescrizione alla responsabilizzazione del TDTR.
- Il RGPD introduce la necessità di un *approccio proattivo* al rischio,

sollecitando i TDTR ad una valutazione preliminare e continua di ogni aspetto potenzialmente critico dei tr. in ogni fase ed attività di essi. *dalla progettazione alla messa in opera*, ed oltre *fino a momento della cessazione*.

Dal rischio alla sicurezza del trattamento

- Più che imporre specifiche misure (come le «vecchie» misure minime), **il RGPD si concentra sui rischi**

che il TDTR deve tenere in considerazione nella «***messa a norma***» dei trattamenti. Infatti,

I dati personali dovrebbero essere trattati in modo da garantirne un'adeguata sicurezza e riservatezza, anche *per impedire l'accesso o l'utilizzo non autorizzato dei dati personali e delle attrezzature* impiegate per il trattamento (39° Cons.).

I rischi del trattamento

I **rischi per i diritti e le libertà** delle persone fisiche possono avere probabilità e gravità diverse e derivano da tr. di d.p. suscettibili di cagionare un danno *fisico*, *materiale* o *immateriale* (75° Cons).

C'è *sempre* un rischio di questa natura se il tr. può comportare

- discriminazioni,
- furto o usurpazione d'identità,
- perdite finanziarie,
- pregiudizio alla reputazione,
- perdita di riservatezza dei d.p. protetti da segreto professionale,
- decifratura non autorizzata della pseudonimizzazione,
- o qualsiasi altro danno economico o sociale significativo;

I rischi del trattamento

… oppure se gli interessati

- rischiano di essere privati dei loro diritti e delle loro libertà
- o venga loro impedito l'esercizio del controllo sui d.p.;

… oppure quando sono trattati dati personali

- che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale,
- nonché dati genetici,
- dati relativi alla salute
- o i dati relativi alla vita sessuale
- o a condanne penali e a reati o alle relative misure di sicurezza…

Riepilogo obblighi generali

- Obblighi connessi con la responsabilizzazione:
  - *Obblighi derivanti da principi di base e diritti dell'interessato*
  - *Attuazione di misure tecniche e organizzative adeguate*
  - *Valutazione dei rischi per diritti e libertà delle persone*
  - *Attuazione di politiche adeguate di protezione dei d.p.*
  - *Dimostrare e documentare il rispetto degli obblighi*
  - *Obbligo di riesame ed aggiornamento delle misure*
- Protezione dei d.p. *by design* e *by default*
- Obbligo di contrattualizzare la contitolarità
- Obbligo di nominare un rappresentante nell'Ue
- Obbligo di «istruire» (*divieto di trattare d.p. senza istruzioni*)
- Obbligo di tenuta di un registro delle attività di tr.
- Obbligo di cooperazione con le Autorità di controllo
- Obbligo di nominare un DPO

Sanzioni e Responsabilità

QUANDO IL TRATTAMENTO NON È CONFORME AL GDPR

Sanzioni per la violazione dei «principi di base» del trattamento

- La violazione delle seguenti disposizioni è soggetta alla sanzione amministrativa pecuniaria fino a 20.000.000 EUR, ovvero – per le imprese – fino al 4% del fatturato mondiale annuo dell'esercizio precedente, se superiore (art. 83,5,a):
  - Articolo 5 – Principi applicabili al trattamento di dati personali
  - Articolo 6 – Liceità del trattamento
  - Articolo 7 – Condizioni per il consenso
  - Articolo 9 – Trattamento di categorie particolari di dati personali

Sanzioni per la violazione dei diritti dell'interessato

La violazione delle seguenti disposizioni è soggetta alla sanzione amministrativa pecuniaria fino a 20.000.000 EUR, ovvero – per le imprese – fino al 4% del fatturato mondiale annuo dell'esercizio precedente, se superiore (art. 83,5,b):

- Articolo 12 – Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato
- Articolo 13 – Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato
- Articolo 14 – Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato
- Articolo 15 – Diritto di accesso dell'interessato

Sanzioni per la violazione dei diritti dell'interessato

- Articolo 16 – Diritto di rettifica
- Articolo 17 – Diritto alla cancellazione («diritto all'oblio»)
- Articolo 18 – Diritto di limitazione di trattamento
- Articolo 19 – Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento
- Articolo 20 – Diritto alla portabilità dei dati
- Articolo 21 – Diritto di opposizione
- Articolo 22 – Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione

Sanzioni per la per violazione degli obblighi del TDIR e del RDIR

La violazione, da parte del TDIR e del RDIR, delle seguenti disposizioni è soggetta alla sanzione amministrativa pecuniaria fino a 10.000.000 EUR, ovvero – per le imprese – fino al 2% del fatturato mondiale annuo dell'esercizio precedente, se superiore (art. 83,4,a):

- Articolo 8 – Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione
- Articolo 11 – Trattamento che non richiede l'identificazione
- Articolo 25 – Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita
- Articolo 26 – Contitolari del trattamento

Sanzioni per la per violazione degli obblighi del TDTR e del RDTR

- Articolo 27 – Rappresentanti di titolari del trattamento o dei responsabili del trattamento non stabiliti nell'Unione
- Articolo 28 – Responsabile del trattamento
- Articolo 29 – Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento
- Articolo 30 – Registri delle attività di trattamento
- Articolo 31 – Cooperazione con l'autorità di controllo
- Articolo 32 – Sicurezza del trattamento
- Articolo 33 – Notifica di una violazione dei dati personali all'autorità di controllo

Sanzioni per la per violazione degli obblighi del TDTR e del RDTR

- Articolo 34 – Comunicazione di una violazione dei dati personali all'interessato
- Articolo 35 – Valutazione d'impatto sulla protezione dei dati
- Articolo 36 – Consultazione preventiva
- Articolo 37 – Designazione del responsabile della protezione dei dati
- Articolo 38 – Posizione del responsabile della protezione dei dati
- Articolo 39 – Compiti del responsabile della protezione dei dati
- Articolo 42 – Certificazione
- Articolo 43 – Organismi di certificazione

Diritti di ricorso dell'interessato

- Nel quadro delle tutele riconosciute all'interessato dal RGPD, oltre al diritto di reclamo all'AC per le violazioni del regolamento (art. 77), sono previsti *due ulteriori strumenti*:
- Art. 78 – Diritto a un ricorso giurisdizionale effettivo *nei confronti dell'autorità di controllo*.
  - Strumento che, peraltro, è posto sorattutto a tutela del TDTR e del RDTR e di altri soggetti, come subito vedremo.
- Art. 79 – Diritto a un ricorso giurisdizionale effettivo *nei confronti del titolare del trattamento o del responsabile del trattamento*.

Ricorso giurisdizionale nei confronti del titolare o del responsabile del trattamento

Possiamo dire che, insieme al reclamo (art. 77) questo sia il rimedio generale di tutela posto a garanzia dei diritti e libertà dell'interessato in caso di violazione degli obblighi di cui al regolamento (art. 79):

- ogni interessato ha il diritto di proporre un ricorso giurisdizionale effettivo *qualora ritenga che i diritti di cui gode a norma del regolamento siano stati violati a seguito di un trattamento*.
- Oltre all'accertamento dell'eventuale violazione di diritti, *attraverso questo strumento* sarà possibile per l'interessato ottenere il risarcimento del danno (Art.82).
- Anche in questo caso, non è pregiudicato alcun altro eventuale rimedio amministrativo o giurisdizionale.

Responsabilità e risarcimento

Chiunque subisca un danno *materiale* o *immateriale* causato da una violazione del regolamento ha il diritto di ottenere il risarcimento del danno dal titolare o dal responsabile del trattamento (art. 82).

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 dello stabilimento* del responsabile
- oppure *della residenza abituale del danneggiato*.

Responsabilità e risarcimento

In via generale la responsabilità è così ripartita:

- il TDTR risponde *per il danno cagionato dal suo trattamento* che violi il regolamento
- il RDTR risponde per il danno causato dal trattamento (del titolare) solo se:
  - non ha adempiuto gli obblighi del regolamento specificatamente diretti ai RDTR
  - o ha agito in modo difforme o contrario *rispetto alle legittime istruzioni del TDTR*.

Entrambi sono esonerati se dimostrano che l'evento dannoso non è loro in alcun modo imputabile (art. 82,3).

Concorso di responsabilità

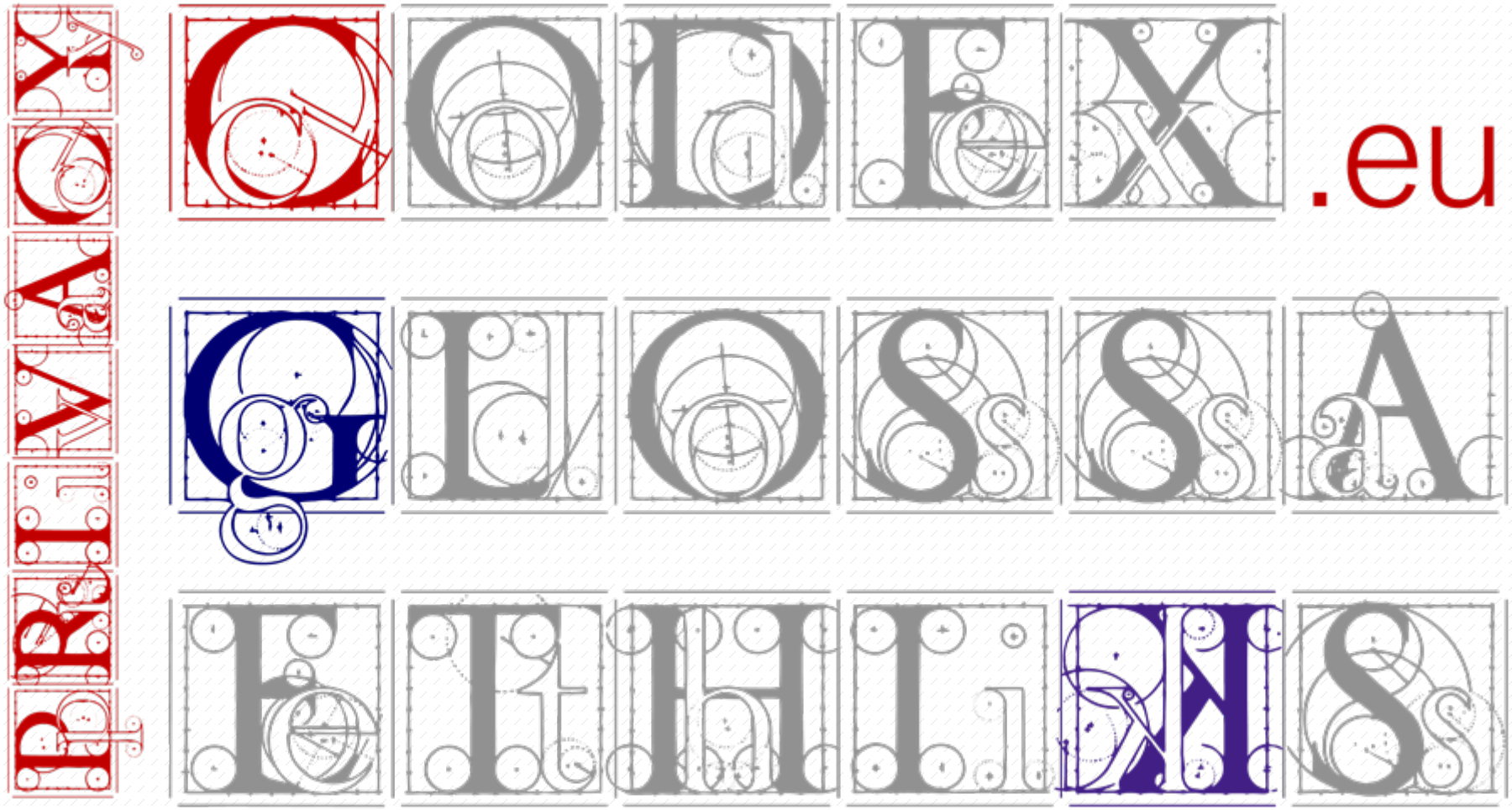
Qualora (art. 82,4)

- più titolari o più responsabili del tr.,
- oppure sia il titolare sia il responsabile del tr.,

siano coinvolti nello stesso trattamento

e siano responsabili dell'eventuale danno causato dal trattamento,

ogni TDTR o RDTR è responsabile in solido per l'intero ammontare del danno, *al fine di garantire il risarcimento effettivo dell'interessato* (salvo rivalsa nei rapporti interni (art. 82,5)).



Fine della presentazione

Avv. Marzio V. Vaglio (www.vaglio.org — www.privacycodex.eu)

Spazio per le domande e la discussione

Grazie per la vostra pazienza… e attenzione