



LEGALE/TERRITORIO/INFRASTRUTTURE

CONFINDUSTRIA VENEZIA
AREA METROPOLITANA DI VENEZIA E ROVIGO

IL NUOVO REGOLAMENTO GENERALE UE SULLA PROTEZIONE DEI DATI PERSONALI N. 679/2016

*Analisi pratica del quadro generale di
insieme e dei nuovi adempimenti privacy.*



Tonucci & Partners

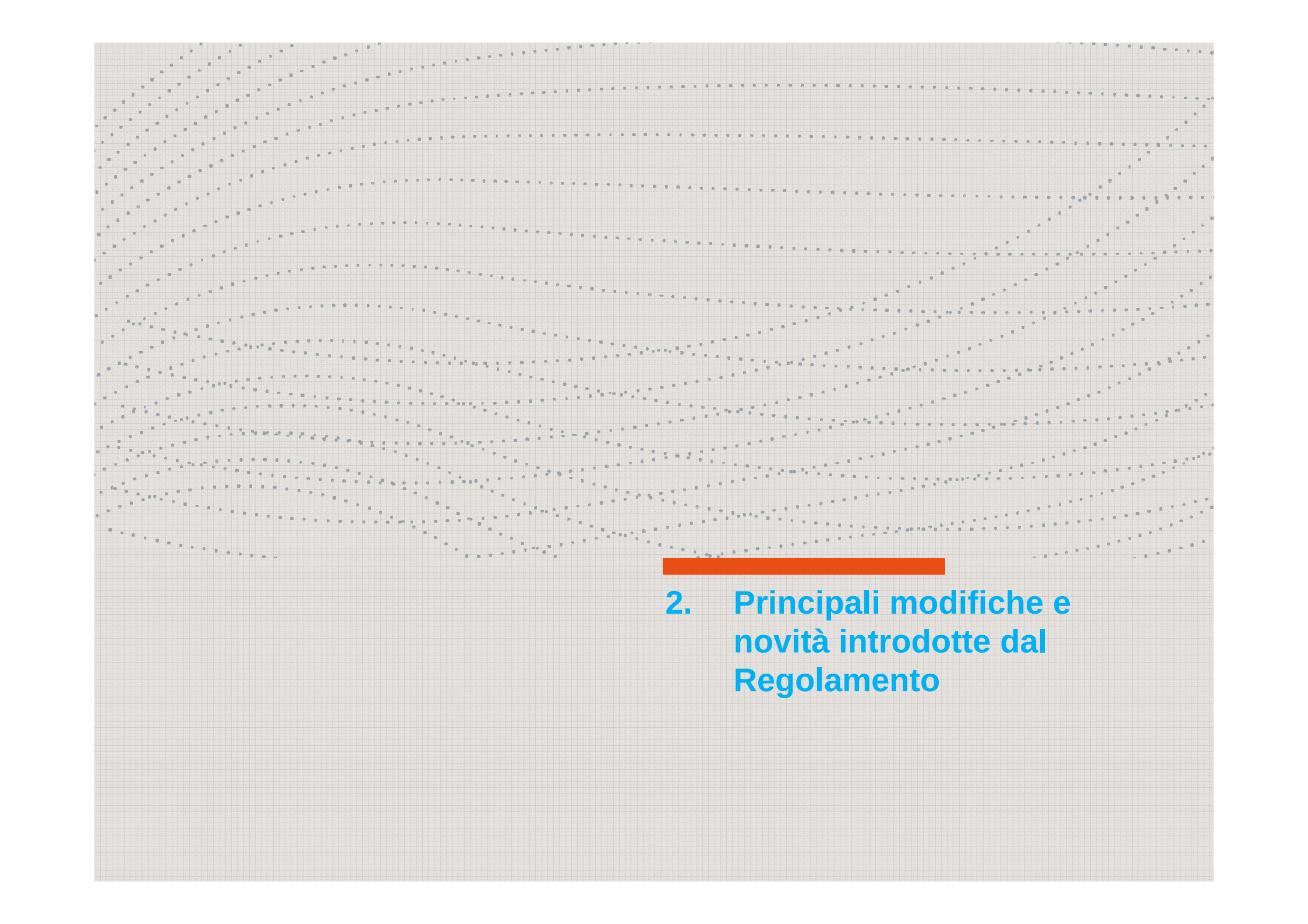
Avv. Alessandro Vasta
Tonucci & Partners – www.tonucci.com
Via Trieste 31/A, Padova (PD)
049-658655
avasta@tonucci.com

**1. Entrata in vigore
e Applicabilità**



ENTRATA IN VIGORE

- ✓ Pubblicazione nella Gazzetta Ufficiale dell'Unione Europea n. 119/2016: **4 Maggio 2016**.
- ✓ Entrata in vigore: **25 Maggio 2016**.
- ✓ Applicabilità in tutti i Paesi della UE: **25 Maggio 2018**.
- ✓ Tutti i soggetti interessati hanno **due anni di tempo** per adeguare alle nuove norme le politiche del trattamento dei dati.
- ✓ Il Regolamento sarà **immediatamente applicabile** senza necessità di recepimento.
- ✓ Per quanto riguarda l'Italia, il Regolamento sostituirebbe (non integralmente) il D. Lgs. n. 196/2003 *Codice in materia di Protezione dei dati personali* (c.d. Codice Privacy) in vigore dal 1 Gennaio 2004 ma sarà **necessario comunque un coordinamento normativo** (Il Garante privacy ha in corso una ricognizione normativa per verificare quali parti del Codice Privacy e quali provvedimenti generali del Garante sopravvivranno alla riforma).



2. Principali modifiche e novità introdotte dal Regolamento



SCHEMA RIEPILOGATIVO

LE MODIFICHE	LE NOVITA'
✓ Modifica di definizioni esistenti	▪ Estensione ambito territoriale
✓ Specificazione dei ruoli e compiti di Titolare e Responsabile	▪ Nuove definizioni (profilazione, dati biometrici, ecc.)
✓ Informativa rafforzata	▪ Il Responsabile della protezione dei dati (c.d. "Data Protection Officer")
✓ Il consenso	▪ Il Registro dei trattamenti
✓ Specificazione di diritti	▪ La valutazione preventiva d'impatto
✓ Inasprimento sanzioni	▪ Notifica dei data breach
	▪ Privacy <i>by design</i> – privacy <i>by default</i>
	▪ Diritto all'oblio e a Portabilità dei dati



AMBITO DI APPLICABILITÀ MATERIALE

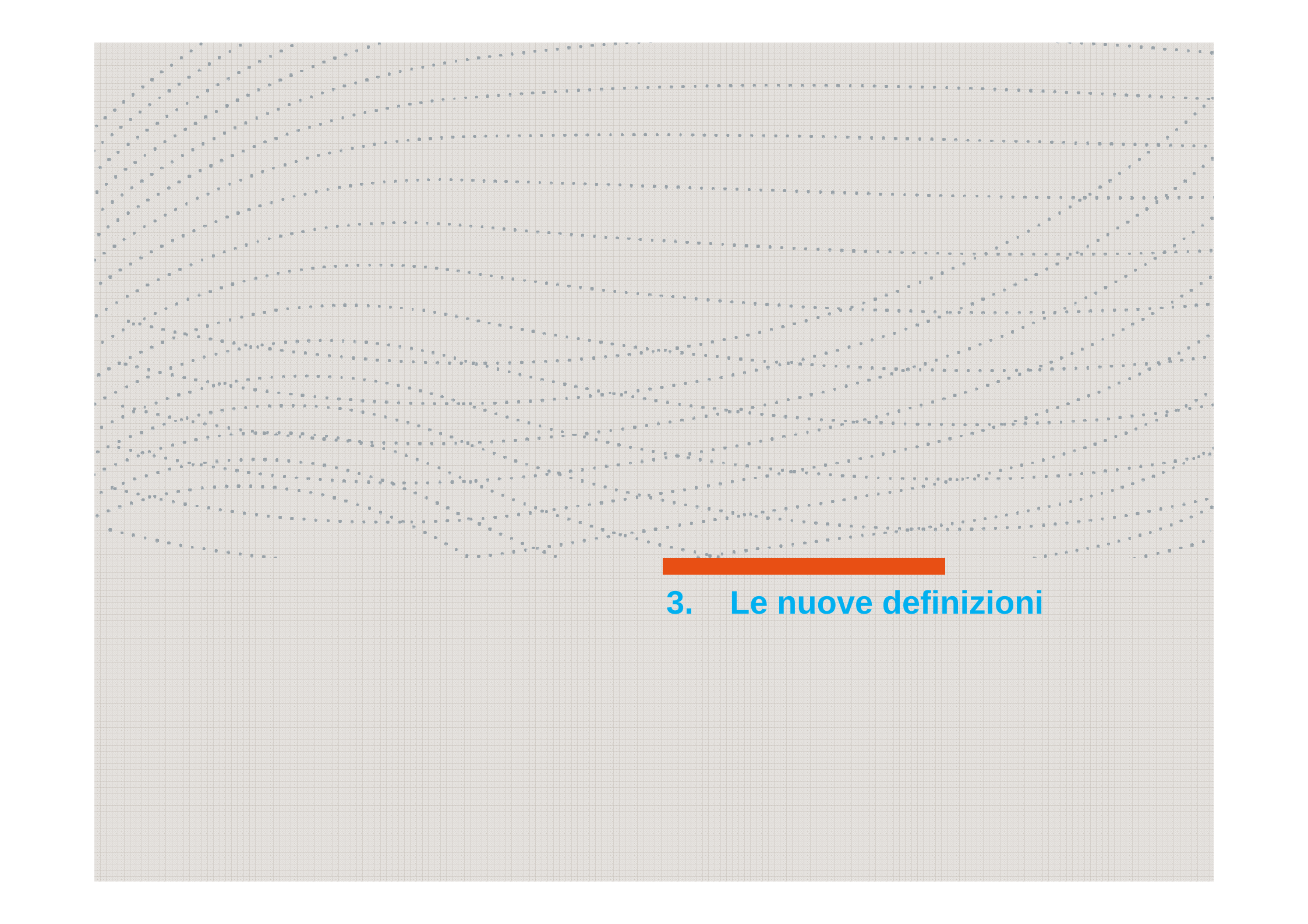
- ✓ Si applica solo al trattamento dei dati personali di persone fisiche;
- ✓ Riguarda trattamenti interamente o parzialmente **automatizzati** o **non automatizzati**, se i dati personali sono contenuti in un archivio o sono destinati a confluirci;
- ✓ Il Regolamento non si applica ai trattamenti di dati personali effettuati:
 - a) da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico;
 - b) da autorità di pubblica sicurezza;
 - c) per attività che non rientrano nell'ambito di applicazione del diritto dell'UE.



AMBITO DI APPLICABILITÀ TERRITORIALE

Il Regolamento si applica:

- 1) al trattamento di dati personali effettuato da un **Titolare o Responsabile stabilito nella UE**, indipendentemente dal fatto che il trattamento sia effettuato o meno nella UE;
- 2) al trattamento di dati personali effettuato da **Titolari o Responsabili non stabiliti nell'UE**, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione, se il **trattamento ha ad oggetto dati personali di interessati che si trovano nella UE** e riguarda (i) **l'offerta di beni o servizi** (anche non a pagamento) ai suddetti interessati oppure (ii) il **monitoraggio** del loro comportamento nel territorio della UE;
- 3) al trattamento effettuato da un Titolare stabilito in uno **Stato extra UE soggetto al diritto di uno Stato UE** in virtù del diritto internazionale pubblico.



3. Le nuove definizioni



PRINCIPALI NUOVE DEFINIZIONI

- ✓ Eliminata la definizione di dati **sensibili** e di **dati giudiziari**;
- ✓ Ora si parla di “**Categorie particolari di dati personali**”: dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;
- ✓ **Dati relativi alla salute**: dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
- ✓ **Dati genetici**: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
- ✓ **Dati biometrici**: dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati Dattiloscopici;



PRINCIPALI NUOVE DEFINIZIONI

- ✓ **Consenso dell'interessato:** qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
- ✓ **Pseudonimizzazione:** il trattamento di dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.



LA PROFILAZIONE

- ✓ Introdotta per la prima volta **una definizione e una regolamentazione del particolare trattamento rappresentato dalla profilazione dell'interessato**, giuridicamente definita come *“qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica”*.
- ✓ In linea generale è vietata (*“L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona”*) a meno che non vi siano circostanze specifiche, tra le quali il **chiaro consenso informato dell'interessato**.
- ✓ I trattamenti di profilazione rappresentano poi uno dei presupposti che **rendono obbligatoria la valutazione preventiva** di impatto sulla protezione dei dati.



PRINCIPALI DEFINIZIONI MODIFICATE

- ✓ **Dato personale:** qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); 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.
- ✓ **Trattamento:** qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

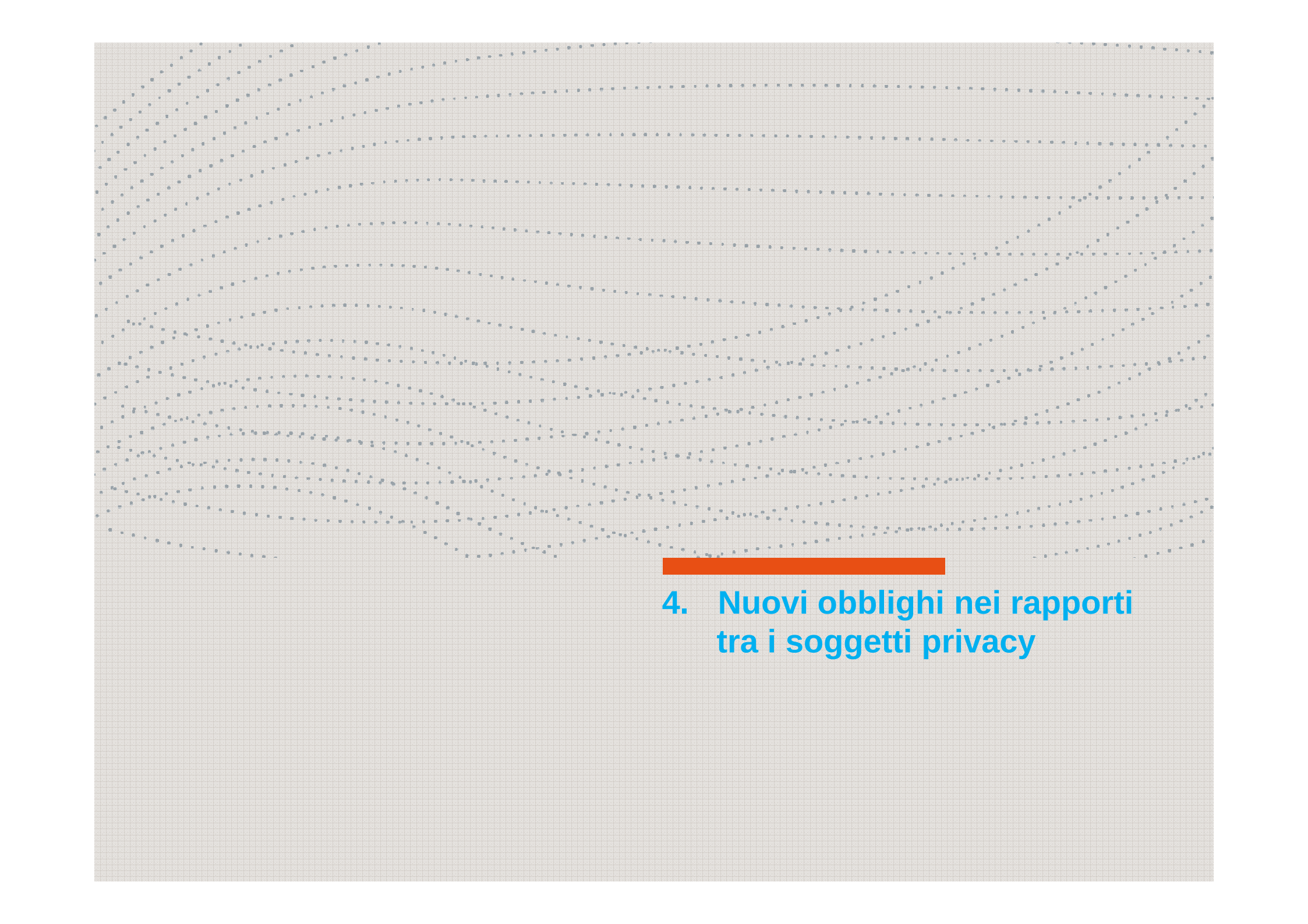


PRINCIPALI DEFINIZIONI MODIFICATE

- ✓ **Titolare del trattamento** : la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali;

- ✓ **Responsabile del trattamento** : la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

- ✓ **Terzo** : la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile



4. Nuovi obblighi nei rapporti tra i soggetti privacy



NUOVI OBBLIGHI NEI RAPPORTI TRA SOGGETTI PRIVACY

il Regolamento introduce **degli obblighi organizzativi nuovi** con riferimento ai loro ruoli e funzioni, come ad esempio i seguenti:

- ✓ il Titolare deve attuare **misure tecniche ed organizzative adeguate per garantire e dimostrare che il trattamento è effettuato conformemente al Regolamento**. Le misure devono essere riesaminate periodicamente e aggiornate, ove necessario. L'adesione a Codici di condotta o a meccanismi di certificazione, può essere utilizzata come elemento per dimostrare il rispetto degli obblighi imposti al Titolare del trattamento;
- ✓ In caso di **contitolarità del trattamento**: i Contitolari devono stipulare tra loro **uno specifico accordo interno** che disciplini in modo trasparente le rispettive responsabilità e rifletta adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo va messo a disposizione dell'interessato;



NUOVI OBBLIGHI NEI RAPPORTI TRA SOGGETTI PRIVACY

- ✓ **Obbligatoria** per il Titolare la **nomina del Responsabile del trattamento**, va documentata con un “*contratto o altro atto giuridico*”, stipulato in forma scritta anche su supporto elettronico, che regoli 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. Ammessa la designazione di Sub-Responsabili previa autorizzazione scritta, specifica o generale del Titolare del trattamento;
- ✓ **Incaricati del trattamento**: categoria di soggetti, identificata con le “**persone autorizzate al trattamento**” non è definita formalmente, ma disciplinata indirettamente. Viene previsto per il Titolare l’obbligo di indicare le persone autorizzate all’interno della sua struttura;

5. La nuova figura del *Data Protection Officer*



Il Responsabile della protezione dei dati (Data Protection Officer)

La **designazione** del DPO è **obbligatoria** (da parte del Titolare o del Responsabile del trattamento) solo se:

1. il trattamento **è effettuato da un'autorità pubblica o da un organismo pubblico**, eccettuate le autorità giurisdizionali;
2. le attività **principali** del Titolare del trattamento o del Responsabile del trattamento consistono in **trattamenti che**, per natura, ambito di applicazione e/o finalità, **richiedono il monitoraggio regolare e sistematico degli interessati su larga scala**;
3. le attività **principali** del Titolare del trattamento o del Responsabile del trattamento consistono nel trattamento, **su larga scala**, di categorie particolari di dati di cui all'art. 9 o 10 del Regolamento (dati che rivelino l'origine razziale o etnica, opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale, dati genetici, biometrici, dati relativi alla salute o alla vita sessuale o orientamento sessuale, o dati relativi a condanne penali e a reati).



Il Responsabile della protezione dei dati (Data Protection Officer)

- ✓ Il DPO va designato in funzione delle **qualità professionali**, della **conoscenza specialistica della normativa** e delle **prassi in materia di protezione dei dati**, e della **capacità di assolvere i propri compiti**.
- ✓ E' **figura apicale**, assolutamente diversa quanto a ruolo e funzioni dal "semplice" responsabile del trattamento.
- ✓ **Può essere un dipendente** del Titolare o del Responsabile del trattamento oppure **un consulente esterno** che assolve i suoi compiti in base a un **contratto di servizi**.
- ✓ Un **gruppo** imprenditoriale **può nominare un unico** DPO.
- ✓ I **dati di contatto** del DPO vanno **comunicati al Garante per la protezione dei dati personali e resi pubblici**.



Il Responsabile della protezione dei dati (Data Protection Officer)

- ✓ Il DPO deve essere **autonomo ed indipendente**:
 - non deve ricevere dal Titolare o dal Responsabile alcuna istruzione per quanto riguarda l'esecuzione dei compiti affidati **né è soggetto a potere disciplinare o sanzionatorio** per l'adempimento dei propri compiti.
 - deve avere le risorse necessarie e il **potere di spesa** per assolvere ai compiti assegnati, accedere ai dati personali e ai trattamenti e per mantenere le proprie conoscenze specialistiche (es. aggiornamento professionale).



Il Responsabile della protezione dei dati (Data Protection Officer)

Il Regolamento individua il **nucleo minimo** dei compiti assegnati al DPO:

- ✓ **Informare e fornire** al Titolare, al Responsabile nonché ai dipendenti che eseguono il trattamento, **consulenza** in merito agli obblighi normativi in materia;
- ✓ **Sorvegliare l'osservanza della normativa** in materia di protezione dei dati personali nonché delle **politiche** in materia del Titolare o del Responsabile del trattamento, compresi l'attribuzione di responsabilità, la sensibilizzazione e formazione del personale che partecipa al trattamento e al controllo in merito;
- ✓ **Fornire**, se richiesto, **pareri** sulla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
- ✓ **Cooperare** con l'Autorità di controllo;
- ✓ **Fungere da punto di contatto con il Garante per la protezione dei dati di personali** per questioni connesse al trattamento.

6. L'informativa all'interessato
rafforzata



L'INFORMATIVA ALL'INTERESSATO RAFFORZATA

- ✓ Rispetto all'art. 13 del Codice Privacy, si prevedono **numerose informazioni aggiuntive** da fornire agli interessati in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro.
- ✓ L'Informativa **va resa per iscritto o con altri mezzi, anche elettronici**. Anche **oralmente**, purché sia richiesto dall'interessato e sia comprovata con altri mezzi l'identità dell'interessato.
- ✓ Le informazioni possono essere fornite anche in combinazione con **icone standardizzate** per dare, in modo facilmente visibile, intelligibile e chiaramente leggibile, un **quadro d'insieme del trattamento previsto**. Se presentate elettronicamente, le icone devono essere leggibili da qualsiasi dispositivo.



L'INFORMATIVA ALL'INTERESSATO RAFFORZATA

Rispetto agli elementi obbligatori da indicare nell'informativa privacy ai sensi dell'art. 13 del Codice Privacy, i Titolari del trattamento dovranno inserire obbligatoriamente anche le seguenti informazioni aggiuntive sul trattamento:

- ✓ i **dati di contatto** della nuova figura del DPO, ove prevista;
- ✓ la **base giuridica del trattamento** a corredo della illustrazione delle finalità del trattamento;
- ✓ qualora il trattamento si basi sulla necessità di perseguire un legittimo interesse del titolare del trattamento o di terzi, **la specificazione di quali siano i legittimi interessi** perseguiti dal titolare del trattamento o da terzi;
- ✓ **l'ambito del trasferimento all'estero** (ovviamente extra UE) o a un'organizzazione internazionale dei dati personali;



L'INFORMATIVA ALL'INTERESSATO RAFFORZATA

- ✓ il **periodo di conservazione** dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- ✓ la **specifica esistenza del diritto alla portabilità dei dati**;
- ✓ l'esistenza del **diritto di revocare il consenso in qualsiasi momento** senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
- ✓ il diritto di **proporre reclamo** al Garante per la protezione dei dati personali;



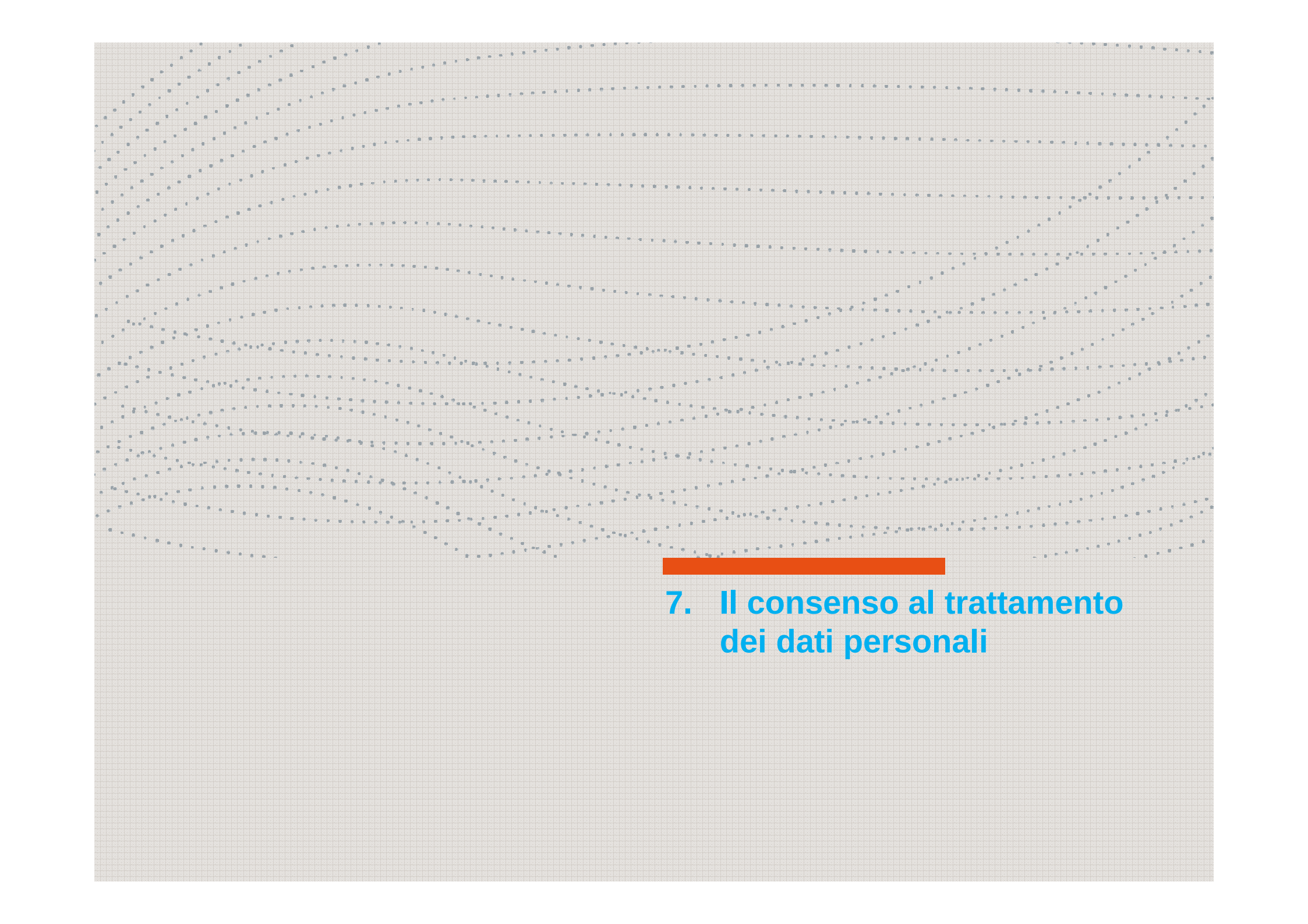
L'INFORMATIVA ALL'INTERESSATO RAFFORZATA

- ✓ la **eventuale esistenza di un processo decisionale automatizzato**, compresa la **profilazione** e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato;
- ✓ la **fonte da cui hanno origine i dati personali** e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico (solo ove i dati non siano raccolti presso l'interessato);
- ✓ le **categorie di dati personali oggetto del trattamento** (solo ove i dati non siano raccolti presso l'interessato).



L'INFORMATIVA ALL'INTERESSATO RAFFORZATA

Nel caso in cui i dati personali oggetto del trattamento non siano raccolti presso l'interessato, l'informativa dovrà essere fornita al più tardi **entro un mese dall'ottenimento** dei dati o, nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato o con un terzo, al più tardi **al momento di tale comunicazione**.



7. Il consenso al trattamento dei dati personali



IL CONSENSO DELL'INTERESSATO

- ✓ Il consenso dell'interessato rappresenta la principale condizione di liceità del trattamento.
- ✓ Il Titolare deve **poter dimostrare** che l'interessato ha prestato il consenso al trattamento. Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso deve **essere presentata in modo chiaramente distinguibile dalle altre materie**, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro, **pena l'invalidità del consenso prestato**.
- ✓ L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento con modalità di esecuzione della revoca del consenso facili come la sua prestazione originaria.



IL CONSENSO DELL'INTERESSATO

✓ È **specificatamente vietato** che l'esecuzione di un contratto o la prestazione di un servizio siano condizionati alla prestazione del consenso al trattamento di dati personali **non necessario** all'esecuzione del contratto o servizio.

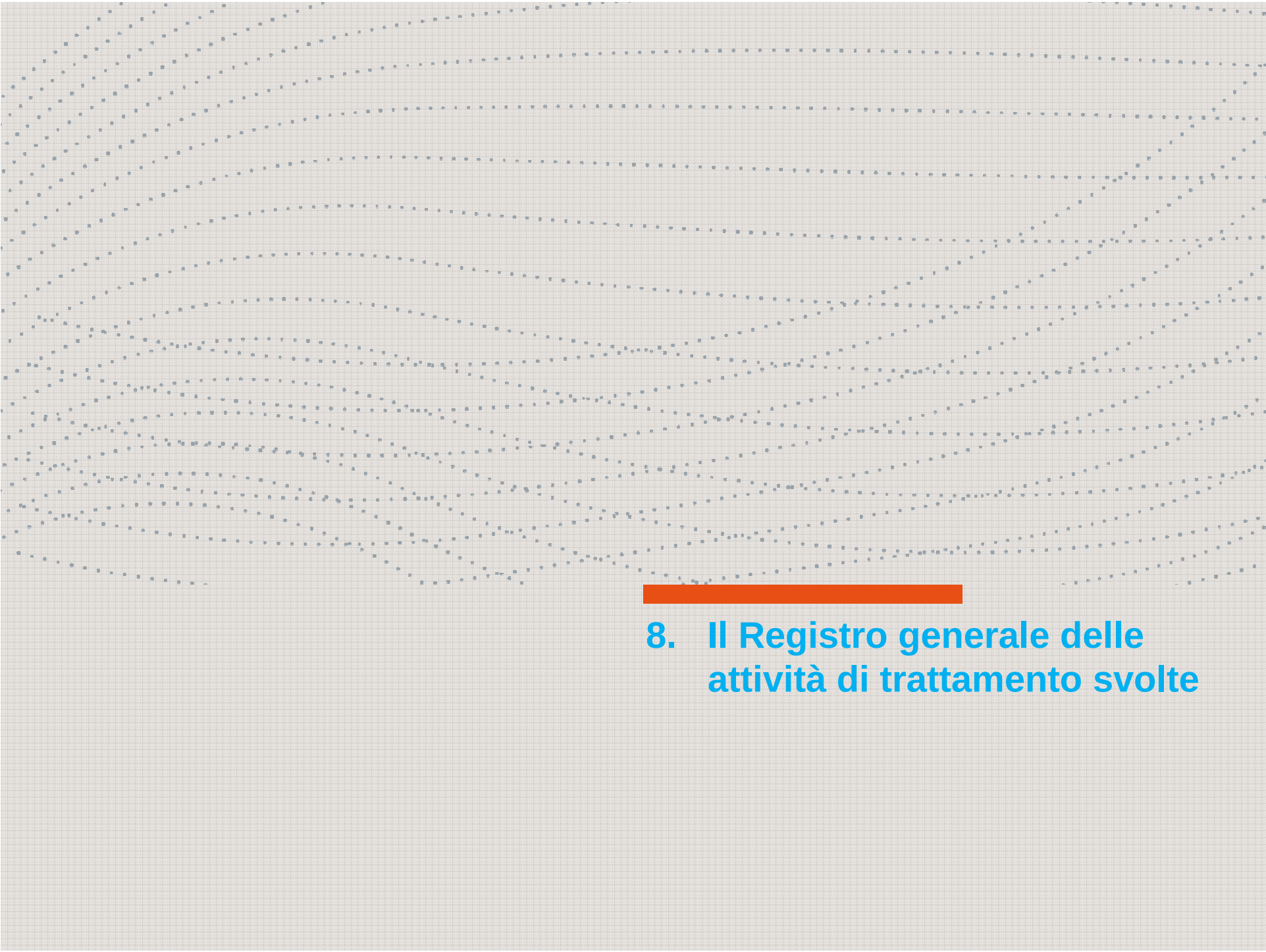
Alla **specificata manifestazione del consenso** è in particolare subordinata:

- (i) la liceità del trattamento (altrimenti vietato, salvo eccezioni) dei dati personali “particolari”;
- (ii) la possibilità – **altrimenti vietata** – di procedere alla **profilazione dell'interessato**;
- (iii) la possibilità di **trasferire i dati personali dell'interessato verso un Paese terzo extra UE** o verso un'organizzazione internazionale.



IL CONSENSO E I MINORI D'ETÀ

- ✓ Se un trattamento di dati nell'ambito **della fornitura ad un minore di un servizio della società dell'informazione** (es. l'accesso a Internet, l'iscrizione a un social network, etc.) prevede l'acquisizione del consenso preventivo, la **raccolta del consenso e il trattamento dei dati del minore sono leciti se egli abbia compiuto almeno 16 anni** (salvo il diritto degli Stati membri di stabilire anche un'età inferiore a tali fini, purché non inferiore ai 13 anni)
- ✓ Il Titolare deve adottare **misure ragionevoli per verificare che il consenso sia prestato** o autorizzato dal titolare della potestà genitoriale sul minore.



8. Il Registro generale delle attività di trattamento svolte



IL REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

- ✓ **Imprese o organizzazioni con numero di dipendenti pari o superiore a 250:** deve essere redatto (anche in formato elettronico) sia dal Titolare che dal Responsabile del trattamento e **va esibito** su richiesta al Garante per la protezione dei dati personali;
- ✓ Imprese **con meno di 250 dipendenti:** obbligo di redazione se il trattamento da esse svolto (i) presenta un rischio per i diritti e le libertà dell'interessato; (ii) non è occasionale o include dati personali "particolari" o relativi a condanne penali e reati.
- ✓ Rappresenta l'elemento fondamentale in relazione all'obbligo di elaborare un **sistema documentale di gestione della privacy** contenente tutti gli atti, regolarmente aggiornati, redatti per soddisfare i requisiti di conformità al Regolamento ("**accountability**")



IL REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

Ove redatto dal Titolare del trattamento, il Registro generale contiene:

- a) **Nome** e **dati di contatto** del Titolare, contitolare, rappresentante del Titolare e DPO;
- b) **Finalità** del trattamento;
- c) Categorie di **interessati e di dati personali**;
- d) **Ambito di comunicazione**, anche verso Paesi terzi;
- e) Ove possibile, **i termini ultimi per la cancellazione** delle diverse categorie dei dati;
- f) Ove possibile, una descrizione generale delle **misure di sicurezza tecniche e organizzative adottate**.



IL REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

Ove redatto dal Responsabile del trattamento, il Registro generale contiene:

- a) Nome e dati di contatto del/i Responsabile/i, del Titolare per cui egli agisce, del rappresentante del Titolare o del Responsabile e del DOP;
- b) Categorie dei trattamenti effettuati per conto di ogni Titolare;
- c) ove applicabile, i trasferimenti di dati personali verso un Paese terzo o un'organizzazione internazionale identificati e eventuali garanzie;
- d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative adottate.

9. Trasferimento dei dati
fuori dell'Unione
Europea.



TRASFERIMENTO DEI DATI PERSONALI EXTRA UE

Il Regolamento non introduce particolari novità rispetto all'attuale quadro

Condizioni di liceità:

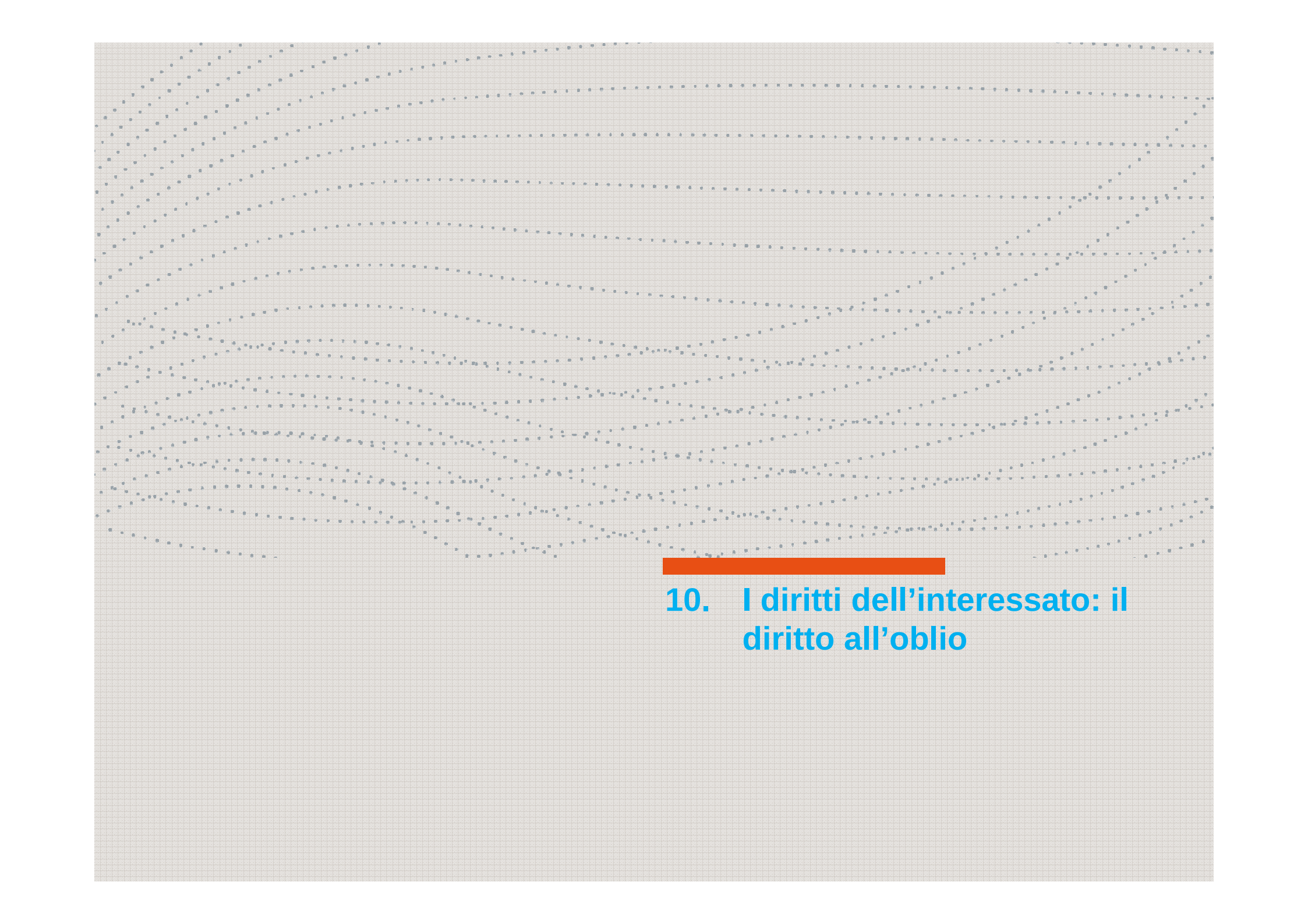
- ✓ **trasferimento sulla base di una decisione di adeguatezza** (ove la Commissione UE abbia deciso che il Paese terzo, un territorio o uno o più settori specifici all'interno del Paese terzo, o l'organizzazione internazionale in questione garantiscono un livello di protezione adeguato; in tal caso il trasferimento non necessita di autorizzazioni specifiche);
- ✓ **trasferimento soggetto a garanzie adeguate** (il Titolare o il Responsabile del trattamento può trasferire dati personali verso un Paese terzo o un'organizzazione internazionale solo se ha fornito garanzie adeguate, come ad esempio le norme vincolanti d'impresa, le clausole contrattuali standard, l'esistenza di un codice di condotta, l'esistenza di un meccanismo di certificazione, specifiche clausole contrattuali).



TRASFERIMENTO DEI DATI PERSONALI EXTRA UE

In assenza delle suddette condizioni, il trasferimento è ammesso **soltanto** se si verifica **una** delle seguenti condizioni:

- a) l'interessato, debitamente informato, abbia **acconsentito** esplicitamente al trasferimento;
- b) il trasferimento sia necessario all'esecuzione di un **contratto** o all'esecuzione di **misure precontrattuali adottate su istanza dell'interessato**;
- c) il trasferimento sia necessario alla conclusione o esecuzione di un **contratto** stipulato tra il Titolare e un terzo **a favore dell'interessato**;
- d) il trasferimento sia necessario per importanti **motivi di pubblico interesse**;
- e) il trasferimento sia necessario per accertare, esercitare o difendere un **diritto in sede giudiziaria**;
- f) il trasferimento sia necessario per **tutelare gli interessi vitali dell'interessato o di terzi**, qualora l'interessato si trovi nell'impossibilità fisica o giuridica di prestare consenso;
- g) il trasferimento sia effettuato a partire da un **registro pubblico**.

The background of the slide is a light gray grid of small dots. Overlaid on this grid are numerous thin, wavy, light blue lines that create a sense of movement and depth. In the bottom right corner, there is a solid orange horizontal bar.

10. I diritti dell'interessato: il diritto all'oblio



DIRITTO ALL'OBLIO

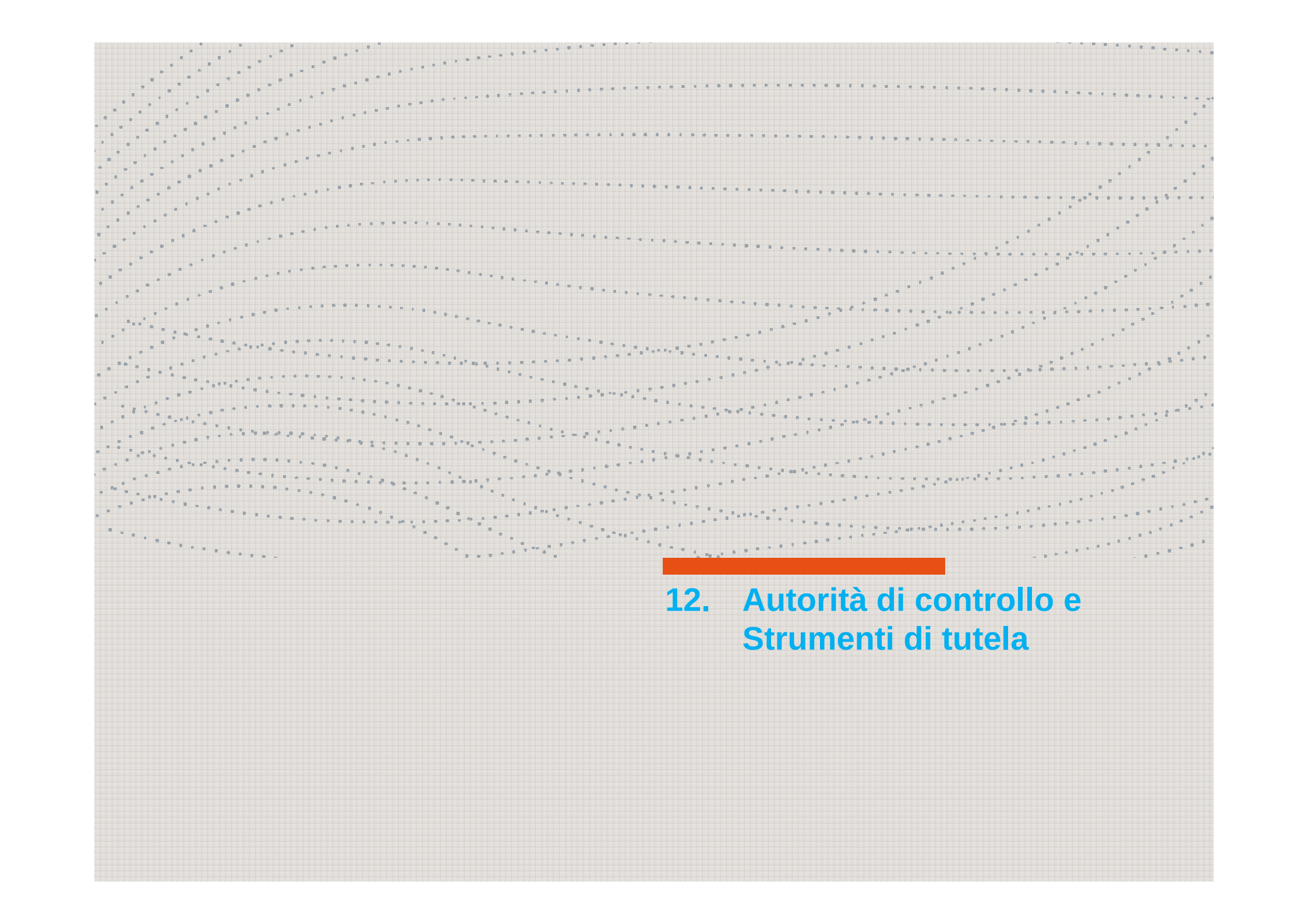
- ✓ **Oggetto:** Diritto dell'interessato ad ottenere, senza giustificato ritardo, la **cancellazione** dei propri dati personali che (i) **non siano più necessari** per le finalità per le quali sono stati raccolti o altrimenti trattati, o (ii) quando l'interessato abbia **revocato il proprio consenso**, o (iii) si sia **opposto al trattamento** dei dati personali che lo riguardano, o (iv) quando il trattamento dei suoi dati personali **non sia altrimenti conforme al Regolamento**.
- ✓ Il Titolare del trattamento che **ha pubblicato on line dati personali deve informare gli altri Titolari del trattamento che trattano tali dati personali di cancellare qualsiasi link** verso tali dati personali o copia o riproduzione di detti dati.
- ✓ Il Titolare può opporsi solo in caso di: esercizio del diritto alla libertà di espressione e di informazione; per adempiere un obbligo legale o un compito di interesse pubblico; per motivi di interesse pubblico nel settore della sanità pubblica; a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici; per accertare, esercitare o difendere un diritto in sede giudiziaria.

11. I diritti dell'interessato: il diritto alla portabilità dei dati



IL DIRITTO ALLA PORTABILITÀ DEI DATI

- ✓ **Oggetto:** diritto dell'interessato di **trasmettere o ottenere la trasmissione di propri dati personali da un Titolare del trattamento a cui li aveva forniti in precedenza ad un altro Titolare**, senza impedimenti;
- ✓ Tale diritto è esercitabile quando: (i) il trattamento è effettuato con mezzi automatizzati; e (ii) il trattamento si basa sul consenso precedentemente rilasciato dall'interessato; o (iii) il trattamento si basa su un contratto o su trattative precontrattuali in corso con l'interessato.
- ✓ L'interessato ha il diritto di **ottenere in formato strutturato**, di uso comune e leggibile da dispositivo automatico, i propri dati personali al fine di trasmetterli a un altro Titolare, ma anche il diritto di ottenere che il primo Titolare a cui ha fornito i dati, li **trasmetta direttamente** a un diverso Titolare, se tecnicamente fattibile.



12. Autorità di controllo e Strumenti di tutela



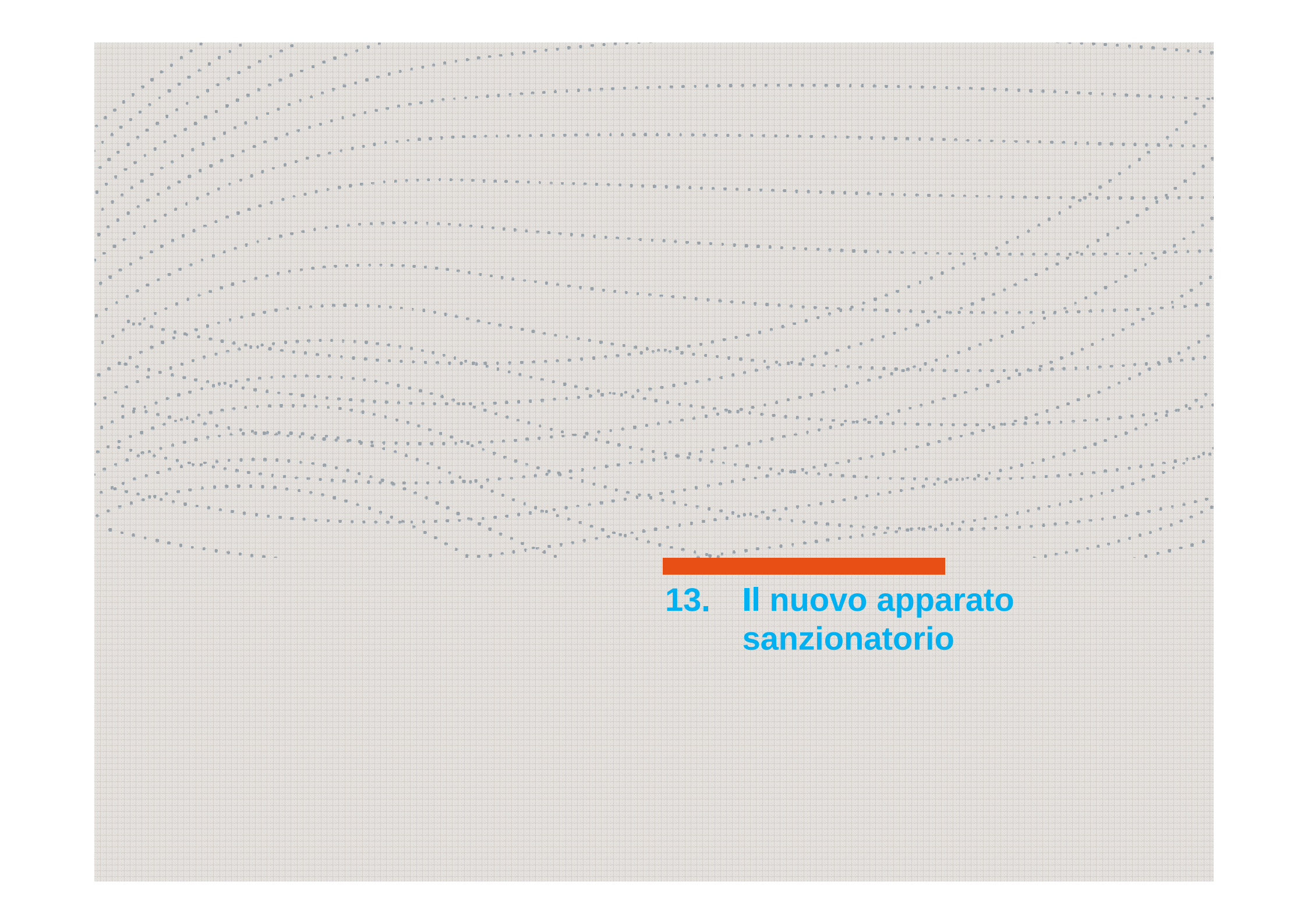
L'AUTORITÀ DI CONTROLLO

- ✓ **L'Autorità di Controllo sorveglia l'applicazione del Regolamento** al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento e di agevolare la libera circolazione dei dati personali all'interno della UE;
- ✓ Ogni Stato membro **nomina** tra le proprie autorità pubbliche indipendenti la propria Autorità di Controllo attraverso una procedura **trasparente**: in Italia, il **Garante per la protezione dei dati personali**;
- ✓ Le Autorità di Controllo dei vari Stati membri **cooperano** e si scambiano informazioni e **assistenza reciproca** per attuare e applicare il Regolamento in modo coerente;
- ✓ L'Autorità di Controllo ha **poteri di indagine, correttivi, autorizzativi, consultivi**, il cui esercizio è soggetto a garanzie adeguate. **Annualmente** deve redigere una **relazione** di attività che trasmette al Parlamento, Governo e altre autorità designate dal diritto nazionale.



STRUMENTI DI TUTELA

- ✓ **Reclamo all'Autorità di controllo** dello Stato di residenza abituale dell'interessato-reclamante o del luogo ove si è verificata la presunta violazione.
- ✓ **Ricorso giurisdizionale effettivo** avverso decisione dell'Autorità di Controllo.
- ✓ **Ricorso giurisdizionale effettivo** nei confronti del Titolare o del Responsabile del trattamento in caso di violazione di diritti tutelati dal Regolamento.



13. Il nuovo apparato sanzionatorio



RESPONSABILITÀ CIVILE

✓ Dal punto di vista **civilistico**, confermata la responsabilità risarcitoria per il c.d. “*danno da trattamento*”: l’art. 82 prescrive difatti che “*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*”.

✓ Chiariti i meccanismi di ripartizione della responsabilità risarcitoria tra Titolare e Responsabile del trattamento, e tra contitolari del trattamento (con la previsione specifica di azioni di regresso reciproche), così come i meccanismi di esonero.

:



SANZIONI AMMINISTRATIVE

1. fino a **10.000.000 EUR**, o per le imprese, fino al **2 % del fatturato mondiale totale annuo dell'esercizio precedente**, se superiore, nel caso di violazione di determinati obblighi posti dal Regolamento;
 2. fino a **20.000.000 EUR**, o per le imprese, fino al **4 % del fatturato mondiale totale annuo dell'esercizio precedente**, se superiore, nel caso di violazione degli obblighi più stringenti posti dal Regolamento (anche nel semplice caso di inosservanza degli ordini del Garante);
- ✓ Le sanzioni amministrative pecuniarie sono inflitte **in aggiunta o in luogo alle sanzioni di cui all'art. 58, par. 2, lett. da a) a h) e j) del Regolamento** (avvertimenti, ammonimenti, ingiunzioni, limitazioni ai trattamenti, ordine di cancellazione, rettifica o limitazioni del trattamento, revoca della certificazione o ingiunzione all'Organismo certificatore di ritirare o non emettere la certificazione, ordine di sospensione dei flussi di dati verso un destinatario)



SANZIONE AMMINISTRATIVA PECUNIARIA	DISPOSIZIONE VIOLATA	OBBLIGO VIOLATO (in sintesi)
Fino a 10.000.000 EUR o, per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore	Art. 8	Verifica che il consenso al trattamento sia prestato o autorizzato dal titolare della responsabilità genitoriale nel caso di offerta diretta di servizi della società dell'informazione a minori di età inferiore a 16 anni
	Art. 11	Obbligo di non conservazione, acquisizione o trattamento di informazioni per identificare l'interessato se le finalità del trattamento non richiedono o non richiedono più l'identificazione dell'interessato
	Art. 25	Adozione di misure tecniche e organizzative atte ad attuare i principi di protezione dei dati, la tutela dei diritti degli interessati e la garanzia che siano trattati, per impostazione predefinita, solo i dati necessari per ogni specifica finalità di trattamento (c.d. <i>privacy by design</i> e <i>by default</i>)
	Art. 28	Designazione del Responsabile del trattamento e rispetto degli obblighi e compiti posti a carico del Responsabile
	Art. 30	Tenuta dei Registri delle attività di trattamento
	Art. 32	Adozione di misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio
	Art. 33	Notifica di una violazione dei dati personali all'autorità di controllo
	Art. 35 e 36	Svolgimento di una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali e conseguente consultazione preventiva dell'Autorità di controllo
	Art. 37- 39	Prescrizioni in tema di designazione del Responsabile della protezione dei dati (Data Protection Officer)



SANZIONE AMMINISTRATIVA PECUNIARIA	DISPOSIZIONE VIOLATA	OBBLIGO VIOLATO (in sintesi)
Fino a 20.000.000 EUR o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore	Art. 5	Rispetto dei principi applicabili al trattamento liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza.
	Art. 6	Rispetto delle condizioni di liceità del trattamento
	Art. 7	- Dimostrazione della prestazione del consenso e del rispetto delle condizioni per il consenso. - Tutela del diritto dell'interessato di revoca del consenso
	Art. 9	Rispetto delle condizioni di liceità del trattamento di categorie particolari di dati personali
	Artt. da 12 a 22	- Obblighi informativi nei confronti dell'interessato - Tutela dei diritti dell'interessato (diritto d'accesso; di rettifica; all'oblio; di limitazione del trattamento; di notifica in caso di rettifica o cancellazione dei dati o limitazione del trattamento; alla portabilità dei dati; di opposizione ; alla profilazione consenziente)
	Artt. da 44 a 49	Obblighi connessi al trasferimento di dati personali verso Paesi terzi o organizzazioni internazionali
	Capo IX	Qualsiasi obbligo previsto dalle legislazioni degli Stati membri per specifiche situazioni di trattamento a norma del Capo IX del Regolamento
	Art. 58	Rispetto di un ordine, di una limitazione di trattamento o di un ordine di sospensione di flussi di dati dell'Autorità di controllo o di un negato accesso ai sensi dell'art. 58, par. I



Tonucci & Partners

Per approfondimenti:

Avv. Alessandro Vasta

Tonucci & Partners – www.tonucci.com

Via Trieste 31/A, Padova (PD)

049-658655

avasta@tonucci.com