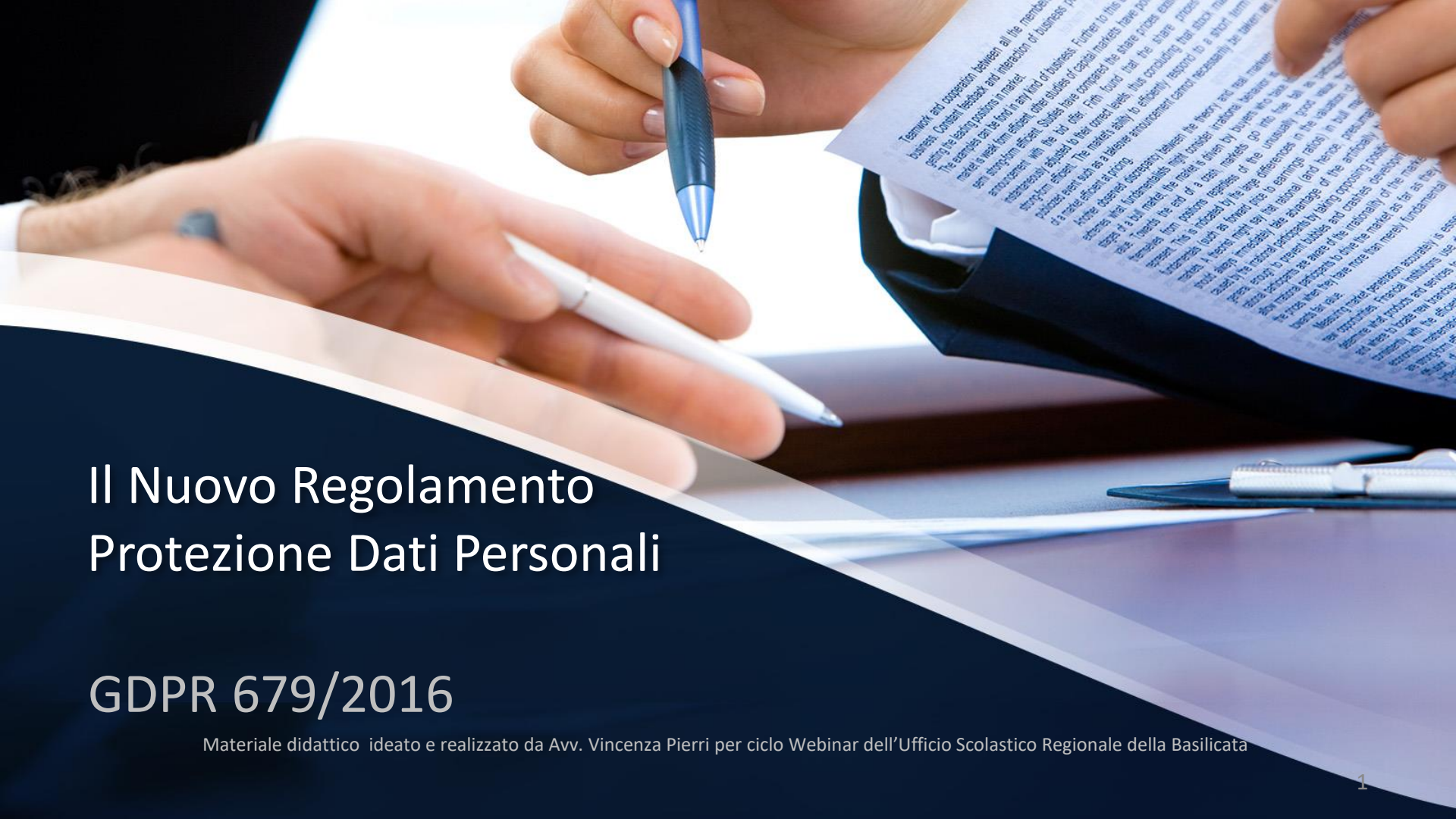


Il Nuovo Regolamento Protezione Dati Personali

GDPR 679/2016

Materiale didattico ideato e realizzato da Avv. Vincenza Pierri per ciclo Webinar dell'Ufficio Scolastico Regionale della Basilicata

Programma

- La sfida dell'accountability, anche per la scuola
- I soggetti coinvolti nel trattamento dei dati
- Il Responsabile del trattamento
- Il sub-responsabile del trattamento
- Il responsabile della protezione dei dati
- Il responsabile esterno
- I principali adempimenti
- L'aggiornamento delle informative
- La nomina e i rapporti con i responsabili del trattamento
- La tenuta del registro delle attività di trattamento
- La conduzione delle valutazioni d'impatto

L’evoluzione della normativa sulla privacy

il 24 maggio 2016 è entrato in vigore a livello di Comunità Europea il nuovo Regolamento Europeo sulla Privacy. GDPR 679/2016

Con l’integrazione del dlgs 101/2018 che di fatto ha riformato il vecchio codice privacy

Che arriva dopo

Dlgs 196/2003 Codice Protezione Dati Personali

Che arrivò dopo

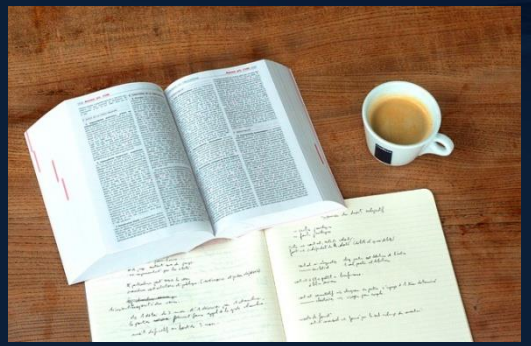
Legge 675/1996 Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali

Le definizioni

Per cominciare a confrontarsi con la normativa sulla Privacy occorre partire dalle «definizioni»

In particolare : art. 4 GDPR 679/2016

Analizzando esso possiamo trovare le prime indicazioni utili per cominciare a capire la materia



Le definizioni

«**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;

Le definizioni

«**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;

Le definizioni

«**profilazione**»: 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;

Le definizioni

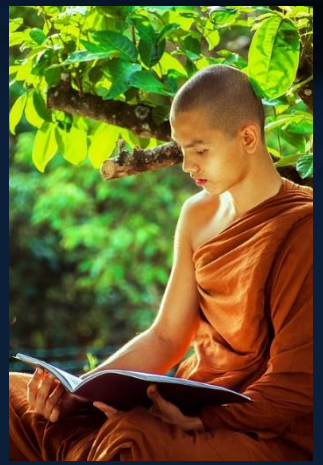
«**pseudonimizzazione**»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

«**archivio**»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

Le definizioni

«**dati particolari**»: dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici,

dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona



Le definizioni

«dati particolari»:

dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza

I soggetti

«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; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

«rappresentante»: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;

I soggetti

«**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;

Art. 29 GDPR

Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento

Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

Il regolamento europeo non prevede espressamente la figura dell'**incaricato**, ma non ne esclude la nomina, facendo riferimento a **persone autorizzate** al trattamento dei dati sotto l'autorità diretta del titolare o del responsabile.

Incaricato, o autorizzato, è il **soggetto persona fisica che effettua materialmente le operazioni di trattamento sui dati personali**.

L’Oggetto

«**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.

«**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**»: i 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

« **dati relativi alla salute**»: i 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

«archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico

Le Azioni

«violazione dei dati personali»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati

«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

«limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro

Il Responsabile del Trattamento (ART. 28 GDPR)

Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a **responsabili del trattamento** che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.

Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento…

I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento.
Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento…

il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il presente regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati

Il contratto o altro atto giuridico di cui ai paragrafi 3 e 4 è stipulato in forma scritta, anche in formato elettronico.

Il Responsabile del Trattamento (ART. 28 GDPR)

- tratta i dati personali soltanto su istruzione documentata del titolare del trattamento.
- garantisce che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza
- adotta tutte le misure richieste ai sensi dell'articolo 32
- assiste il titolare del trattamento con misure tecniche e organizzative adeguate
- su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti,

Il Responsabile del Trattamento (ART. 28 GDPR)

Il titolare del trattamento risponde della gestione effettuata dal responsabile,

È una vera e propria scelta fra quanti presentino garanzie sufficienti in termini di conoscenza specialistica,

affidabilità e risorse, per mettere in atto le misure tecniche e organizzative richieste dal Regolamento,

e che le sue decisioni siano conformi alle leggi.

Il responsabile del trattamento dovrà avere una **competenza qualificata** e risorse tecniche adeguate

GLI OBBLIGHI ?

1) Il responsabile ha **obblighi di trasparenza**. Ci sarà un contratto/atto giuridico (ad es. nomina) in tal modo il rapporto tra titolare e responsabile, sarà definito quanto gli obblighi e i limiti del trattamento dati. Il responsabile riceverà, tramite l'atto giuridico (cioè per iscritto), tutte le istruzioni in merito ai trattamenti operati per conto del titolare, alle quali dovrà attenersi.

Nell'adempiere il responsabile del trattamento dovrà mettere a disposizione del titolare (rectius documentare) tutti gli elementi che dimostrino l'adempimento degli obblighi di cui all'art. 28

2) dovrà tenere il **registro dei trattamenti svolti**

Il Responsabile del Trattamento (ART. 28 GDPR)

GLI OBBLIGHI ?

3) il responsabile ha l'obbligo di **garantire la sicurezza dei dati**. Per adempiere a ciò avrà come riferimento l'art. 32 GDPR,

tra le quali anche le misure di attuazione dei principi di privacy by design e by default, dovrà inoltre **garantire la riservatezza dei dati, vincolando i dipendenti**, dovrà informare il titolare delle violazioni avvenute, e dovrà occuparsi della cancellazione dei dati alla fine del trattamento.

4) il titolare del trattamento ed il responsabile, devono adottare le **misure tecniche ed organizzative** tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, 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.

5) il responsabile ha l'obbligo di **avvisare, assistere e consigliare il titolare**. Dovrà, quindi, consentire e contribuire alle attività di revisione, comprese le ispezioni (o audit), realizzate dal titolare del trattamento, dovrà avvisare il titolare se ritiene che un'istruzione ricevuta viola qualche norma in materia, dovrà prestare assistenza al titolare per l'evasione delle richieste degli interessati, dovrà avvisare il titolare in caso di violazioni dei dati, e assisterlo nella conduzione di una valutazione di impatto (DPIA).

Il Responsabile del Trattamento (ART. 28 GDPR)

MISURE DI SICUREZZA

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio:

- la pseudonimizzazione e la cifratura dei dati personali
- la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico
- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento

Il Responsabile del Trattamento (ART. 28 GDPR)

LE RESPONSABILITA’

Il responsabile risponde per il danno causato dal trattamento solo in caso di non corretto adempimento degli obblighi previsti dalle norme in capo al responsabile stesso, oppure se ha agito in modo difforme rispetto alla istruzioni del titolare del trattamento. ART. 82 GDPR

Il Responsabile del Trattamento (ART. 28 GDPR)

LE RESPONSABILITA'

- 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.
- Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento. Un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento.
- Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, a norma del paragrafo 2 se dimostra che l'evento dannoso non gli è in alcun modo imputabile.
- ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato.

Il Responsabile del Trattamento (ART. 28 GDPR)

LE RESPONSABILITA'

Il responsabile risponde per il danno causato dal trattamento

DANNI
- materiali
- immateriali

Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità ….se dimostra che l'evento dannoso non gli è in alcun modo imputabile.

Il Responsabile del Trattamento (ART. 28 GDPR)

LE RESPONSABILITA'

Esemplificando il responsabile potrebbe rispondere nei casi in cui:
- travalica le istruzioni del titolare;
- agisce in contrasto con le istruzioni del titolare;
- non assiste il titolare (ad esempio per le violazioni dei dati o la valutazione di impatto);
- non pone a disposizione del titolare le informazioni necessarie per un audit;
- non informa il titolare che una sua istruzione è in violazione della normativa;
- pur essendovi obbligato, non designa il DPO;
- designa un sub-responsabile non essendo stato previamente autorizzato;
- designa un sub-responsabile che non offre garanzie sufficienti;
- non tiene il registro dei trattamenti.

Il Responsabile del Trattamento (ART. 28 GDPR)

Rapporti fra Titolare e Responsabile del trattamento

I trattamenti effettuati dal Responsabile devono essere **disciplinati da una nomina** (in caso di attori della stessa organizzazione) **o da un atto giuridico (contratto** in caso di attori appartenenti ad organizzazioni diverse) **che vincoli Titolare e Responsabile** e che contenga gli accordi stabiliti tra i due attori.

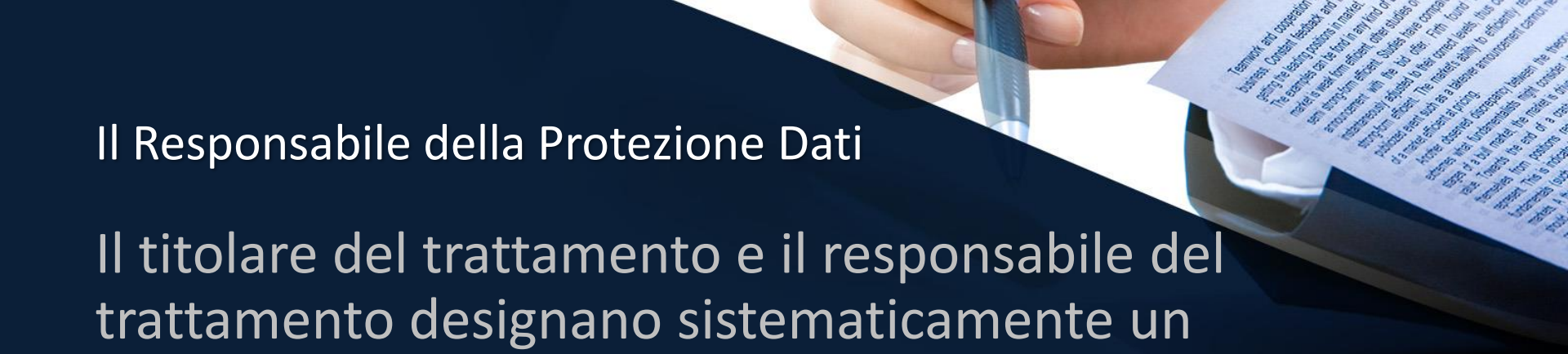
Il rapporto tra i due attori è pertanto molto stretto e definitio:

Titolare e Responsabile hanno diverse attribuzioni ma…

obblighi condivisi, **primo tra tutti la tutela dei diritti degli interessati in conformità a quanto prescritto dal Regolamento**.

Il Titolare nominerà quindi un Responsabile solo dopo averne attentamente pesato caratteristiche e competenze

il Responsabile non potrà avere un atteggiamento "passivo" ma **dovrà proattivamente collaborare, suggerire e adoperarsi affinché il trattamento a lui affidato si svolga entro confini ben definiti, con responsabilità chiare e reciprocità d'impegni**



Il Responsabile della Protezione Dati

Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta:

1) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;

2) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro 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 personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10.

I Principali Adempimenti

1) <u>Applicazione dei principi fondamentali in materia di trattamento dati</u>

I dati debbono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato.
Le finalità devono essere determinate, esplicite e legittime;
i dati: adeguati, pertinenti, esatti ed aggiornati, oltre che…
limitati a quanto necessario rispetto alle finalità, e comunque da …
trattare in modo da garantirne un'adeguata sicurezza.

Proviamo a fare degli esempi di trattamento
Contrario alla legge

I Principali Adempimenti

2) Acquisizione del consenso da parte dell'interessato e casistica di esonero dal relativo obbligo

Ciascun titolare deve distinguere i casi in cui per eseguire un trattamento è richiesto il (previo) consenso dell'interessato, da quelli in cui non è necessario acquisirlo. La richiesta del consenso deve essere presentata in modo distinto da altre richieste, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Quando per un trattamento è necessario il consenso, il titolare deve essere in grado di dimostrare che il consenso è stato effettivamente prestato.

Il che significa….che NON SEMPRE OCCORRE ACQUISIRE IL CONSENSO

I Principali Adempimenti

2) Acquisizione del consenso da parte dell'interessato e casistica di esonero dal relativo obbligo

Il che significa….che NON SEMPRE OCCORRE ACQUISIRE IL CONSENSO

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

il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;

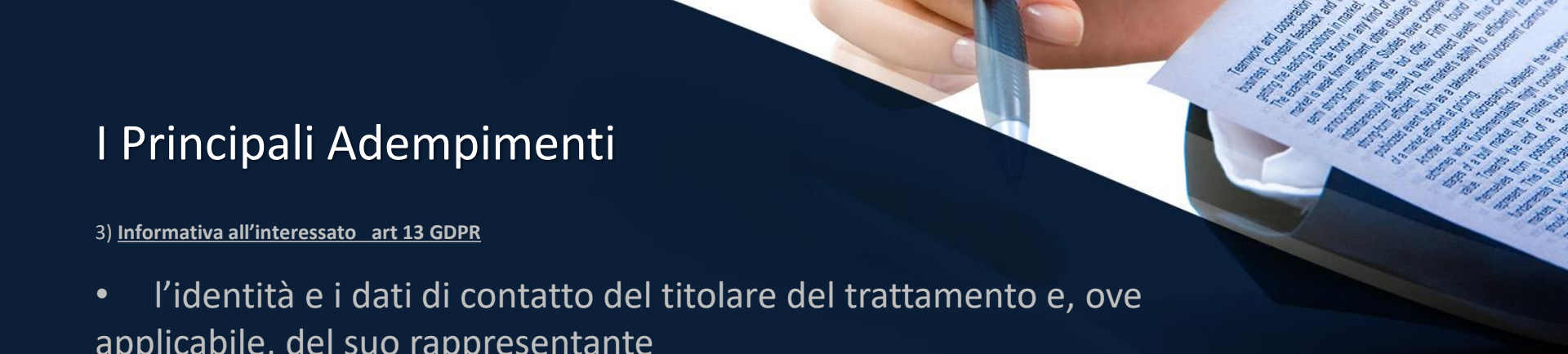
il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;

il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

I Principali Adempimenti

3) **Informativa all'interessato**

Adempimento basilare per qualsiasi titolare, si giova necessariamente di una buona capacità di analisi (in particolare) dei flussi dei trattamenti. L'informativa richiesta dal Regolamento UE è più ricca di informazioni di quella attuale e la sua redazione è operazione niente affatto banale:
Per esempio,
il titolare deve esplicitarvi il periodo di conservazione dei dati personali,
ovvero i criteri utilizzati per determinare tale periodo.
Non in ultimo, il linguaggio dell'informativa deve essere
semplice e chiaro.
Si distinguono le due fattispecie in cui la comunicazione delle informazioni è da correlare alla raccolta dei dati presso l'interessato ovvero presso un soggetto diverso.



I Principali Adempimenti

3) **Informativa all'interessato art 13 GDPR**

- l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante
- i dati di contatto del responsabile della protezione dei dati, ove applicabile
- le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento
- gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
- il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

I Principali Adempimenti

3) **<u>Il rispetto dei diritti dell'interessato</u>**

Il Regolamento formalizza un ampio catalogo di diritti che spettano all'interessato.
Si tratta del
diritto di accesso,
del diritto di rettifica,
del diritto alla cancellazione (più noto come diritto all'oblio),
diritto di limitazione del trattamento,
diritto alla portabilità dei dati,
diritto di opposizione al trattamento,
con gli eventuali connessi obblighi di notifica/comunicazione gravanti
sul titolare.

I Principali Adempimenti

4) **<u>Misure di sicurezza adeguate</u>**

Il titolare del trattamento deve adottare misure tecniche e organizzative adeguate al fine di garantire, ed essere in grado di dimostrare, la conformità del trattamento al Regolamento, tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche. Le dette misure debbono essere periodicamente riesaminate e aggiornate.

I Principali Adempimenti

4) **Misure di sicurezza adeguate**

- a) la pseudonimizzazione e la cifratura dei dati personali;
- b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

I Principali Adempimenti

5) **Progettazione della “materia Privacy”**

Privacy by Design

Tenendo conto delle specifiche caratteristiche del trattamento e dei connessi profili di rischio per i diritti e le libertà delle persone fisiche, all'atto del trattamento ovvero di determinare i mezzi del medesimo il titolare adotta misure tecniche e organizzative adeguate, in modo da attuare efficacemente i principi di protezione dei dati e da garantire nel trattamento i requisiti del Regolamento e la tutela dei diritti degli interessati.

Privacy by Default

Il titolare del trattamento attua misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ciascuna finalità del trattamento.
Obbligo che vale per la quantità dei dati raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità ai dati stessi.

I Principali Adempimenti

7) Obbligo di istruzione

Il titolare del trattamento deve previamente istruire tutti coloro che siano autorizzati ad accedere ai dati personali, compreso il responsabile del trattamento.

Il Responsabile della Protezione Dati

Il **Data Protection Officer** (DPO), o anche **Responsabile per la Protezione dei Dati** (RPD), è una figura introdotta dal nuovo regolamento europeo in materia di protezione di dati personali.

il DPO è un **consulente esperto** che va ad affiancare il titolare nella gestione delle problematiche del trattamento dei dati personali, in tal modo si garantisce che un soggetto qualificato si occupi in maniera esclusiva della materia della protezione dei dati personali, aggiornandosi sui rischi e le misure di sicurezza, in considerazione della crescente importanza e complessità del settore.

Il Responsabile della Protezione Dati

Il titolare del trattamento e il responsabile del trattamento **designano sistematicamente un responsabile della protezione dei dati** ogniqualvolta :

il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;

le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli
interessati su larga scala

le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10.

Il Responsabile della Protezione Dati

Il responsabile della protezione dei dati è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39.

Il responsabile della protezione dei dati può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi.

Il titolare del trattamento o il responsabile del trattamento pubblica i dati di contatto del responsabile della protezione dei dati e li comunica all'autorità di controllo.

Il Responsabile della Protezione Dati

Cosa fa ?

informa e fornisce consulenza al titolare del trattamento o al responsabile del trattamento

sorveglia l'osservanza del regolamento GDPR

fornisce, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati

coopera con l'autorità di controllo

Funge da punto di contatto per l'autorità di controllo per questioni connesse al trattamento

Il Responsabile della Protezione Dati

Egli gode di una particolare posizione di garanzia

Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti. Il responsabile della protezione dei dati non è rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti. Il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento.

Gli interessati possono contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento.

Il Registro dei Trattamenti

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

L'onere della tenuta del registro è – dunque - a carico del titolare e, se nominato, del responsabile del trattamento. La tenuta del registro costituisce uno dei principali elementi di accountability del titolare , in quanto è utile per una completa ricognizione e valutazione dei trattamenti svolti, e quindi finalizzato anche all' analisi del rischio e ad una corretta pianificazione dei trattamenti.

Il Registro dei Trattamenti

Tale registro contiene una serie di informazioni: ART 30 GDPR

- il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
- le finalità del trattamento;
- una descrizione delle categorie di interessati e delle categorie di dati personali;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

Il Registro dei Trattamenti

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

Il registro deve essere tenuto in **forma scritta, anche in formato elettronico**, e va esibito al Garante in caso di verifiche.
il registro deve essere
1) costantemente aggiornato.
2) Verificabile (nel senso che deve avere data certa sia per la **data della sua prima istituzione** o creazione sia per la **data dell'ultimo aggiornamento**.

Il Registro dei Trattamenti

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

esenzioni dall'obbligo ?

Gli obblighi di cui ai paragrafi 1 e 2 non si applicano alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare :

1) un rischio per i diritti e le libertà dell'interessato,
2) il trattamento non sia occasionale o
3) includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1 (razza, religione, etnia, ecc),
4) o i dati personali relativi a condanne penali e a reati di cui all'articolo 10.

E' difficile immaginare un ufficio pubblico non soggetto all'obbligo di tenere il registro

L’Informativa

L'informativa è una comunicazione rivolta all'interessato che ha lo scopo di Informare il cittadino, anche prima che diventi interessato, sulle finalità e le Modalità dei trattamenti operati dal titolare del trattamento

Essa è condizione, non tanto del rispetto del diritto individuale ad essere informato, quanto del **dovere del titolare** del trattamento di assicurare la trasparenza e correttezza dei trattamenti

L’Informativa

L'informativa è dovuta **ogni qual volta vi sia un trattamento di dati**.

L'obbligo di informare gli interessati va adempiuto prima o al massimo al momento di dare avvio alla raccolta dei dati.

Non sussiste obbligo di fornire l'informativa se il trattamento riguarda dati anonimi (es. aggregati) o dati di enti o persone giuridiche.

in alcuni casi non è necessaria l'informativa

1) i dati sono trattati in base ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria
2) il trattamento è connesso allo svolgimento delle "investigazioni difensive" in materia penale (art. 38 norme di attuazione del c.p.p.) o alla difesa di un diritto in sede giudiziaria

L’Informativa

Essa ha un contenuto mimino definito dal Regolamento Europeo (artt. 13 e 14)

Fra i più importanti elementi che essa deve contenere vi sono senz’altro:

Finalità del trattamento

Base giuridica di esso

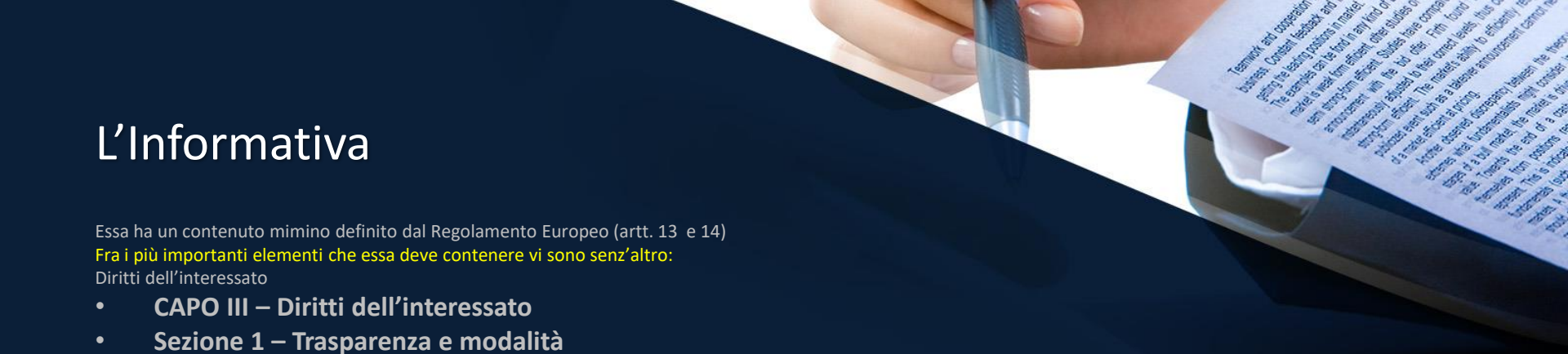
Soggetti destinatari ai quali possono essere comunicati i dati

Periodo di conservazione dei dati

Diritti dell’interessato

Presenza dei Cookie

L’Informativa



Essa ha un contenuto mimino definito dal Regolamento Europeo (artt. 13 e 14)
Fra i più importanti elementi che essa deve contenere vi sono senz’altro:
Diritti dell’interessato

- **CAPO III – Diritti dell’interessato**
- **Sezione 1 – Trasparenza e modalità**
  Articolo 12 – Informazioni, comunicazioni e modalità trasparenti per l’esercizio dei diritti dell’interessato
- **Sezione 2 – Informazione e accesso ai dati personali**
  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
- **Sezione 3 – Rettifica e cancellazione**
  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
- **Sezione 4 – Diritto di opposizione e processo decisionale automatizzato relativo alle persone fisiche**
  Articolo 21 – Diritto di opposizione
  Articolo 22 – Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione

Il Regime Sanzionatorio

Il GDPR prevede che e la violazione di talune delle norme in esso previste comporta sanzioni di diverso tipo, tra le quali anche le sanzioni pecuniarie.

In realtà le sanzioni sono specificatamente delineate dal dlgs 101/2018

Il Regime Sanzionatorio

In presenza di una violazione si possono avere diverse conseguenze:

1) l'autorità di controllo può imporre al titolare delle misure procedurali o tecniche di natura correttiva, da attuare nell'immediatezza, compreso il potere di **limitare, sospendere o addirittura bloccare i trattamenti**

Il Regime Sanzionatorio

In presenza di una violazione si possono avere diverse conseguenze:

2) Nel caso in cui la violazione comporti danni agli interessati, il titolare, insieme al responsabile del trattamento, dovrà provvedere al risarcimento dei danni, materiali e morali

Il Regime Sanzionatorio

Sanzioni correttive

- rivolgere **avvertimenti** al titolare o al responsabile del trattamento sul fatto che i trattamenti previsti possono violare le norme;
- rivolgere **ammonimenti** al titolare o al responsabile del trattamento ove i trattamenti abbiano violato le norme;
- **ingiungere** al titolare o al responsabile del trattamento di soddisfare le richieste dell'interessato di esercitare i relativi diritti;
- **ingiungere** al titolare o al responsabile del trattamento di conformare i trattamenti alle norme, specificando eventualmente le modalità e i termini per la conformità;

Il Regime Sanzionatorio

Sanzioni correttive

- imporre una **limitazione provvisoria o definitiva** al trattamento, sospendere temporaneamente il trattamento, o vietare del tutto;
- ordinare la **rettifica, la cancellazione o l'aggiornamento** dei dati personali
- revocare le certificazioni o ingiungere all'organismo di certificazione di ritirare le certificazioni rilasciate se i requisiti non sono soddisfatti
- infliggere le sanzioni amministrative pecuniarie; ordinare la sospensione dei flussi di dati verso un destinatario in un paese terzo o un'organizzazione internazionale.

Il Regime Sanzionatorio

In presenza di una violazione si possono avere diverse conseguenze:

4) la violazione può portare all'applicazione di **eventuali sanzioni penali**, se lo Stato si è avvalso della possibilità di introdurre tali sanzioni all'interno Del suo ordinamento

Il Regime Sanzionatorio

eventuali sanzioni penali, casistica:

- il trattamento illecito dei dati
- la comunicazione e la diffusione illecita di dati personali oggetto di trattamento su larga scala
- l'acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala
- la falsità nelle dichiarazioni al garante
- l'interruzione dell'esecuzione di compiti e poteri del garante
- l'inosservanza dei provvedimenti del garante

Il Regime Sanzionatorio

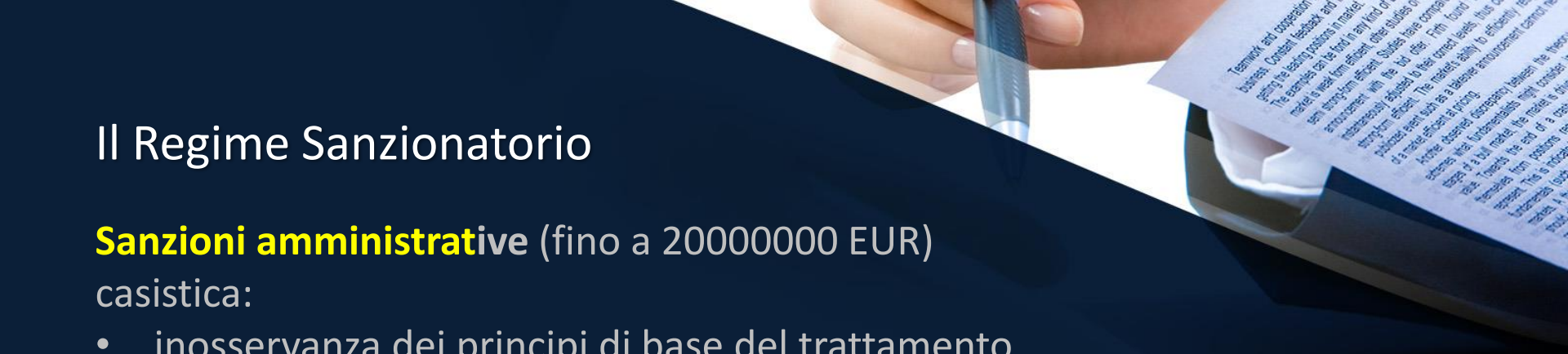
In presenza di una violazione si possono avere diverse conseguenze:

3) la violazione può portare all'applicazione di **sanzioni amministrative** da parte dell'autorità di controllo

Il Regime Sanzionatorio

Sanzioni amministrative (fino a 10000000 EUR) casistica:

1) Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione (ad es. social network);
2) Trattamento che non richiede l'identificazione
3) Inadempimenti per gli oneri da 25 a 39
4) Certificazione



Il Regime Sanzionatorio

Sanzioni amministrative (fino a 20000000 EUR)
casistica:

- inosservanza dei principi di base del trattamento, comprese le condizioni relative al consenso, a degli articoli 5, 6, 7 e 9;
- inosservanza dei diritti degli interessati a norma degli articoli da 12 a 22
- inosservanza dei trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale a norma degli articoli da 44 a 49

Grazie per l’attenzione

Credits & Contacts

Il presente materiale didattico è opera intellettuale dell'avv. Vincenza Pierri concessa in uso gratuito per l'Ufficio Scolastico Regionale per la Basilicata

Ogni altro utilizzo è riservato

Si indicano e ringraziano quali fonti:

https://www.cyberlaws.it/2017/articolo-4-gdpr-regolamento-generale-sulla-protezione-dei-dati-ue2016679/

https://protezionedatipersonali.it/responsabile-del-trattamento

https://www.puntosicuro.it/security-C-124/privacy-C-89/privacy-titolare-responsabile-un-rapporto-chiaro-stretto-AR-16323/

Tutte le immagini sono royalty free e si ringrazia la fonte

https://pixabay.com/it/

Per Contatti

enpierri@gmail.com (Data Protection Officer presso Comune di Salerno, Comune di Siano (Sa) , Conservatorio Cimarosa Avellino)

giordalfonso@gmail.com (funzionario direttore Ministero Interno)