

INCONTRO DI FORMAZIONE

Corneliano d'Alba – 2 luglio 2020

LA PRIVACY NELL'ENTE LOCALE

ELEMENTI BASE PER LA CORRETTA APPLICAZIONE DEL REG EU 679/16
NEI COMUNI DI CORNELIANO E PIOBESI D'ALBA

Avv. Marco Galvagno – il DPO dell'Ente

registro di certificazione KHC DPO2455 scad. 15.01.2023

Tutti i diritti sono riservati . E' consentita la sola lettura.
E' vietato ogni tipo di riproduzione anche solo parziale.

PROGRAMMA

1° Modulo

IL NUOVO REGOLAMENTO EUROPEO

CONTESTO NORMATIVO

AMBITO DI APPLICAZIONE

DEFINIZIONI

PRINCIPI

DIRITTI DELL'INTERESSATO

ATTORI

2° Modulo

I PRINCIPALI ADEMPIMENTI

INFORMATIVE

CONSENSO INFORMATO

REGISTRO DEI TRATTAMENTI

NOMINA DEL DPO

DPIA

ALTRI STRUMENTI DI ACCOUNTABILITY

SCHEMI RIASSUNTIVI (DIFFERENZE TRA IL VECCHIO 196/03 e GDPR)

Modulo 1

IL NUOVO REGOLAMENTO EUROPEO

CONTESTO NORMATIVO

AMBITO DI APPLICAZIONE

DEFINIZIONI

PRINCIPI

DIRITTI DELL'INTERESSATO

ATTORI

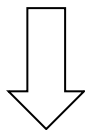


REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)

Direttiva UE/2016/680 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati



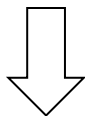
REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.



**25
Maggio
2018**

ENTRATA IN VIGORE

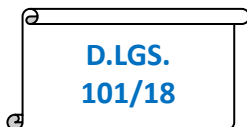
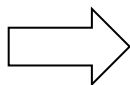
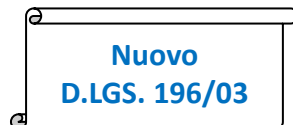
Pubblicato sulla Gazzetta Ufficiale dell'Unione Europea (GUUE) il 4 maggio 2016 - è applicabile in via diretta in tutti i Paesi UE dal 25 maggio 2018.



**19
settembre
2018**

ENTRATA IN VIGORE della NORMATIVA di ARMONIZZAZIONE

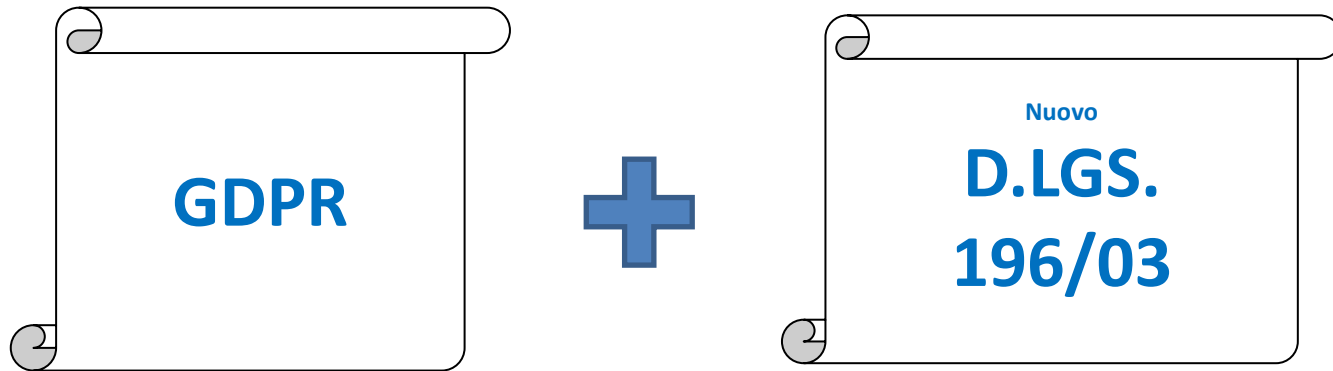
D.Lgs 10 Agosto 2018 n. 101, pubblicato sulla Gazzetta Ufficiale il 4 settembre 2018 - è applicabile dal 19 settembre 2018.



GDPR

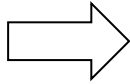


Nuovo
**D.LGS.
196/03**



QUANDO SI APPLICANO?

- Art. 1 – OGGETTO
- Art. 2 - MATERIALE
- Art. 3 - TERRITORIALE



SI APPLICA

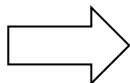
PROTEZIONE



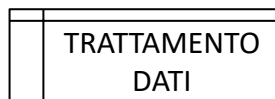
PERSONE FISICHE

Capo I
Disposizioni Generali

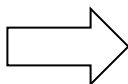
2. Ambito di
applicazione
materiale



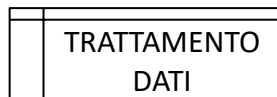
SI APPLICA



AUTOMATIZZATO



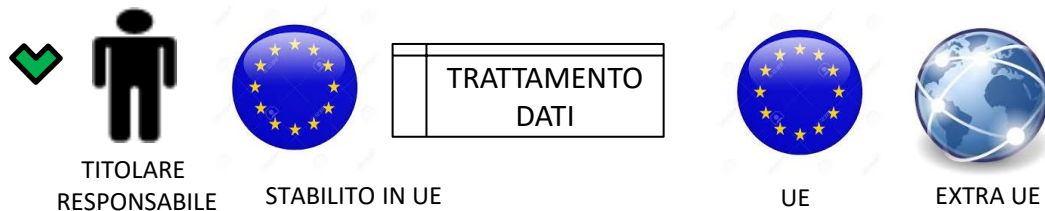
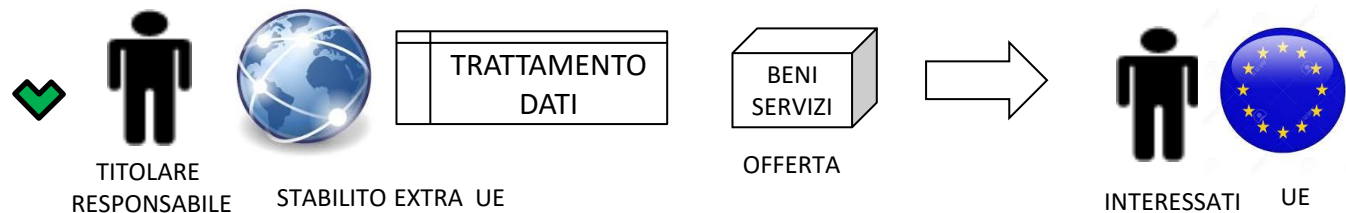
NON SI APPLICA

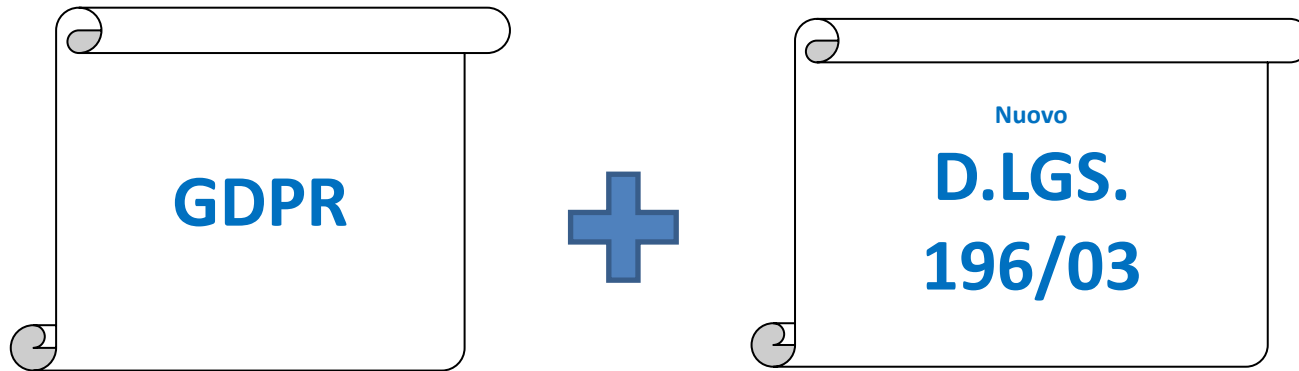


FINALITA'
PERSONALE O DOMESTICO



FINALITA'
ISTITUZIONALI





Art. 4 - DEFINIZIONI:

- **DATO PERSONALE**
- **TRATTAMENTO**

Dato Personale

***“... qualsiasi informazione
riguardante una **persona fisica**
identificata o identificabile, ...”***

Art. 4

GDPR

D.LGS.
196/03

DEFINIZIONI

Natura dei Dati

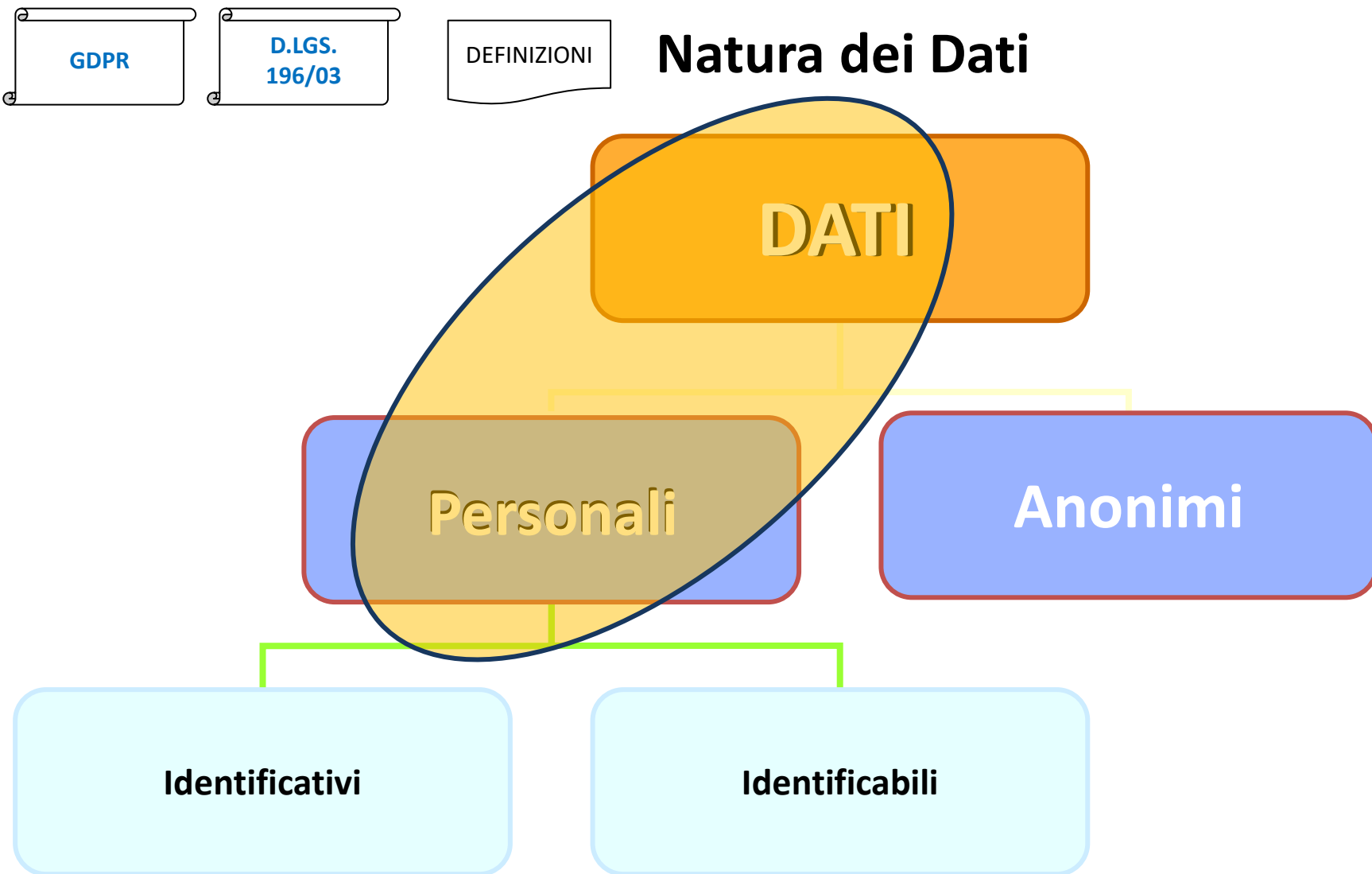
DATI

Personali

Anonimi

Identificativi

Identificabili

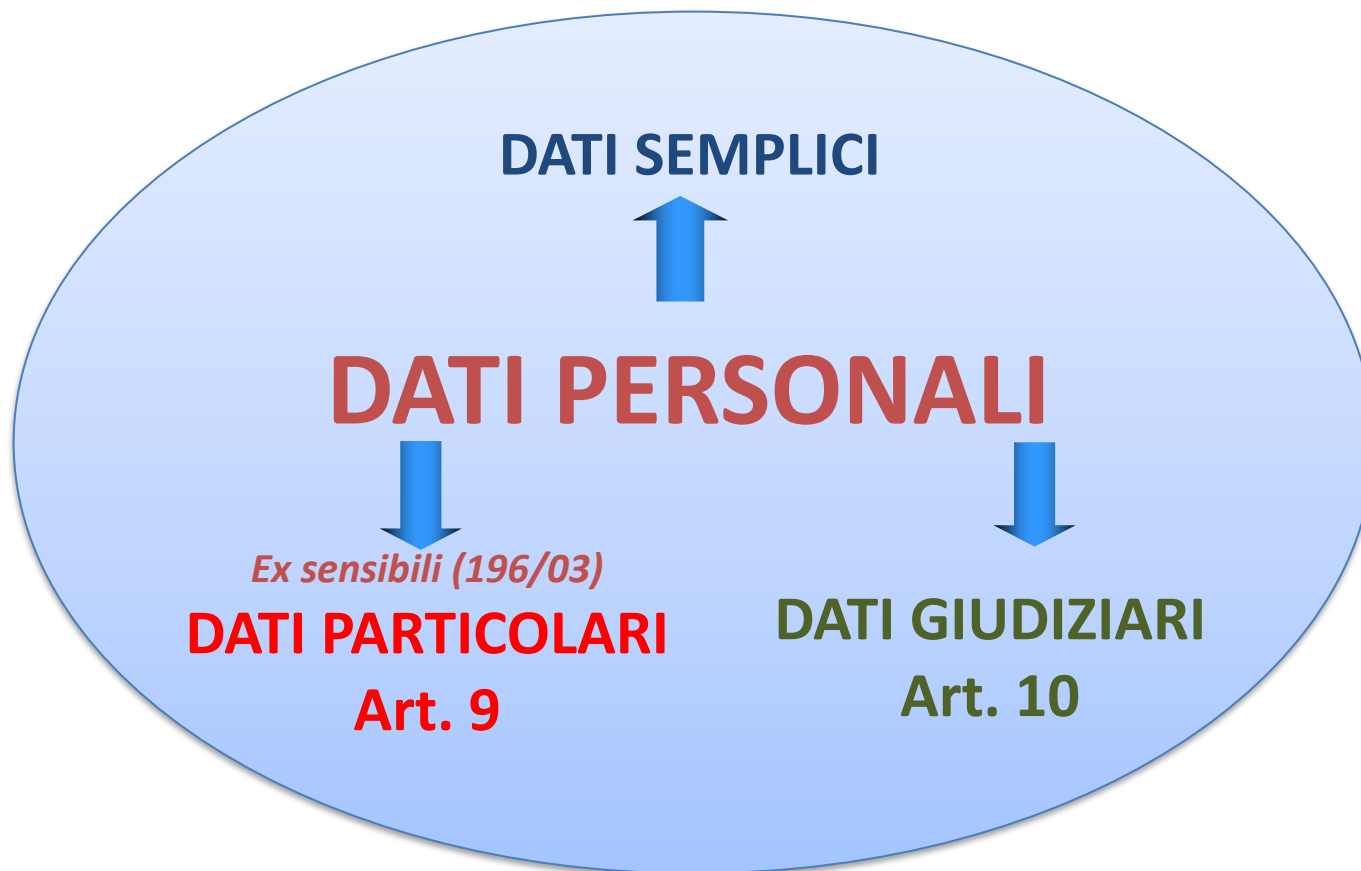


GDPR

D.LGS.
196/03

DEFINIZIONI

Natura dei Dati



Dati Particolari (art. 9)

Tutti i dati personali **che rivelano:**

- Origine razziale o etnica,
- Opinioni politiche,
- Convinzioni religiose o filosofiche,
- Appartenenza sindacale,
- **Dati genetici art. 4,**
- **Dati Biometrici art. 4,**
- Dati relativi alla salute,
- Vita o orientamento sessuale.



DEFINIZIONI

Trattamento

“... qualsiasi operazione o insieme di operazioni ... applicate a dati personali ...”

Art. 4



Esempi di Trattamento

- Raccolta
- Registrazione
- Organizzazione
- Strutturazione
- Conservazione
- Elaborazione
- Modifica
- Estrazione
- Consultazione
- Uso
- Raffronto
- Interconnessione
- Blocco
- Comunicazione
- Diffusione
- Cancellazione
- Distruzione
- Limitazione
- **Profilazione**

“... a) "comunicazione", il dare conoscenza dei dati personali a uno o piu' soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate, ai sensi dell'articolo 2-*quaterdecies*, al trattamento dei dati personali sotto l'autorita' diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione; ...”

**Art. 2-ter
d.lgs 196/03**

DEFINIZIONI

Comunicazione

“... b) "diffusione", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

*Art. 2-ter d.lgs 196/03 (Base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri) *art. introdotto dal d.lgs 101/18*



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; ...”

Art. 4 GDPR



Principi applicabili al trattamento dei dati personali (art. 5)

I dati personali devono essere trattati secondo i principi di:

- Liceità,
- Correttezza,
- Trasparenza,
- Limitazione delle finalità,
- Minimizzazione dei dati,
- Esattezza,
- Limitazione della conservazione,
- Integrità,
- Riservatezza,
- Responsabilizzazione.



Liceità del trattamento

Art. 6 – dati personali (semplici)

Il trattamento è lecito solo se ricorre almeno una delle seguenti condizioni:

- a) l'interessato ha espresso il **consenso** al trattamento dei propri dati personali per una o più specifiche finalità;
- b) 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;
- c) il trattamento è necessario per adempiere un **obbligo legale** al quale è soggetto il titolare del trattamento;
- d) il trattamento è necessario per la **salvaguardia degli interessi vitali** dell'interessato o di un'altra persona fisica;
- e) 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 (Art. 2 ter del Dlgs. 196/2003);
- f) SOLO PER PRIVATI – **legittimo interesse**.



Liceità del trattamento

Art. 9 – dati particolari

Il trattamento è vietato a meno che :

- a) l'interessato abbia prestato il proprio **consenso esplicito** al trattamento di tali dati personali **per una o più finalità specifiche**;
- b) il trattamento sia necessario per **assolvere gli obblighi** ed **esercitare i diritti** in materia di **diritto del lavoro e della sicurezza sociale e protezione sociale**;
- c) il trattamento sia necessario per **tutelare un interesse vitale** dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
- d) il trattamento sia effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro (in casi particolari);
- e) il trattamento riguardi dati personali resi manifestamente pubblici dall'interessato;

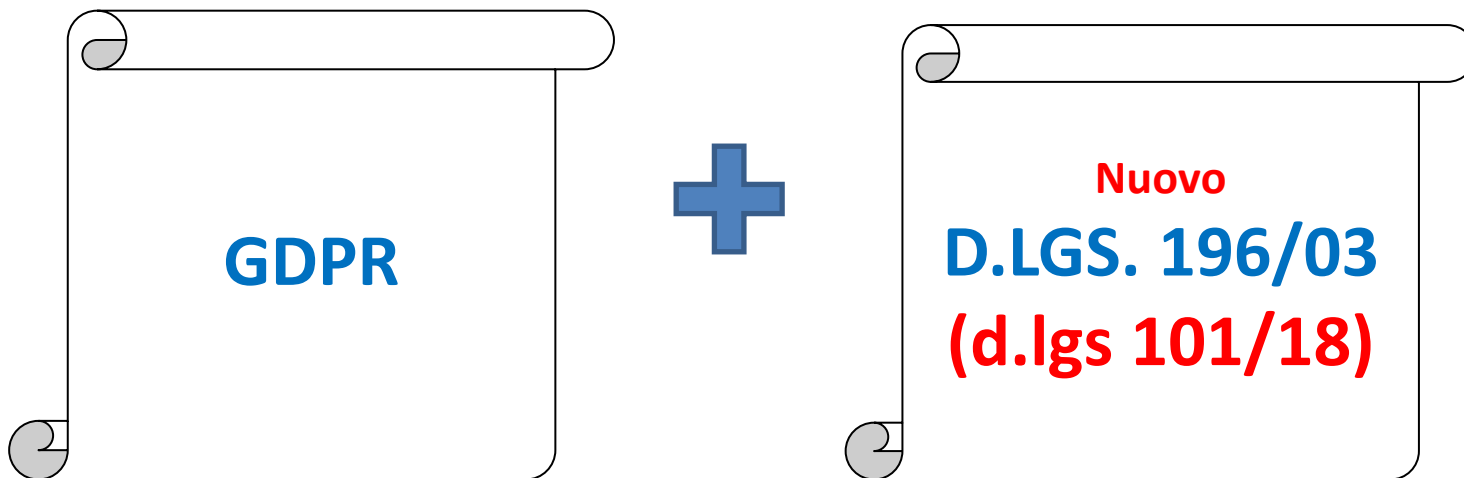
Liceità del trattamento

Art. 9 – dati particolari

Il trattamento è vietato a meno che:

- f) il trattamento sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o (...) vengano esercitate funzioni giurisdizionali;
- g) il trattamento è **necessario per motivi di interesse pubblico rilevante**, ...
proporzionato alla finalità perseguita ([art. 2 – sexies d.lg.s 196/03](#));
- h) il trattamento è necessario per finalità di **medicina preventiva o di medicina del lavoro**;
- i) il trattamento è necessario per motivi di **interesse pubblico nel settore della sanità pubblica**;
- j) il trattamento è necessario a fini di **archiviazione nel pubblico interesse, di ricerca scientifica o storica**;

NEW



art. 2 – sexies

Trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante

1. I trattamenti delle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, del Regolamento, necessari per motivi di interesse pubblico rilevante ai sensi del paragrafo 2, lettera g), del medesimo articolo, sono ammessi qualora siano previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o, nei casi previsti dalla legge, di regolamento che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

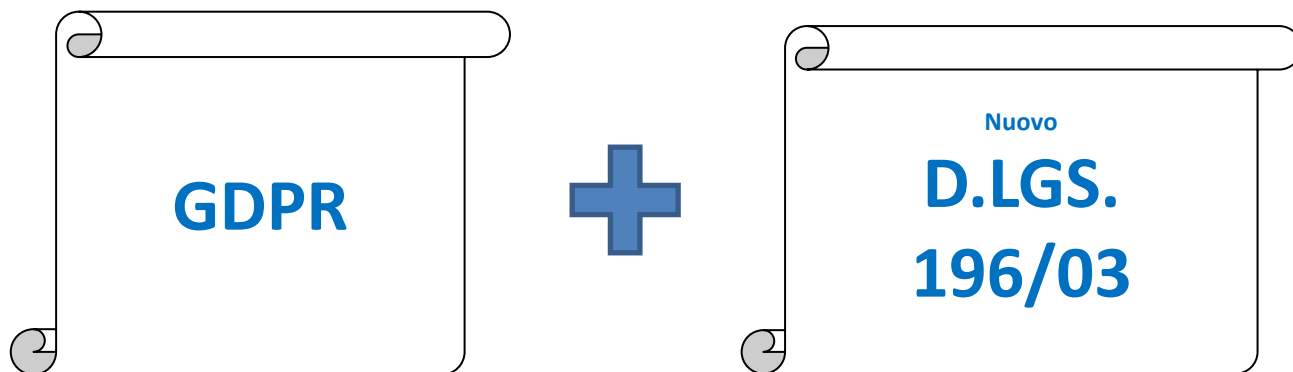
2. Fermo quanto previsto dal comma 1, si considera rilevante l'interesse pubblico relativo a trattamenti effettuati da soggetti che svolgono compiti di interesse pubblico o connessi all'esercizio di pubblici poteri nelle seguenti materie:

- a) accesso a documenti amministrativi e accesso civico;
- b) tenuta degli atti e dei registri dello stato civile, delle anagrafi della popolazione residente in Italia e dei cittadini italiani residenti all'estero, e delle liste elettorali, nonché rilascio di documenti di riconoscimento o di viaggio o cambiamento delle generalità;
- c) tenuta di registri pubblici relativi a beni immobili o mobili;
- d) tenuta dell'anagrafe nazionale degli abilitati alla guida e dell'archivio nazionale dei veicoli;
- e) cittadinanza, immigrazione, asilo, condizione dello straniero e del profugo, stato di rifugiato;
- f) elettorato attivo e passivo ed esercizio di altri diritti politici, protezione diplomatica e consolare, nonché documentazione delle attività istituzionali di organi pubblici, con particolare riguardo alla redazione di verbali e resoconti dell'attività di assemblee rappresentative, commissioni e di altri organi collegiali o assembleari;
- g) esercizio del mandato degli organi rappresentativi, ivi compresa la loro sospensione o il loro scioglimento, nonché l'accertamento delle cause di ineleggibilità, incompatibilità o di decadenza, ovvero di rimozione o sospensione da cariche pubbliche;
- h) svolgimento delle funzioni di controllo, indirizzo politico, inchiesta parlamentare o sindacato ispettivo e l'accesso a documenti riconosciuto dalla legge e dai regolamenti degli organi interessati per esclusive finalità direttamente connesse all'espletamento di un mandato elettivo;
- i) attività dei soggetti pubblici dirette all'applicazione, anche tramite i loro concessionari, delle disposizioni in materia tributaria e doganale;
- l) attività di controllo e ispettive;
- m) concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti e abilitazioni;

- n) conferimento di onorificenze e ricompense, riconoscimento della personalita' giuridica di associazioni, fondazioni ed enti, anche di culto, accertamento dei requisiti di onorabilita' e di professionalita' per le nomine, per i profili di competenza del soggetto pubblico, ad uffici anche di culto e a cariche direttive di persone giuridiche, imprese e di istituzioni scolastiche non statali, nonche' rilascio e revoca di autorizzazioni o abilitazioni, concessione di patrocinii, patronati e premi di rappresentanza, adesione a comitati d'onore e ammissione a cerimonie ed incontri istituzionali;
- o) rapporti tra i soggetti pubblici e gli enti del terzo settore;
- p) obiezione di coscienza;
- q) attivita' sanzionatorie e di tutela in sede amministrativa o giudiziaria;
- r) rapporti istituzionali con enti di culto, confessioni religiose e comunita' religiose;
- s) attivita' socio-assistenziali a tutela dei minori e soggetti bisognosi, non autosufficienti e incapaci;
- t) attivita' amministrative e certificatorie correlate a quelle di diagnosi, assistenza o terapia sanitaria o sociale, ivi incluse quelle correlate ai trapianti d'organo e di tessuti nonche' alle trasfusioni di sangue umano;
- u) compiti del servizio sanitario nazionale e dei soggetti operanti in ambito sanitario, nonche' compiti di igiene e sicurezza sui luoghi di lavoro e sicurezza e salute della popolazione, protezione civile, salvaguardia della vita e incolumita' fisica;
- v) programmazione, gestione, controllo e valutazione dell'assistenza sanitaria, ivi incluse l'instaurazione, la gestione, la pianificazione e il controllo dei rapporti tra l'amministrazione ed i soggetti accreditati o convenzionati con il servizio sanitario nazionale;
- z) vigilanza sulle sperimentazioni, farmacovigilanza, autorizzazione all'immissione in commercio e all'importazione di medicinali e di altri prodotti di rilevanza sanitaria;

- aa) tutela sociale della maternita' ed interruzione volontaria della gravidanza, dipendenze, assistenza, integrazione sociale e diritti dei disabili;
- bb) istruzione e formazione in ambito scolastico, professionale, superiore o universitario;
- cc) trattamenti effettuati a fini di archiviazione nel pubblico interesse o di ricerca storica, concernenti la conservazione, l'ordinamento e la comunicazione dei documenti detenuti negli archivi di Stato negli archivi storici degli enti pubblici, o in archivi privati dichiarati di interesse storico particolarmente importante, per fini di ricerca scientifica, nonche' per fini statistici da parte di soggetti che fanno parte del sistema statistico nazionale (Sistan);
- dd) instaurazione, gestione ed estinzione, di rapporti di lavoro di qualunque tipo, anche non retribuito o onorario, e di altre forme di impiego, materia sindacale, occupazione e collocamento obbligatorio, previdenza e assistenza, tutela delle minoranze e pari opportunita' nell'ambito dei rapporti di lavoro, adempimento degli obblighi retributivi, fiscali e contabili, igiene e sicurezza del lavoro o di sicurezza o salute della popolazione, accertamento della responsabilita' civile, disciplinare e contabile, attivita' ispettiva.

3. Per i dati genetici, biometrici e relativi alla salute il trattamento avviene comunque nel rispetto di quanto previsto dall'articolo 2-septies.



I SOGGETTI:

- Titolare
- Responsabile
- Addetto
- **Data Protection Officer (DPO)**



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; ...”*

Art. 4



Obblighi del titolare del trattamento

- **Responsabilità:** mettere in atto le misure tecniche e organizzative adeguate per garantire ed essere in grado di dimostrare, che il trattamento è conforme al GDPR;
- **Privacy by design:** mettere in atto misure tecniche e organizzative adeguate sia al momento di determinare i mezzi del trattamento, sia all'atto del trattamento stesso;
- **Privacy by default:** mettere in atto misure tecniche ed organizzative adeguate per impostazione predefinita

Cotitolari del trattamento

*“...due o più titolari del trattamento che determinano congiuntamente le **finalità** e i **mezzi** del trattamento.*

Essi determinano mediante un accordo interno le rispettive responsabilità...”

Art. 26



DEFINIZIONI

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. 4



Obblighi del responsabile del trattamento

- Deve garantire di mettere in atto misure tecniche ed organizzative adeguate;
- Non può ricorrere ad un altro responsabile senza previa autorizzazione del Titolare del trattamento;
- I suoi trattamenti devono essere disciplinati da un contratto o da un altro atto giuridico



DPO (**Data Protection Officer**)

Responsabile della protezione dei 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. ...”

Art. 37



DPO (Data Protection Officer)

Responsabile della protezione dei dati



COMPITI:

- a) informare e fornire consulenza al titolare del trattamento;
- b) sorvegliare l'osservanza della normativa in materia di privacy;
- c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati;
- d) cooperare con l'autorità di controllo;
- e) fungere da punto di contatto per l'autorità di controllo.



DPO (Data Protection Officer)

Responsabile della protezione dei dati



La DESIGNAZIONE è obbligatoria quando:

- a) Se il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico
- b) Se 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;
- c) Se 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.

Gli autorizzati al trattamento

le persone che operano sotto la diretta autorità del titolare o del responsabile del trattamento previamente autorizzate

Art. 2 - quaterdecies



Gli autorizzati al trattamento

**L'addetto “...non può trattare tali dati se
non è istruito ...”**

Art. 29 GDPR

I PRINCIPALI ADEMPIMENTI

- Informativa
- Consenso informato
- **Registro dei trattamenti**
- **Nomina del DPO**
- **DPIA**
- Nomina dei Responsabili e autorizzati
- ~~Misure minime di sicurezza (all. B)~~
- **Altri strumenti di Accountability**

NEW

NEW

NEW

NEW

Modulo 2

I PRINCIPALI ADEMPIMENTI

INFORMATIVE

CONSENSO INFORMATO

REGISTRO DEI TRATTAMENTI

NOMINA DEL DPO

DPIA

STRUMENTI DI ACCOUNTABILITY (documenti e procedure)

SCHEMI RIASSUNTIVI (DIFFERENZE TRA IL VECCHIO

196/03 e GDPR)



I PRINCIPALI ADEMPIMENTI

- **Informativa**



L'INFORMATIVA Art.13

Quando i dati sono raccolti presso l'interessato deve contenere:

- Identità e **dati di contatto** del Titolare;
- **Dati di contatto del DPO;**
- Finalità del trattamento;
- **Condizione di liceità:** base giuridica o legittimo interesse (privati);
- Eventuali destinatari o categorie di destinatari;
- **modalità del trattamento;**
- Periodo di conservazione;
- Diritti spettanti all'interessato;
- Facoltà di proporre reclamo ex art.77;
- Diritto di revoca del consenso (solo se è condizione di liceità);
- Natura obbligatoria o meno e conseguenze di un eventuale rifiuto;
- **l'ambito di diffusione dei dati;**
- Eventuale processo automatizzato.



Quando? Al momento della raccolta.



L'INFORMATIVA Art. 14

Quando i dati sono raccolti presso terzi deve contenere:

- Identità e **dati di contatto** del Titolare;
- **Dati di contatto del DPO;**
- Finalità del trattamento;
- **Categorie di dati personali;**
- **Condizione di liceità:** base giuridica o legittimo interesse (privati);
- **modalità del trattamento**
- Destinatari o eventuali categorie di destinatari;
- Periodo di conservazione;
- Diritti spettanti all'interessato;
- Diritto di revoca del consenso;
- L'ambito di diffusione dei dati;
- Facoltà di proporre reclamo ex art. 77;
- La fonte (con indicazione se trattasi di fonte accessibile al pubblico);
- Eventuale processo automatizzato.



Quando? entro 1 mese dall'ottenimento, al primo contatto, alla prima comunicazione a terzi.

I PRINCIPALI ADEMPIMENTI

Consenso informato

ATTENZIONE!

**L'ENTE LOCALE NON RICORRE QUASI MAI
AL CONSENSO**



CONSENSO INFORMATO

Qualora il trattamento sia basato sul **consenso** dell'interessato, nell'informativa:

- Il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso;
- La richiesta deve essere fatta utilizzando un linguaggio chiaro e semplice;
- L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento.

I PRINCIPALI ADEMPIMENTI

- **Registro dei trattamenti**

A small, tilted rectangular tag with a black border and a white background, containing the word "NEW" in red capital letters.
NEW



REGISTRO DEI TRATTAMENTI

Chi ha l'obbligo di tenerlo:

- Ogni Titolare per le attività di trattamento svolte sotto la propria responsabilità,
- Ogni Responsabile del trattamento per le categorie di attività svolte per conto di un titolare

Qualora siano:

- Enti o organizzazioni >250 dip.
- Tutti i sogg. che effettuano trattamenti non occasionali che possono essere rischiosi per diritti e libertà dell'interessato o includano dati particolari.

IL REGISTRO DEI TRATTAMENTI

*Estratto del Registro
Comune di San Damiano D'Asti*

Consenso degli Interessati: NO									
Categorie di destinatari a cui i dati sono o possono essere comunicati: Dipendenti formalmente nominati ed autorizzati al trattamento									
Analisi dei rischi e valutazione d'impatto sulla protezione dei dati personali e AI: 2) di descrizione generale: documentazione in fase di stesura a cura di SAT scari Sistemi Informativi									
REGISTRO DEI TRATTAMENTI									
Unità Organizzativa	Denominazione del trattamento	Finalità del trattamento	Contenitori di dati e loro ubicazione	Categorie di interessati	Categorie di dati personali	Categorie di destinatari a cui i dati sono o possono essere comunicati	Denominazione responsabili esterni (se presenti)	Descrizione generale delle misure di sicurezza adottate	Tipologia
	ACCERTAMENTI IM- ESPORTE E SEGNALAZIONI	Attività di controllo e ispezioni, vigilanza edilizia, tutela pubblica e privata incolumità, vigilanza ambientale e ordine	archivio corrente armati su sede di via Alcide 36 archivio deposito su via Gianone, data center	cittadini, professionisti, imprenditori	dati identificativi delle persone, delle proprietà, sanitari e giudiziali	cittadini, imprese, consulenti professionisti dell'interessato, P.A., servizio di giustizia e di polizia	SAT scari (sistemi informatici tecnici)	sicurezza informatica (vd documento SAT scari allegato 2) sicurezza edilizia (allegato 3)	
	SANZIONI CODICE DELLA STRADIA	Applicazione codice della strada	archivio corrente presso armadi di via Italia 40 bis, archivio deposito presso via Gianone, data center e data center Haggoli archivio corrente	cittadini e imprese	dati identificativi relativi alla proprietà del veicolo e ai conducitori	proprietari del veicolo e se- dienstori e conducenti Motorizzazione, Prefettura	SAT scari (sistemi informatici tecnici), Haggoli SpA, Traffic Technology srl, Fisite balance, Defender	sicurezza informatica (vd documento SAT scari allegato 2) sicurezza edilizia (allegato 3)	
					dati identificativi relativi utenti della				

- 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
- i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- una descrizione generale delle misure di sicurezza tecniche e organizzative



I PRINCIPALI ADEMPIMENTI

- **Nomina del DPO**



I PRINCIPALI ADEMPIMENTI

- **DPIA**

DPIA (Data Protection Impact Assessment o valutazione d'impatto)

strumento con il quale il titolare del trattamento conduce **un'analisi dei rischi** ed effettua una valutazione dell'impatto delle varie attività di trattamento di dati personali sui diritti degli interessati.

DPIA (QUANDO DEVE ESSERE CONDOTTA?)

- a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;*
- b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o*
- c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.*



GDPR

I PRINCIPALI ADEMPIMENTI

- **Altri strumenti di Accountability
(documenti e procedure)**



Altri strumenti di Accountability

(organizzazione, documenti e procedure)

Esempio 1:

LA FORMAZIONE

Deve essere documentata (materiale, test di apprendimento, registrazioni, ecc...)

Esempio 2:

LA GESTIONE DEGLI INCIDENTI

Occorre prevedere una procedura adeguata e documentata (buone prassi, procedure, FAQ, formazione, esercitazioni, test, ecc...)

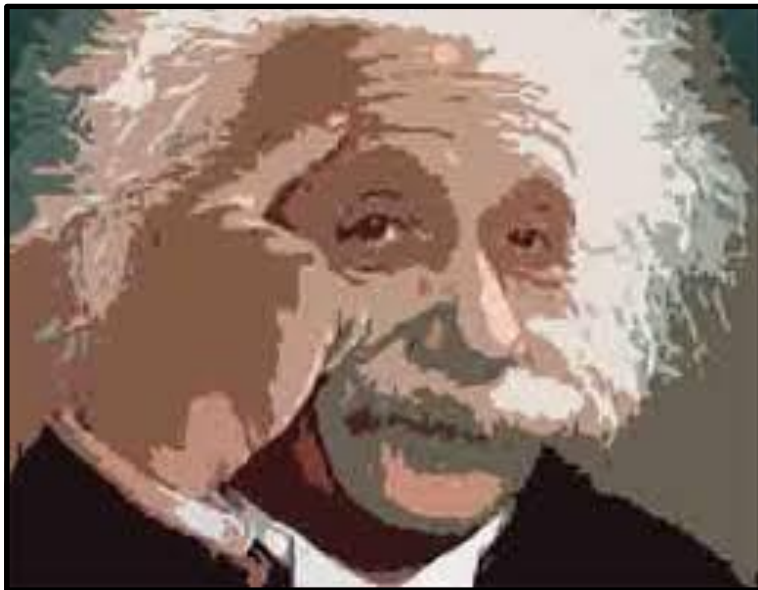
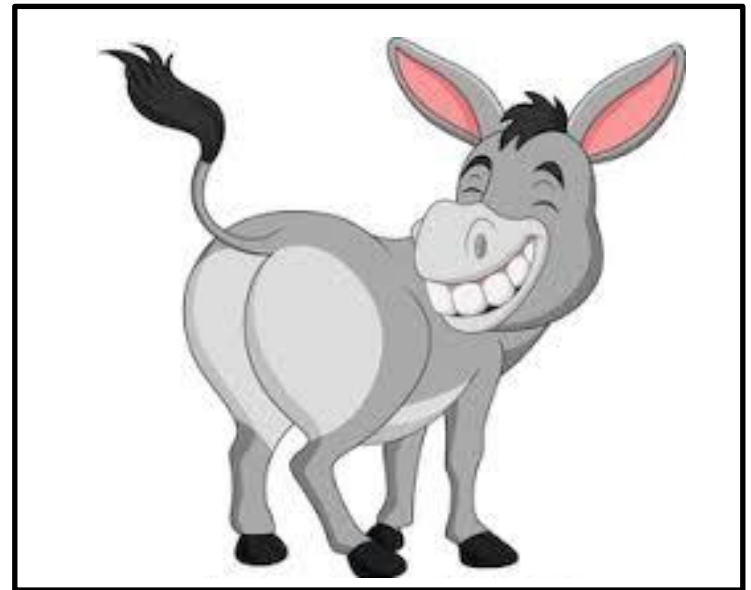
Esempio 3:

LA GESTIONE DELLA TRASPARENZA IN MODALITA' GDPR COMPLIANT

Buone prassi, procedure, FAQ, formazione, esercitazioni, ecc...)

Esempio 1:

LA FORMAZIONE





FORMAZIONE

Come si declina in termini di accountability?

Predisposizione di un piano Formativo (tempi, contenuti, destinatari, relatori,)

Esecuzione del piano formativo

Per ogni sessione:

Allegato 1 - Registro partecipanti

Allegato 2 - Materiale formativo

Allegato 3 - Test di valutazione

Allegato 4 – Verbali di formazione interna

Allegato 4 - Istruzioni ai dipendenti

Esempio 2

Gestione di un incidente (DATA BREACH)

Data Breach?

«Quando ci capiterà sapremo cosa fare!»

«figurati, a chi interessano i nostri dati?»

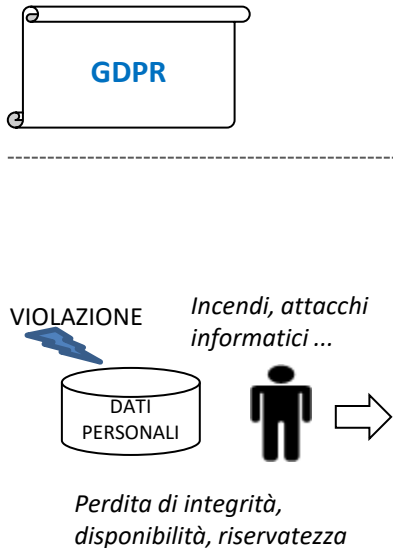




DATA BREACH

Come si declina in termini di accountability?

GDPR



Il soggetto informa tempestivamente il proprio dirigente/PO
Il Dirigente/PO, sentito il Sindaco, effettua una prima valutazione del rischio per i diritti e le libertà degli interessati.

Importante: dal momento in cui si è avuta conoscenza (decorrenza 72 ore)

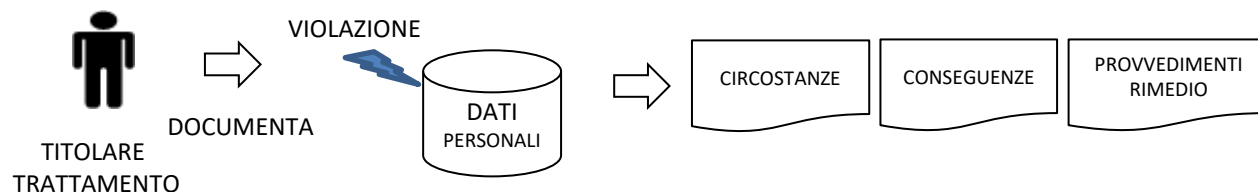


SINDACO
Convoca unità di crisi: (resp. IT – dirigente/PO– DPO)

Importante: ogni componente dell'unità di crisi ha indicato recapito telefonico di rete fissa, recapito telefonico rete mobile, mail.

Riunione unità di crisi presso la sede legale dell'Ente

Tutte le volte che si rileva un incidente, a prescindere dall'obbligo di notifica e/o di comunicazione agli interessati



All. 1/a

COMUNE - TITOLARE DEL TRATTAMENTO

NO

NESSUN
OBBLIGO DI
NOTIFICA

SI

72
H
NOTIFICA

Art.55

SI

OLTRE ALLA NOTIFICA

COMUNICAZIONE

Valutare strumenti più appropriati

indicazioni per proteggersi e limitare ulteriori danni



AUTORITA' DI CONTROLLO



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI



INTERESSATI

Un esempio di procedura di DATA BREACH

Procedura (chi fa che cosa)

Procedura: Descrizione di chi fa che cosa

Allegato 1 - Modulo per la raccolta di informazioni sulla violazione dei dati

Allegato 2 - Metodologia di valutazione del rischio connesso alla violazione

Allegato 3 - Modello di notifica al Garante

Allegato 4 - Comunicazione della violazione all'interessato

Allegato 5 - Registro delle violazioni

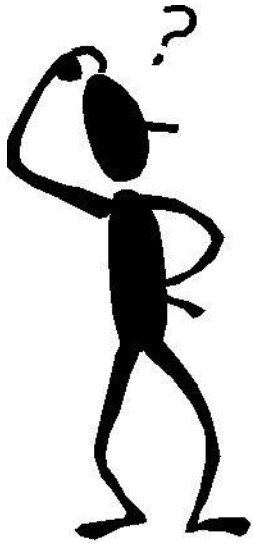
Allegato 6 - Esempi di violazioni di dati

Enti Locali / PA

Delibera di approvazione della procedura

Esempio 3:

LA GESTIONE DELLA TRASPARENZA IN MODALITA' GDPR COMPLIANT





I DIRITTI DELL'INTERESSATO

Articolo 15

Diritto di accesso dell'interessato (C63, C64)

Articolo 16

Diritto di rettifica (C65)

Articolo 17

Diritto alla cancellazione («diritto all'oblio») (C65, C66)

Articolo 18

Diritto di limitazione di trattamento (C67)

Articolo 19

Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento (C31)

Articolo 20

Diritto alla portabilità dei dati (C68)

Articolo 21

Diritto di opposizione (C69, C70)

Articolo 22

diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione(C71, C72)

**Art. 7
D.lgs 196/03
abrogato**

IL TITOLARE E LA TUTELA DELL'INTERESSATO

Articolo 12

Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato (C58-C60, C64)

“Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte ... le comunicazioni di cui agli articoli da 15 a 22 e all'articolo 34 (violazione) relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro...”

“Il titolare del trattamento fornisce all'interessato le informazioni relative all'azione intrapresa riguardo a una richiesta ai sensi degli articoli da 15 a 22 senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa...”

IL TITOLARE E LA TUTELA DELL'INTERESSATO

Mezzi di ricorso, responsabilità e sanzioni

Artt.77 e 78

Fatto salvo ogni altro ricorso amministrativo o giurisdizionale, l'interessato che ritenga che il trattamento che lo riguarda violi il presente regolamento ha il diritto di proporre reclamo a un'autorità di controllo, segnatamente nello Stato membro in cui risiede abitualmente, lavora oppure del luogo ove si è verificata la presunta violazione.

L'autorità di controllo a cui è stato proposto il reclamo informa il reclamante dello stato o dell'esito del reclamo, compresa la possibilità di un ricorso giurisdizionale ai sensi dell'articolo 78”.

qualora il Garante non tratti un reclamo o non informi il reclamante entro tre mesi dello stato o dell'esito del reclamo proposto ai sensi dell'articolo 77.

In ogni caso, ogni persona fisica o giuridica ha il diritto di proporre un ricorso giurisdizionale effettivo avverso una decisione giuridicamente vincolante dell'autorità di controllo che la riguarda.



IL TITOLARE E LA TUTELA DELL'INTERESSATO

Mezzi di ricorso, responsabilità e sanzioni

Artt.79

Oltre a quanto detto prima...

ogni interessato ha il diritto di proporre un ricorso giurisdizionale effettivo qualora ritenga che i diritti di cui gode a norma del presente regolamento siano stati violati a seguito di un trattamento.

Le azioni **nei confronti del titolare del trattamento o del responsabile** del trattamento sono promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui il titolare del trattamento o il responsabile del trattamento ha uno stabilimento.

IL TITOLARE E LA TUTELA DELL'INTERESSATO

Mezzi di ricorso, responsabilità e sanzioni

Articolo 82

Diritto al risarcimento e responsabilità (C142, C146, C147)

1. *Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere **il risarcimento del danno** dal **titolare** del trattamento o dal **responsabile** del trattamento.*
2. *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.*
3. *Il titolare del trattamento o il responsabile del trattamento è **esonерato dalla responsabilità**, a norma del paragrafo 2 se **dimostra che l'evento dannoso non gli è in alcun modo imputabile**.*

(Inversione onere della prova)



IL TITOLARE E LA TUTELA DELL'INTERESSATO

Mezzi di ricorso, responsabilità e sanzioni

Articolo 83

Condizioni generali per infliggere sanzioni amministrative pecuniarie
(C148, C150-C152)

Ogni autorità di controllo provvede affinché le sanzioni amministrative pecuniarie inflitte ai sensi del presente articolo in relazione alle violazioni del presente regolamento di cui ai paragrafi 4, 5 e 6 siano in ogni singolo caso effettive, proporzionate e dissuasive.



SANZIONI

Articolo 83

Condizioni generali per infliggere sanzioni amministrative pecuniarie
(C148, C150-C152)

Per la PA la violazione delle seguenti disposizioni
è soggetta a sanzioni amministrative pecuniarie
fino a 10 000 000 EUR

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



SANZIONI

E fino a **20 000 000 EUR** per la violazione di

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

SANZIONI

Articolo 84

Gli Stati membri stabiliscono le norme relative alle altre sanzioni per le violazioni del presente regolamento in particolare per le violazioni non soggette a sanzioni amministrative pecuniarie a norma dell'articolo 83, e adottano tutti i provvedimenti necessari per assicurarne l'applicazione.

**ART. 166
d.lgs 196/03**

**Sanzioni
amministrative**

**Sanzioni
penali**

**ART. 167
ART. 167 – bis
ART. 167 – ter
ART. 168
ART. 170
ART. 171
d.lgs 196/03**

LA TUTELA DELL'INTERESSATO

LE SANZIONI

AUTORITA' DI CONTROLLO

Capo VI
Autorità di controllo
indipendenti

Sezione 2
Competenza, compiti e
poteri

58 Poteri



AUTORITA' DI CONTROLLO



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

POTERI DI
INDAGINE

POTERI
CORRETTIVI

POTERI
AUTORIZZATIVI
E CONSULTIVI

Capo VI
Autorità di controllo
indipendenti

Sezione 2
Competenza, compiti e
poteri

58 Poteri



AUTORITA' DI CONTROLLO



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

POTERI DI
INDAGINE

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

condurre indagini sotto forma di attività di revisione sulla protezione dei dati

Capo VI
Autorità di controllo
indipendenti

Sezione 2
Competenza, compiti e
poteri

58 Poteri



AUTORITA' DI CONTROLLO



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

POTERI DI
INDAGINE

effettuare un riesame delle certificazioni rilasciate
in conformità dell'articolo 42, paragrafo 7

notificare al titolare del trattamento o al
responsabile del trattamento le presunte
violazioni del presente regolamento

Capo VI
Autorità di controllo
indipendenti

Sezione 2
Competenza, compiti e
poteri

58 Poteri



AUTORITA' DI CONTROLLO



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

POTERI DI
INDAGINE

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

ottenere accesso a tutti i locali del titolare del trattamento e del responsabile del trattamento, compresi tutti gli strumenti e mezzi di trattamento dei dati, in conformità con il diritto dell'Unione o il diritto processuale degli Stati membri.

Capo VI
Autorità di controllo
indipendenti

Sezione 2
Competenza, compiti e
poteri

58 Poteri



AUTORITA' DI CONTROLLO



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

POTERI
CORRETTIVI

rivolgere avvertimenti al titolare del trattamento o al responsabile del trattamento sul fatto che i trattamenti previsti possono verosimilmente violare le disposizioni del presente regolamento

rivolgere ammonimenti al titolare e del trattamento o al responsabile del trattamento ove i trattamenti abbiano violato le disposizioni del presente regolamento

Capo VI
Autorità di controllo
indipendenti

Sezione 2
Competenza, compiti e
poteri

58 Poteri



AUTORITA' DI CONTROLLO



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

POTERI
CORRETTIVI

ingiungere al titolare del trattamento o al responsabile del trattamento di soddisfare le richieste dell'interessato di esercitare i diritti loro derivanti dal presente regolamento

ingiungere al titolare del trattamento o al responsabile del trattamento di conformare i trattamenti alle disposizioni del presente regolamento, se del caso, in una determinata maniera ed entro un determinato termine;

Capo VI
Autorità di controllo
indipendenti

Sezione 2
Competenza, compiti e
poteri

58 Poteri



AUTORITA' DI CONTROLLO



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

POTERI
CORRETTIVI

ingiungere al titolare del trattamento di
comunicare all'interessato una violazione dei dati
personali

imporre una limitazione provvisoria o definitiva al
trattamento, incluso il divieto di trattamento

Capo VI
Autorità di controllo
indipendenti

Sezione 2
Competenza, compiti e
poteri

58 Poteri



AUTORITA' DI CONTROLLO



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

POTERI
CORRETTIVI

ordinare la rettifica, la cancellazione di dati personali o la limitazione del trattamento a norma degli articoli 16, 17 e 18 e la notificazione di tali misure ai destinatari cui sono stati comunicati i dati personali ai sensi dell'articolo 17, paragrafo 2, e dell'articolo 19

revocare la certificazione o ingiungere all'organismo di certificazione di ritirare la certificazione rilasciata a norma degli articoli 42 e 43, oppure ingiungere all'organismo di certificazione di non rilasciare la certificazione se i requisiti per la certificazione non sono o non sono più soddisfatti

Capo VI
Autorità di controllo
indipendenti

Sezione 2
Competenza, compiti e
poteri

58 Poteri



AUTORITA' DI CONTROLLO



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

POTERI
CORRETTIVI

infliggere una sanzione amministrativa pecuniaria ai sensi dell'articolo 83, in aggiunta alle misure di cui al presente paragrafo, o in luogo di tali misure, in funzione delle circostanze di ogni singolo caso;

ordinare la sospensione dei flussi di dati verso un destinatario in un paese terzo o un'organizzazione internazionale.

Capo VI
Autorità di controllo
indipendenti

Sezione 2
Competenza, compiti e
poteri

58 Poteri



AUTORITA' DI CONTROLLO



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

POTERI
AUTORIZZATIVI
E CONSULTIVI

fornire consulenza al titolare del trattamento,
secondo la procedura di consultazione preventiva
di cui all'articolo 36

rilasciare, di propria iniziativa o su richiesta, pareri
destinati al parlamento nazionale, al governo dello
Stato membro, oppure, conformemente al diritto
degli Stati membri, ad altri organismi e istituzioni e
al pubblico su questioni riguardanti la protezione
dei dati personali;

Capo VI
Autorità di controllo
indipendenti

Sezione 2
Competenza, compiti e
poteri

58 Poteri



AUTORITA' DI CONTROLLO



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

POTERI
AUTORIZZATIVI
E CONSULTIVI

autorizzare il trattamento di cui all'articolo 36, paragrafo 5, se il diritto dello Stato membro richiede una siffatta autorizzazione preliminare;

rilasciare un parere sui progetti di codici di condotta e approvarli, ai sensi dell'articolo 40, paragrafo 5;

Capo VI
Autorità di controllo
indipendenti

Sezione 2
Competenza, compiti e
poteri

58 Poteri



AUTORITA' DI CONTROLLO



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

POTERI
AUTORIZZATIVI
E CONSULTIVI

accreditare gli organismi di certificazione a norma
dell'articolo 43;

rilasciare certificazioni e approvare i criteri di
certificazione conformemente all'articolo 42,
paragrafo 5;

Capo VI
Autorità di controllo
indipendenti

Sezione 2
Competenza, compiti e
poteri

58 Poteri



AUTORITA' DI CONTROLLO



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

POTERI
AUTORIZZATIVI
E CONSULTIVI

adottare le clausole tipo di protezione dei dati di cui all'articolo 28, paragrafo 8, e all'articolo 46, paragrafo 2, lettera d);

autorizzare le clausole contrattuali di cui all'articolo 46, paragrafo 3, lettera a);

Capo VI
Autorità di controllo
indipendenti

Sezione 2
Competenza, compiti e
poteri

58 Poteri



AUTORITA' DI CONTROLLO



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

POTERI
AUTORIZZATIVI
E CONSULTIVI

autorizzare gli accordi amministrativi di cui
all'articolo 46, paragrafo 3, lettera b);

approvare le norme vincolanti d'impresa ai sensi
dell'articolo 47.

SCHEMI RIASSUNTIVI

DIFFERENZE TRA IL VECCHIO DISPOSTO DEL 196/03 e GDPR



GDPR + nuova 196/03

VS

VECCHIO D.LGS. 196/03



MODIFICA DI ISTITUTI
GIÀ NOTI

Informativa

Consenso

Diritto di accesso



DATI PERSONALI
CATEGORIE
PARTICOLARI

Nuova classificazione dei dati, **nuovi concetti**

GDPR

Capo II
Principi

Art. 4

profilazione



DIRITTI

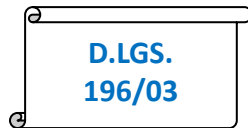
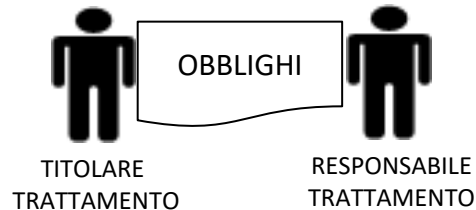
INTERESSATO

Nuovi diritti

GDPR

Capo III
Diritti
dell'Interessato

- Diritto all'oblio
- Limitazione del trattamento
- Portabilità dei dati
- Si sommano a (accesso e rettifica)



ACCOUNTABILITY

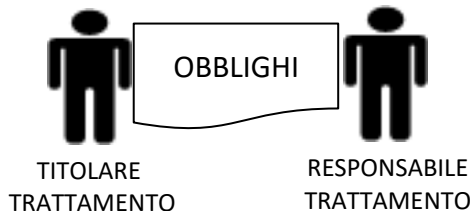
Nuovi obblighi e responsabilità



Capo IV
Titolari del Trattamento e
Responsabili Trattamento

Sezione 1
Obblighi Generali

Artt. 5, 6,
24



PRIVACY BY DEFAULT PRIVACY BY DESIGN

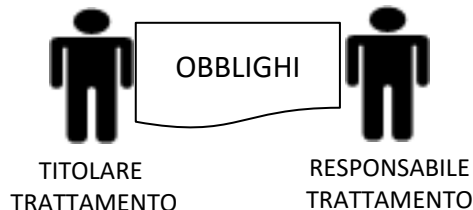
Nuovi obblighi e responsabilità



Capo IV
Titolari del Trattamento e
Responsabili Trattamento

Sezione 1
Obblighi Generali

Art. 24



REGISTRO TRATTAMENTI

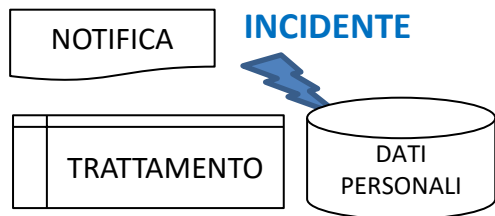
Nuovi obblighi e responsabilità



Capo IV
Titolari del Trattamento e
Responsabili Trattamento

Sezione 1
Obblighi Generali

Art. 30



DATA BREACH

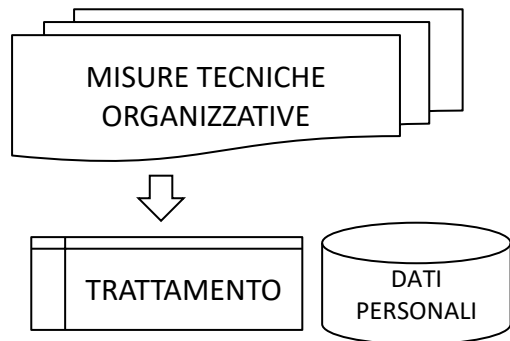
Nuova gestione delle violazioni “privacy” e loro notifica



Capo IV
Titolari del Trattamento e
Responsabili Trattamento

Sezione 2
Sicurezza dei dati
personali

Artt.
33,34



RISK ASSESTEMENT

Nuovo approccio alla sicurezza del trattamento



Capo IV
Titolari del Trattamento e
Responsabili Trattamento

Sezione 2
Sicurezza dei dati
personali

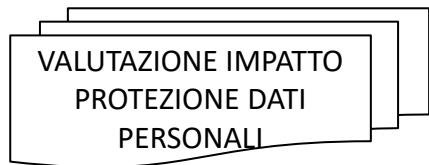
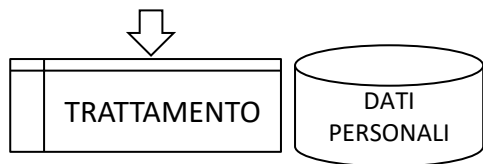
Artt.
32-36

Art. 32, LETT 2

RESILIENZA

SU BASE PERMANENTE

*E' il paradigma della **Ratio** sottesa al Regolamento e della nuova concezione di sicurezza: proteggere i dati come valore assoluto, a prescindere dalle possibili violazioni o danni agli interessati*



Valutazione Impatto Protezione Dati Personali



Capo IV
Titolari del Trattamento e
Responsabili Trattamento

Sezione 3
Valutazione di Impatto sulla
protezione dei dati e
consultazione preventiva

DPIA



RISCHIO



In generale: nuovo approccio alla gestione del rischio



Capo IV
Titolari del Trattamento e
Responsabili Trattamento



RISCHIO



Codici di condotta e Certificazione



COMPLIANCE
ACCOUNTABILITY



Capo IV
Titolari del Trattamento e
Responsabili Trattamento

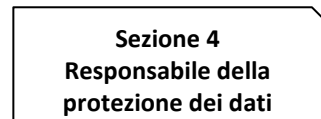
Sezione 5
Codici di condotta
E Certificazione



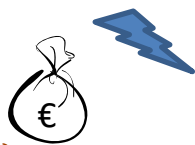
RESPONSABILE
PROTEZIONE
DATI PERSONALI

**RESPONSABILE DELLE
PROTEZIONE DEI DATI**

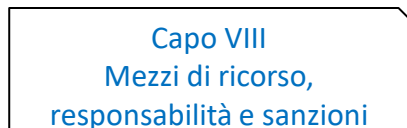
Nuova figura del Responsabile Protezione Dati Personali ("DPO Data Protection Officer")



SANZIONI



Sanzioni significativamente più severe



PENE SEVERE



Nuovi reati

