

## UNIVERSITÀ DEGLI STUDI DI ROMA «TOR VERGATA»

«La Direttiva europea NIS, Network and Information Security e il GDPR: soggetti attuatori, competenze, obblighi e prospettive nel processo di recepimento e a regime»

**Elisabetta ZUANELLI**

**Coordinatore del Piano di formazione nazionale in cybersecurity, cyberthreat, privacy  
Partenariato PP Università degli Studi di Roma “Tor Vergata”, Poste Italiane, Clariter Texi, Pragmema, Profice,  
Supercom, Istituto per il governo societario ([www.cybersecurityprivacy.it](http://www.cybersecurityprivacy.it))**

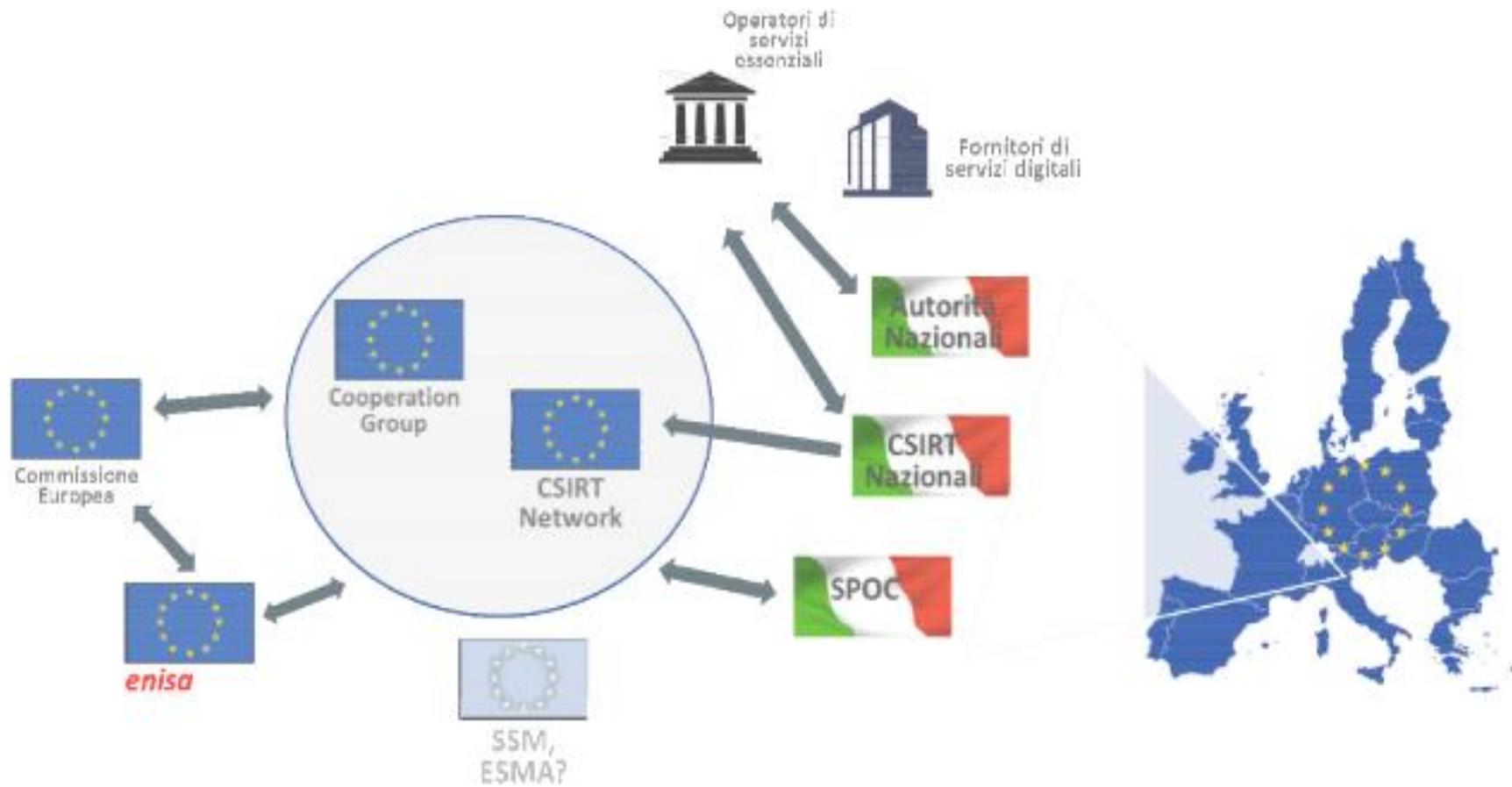
***Presidente del Centro di Ricerca e Sviluppo dell'E-Content/Università degli Studi di Roma «Tor Vergata»  
(CReSEC/[www.cresec.com](http://www.cresec.com))***

## *Lo scenario quantitativo degli attacchi cyber*

- L'80% delle aziende europee ha subito almeno un incidente cybersecurity nel 2015
- Il numero di incidenti di sicurezza per tutte le industrie nel mondo è cresciuto del 38% nel 2015

- scadenze
- soggetti attuatori
- competenze
- operatori di servizi essenziali
- fornitori di servizi digitali

# L'architettura NIS



- La Direttiva NIS : in vigore da agosto 2016
- Gli stati membri: 21 mesi per adottare le necessarie misure di implementazione a livello di legislazione nazionale
- 6 mesi supplementari per identificare gli operatori delle infrastrutture critiche nazionali
- Il recepimento: 9 maggio 2018
- La transizione:
  - ▣ gruppo di cooperazione e rete CSIRT: operativo dal 9 febbraio 2017
  - ▣ gruppo di cooperazione assiste gli stati membri per l'identificazione degli operatori dei servizi essenziali e gli effetti negativi: da 9 febbraio 2017 a 9 novembre 2018



# *Riesame*

- Due anni dopo l'entrata in vigore della direttiva NIS e ogni 18 mesi successivi, la Rete CSIRTs produrrà una relazione per valutare l'esperienza acquisita con la cooperazione operativa, ivi comprese le conclusioni e le raccomandazioni emerse. La relazione sarà inviata alla Commissione.
- Riesame del funzionamento della direttiva (art. 23): entro il 9 maggio 2018 la Commissione presenta al Parlamento europeo e al Consiglio una relazione sulla coerenza nell'identificazione degli operatori dei servizi essenziali
- Riesame periodico

# *Il rapporto con le norme di contesto*

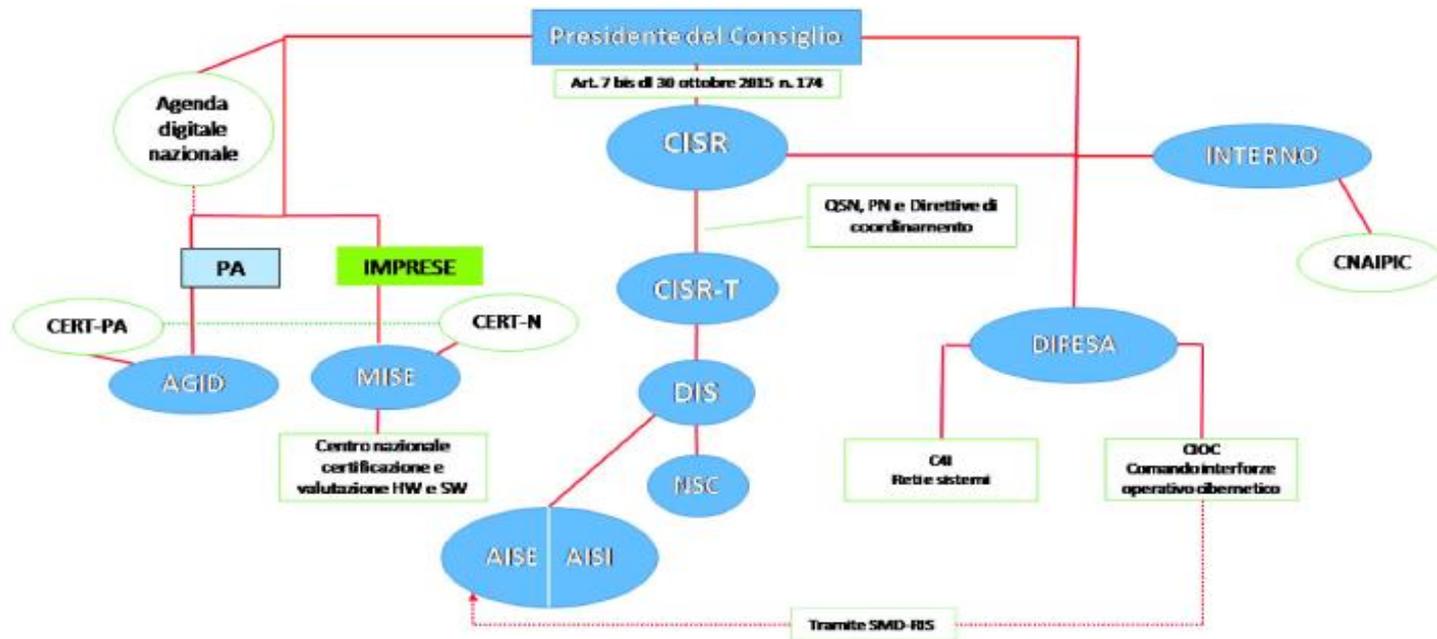
- il GDPR e la Direttiva 95/46
- le norme settoriali UE
- le norme locali nazionali
- le norme internazionali

## QUADRO STRATEGICO NAZIONALE (QSN)

### INDIRIZZI STRATEGICI

1. Potenziamento delle capacità di difesa delle Infrastrutture Critiche nazionali e degli attori di rilevanza strategica per il sistema-Paese
2. Miglioramento, secondo un approccio integrato, delle capacità tecnologiche, operative e di analisi degli attori istituzionali interessati
3. Incentivazione della cooperazione tra istituzioni ed imprese nazionali
4. Promozione e diffusione della cultura della sicurezza cibernetica
5. Rafforzamento della cooperazione internazionale in materia di sicurezza cibernetica
6. Rafforzamento delle capacità di contrasto alle attività e contenuti illegali *on-line*

## ARCHITETTURA NAZIONALE CYBER



# Il piano nazionale

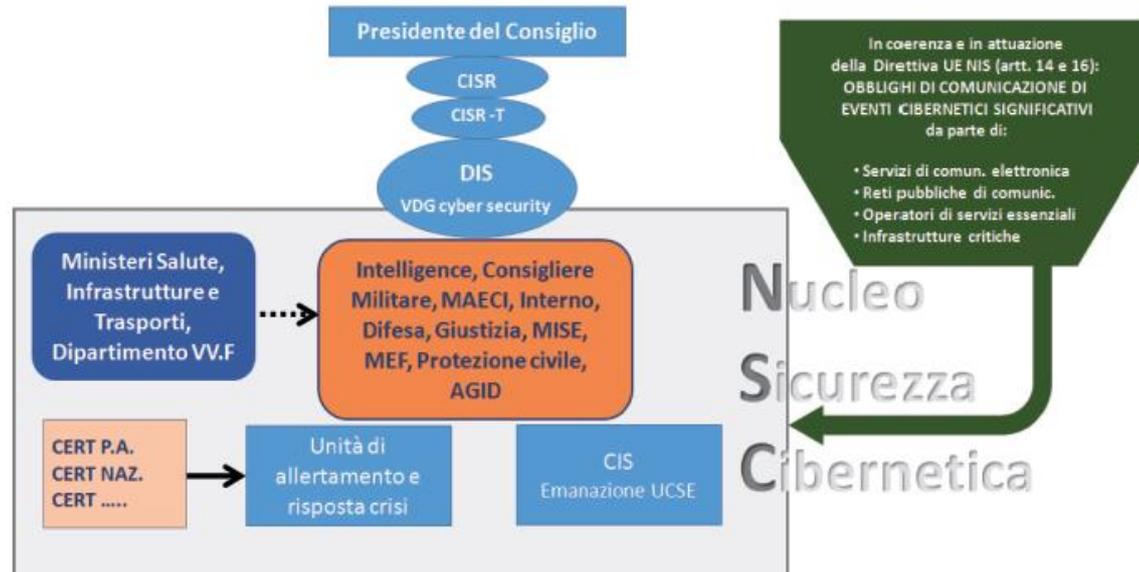
## PIANO NAZIONALE (PN)

### INDIRIZZI OPERATIVI

1. Potenziamento capacità di *intelligence*, di polizia e di difesa civile e militare
2. Potenziamento dell'organizzazione e delle modalità di coordinamento e di interazione a livello nazionale tra soggetti pubblici e privati
3. Promozione e diffusione della cultura della sicurezza informatica. Formazione ed addestramento
4. Cooperazione internazionale ed esercitazioni
5. Operatività delle strutture nazionali di *incident prevention, response e remediation*
6. Interventi legislativi e *compliance* con obblighi internazionali
7. *Compliance a standard* e protocolli di sicurezza
8. Supporto allo sviluppo industriale e tecnologico
9. Comunicazione strategica e operativa
10. Risorse
11. Implementazione di un sistema di *cyber risk management* nazionale

# La gestione delle crisi

## NUOVO SISTEMA DI GESTIONE DELLE CRISI



# *I soggetti attuatori*

- La Commissione
- La *governance* degli Stati membri
- La/e Autorità
- Il gruppo di cooperazione
- Il CSIRT nazionale
- La rete di CSIRT
- Enisa
- Il punto di contatto unico

## *Le aziende: obblighi e sanzioni*

Gli operatori di servizi essenziali (scad. 9 novembre 2018)

- Elenco
- Obblighi: *risk assessment e risk evaluation*
- *La compliance*: Ue e internazionali (framework NIST, COBIT, ISO, ISA, ecc.)
- Le notifiche
- Le sanzioni
- L'impatto: criteri di valutazione
- Giurisdizione e territorialità

# *Identificazione degli operatori di servizi essenziali*

1. Entro il 9 novembre 2018, gli Stati membri identificano, per ciascun settore e sottosettore gli operatori di servizi essenziali con una sede nel loro territorio.

2. I criteri per l'identificazione degli operatori di servizi essenziali sono i seguenti:

- a) un soggetto fornisce un servizio che è essenziale per il mantenimento di attività sociali e/o economiche fondamentali;
- b) la fornitura di tale servizio dipende dalla rete e dai sistemi informativi;
- c) un incidente avrebbe effetti negativi rilevanti sulla fornitura di tale servizio.

3. Ciascuno Stato membro istituisce un elenco dei servizi

## *Tipologia degli operatori di servizi essenziali*

Gli operatori di servizi essenziali sono aziende private o enti pubblici con un ruolo importante per la società e l'economia nei seguenti settori:

- Energia: elettricità, petrolio e gas.
- Trasporto: aereo, ferroviario, marittimo e stradale.
- Bancario: gli istituti di credito.
- Infrastrutture dei mercati finanziari: le sedi di negoziazione e le controparti centrali.
- Salute: ambienti sanitari.
- Acqua: fornitura di acqua potabile e distribuzione.
- Infrastruttura digitale: specificamente gli Internet Exchange point, i fornitori di servizi DNS ( Domain Name System) e i registri TLD (Top Level Domain).

# La Internet exchange map



## *Effetti negativi rilevanti*

fattori intersettoriali:

- a) il numero di utenti che dipendono dal servizio fornito dal soggetto interessato;
- b) la dipendenza di altri settori di cui all'allegato II dal servizio fornito da tale soggetto;
- c) l'impatto che gli incidenti potrebbero avere, in termini di entità e di durata, sulle attività economiche e sociali o sulla pubblica sicurezza;
- d) la quota di mercato di detto soggetto;
- e) la diffusione geografica relativamente all'area che potrebbe essere interessata da un incidente;
- f) l'importanza del soggetto per il mantenimento di un livello sufficiente del servizio, tenendo conto della disponibilità di strumenti alternativi per la fornitura di tale servizio.

fattori settoriali: ove opportuno

- **misure tecniche e organizzative** adeguate e proporzionate alla gestione dei rischi posti alla sicurezza delle reti e dei sistemi informativi che usano nelle loro operazioni
- tenuto conto delle conoscenze più aggiornate in materia, dette misure **assicurano un livello di sicurezza della rete e dei sistemi informativi** adeguato al rischio esistente
- misure adeguate per **prevenire e minimizzare l'impatto di incidenti** a carico della sicurezza della rete e dei sistemi informativi utilizzati per la fornitura di tali servizi essenziali, al fine di **assicurare la continuità di tali servizi.**
- **notifiche** senza indebito ritardo all'autorità competente o al CSIRT gli incidenti aventi un impatto rilevante sulla continuità dei servizi essenziali prestati.

## *Obblighi di attuazione*

Fornire all'Autorità

- a) **le informazioni necessarie per valutare la sicurezza rete e dei sistemi informativi**, compresi i documenti relativi alle politiche di sicurezza;
- b) la prova dell'effettiva attuazione delle politiche di sicurezza, come i **risultati di un audit sulla sicurezza svolto dall'autorità competente o da un revisore abilitato** e, in quest'ultimo caso, metterne a disposizione dell'autorità competente i risultati, inclusi gli elementi di prova.

## *Impatto dell'incidente*

- a) **il numero di utenti** interessati dalla perturbazione del servizio essenziale;
- b) **la durata** dell'incidente;
- c) **la diffusione geografica** relativamente all'area interessata dall'incidente.

- I fornitori: identità
- Obblighi
- Giurisdizione e territorialità

# *Le tipologie dei fornitori di servizi digitali*

1. Mercato online
2. Motore di ricerca online
3. Servizi nella nuvola (cloud computing)

# *Obblighi in materia di sicurezza e notifica degli incidenti ( Art. 16)*

- I fornitori di servizi digitali devono **identificare e adottare misure tecniche e organizzative** adeguate e proporzionate alla gestione dei rischi posti alla sicurezza della rete e dei sistemi informativi
- Elementi da considerare:
  - a) la sicurezza dei sistemi e degli impianti;
  - b) trattamento degli incidenti;
  - c) gestione della continuità operativa;
  - d) monitoraggio, audit e test;
  - e) conformità con le norme internazionali.

- Misure preventive
- Riduzione dell'impatto
- Notifica all'Autorità competente o al CSIRT

## *Valutazione d'impatto*

- a) il **numero di utenti** interessati dall'incidente, in particolare gli utenti che dipendono dal servizio per la fornitura dei propri servizi;
- b) la **durata** dell'incidente;
- c) la **diffusione geografica** relativamente all'area interessata dall'incidente;
- d) la **portata della perturbazione del funzionamento del servizio**;
- e) la **portata dell'impatto sulle attività economiche e sociali**.

NB

L'obbligo di notificare un incidente si applica soltanto qualora il fornitore di servizi digitali abbia accesso alle informazioni necessarie per valutare l'impatto di un incidente nei confronti dei parametri di cui al primo comma.

## *Giurisdizione e territorialità*

1. Un fornitore di servizi digitali è considerato soggetto alla **giurisdizione dello Stato membro in cui ha lo stabilimento principale.**
2. Un fornitore di servizi digitali che non è stabilito nell'Unione, ma offre servizi di cui all'allegato III all'interno dell'Unione, designa un **rappresentante** nell'Unione.
3. La designazione di un rappresentante da parte di un fornitore di servizi digitali fa salve le **azioni legali che potrebbero essere avviate nei confronti del fornitore stesso di servizi digitali.**

## *Sanzioni*

- Gli Stati membri stabiliscono le **norme relative alle sanzioni** da irrogare in caso di violazione delle disposizioni nazionali di attuazione della presente direttiva e adottano tutti i provvedimenti necessari per la loro applicazione.
- Le sanzioni previste sono **effettive, proporzionate e dissuasive**.
- Gli Stati membri notificano tali **norme e provvedimenti alla Commissione entro il 9 maggio 2018** e provvedono a darle immediata notifica di ogni successiva modifica.

# Problematicità 1

- ione NIS con GDPR (cessazione delle norme pregresse e *eprivacy*)
- Correlaz

Il Garante europeo della protezione dei dati è stato consultato conformemente all'articolo 28, paragrafo 2, del regolamento (CE) n. 45/2001 e ha espresso un parere il 14 giugno 2013 (4).

Il trattamento di dati personali ai sensi della presente direttiva è effettuato ai sensi della direttiva 95/46/CE. 2. Il trattamento di dati personali da parte di istituzioni e organismi dell'Unione ai sensi della presente direttiva è effettuato a norma del regolamento (CE) n. 45/2001.

# Correlazione con le norme intersettoriali e settoriali, operatori vari, recepimento nazionale, coordinamento attività

- Trasporto via acqua
- Settore bancario
- Sorveglianza dell'Eurosistema sui sistemi di pagamento e di regolamento
- Sistemi di intermediazione online
- Accordi paralleli (es. *privacy shield* e DSM)
- Disomogeneità possibile nell'identificazione degli operatori di servizi essenziali e gli operatori di servizi digitali (liste di servizi e di operatori)
- Sanzioni: diverse per stato membro e da armonizzare
- Notifiche (parametri, referenti ( Autorità e/o CSIRT)
- Riferimento a standard internazionali ( europei e non): concorrenza vendor
- Compliance vs sicurezza
- Giurisdizione: localizzazione della sede e/o del rappresentante
- Interazione tra Commissione, gruppo di cooperazione, Autorità, rete dei CSIRT, Enisa, punti unici di contatto, ecc.

# Il GDPR: considerazioni cpmplressive

## *Articolo 1*

### *Oggetto e finalità*

1. Il presente regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al **trattamento dei dati personali**, nonché norme relative alla **libera circolazione di tali dati**.
2. Il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali.
3. La **libera circolazione dei dati personali nell'Unione non può essere limitata né vietata** per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

## *Articolo 2*

### *Ambito di applicazione materiale*

1. Il presente regolamento si applica **al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato** di dati personali contenuti in un archivio o destinati a figurarvi.

# Il trattamento dei dati: Art.4

## 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:

- 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
- la diffusione o qualsiasi altra forma di messa a disposizione
- il raffronto o l'interconnessione
- la limitazione
- la cancellazione o la distruzione

# I soggetti indirizzati

- "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;
- "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;
- il titolare del trattamento e il responsabile del trattamento designano sistematicamente un «responsabile della protezione dei dati»
- "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;
- "destinatario": la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi.

# I dati e le violazioni

- dati genetici
- dati biometrici
- dati relativi alla salute
- la distruzione
- la perdita
- la modifica
- la divulgazione non autorizzata
- l'accesso ai dati personali trasmessi, conservati o comunque trattati

# Capi problematici

**CAPO IV**

**SEZIONE 4**

**RESPONSABILE DELLA PROTEZIONE DEI DATI**

**CAPO V**

**TRASFERIMENTI DI DATI PERSONALI VERSO PAESI TERZI**

**CAPO VIII**

**MEZZI DI RICORSO, RESPONSABILITÀ E SANZIONI**

# Violazioni e sanzioni 1

**4.** In conformità del paragrafo 2 , la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 10 000 000 EUR, o per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:

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

## Violazioni e sanzioni 2

**5.** In conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 20 000 000 EUR, o per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:

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

## Violazioni e sanzioni 3

6. In conformità del paragrafo 2 del presente articolo, l'inosservanza di un ordine da parte dell'autorità di controllo di cui all'articolo 58, paragrafo 2, è soggetta a sanzioni amministrative pecuniarie fino a 20 000 000 EUR, o per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

# *Alcune problematicità*

- La nozione di dato nella NIS e nel GDPR
- I diritti del soggetto interessato
- Codici di condotta e certificazione
- Il diritto alla *explanation*
- Registri delle attività di trattamento
- La PIA
- La giurisdizione e gli accordi internazionali

(considerando 72): utilizzo di  
intelligenza artificiale