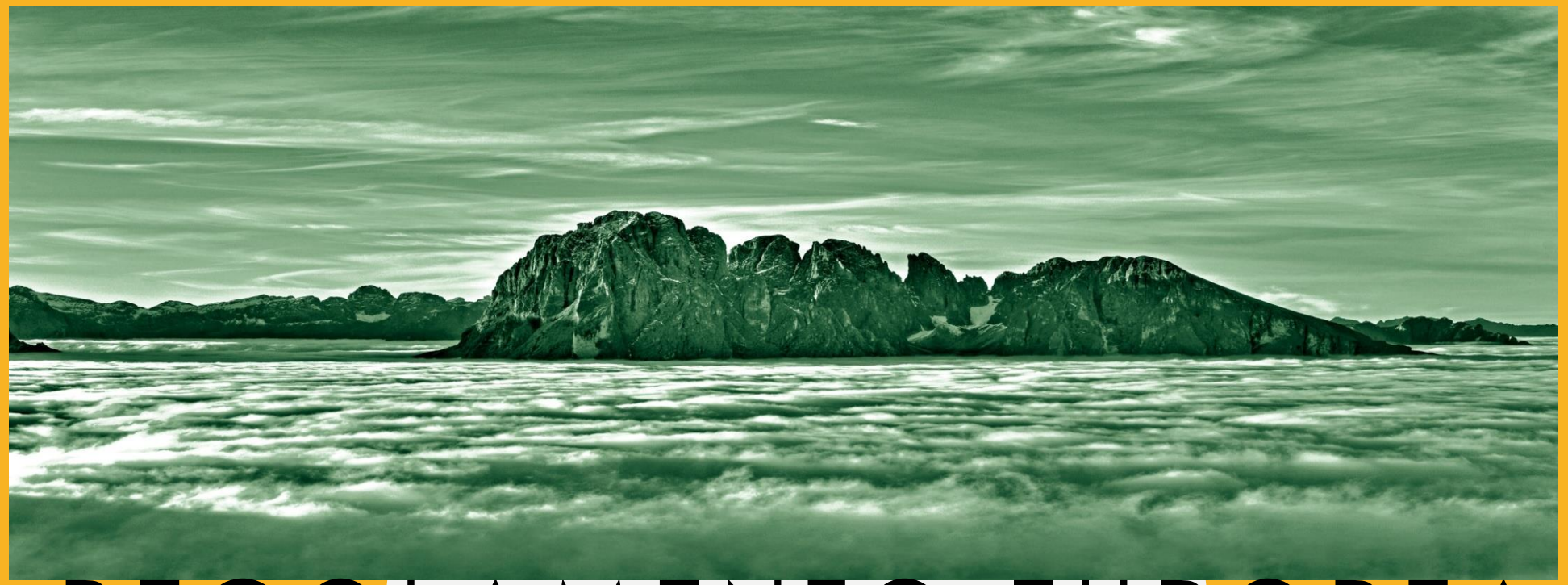


REGOLAMENTO EUROPEA SULLA PROTEZIONE DEI DATI N. 679/2016/UE

NOVITÀ

DSGVO
GDPR

“Se non lo sai spiegare in modo semplice,
non l’hai capito abbastanza bene”

(Albert Einstein)

COSA DOVEVA ESSERE CONSIDERATO FINORA …

- Legislazione nazionale

- Codice della privacy (d.lgs. 196/2003)
- Legge sulle telecomunicazioni (LTC)
- Codice civile italiano

- Autorità garante della protezione dei dati

REGOLAMENTO DI BASE SULLA PROTEZIONE DEI DATI NELL'UE (UE-DSGVO)

Oggetto e obiettivi

- Il presente regolamento stabilisce norme relative alla tutela delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati.
- Il presente regolamento tutela i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali.
- La libera circolazione dei dati personali all'interno dell'Unione non è limitata o vietata per motivi di tutela delle persone fisiche con riguardo al trattamento dei dati personali.

CHE COSA CI ASPETTA …

- Quadro unico europeo
  - Regolamento (UE) n. 679/2016/UE - Regolamento di base sulla protezione dei dati

GDPR

- Tempistiche
  - Entrata in vigore prevista per il 24 maggio 2016
  - A partire dal 25 maggio 2018 il Regolamento diventa lo strumento normativo principale.
  - 06 maggio 2018: Scadenza per l'entrata in vigore delle leggi nazionali di applicazione del regolamento da parte degli Stati membri

PROTEZIONE DEI DATI E AUTODETERMINAZIONE INFORMATIVA

– Armonia con altri diritti

- Il trattamento dei dati personali dovrebbe essere al servizio dell'umanità. Il diritto alla protezione dei dati personali non è un diritto illimitato; deve essere visto in termini di funzione sociale e ponderato con altri diritti fondamentali, nel rispetto del principio di proporzionalità. Il presente regolamento rispetta tutti i diritti fondamentali e osserva tutte le libertà e i principi riconosciuti dalla Carta e sanciti dai Trattati Europei, in particolare il rispetto della vita privata e della vita familiare, delle abitazioni e delle comunicazioni, della protezione dei dati personali, della libertà di pensiero, di coscienza e di religione, della libertà di espressione e di informazione, della libertà imprenditoriale, il diritto a un ricorso effettivo e a un giudice imparziale e della diversità delle culture, delle religioni e delle lingue.

DEFINIZIONI IMPORTANTI
ART. 4

1. Dati personali:
   - Tutte le informazioni relative a una persona fisica identificata o identificabile
   - La persona deve essere direttamente o indirettamente identificabile
   - Ad esempio, indirizzi IP, account nei social network.

   Trattamento
   - Qualsiasi trattamento effettuato con o senza l'ausilio di procedure automatizzate in relazione a dati personali.

DEFINIZIONI IMPORTANTI
ART. 4

2. Pseudonimizzazione:
   - trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a una specifica persona interessata senza l'uso di informazioni supplementari, a condizione che tali informazioni supplementari siano conservate separatamente

   - NON "solo" anonimizzazione

DEFINIZIONI IMPORTANTI
ART. 4

3. Profiling:
   - Trattamento automatizzato di dati personali, consistente nell'utilizzo di dati personali atti a valutare o prevedere taluni aspetti personali di una persona fisica, in particolare aspetti relativi alla gestione del lavoro, alla situazione economica, allo stato di salute, alle preferenze personali, agli interessi, all'affidabilità, al comportamento, al luogo di residenza o di trasferimento della persona fisica.

DEFINIZIONI IMPORTANTI
ART. 4

4. Dati sensibili:
   - I **dati personali da cui sono ricavati:**
     - **Razza e origine etnica**
     - **Pareri politici**
     - **Convinzioni religiose e ideologiche**
     - **Appartenenza al sindacato**
     - **Dati genetici**
     - **Dati biometrici per l'identificazione univoca delle persone fisiche**
     - **Cartelle cliniche**
     - **Dati sulla vita sessuale o sull'orientamento sessuale**

DEFINIZIONI IMPORTANTI
ART. 4

5. Trattamento lecito:
   - Consenso dell'interessato al trattamento per una o più finalità
   - Esecuzione di un contratto di cui la persona interessata è parte
   - Adempimento di un obbligo legale
   - Salvaguardia degli interessi vitali dell'interessato
   - Esecuzione di una missione di interesse pubblico/esercizio di pubblici poteri
   - Protezione di interessi giustificati (ad es. amministrazione di un'associazione senza scopo di lucro, ONLUS)

5. Trattamento lecito:

- La legalità non si basa solo sui principi di „Proporzionalitá“ (Art. 5 Abs. 1 lit. b), „Transparenza“ (Art. 5 Abs. 1 lit. a), „Minimizzazione die dati“ (Art. 5 Abs. 1 lit. c), „Correttezza“ (Art. 5 Abs. 1 lit. d), „Limitazione dello spazio di memoria“ (Art. 5 Abs. 1 lit. c) e „Integritá e riservatezza“ (Art. 5 Abs. 1 lit. f), in particolare il principio dell'accantonamento (art. 5 comma 1 lettera b).

PRINCIPI DI LEGALITÁ

s

DEFINIZIONI IMPORTANTI
ART. 4

6. Consenso:
   - Volontari per il caso specifico, in una dichiarazione di intenti informata e inequivocabile, sotto forma di una dichiarazione o altra indicazione chiara che l'interessato acconsente al trattamento dei suoi dati personali.

   - Possibile a 16 anni di età

DEFINIZIONI IMPORTANTI
ART. 4

7. **Titolare del trattamento**
   - Valuta la probabilità del verificarsi e la gravità dei rischi per i diritti e le libertà delle persone fisiche.
   - Attuazione delle misure tecniche e organizzative
   - Registro delle attività di trattamento

   - **La persona giuridica o il rappresentante legale**

   - **Responsabile in solido del trattamento?**

DEFINIZIONI IMPORTANTI
ART. 4

8. Responsabile del trattamento
   - **Trattamento dei dati personali per conto di un responsabile/titolare**
   - **Responsabile dell'attuazione delle misure tecniche e organizzative**
   - **Efficacia giuridica come nomina**
   - **Registro delle attività di trattamento**
   - **Cancellazione o restituzione di tutti i dati dopo la cessazione del mandato**

   - **prevalentemente esterno**

DEFINIZIONI IMPORTANTI
ART. 4

8. Responsabile del trattamento:

- Oneri
  - Possibilmente nomina DPO
  - Misure di sicurezza tecniche e organizzative
  - Avviso obbligatorio
  - Responsabilità per inadempimento
  - Valutazione dei rischi
  - Elenco dei trattamenti
  - Adempimento dei diritti degli interessati

DEFINIZIONI IMPORTANTI
ART. 4

9. Responsabile della protezione dei dati (DPO):
   - **Obbligatorio** per:
     - Autorità pubbliche ed enti pubblici (escluse le autorità giudiziarie)
     - organizzazioni la cui attività principale richiede un controllo esteso, regolare e sistematico delle persone interessate
     - Ampio trattamento di dati sensibili o di dati giudiziari
   - **Facoltativo per tutte le altre realtá:**
   - Interno o esterno
   - Nessun conflitto di interessi
   - Funzione consultiva, ma anche funzione di vigilanza

DEFINIZIONI IMPORTANTI
ART. 4

10. 10. Principi:

- **rettitudine**, trattamento secondo buona fede
- trasparenza
- **Trattamento secondo le finalità prestabilite**
- **Minimizzazione dei dati**
- Limitazione dello spazio di memoria
- **correttezza**
- integrità e riservatezza
- **responsabilizzazione**

DEFINIZIONI IMPORTANTI
ART. 4

1111. Data breach:

- Violazione dei dati personali (furto, distruzione, manipolazione)
- Rischio maggiore è interno: fattore umano
- Notifica alla polizia postale e all'Autorità garante
- Notifica agli interessati (se sussite un rischio elevato per i loro diritti e libertà)
- Notifica al DPO

DEFINIZIONI IMPORTANTI
ART. 4

Diritti degli interessati:

- Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritto degli interessati (art. 12)
- Informazioni da fornire all'interessato (art. 13 s.)
- **Diritto di accesso (art. 15)**
- **Diritto di rettifica (art. 16)**
- **Diritto di opposizione (Art. 21)**
- **Diritto di limitazione di trattamento (art. 18)**
- **Diritto alla cancellazione (art. 17)**
- Diritto di portabilità dei dati (art. 20)
- Diritto di notifica in caso di data breach

DEFINIZIONI IMPORTANTI

Diritti degli interessati:

- **Diritto all'informazione (Art. 15)**
  - trattamento dei dati
  - Categorie di dati personali
  - Categorie di destinatari
  - tempo di conservazione
  - diritti in questione
  - Copia di tutti i dati elaborati

Risposte entro 30 giorni dal ricevimento della richiesta di accesso

DEFINIZIONI IMPORTANTI

Diritti degli interessati:

- **Diritto di rettifica (art. 16)**
  - Adempimento immediato
  - Anche integrazione di dati incomplete

DEFINIZIONI IMPORTANTI

Diritti degli interessati:

- **Diritto di opposizione (Art. 21)**
  - Nessun ulteriore trattamento
  - Resta ferma la liceità del trattamento già effettuato
  - Marketing & profilazione: opposizione possibile in ogni momento

DEFINIZIONI IMPORTANTI

Diritti degli interessati:

- **Diritto di limitazione di trattamento (art. 18)**
  - Se è contestata l'esattezza dei dati personali e per il periodo necessario a rimuovere il dubbio
  - Trattamento illecito
  - Esaurita o manca la finalità di trattamento
  - In caso di opposizione al trattamento dei dato

DEFINIZIONI IMPORTANTI

Diritto di recesso:

- **Diritto di recesso (Art. 17)**
  - Lo scopo del trattamento è stato raggiunto
  - Revoca del consenso al trattamento dei dati
  - Obiezione al trattamento dei dati
  - Trasformazione illegale
  - Obbligo legale

DEFINIZIONI IMPORTANTI

Cancellazione di dati accessibili al pubblico.

Eccezione:

- libertà di espressione
- Difesa in tribunale
- Interesse pubblico, storico o statistico,
- Obbligo legale di magazzinaggio

GDPR STEP DI IMPLEMENTAZIONE…

REQUISITI PRINCIPALI DEL DSGVO

Organizzazione

- Nomina di un responsabile della protezione dei dati
- Misure tecniche e organizzative

Procedimento

- Notifica di violazioni della protezione dei dati entro 72 ore
- Valutazione dell'impatto sulla vita privata

Tecnologie

- „ePrivacy by Design“ & „Privacy by Default“
- Stato dell´arte

Prerogative

- Consenso separato per ogni utilizzo
- Revoca del consenso e "diritto all'oblio“

ESAME DELLE LEGGI APPLICABILI - OBBLIGO DI SEGRETO PROFESSIONALE

NOZIONI DI BASE SULLA LICEITÀ DEL TRATTAMENTO DEI DATI

5. Controllo di tutte le lettere di informazione e dichiarazioni di consenso
   - modificazioni
   - Compilare la lettera d'informazione e inviarla alle persone interessate.
   - Dichiarazioni di consenso complete e ottenere il consenso degli interessati

TRATTAMENTO DEI DATI PER SCOPI PROPRI O DI TERZI

TRATTAMENTO DEI DATI PER CONTO TERZI - DIRITTI, DOVERI, CONSEGUENZE E RESPONSABILITÀ

STATUS GIURIDICO, COMPITI E OBBLIGHI DEL RESPONSABILE DELLA PROTEZIONE DEI DATI / DELL'AZIENDA

Ho bisogno di un DPO (art. 37 ss.)?

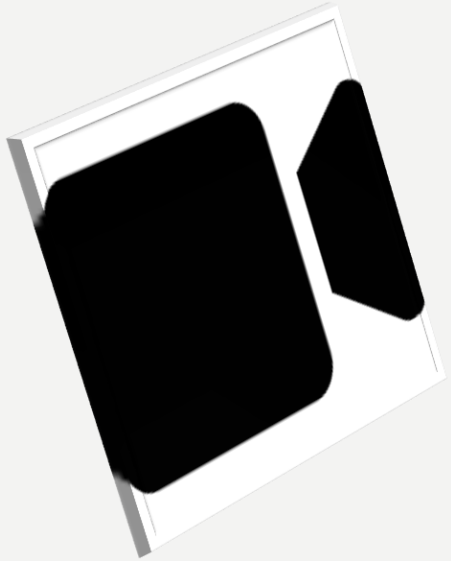
- Entrare in contatto con potenziali candidati
- Raccolta di curriculum
- Effettuare colloqui
- Nomine
- Notifica all'Autorità garante

CONTROLLO PRELIMINARE / VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI

Valutazione d‘impatto (art. 35)

- Solo se sussiste un rischio elevato per i diritti e le libertà di persone fisiche
- Valutazione degli effetti del trattamento sulla protezione dei dati personali
- Consultare il DPO
- Obbligatorio se:
  - profilazione: valutazione sistematica e globale di aspetti personali relativi a persone fisiche
  - Trattamento su **larga scala di dati sensibili e giudiziari**
  - Sorveglianza sistematica su larga scala di zone accessibili al pubblico
- Contenuto: valutazione d‘impatto, giustificazione del trattamento, misure di sicurezza, …

CONTROLLO OTTICO- SORVEGLIANZA ELETTRONICA (VIDEO) E GEOLOCALIZZAZIONE



FORMAZIONE

Formazione del personale

- Quali dati vengono elaborati?
- Quali norme di sicurezza devono essere rispettate?
- Che cosa non si deve fare?

- Consiglio: Ottenere un impegno scritto per la riservatezza e il rispetto della protezione dei dati

Obbligo di informare l'interessato ai sensi dell’art. 15

OBBLIGHI DI DOCUMENTAZIONE (REPERTORIO DELLE PROCEDURE)

l'istituzione di un registro delle attività di trattamento (art. 30)

- Determinazione della persona responsabile/proprietario
- Determinare gli scopi del trattamento
- Determinazione delle persone interessate
- Quali terzi ricevono i dati (ad es. ufficio del personale)
- È in corso l'esportazione dei dati?
- Termini per la cancellazione dei dati
- Descrizione delle misure tecniche e organizzative

USO PRIVATO / AZIENDALE DI INTERNET E DELLA POSTA ELETTRONICA

MISURE TECNICO-ORGANIZZATIVE

Misure tecniche e organizzative:

- Accertare lo stato ATTUALE (nell'elenco delle attività di elaborazione)
- Determinare il potenziale di miglioramento
- Creare un piano di implementazione
- formazione del personale

STUDIO DI CASI DI RISCHIO

Misure tecniche e organizzative :

- Privacy per design
- Privacy per impostazione predefinita

- Attraverso la progettazione tecnologica e le preimpostazioni, devono essere elaborati solo i dati necessari per l'applicazione specifica.
- Attuare misure tecniche e organizzative adeguate.
- Garanzie in materia di protezione dei dati nella fase di sviluppo
- Stato dell'arte, costi di attuazione, natura e portata delle finalità del trattamento, probabilità di accadimento e possibili conseguenze

IT- / SICUREZZA DATI

Misure tecniche e organizzative :

- controlli di accesso
- Controlli del supporto dati
- controlli di stoccaggio
- controlli utente
- controlli di accesso
- Controlli della trasmissione
- controlli del trasporto
- recuperabilità
- attendibilità
- integrità dei dati

AUDIT ESTERNO IN MATERIA DI PROTEZIONE E PROTEZIONE DEI DATI

RESPONSABILITÀ DELLA DIREZIONE

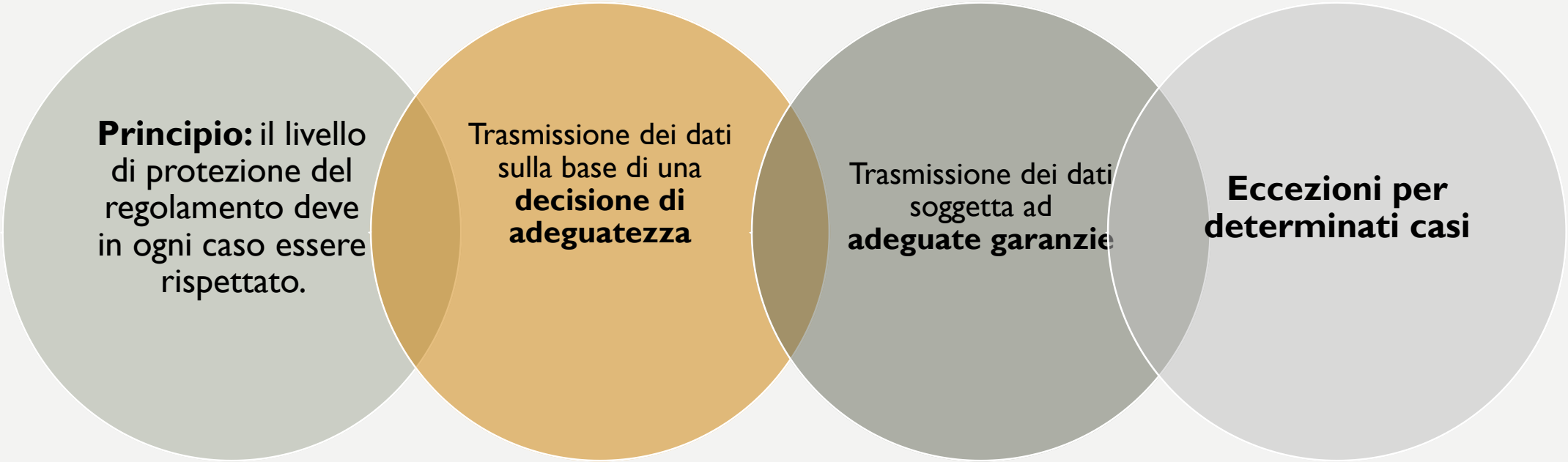
privacy by design (tutela della vita privata fin dalla progettazione) / privacy by default (tutela della vita privata fin dalla progettazione) (articolo 25):
solo i dati necessari per la specifica applicazione devono essere elaborati attraverso la progettazione tecnica e le impostazioni predefinite,A tal fine devono essere adottate misure tecniche e organizzative adeguate (ad es. pseudonimizzazione).Le garanzie in materia di protezione dei dati devono essere integrate già nella prima fase di sviluppo.Considerazione dello stato dell'arte, dei costi di attuazione, del tipo/ambito/circostanze e delle finalità del trattamento, nonché della diversa probabilità che si verifichino e della diversa gravità dei rischi per i diritti e le libertà. Tradotto con www.DeepL.com/Translator

RESPONSABILITÀ DEL RESPONSABILE AZIENDALE DELLA PROTEZIONE DEI DATI

- Ciò è disciplinato della GDPR 679/2016.

TRASFERIMENTO DEI DATI E PORTABILITÀ DELLE TRANSAZIONI - PROTEZIONE DELLA PRIVACY UE-USA

TRATTAMENTO TRANSFRONTALIERO DEI DATI (ARTICOLO 44 SEG.)



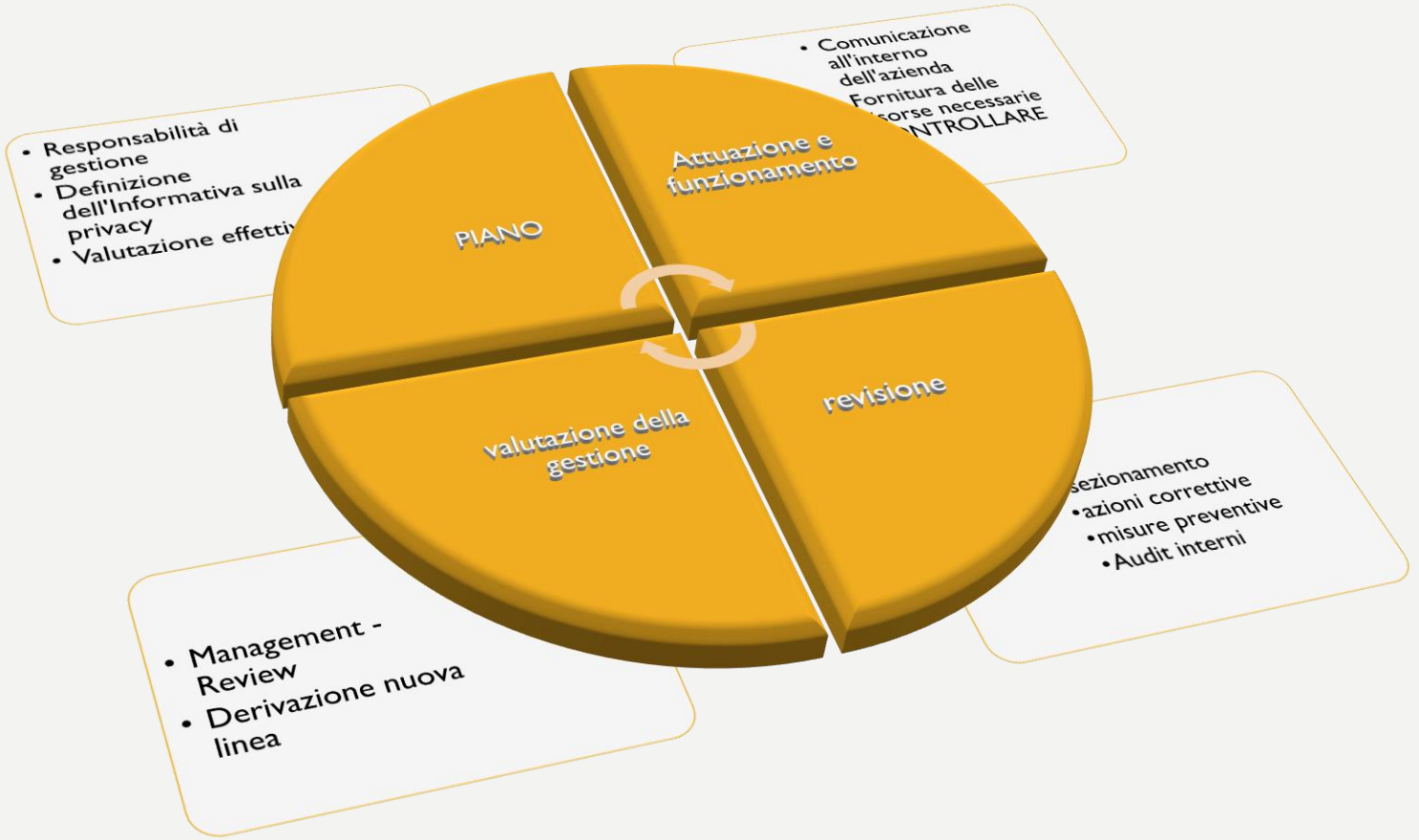
DIRITTO DI APPELLO - PROCEDURA

- **Procedimenti** paralleli (articoli 77 e 78): possibilità di ricorso sia dinanzi alle autorità di vigilanza che in sede giudiziaria.
- Potere di citare in giudizio le associazioni (articolo 80) per le organizzazioni senza scopo di lucro
- il risarcimento (art. 82) dei danni materiali e morali
  - Responsabilitá solidale in caso di pluralità di persone lese
  - Attenzione: Responsabilità dell'incaricato del trattamento degli ordini

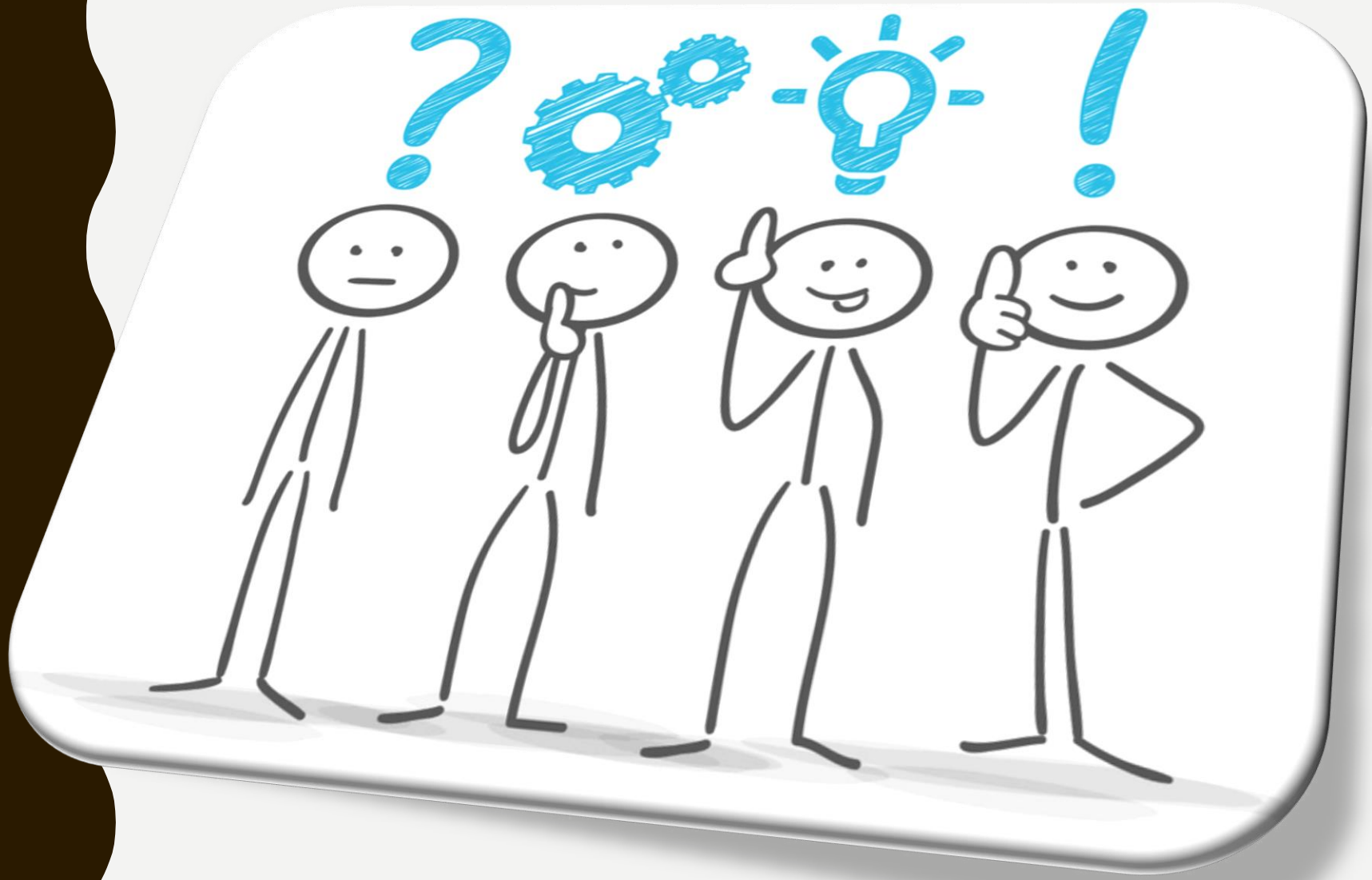
SANZIONI

- oltre agli ampi diritti di indagine, di azione penale, di consulenza e di consultazione, l'autorità di controllo può anche prevedere sanzioni amministrative (articoli 83 e seguenti).
- Nella peggiore delle ipotesi, le ammende possono ammontare a 20 milioni o al 4% del fatturato annuo mondiale, a seconda di quello che risulta essere più elevato;
- Inoltre, i ministeri possono stabilire ulteriori norme in materia di sanzioni efficaci, proporzionate e dissuasive in caso di violazione;

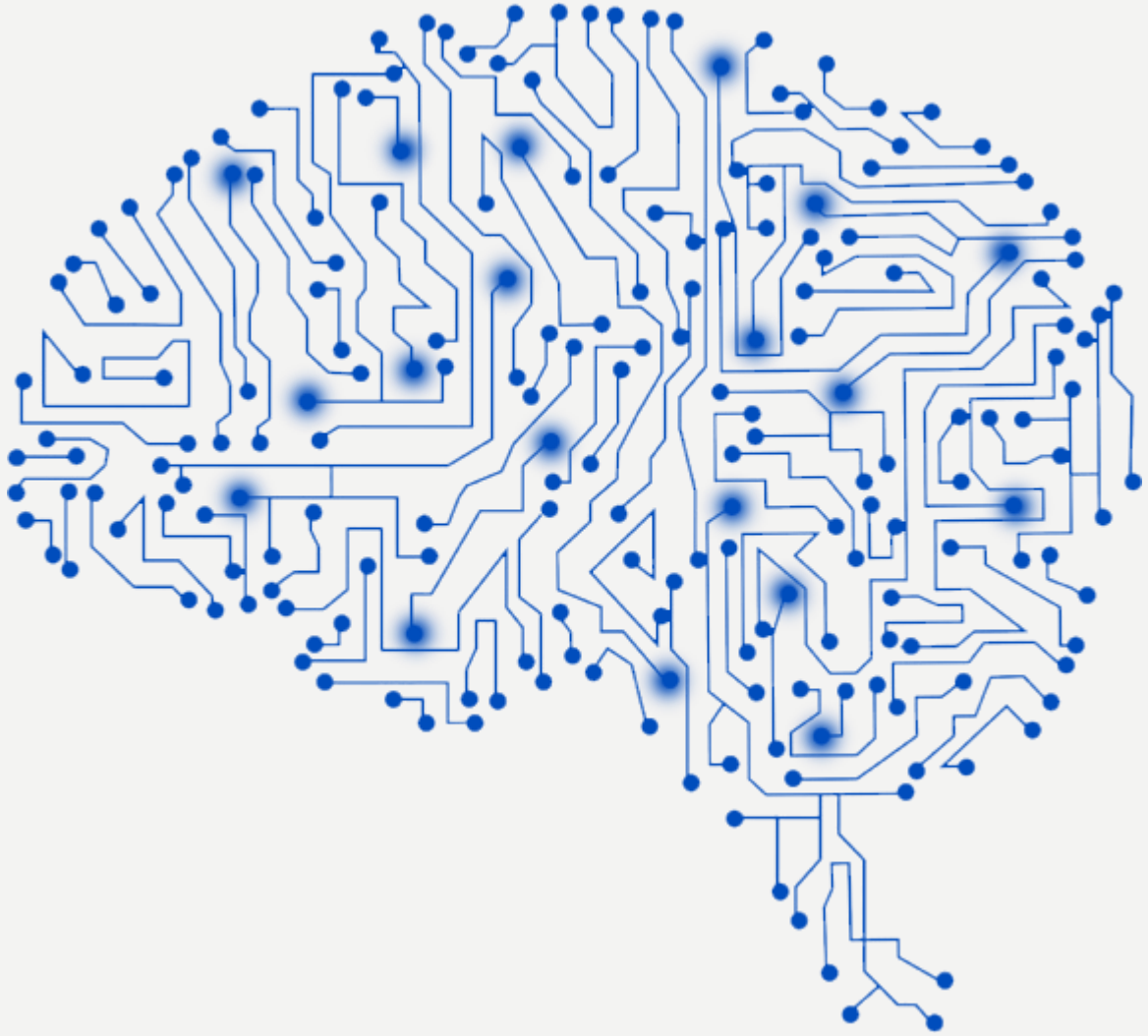
ATTUAZIONE PRATICA DEL DSGVO



INFINE …



- quesiti
- pulsioni
- proposte



GRAZIE PER IL TEMPO CHE CI HA DEDICATO

Tratta tutti come vorresti essere trattato tu stesso.....

inclusi i tuoi dati!

IFK Consulting GmbH

Vittorio Veneto Straße 67

39042 Brixen

Tel. 0472 831 107

info@ifkconsulting.com