Il nuovo regolamento UE in materia di protezione dei dati personali

Sviluppi e impatti per i soggetti pubblici

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

A TUTELA DI UN DIRITTO FONDAMENTALE

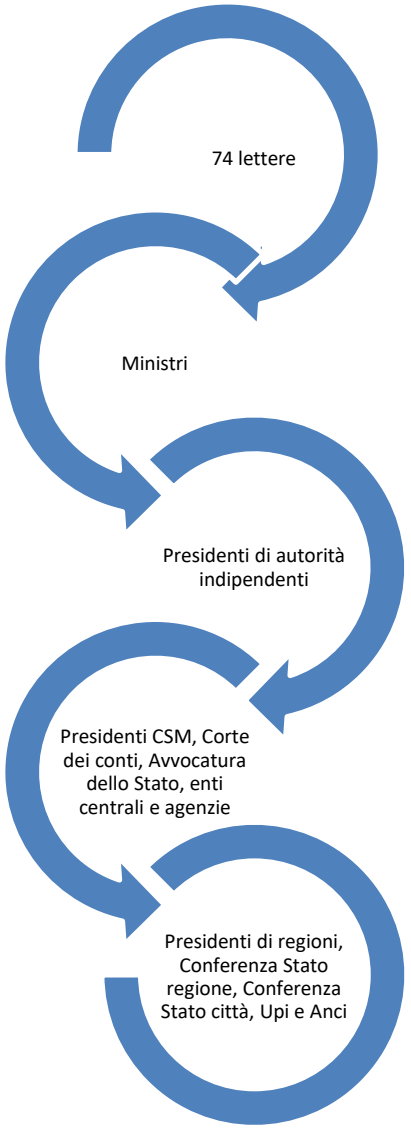
Dati personali e pubblica amministrazione
Il principio di responsabilizzazione e l'interazione con l'Autorità

Francesco Modafferi

Dirigente del Dipartimento libertà pubbliche e sanità

Punto di partenza - Iniziativa del 24 maggio

"Il Regolamento n. 2016/679, costituisce la vera architrave del nuovo sistema di regole in materia di protezione dei dati personali e si applicherà esattamente tra 365 giorni, a partire dal 25 maggio 2018, in tutti i Paesi UE".



Adattamento, integrazione e «margini di flessibilità»

Ove il regolamento preveda specificazioni o limitazioni delle sue norme ad opera del diritto degli Stati membri, gli Stati membri possono, nella misura necessaria per la coerenza e per rendere le disposizioni nazionali comprensibili alle persone cui si applicano, integrare elementi del regolamento nel proprio diritto nazionale

Sebbene i suoi obiettivi e principi rimangano tuttora validi, la direttiva 95/46/CE non ha impedito la frammentazione dell'applicazione della protezione dei dati personali nel territorio dell'Unione, né ha eliminato l'incertezza giuridica o la percezione, largamente diffusa nel pubblico, che in particolare le operazioni online comportino rischi per la protezione delle persone fisiche

SI

Il regolamento prevede un margine di manovra degli Stati membri per precisarne le norme, con riguardo al trattamento dei «dati sensibili», per quanto riguarda il trattamento per l'adempimento di un obbligo legale e per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri. In tal senso, il regolamento non esclude che il diritto degli Stati membri stabilisca con maggiore precisione le condizioni alle quali il trattamento è lecito

Un'efficace protezione dei dati personali in tutta l'Unione presuppone il rafforzamento e la disciplina dettagliata dei diritti degli interessati e degli obblighi di coloro che effettuano e determinano il trattamento dei dati personali, nonché poteri equivalenti per controllare e assicurare il rispetto delle norme di protezione dei dati personali e sanzioni equivalenti per le violazioni negli Stati membri

NO

Francesco Modafferi
Dirigente del Dipartimento libertà pubbliche e sanità

Cosa è successo nel frattempo?

La delega al governo

Nell'ambito del disegno di legge per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea (Legge di delegazione europea 2016-2017) è stata prevista la delega al Governo per dare attuazione alla Direttiva (UE) 2016/680 (art. 11) e adeguare la normativa nazionale alle disposizioni del RGPD (art. 13), fissando i seguenti principi e criteri direttivi:

ABROGARE espressamente le disposizioni del Codice in materia di trattamento dei dati personali, decreto legislativo 30 giugno 2003, n. 196 (d'ora in poi Codice), incompatibili con le disposizioni contenute nel RGPD;

MODIFICARE il Codice limitatamente a quanto necessario per dare attuazione alle disposizioni non direttamente applicabili contenute nel RGPD e coordinare le disposizioni vigenti in materia di protezione dei dati personali con le disposizioni del RGPD;

PREVEDERE, ove opportuno, il ricorso a specifici provvedimenti attuativi e integrativi adottati dal Garante per la protezione dei dati personali nell'ambito e per le finalità previsti dal RGPD;

ADEGUARE il sistema sanzionatorio, penale e amministrativo, vigente alle disposizioni del RGPD, con previsione di sanzioni penali e amministrative efficaci, dissuasive e proporzionate alla gravità delle violazioni commesse.

Le norme relative all'adeguamento della disciplina al RGPD dovranno essere adottate entro sei mesi dall'entrata in vigore della legge di delegazione.

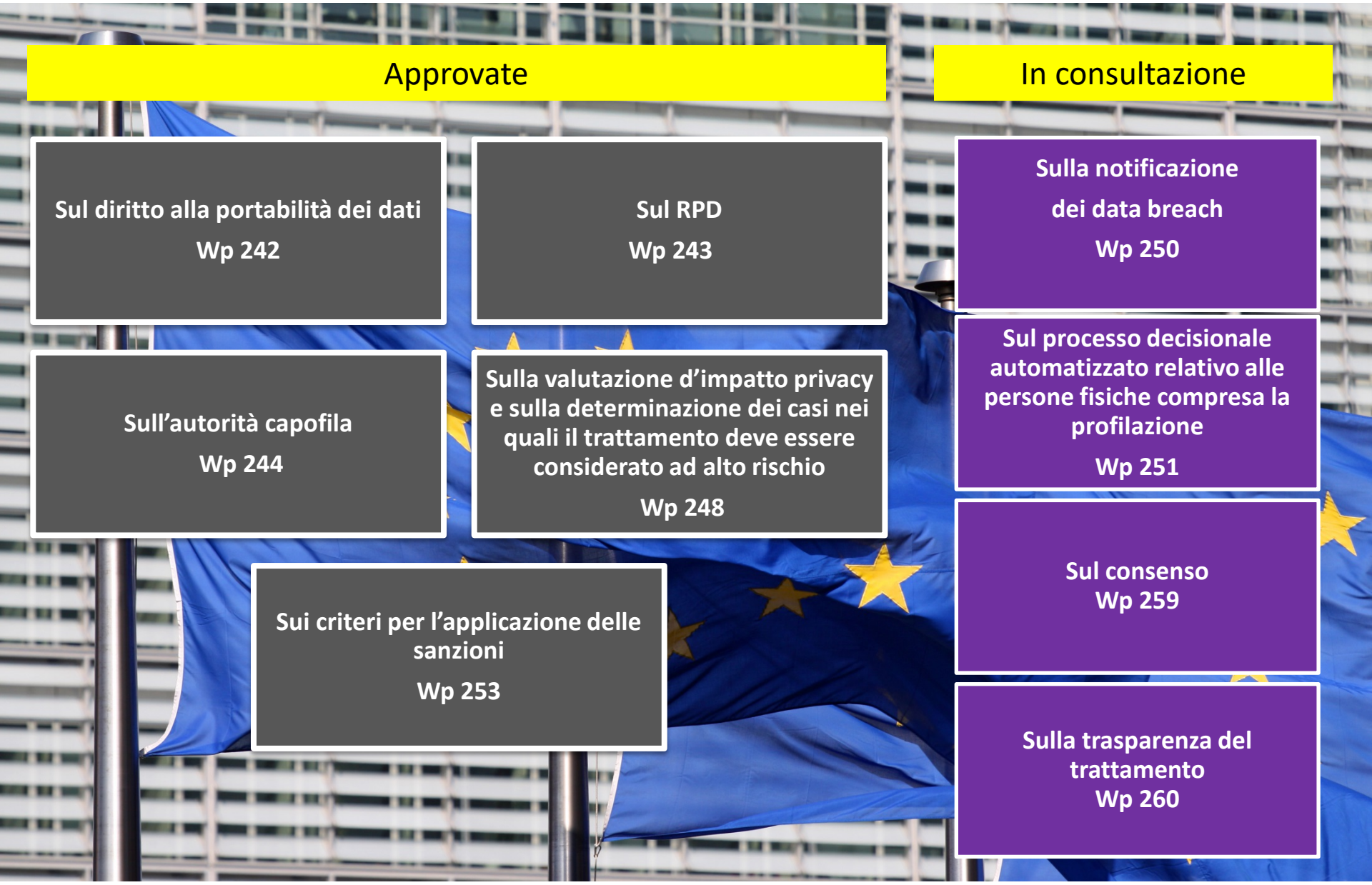
Francesco Modafferi
Dirigente del Dipartimento libertà pubbliche e sanità

Se tutto andrà bene...

Un decreto legislativo che conterrà:

- Le regole nazionali sulla protezione dei dati in ambito pubblico, sanitario, ricerca e statistica
- Le regole nazionali sull'autorità
- Le regole procedurali sulle sanzioni amministrative
- Le sanzioni penali

Linee guida Gruppo art. 29



Approvate

- Sul diritto alla portabilità dei dati
  Wp 242
- Sul RPD
  Wp 243
- Sull'autorità capofila
  Wp 244
- Sulla valutazione d'impatto privacy e sulla determinazione dei casi nei quali il trattamento deve essere considerato ad alto rischio
  Wp 248
- Sui criteri per l'applicazione delle sanzioni
  Wp 253

In consultazione

- Sulla notificazione dei data breach
  Wp 250
- Sul processo decisionale automatizzato relativo alle persone fisiche compresa la profilazione
  Wp 251
- Sul consenso
  Wp 259
- Sulla trasparenza del trattamento
  Wp 260

1. Quali sono i soggetti tenuti alla designazione del RPD?

2. Nel caso in cui il RPD sia un dipendente quale qualifica deve avere?

3. Quali certificazioni risultano idonee a legittimare il RPD?

4. Con quale atto formale deve essere designato il RPD?

5. La designazione di un RPD interno richiede necessariamente anche la costituzione di un apposito ufficio?

6. È ammissibile che uno stesso titolare / responsabile del trattamento abbia più di un RPD?

7. Quali sono gli ulteriori compiti e funzioni che possono essere assegnati a un RPD?

Le indicazioni del Garante sul responsabile della protezione dei dati

15 dicembre 2017

Il sistema è quindi ancora in costruzione

Fr[illegible]co Modafferi
Dirigente del Dipartimento
libertà pubbliche e sanità

Il programma di oggi

1. Principi e diritti
2. Organizzazione privacy
3. RPD
4. Registri
5. Valutazione di impatto
6. Data breach

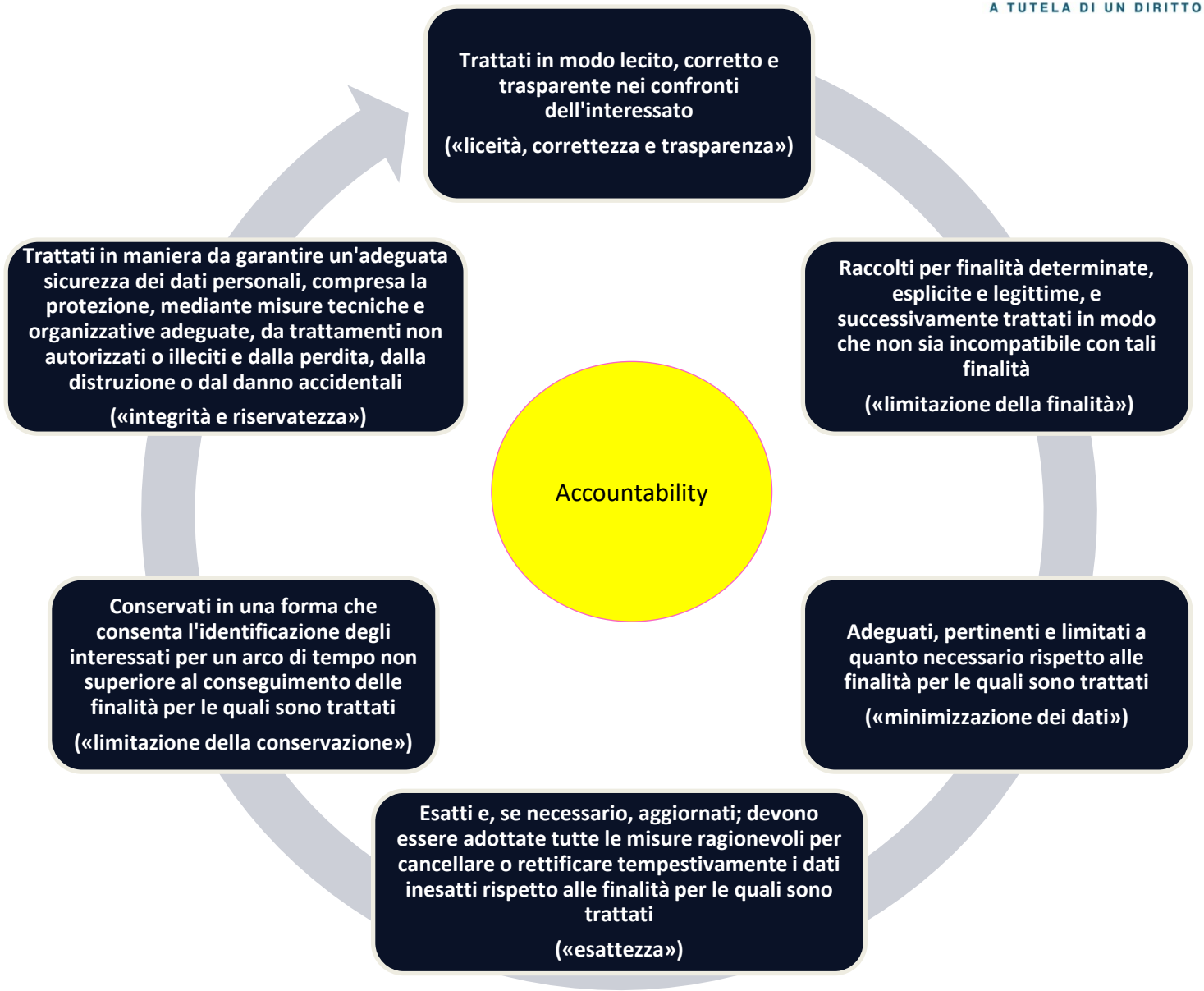
D

Francesco Modafferi
Dirigente del Dipartimento libertà pubbliche e sanità

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI
A TUTELA DI UN DIRITTO FONDAMENTALE

Principio di Accountability

Francesco Modafferi
Dirigente del Dipartimento
libertà pubbliche e sanità



Francesco Modafferi
Dirigente del Dipartimento libertà pubbliche e sanità

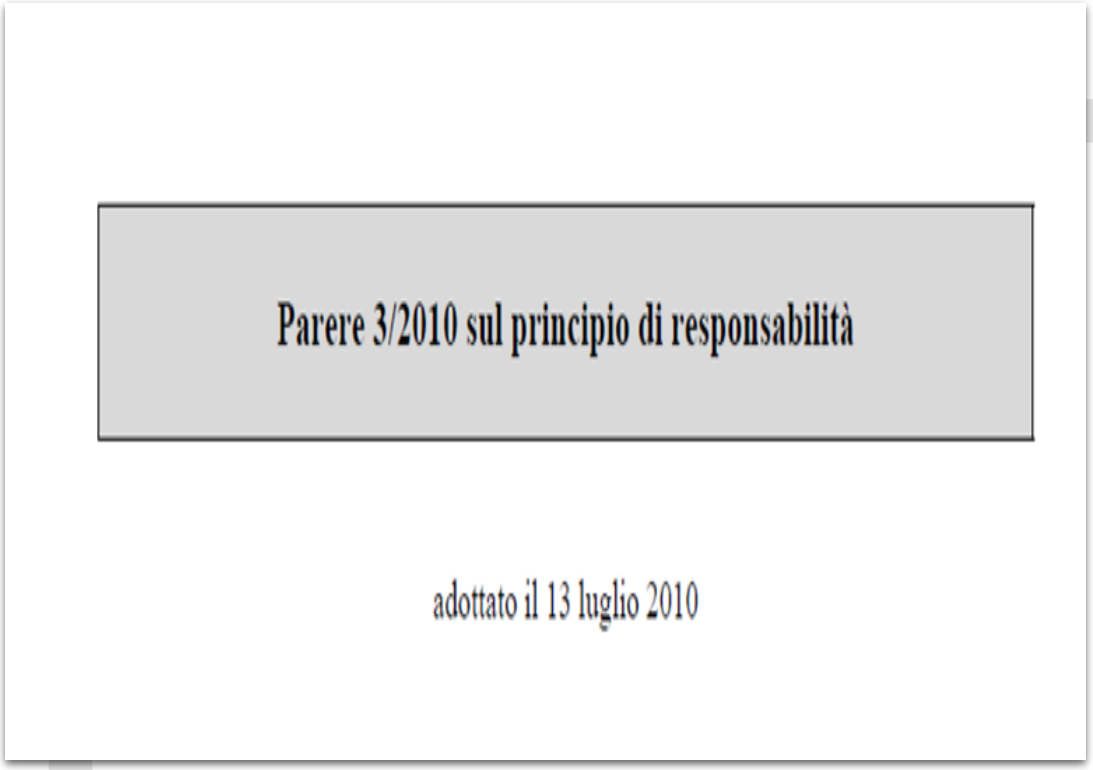
Dalla forma alla sostanza

Il titolare del trattamento è:

competente per il rispetto dei principi applicabili al trattamento di dati personali

in grado di comprovarlo («responsabilizzazione»)

Francesco Modafferi
Dirigente del Dipartimento libertà pubbliche e sanità



Principio di «responsabilizzazione»

L'architettura giuridica dei meccanismi di responsabilità prevede un obbligo di base vincolante per tutti i titolari del trattamento che comprende due elementi:

- **l'attuazione di misure e/o procedure**
- **la conservazione delle relative prove.**

La nuova disposizione non mira ad assoggettare i titolari del trattamento a nuovi principi, ma a garantire l'effettiva osservanza di quelli esistenti

Francesco Modafferi
Dirigente del Dipartimento libertà pubbliche e sanità

Francesco Modafferi
Dirigente del Dipartimento libertà pubbliche e sanità

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI
A TUTELA DI UN DIRITTO FONDAMENTALE

L'aver attuato e verificato le misure influisce sul grado di responsabilità del titolare o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto

Le procedure interne sul trattamento dei dati personali (policies/istruzioni) erano conosciute e applicate nell'ambito dell'organizzazione? (Art. 24).

Il titolare del trattamento ha implementato misure tecniche per implementare il principio di protezione by design o by default (art.25)?

Linee guida sull'applicazione delle sanzioni amministrative del 3 ottobre 2017

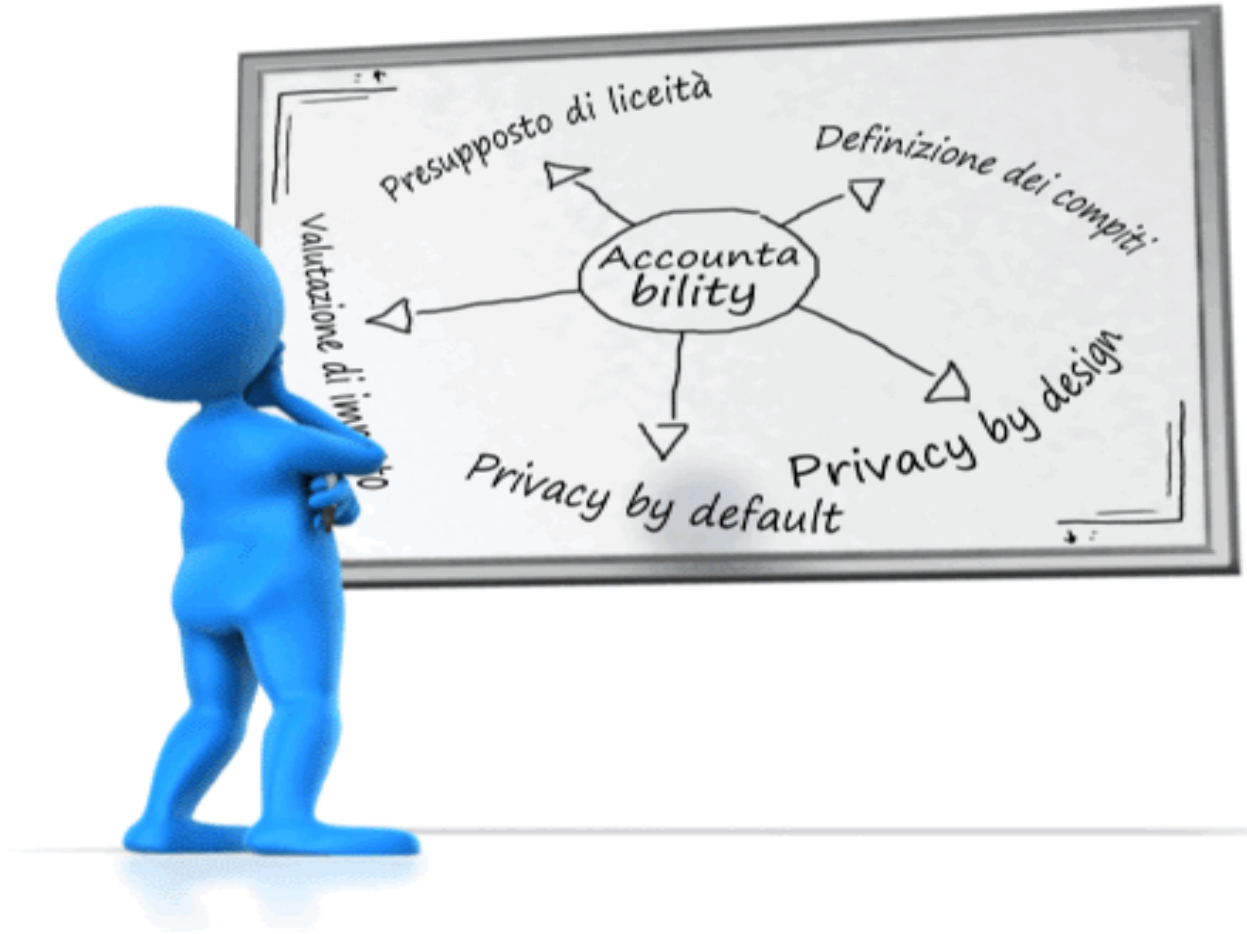
WP 253

Il titolare o il responsabile del trattamento hanno implementato un appropriato livello di sicurezza dei dati (art. 32)?

Il titolare del trattamento ha implementato misure organizzative per implementare il principio di protezione by design o by default in tutti gli ambiti dell'organizzazione (art. 25)?

Francesco Modafferi
Dirigente del Dipartimento libertà pubbliche e sanità

Necessità di un approccio sistemico



Francesco Modafferi
Dirigente del Dipartimento libertà pubbliche e sanità