RISCHI E INCIDENTI

RGPD

REGOLAMENTO (UE) 2016/679

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Il bilancio dei primi 4 mesi di applicazione

Un primo bilancio sull'applicazione in Italia, a partire dal 25 maggio, del **Regolamento europeo in materia di protezione dei dati personali** mostra come pubbliche amministrazioni, mondo delle imprese e cittadini abbiano colto l'importanza del nuovo quadro giuridico e le opportunità che esso offre in termini di tutela e garanzie per le persone.

Comunicazioni dei dati di contatto degli RPD

40.738

Reclami e segnalazioni

2.547

(1.795 nello stesso periodo 2017)

Notificazioni di Data Breach

305

Contatti con l'URP

circa 7.200

(circa 4.400 nello stesso periodo 2017)

Dati aggiornati al 28 settembre 2018

www.garanteprivacy.it

RISCHI E MISURE DI SICUREZZA

(83) Per mantenere la sicurezza e prevenire trattamenti in violazione al presente regolamento, il titolare del trattamento o il responsabile del trattamento dovrebbe valutare i rischi inerenti al trattamento e attuare misure per limitare tali rischi, quali la cifratura. Tali misure dovrebbero assicurare un adeguato livello di sicurezza, inclusa la riservatezza, tenuto conto dello stato dell'arte e dei costi di attuazione rispetto ai rischi che presentano i trattamenti e alla natura dei dati personali da proteggere. Nella valutazione del rischio per la sicurezza dei dati è opportuno tenere in considerazione i rischi presentati dal trattamento dei dati personali, come la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati, che potrebbero cagionare in particolare un danno fisico, materiale o immateriale.

Articolo 32

Sicurezza del trattamento (C83)

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

SICUREZZA: PERCHE'?

Per garantire che:

- i dati non vadano distrutti o persi anche in modo accidentale
- solo le persone autorizzate possano avere accesso ai dati
- non siano effettuati trattamenti contrari alle norme di legge o diversi da quelli per cui i dati erano stati raccolti.

3 ELEMENTI FONDAMENTALI

RISERVATEZZA: il dato deve essere accessibile solamente agli incaricati e ai responsabili della gestione del dato stesso o a soggetti con specifiche autorizzazioni alla visualizzazione inerenti la materia di trattamento del dato.

Esempio 1 – doc WORD salvato su server

Esempio 2 – custodia del documento stampato

Esempio 3 – solo gli autorizzati devono conoscere i beneficiari di un contributo

3 ELEMENTI FONDAMENTALI

INTEGRITA’ : il dato deve essere protetto da possibili modifiche o manomissioni. Vi deve essere la certezza che il dato trattato sia esatto e veritiero.

Esempio - Il dato presente in una banca dati anagrafica deve essere accessibile in modifica solamente attraverso l’autenticazione del soggetto autorizzato e incaricato al trattamento.

3 ELEMENTI FONDAMENTALI

DISPONIBILITA’ : certezza di poter ottenere, accedere ed utilizzare il dato nel momento in cui se ne ha la necessità da parte dei soggetti autorizzati al trattamento del dato stesso.

Esempio 1 - Un dato contenuto in un sistema informatico, in caso di caduta di alimentazione elettrica diventa indisponibile.

Esempio 2 - Un dato situato presso una risorsa ad accesso esclusivo (PC, oppure armadio) diventa indisponibile in caso di assenza dell’utilizzatore.

Esempio 3 – l’albo pretorio non è raggiungibile

COME GARANTIRE LA SICUREZZA DEI DATI

Per assicurare la riservatezza, l'integrità e la disponibilità dei dati occorre mettere in sicurezza da possibili minacce tutte le risorse coinvolte nel loro trattamento:

- Risorse logistiche (luoghi fisici e attrezzature)
- Risorse hardware (pc, server, apparati di rete)
- Risorse software (programmi, sistemi operativi)
- Archivi cartacei e informatici

MANUALE DELLE MISURE

MANUALE DELLE MISURE

SI.NET
Servizi Informatici

DATA BREACH

Articolo 33

Notifica di una violazione dei dati personali all'autorità di controllo (C85, C87, C88)

1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

Il titolare del trattamento dovrà comunicare eventuali violazioni dei dati personali (*data breach*) all'Autorità nazionale di protezione dei dati.
Se la violazione dei dati rappresenta una minaccia per i diritti e le libertà delle persone, il titolare dovrà informare in modo chiaro, semplice e immediato anche tutti gli interessati e offrire indicazioni su come intende limitare le possibili conseguenze negative.

DATA BREACH

SI.NET Servizi Informatici

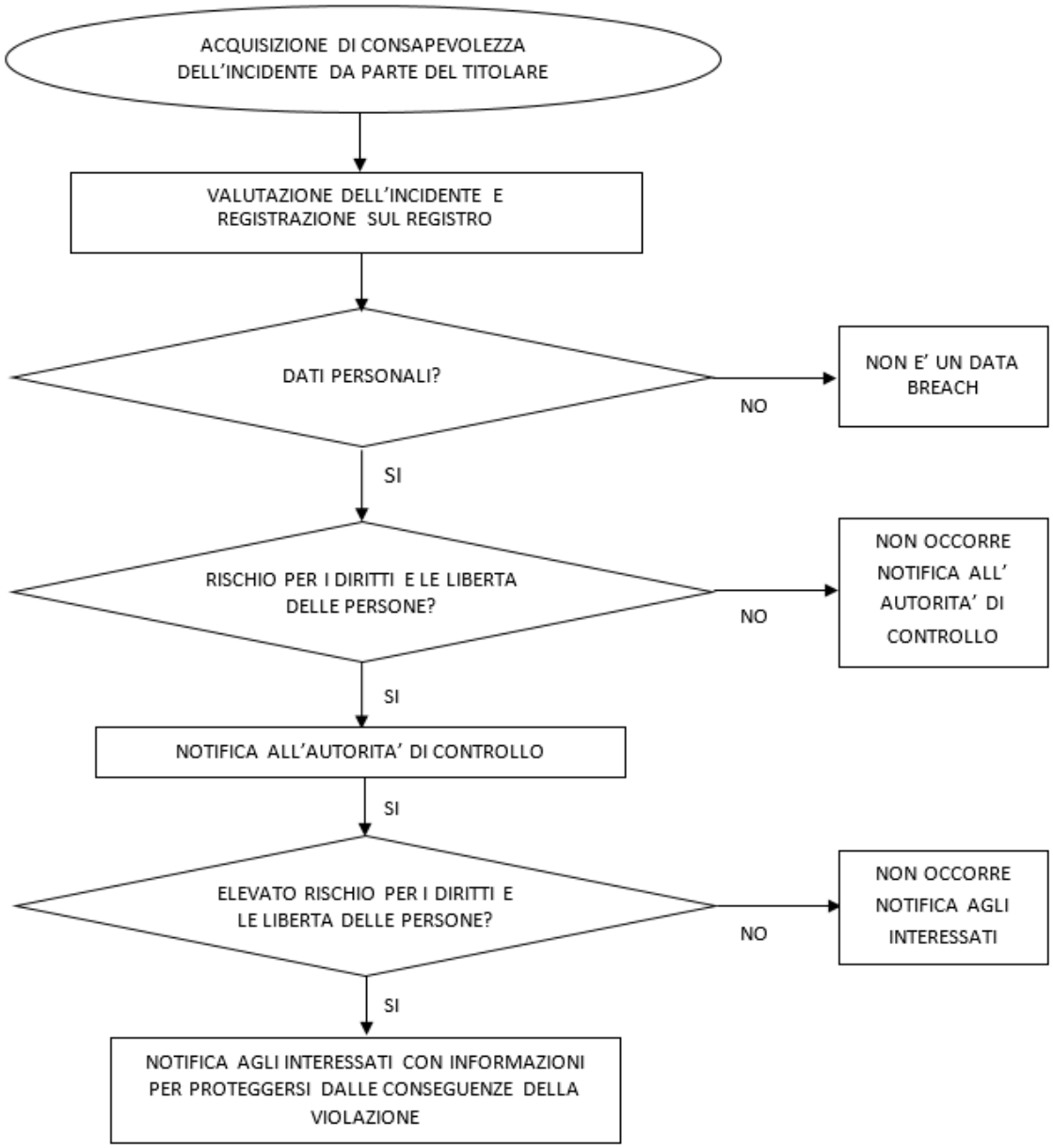
COSA CAMBIA

- A partire dal 25 maggio 2018, **tutti i titolari** – e non soltanto i fornitori di servizi di comunicazione elettronica accessibili al pubblico, come avviene oggi – dovranno notificare all'Autorità di controllo le violazioni di dati personali di cui vengano a conoscenza, **entro 72 ore** e comunque "senza ingiustificato ritardo", ma **soltanto se ritengono probabile che da tale violazione derivino rischi** per i diritti e le libertà degli interessati (si veda considerando 85). Pertanto, **la notifica all'Autorità** dell'avvenuta violazione **non è obbligatoria**, essendo subordinata alla valutazione del rischio per gli interessati che spetta, ancora una volta, al titolare. Se la probabilità di tale rischio è elevata, si dovrà informare delle violazione anche gli interessati, sempre "senza ingiustificato ritardo"; fanno eccezione le circostanze indicate al paragrafo 3 dell'art. 34, che coincidono solo in parte con quelle attualmente menzionate nell'art. 32-bis del Codice. **I contenuti della notifica** all'Autorità e della comunicazione agli interessati sono indicati, **in via non esclusiva, agli art. 33 e 34 del regolamento**.

Raccomandazioni

Tutti i titolari di trattamento dovranno in ogni caso **documentare le violazioni** di dati personali subite, anche se non notificate all'autorità di controllo e non comunicate agli interessati, nonché le relative circostanze e conseguenze e i provvedimenti adottati (si veda art. 33, paragrafo 5); tale obbligo non è diverso, nella sostanza, da quello attualmente previsto dall'art. 32-bis, comma 7, del Codice.
Si raccomanda, pertanto, ai titolari di trattamento di adottare le misure necessarie a documentare eventuali violazioni, essendo peraltro tenuti a fornire tale documentazione, su richiesta, al Garante in caso di accertamenti.

DATA BREACH – STEP OPERATIVI



DATA BREACH E'…

SCENARI: DISTRUZIONE

Un insieme di dati personali, a seguito di incidente o azione fraudolenta, **non è più nella disponibilità del titolare**, né di altri. In caso di richiesta del dato da parte dell'interessato non sarebbe possibile produrlo.

SCENARI: PERDITA

Un insieme di dati personali, a seguito di incidente o azione fraudolenta, **non è più nella disponibilità del titolare, ma potrebbe essere nella disponibilità di terzi (lecitamente o illecitamente)**. In caso di richiesta di dato da parte dell'interessato non sarebbe possibile produrlo, ed è possibile che terzi possano avere impropriamente accesso al dato.

SCENARI: MODIFICA

Un insieme di dati personali, a seguito di incidente o azione fraudolenta, è stato **irreversibilmente modificato, senza possibilità di ripristinare lo stato originale**. In caso di richiesta del dato da parte dell'interessato **non sarebbe possibile produrlo con certezza che non sia stato alterato**.

SCENARI: DIVULGAZIONE NON AUTORIZZATA

Un insieme di dati personali (e riconducibili all'individuo direttamente o indirettamente), a seguito di incidente o azione fraudolenta, viene **trasmesso a terze parti senza il consenso dell'interessato o in violazione del regolamento dell'organizzazione**.

SCENARI: ACCESSO NON AUTORIZZ.

Un insieme di dati personali (e riconducibili all'individuo direttamente o indirettamente) sono stati resi **disponibili per un intervallo di tempo a persone (anche incaricati dal titolare) non titolati ad accedere al dato secondo principio di pertinenza e non eccedenza**, o secondo i regolamenti dell'organizzazione.

SCENARI: INDISPONIBILITA' TEMPORANEA DEL DATO

Un insieme di dati personali, a seguito di incidente, azione fraudolenta o involontaria, è **non disponibile per un periodo di tempo che lede i diritti dell'interessato**.

WP29 - CASO 1

Un titolare ha archiviato un backup di un archivio di dati personali crittografati su una chiave USB. La chiave viene rubata.

WP29 - CASO 1

Un titolare ha archiviato un backup di un archivio di dati personali crittografati su una chiave USB. La chiave viene rubata.

Notifica all'Autorità di Controllo: NO

Notifica all'interessato: NO

WP29 - CASO 2

Un titolare gestisce un servizio online. A seguito di un attacco informatico su quel servizio, i dati personali degli individui vengono rubati.

WP29 - CASO 2

Un titolare gestisce un servizio online. A seguito di un attacco informatico su quel servizio, i dati personali degli individui vengono rubati.

Notifica all'Autorità di Controllo: SI, riferire all'autorità di vigilanza se vi sono probabili conseguenze per le persone.

Notifica all'interessato: SI, riferire alle persone a seconda della natura dei dati personali interessati e se la gravità delle probabili conseguenze per gli individui è elevata.

WP29 - CASO 3

Una breve interruzione di corrente di alcuni minuti presso il call center di un titolare significa che i clienti non sono in grado di chiamare il titolare e accedere ai loro record.

WP29 - CASO 3

Una breve interruzione di corrente di alcuni minuti presso il call center di un titolare significa che i clienti non sono in grado di chiamare il titolare e accedere ai loro record.

Notifica all'Autorità di Controllo: NO

Notifica all'interessato: NO

WP29 - CASO 4

Un titolare subisce un attacco ransomware che provoca la crittografia di tutti i dati. Non sono disponibili back-up e i dati non possono essere ripristinati. Durante le indagini, diventa chiaro che l'unica funzionalità del ransomware era quella di crittografare i dati e che non c'erano altri malware presenti nel sistema.

WP29 - CASO 4

Un titolare subisce un attacco ransomware che provoca la crittografia di tutti i dati. Non sono disponibili back-up e i dati non possono essere ripristinati. Durante le indagini, diventa chiaro che l'unica funzionalità del ransomware era quella di crittografare i dati e che non c'erano altri malware presenti nel sistema.

Notifica all'Autorità di Controllo: SI, riferire all'autorità di vigilanza, se ci sono probabili conseguenze per gli individui in quanto si tratta di una perdita di disponibilità.
Notifica all'interessato: SI, riferire ai singoli, a seconda della natura dei dati personali interessati e del possibile effetto della mancanza di disponibilità dei dati, nonché di altre possibili conseguenze.

WP29 - CASO 5

Un individuo telefona al call center di una banca per segnalare una violazione dei dati. L'individuo ha ricevuto una dichiarazione mensile per qualcun altro.
Il titolare del trattamento intraprende un'investigazione breve (ossia completata entro 24 ore) e stabilisce con ragionevole certezza che si è verificata una violazione dei dati personali e se ha un difetto sistemico che potrebbe significare che altri individui sono o potrebbero essere interessati.

WP29 - CASO 5

Un individuo telefona al call center di una banca per segnalare una violazione dei dati. L'individuo ha ricevuto una dichiarazione mensile per qualcun altro.
Il titolare del trattamento intraprende un'investigazione breve (ossia completata entro 24 ore) e stabilisce con ragionevole certezza che si è verificata una violazione dei dati personali e se ha un difetto sistemico che potrebbe significare che altri individui sono o potrebbero essere interessati.

Notifica all'Autorità di Controllo: SI
Notifica all'interessato: Solo le persone colpite vengono avvisate se c'è un rischio elevato ed è chiaro che gli altri non sono stati colpiti.

WP29 - CASO 6

Un titolare gestisce un sito di e-commerce e ha clienti in più Stati membri. Il sito subisce un attacco informatico e usernames, password e cronologia degli acquisti sono pubblicati online dall'attaccante.

WP29 - CASO 6

Un titolare gestisce un sito di e-commerce e ha clienti in più Stati membri. Il sito subisce un attacco informatico e usernames, password e cronologia degli acquisti sono pubblicati online dall'attaccante.

Notifica all’Autorità di Controllo: SI, segnalare all'autorità di vigilanza principale se coinvolge l'elaborazione transfrontaliera.

Notifica all’interessato: SI, poiché potrebbe portare ad alto rischio.

WP29 - CASO 7

I dati personali di un gran numero di studenti vengono erroneamente inviati alla mailing list sbagliata con più di 1000 destinatari.

WP29 - CASO 7

I dati personali di un gran numero di studenti vengono erroneamente inviati alla mailing list sbagliata con più di 1000 destinatari.

Notifica all'Autorità di Controllo: SI, occorre riferire all'Autorità di Vigilanza.

Notifica all'interessato: SI, riferire alle persone in base alla portata e al tipo di dati personali coinvolti e alla gravità delle possibili conseguenze.

WP29 - CASO 8

Una e-mail di marketing diretto viene inviata ai destinatari nei campi "a:" o "cc:", consentendo in tal modo a ciascun destinatario di vedere l'indirizzo e-mail di altri destinatari.

WP29 - CASO 8

Una e-mail di marketing diretto viene inviata ai destinatari nei campi "a:" o "cc:", consentendo in tal modo a ciascun destinatario di vedere l'indirizzo e-mail di altri destinatari.

Notifica all'Autorità di Controllo: SI, la notifica all'autorità di vigilanza può essere obbligatoria se un numero elevato di persone è interessato, se vengono rivelati dati sensibili (ad esempio una mailing list di uno psicoterapeuta) o se altri fattori presentano rischi elevati (ad esempio, la posta contiene le password iniziali).
Notifica all'interessato: SI, occorre riferire alle persone in base alla portata e al tipo di dati personali coinvolti e alla gravità delle possibili conseguenze.

COSA FARE IN CASO DI INCIDENTE

In caso di incidente è necessario contattare immediatamente il Responsabile Protezione Dati, al fine di analizzare la tipologia di incidente e stabilire se è un data breach da segnalare al Garante della Privacy (ed eventualmente agli interessati)

INTERAZIONI NORMATIVE

GDPR

D.Lgs. 196/2003

Circ. AgID 2/2017

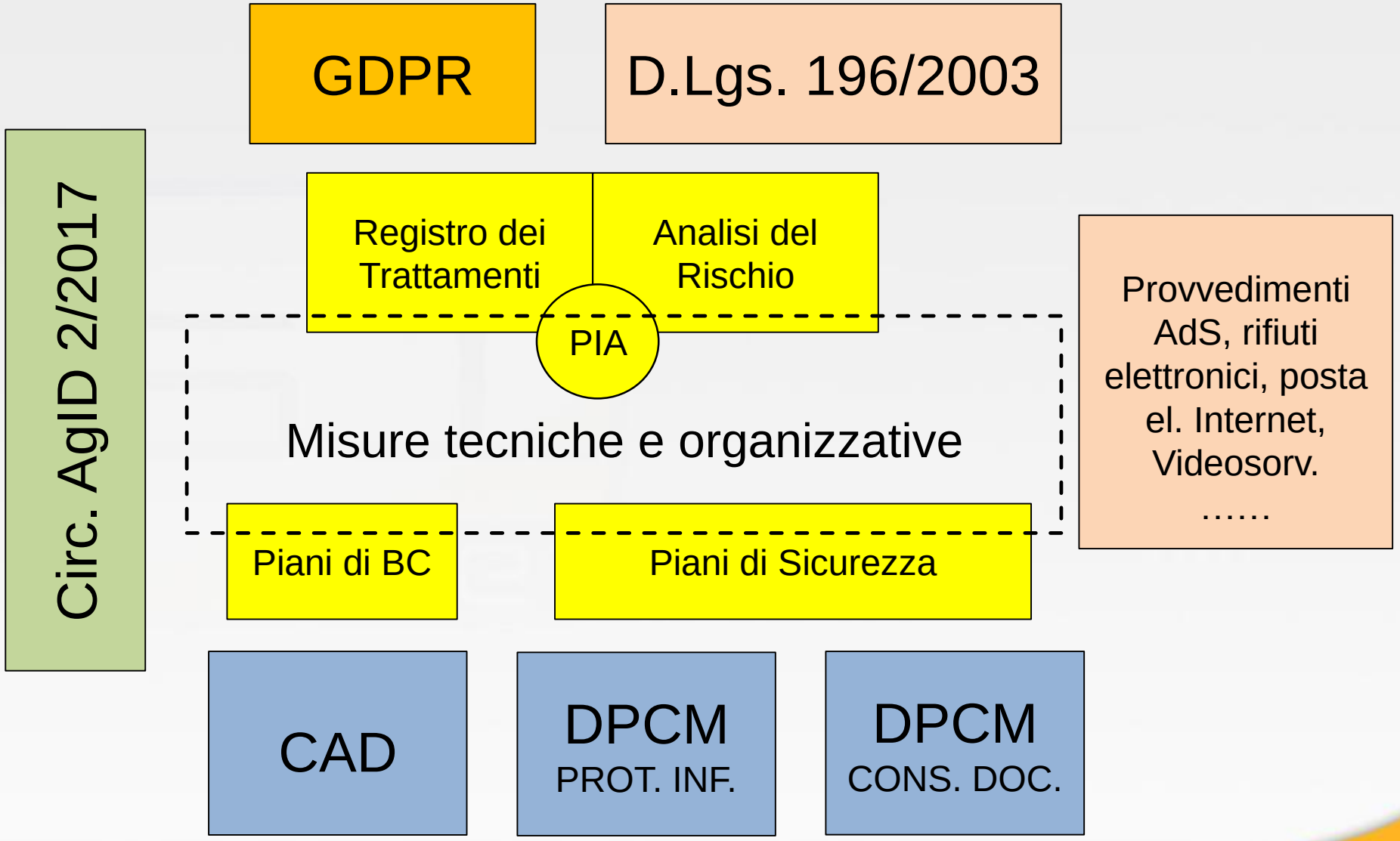
Provvedimenti AdS, rifiuti elettronici, posta el. Internet, Videosorv.
……

CAD

DPCM
PROT. INF.

DPCM
CONS. DOC.

SISTEMA GESTIONE PRIVACY (SGP)



Grazie per l'attenzione

aldo.lupi@sinetinformatica.it

Per seguire l'innovazione nella PA:

www.sinetinformatica.it

www.sinetinformatica.it/twitter

www.sinetinformatica.it/facebook