IL NUOVO REGOLAMENTO EUROPEO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI: DA OBBLIGO A OPPORTUNITÀ

INTERAZIONI NORMATIVE

GDPR

D.Lgs. 196/2003

Circ. AgID 2/2017

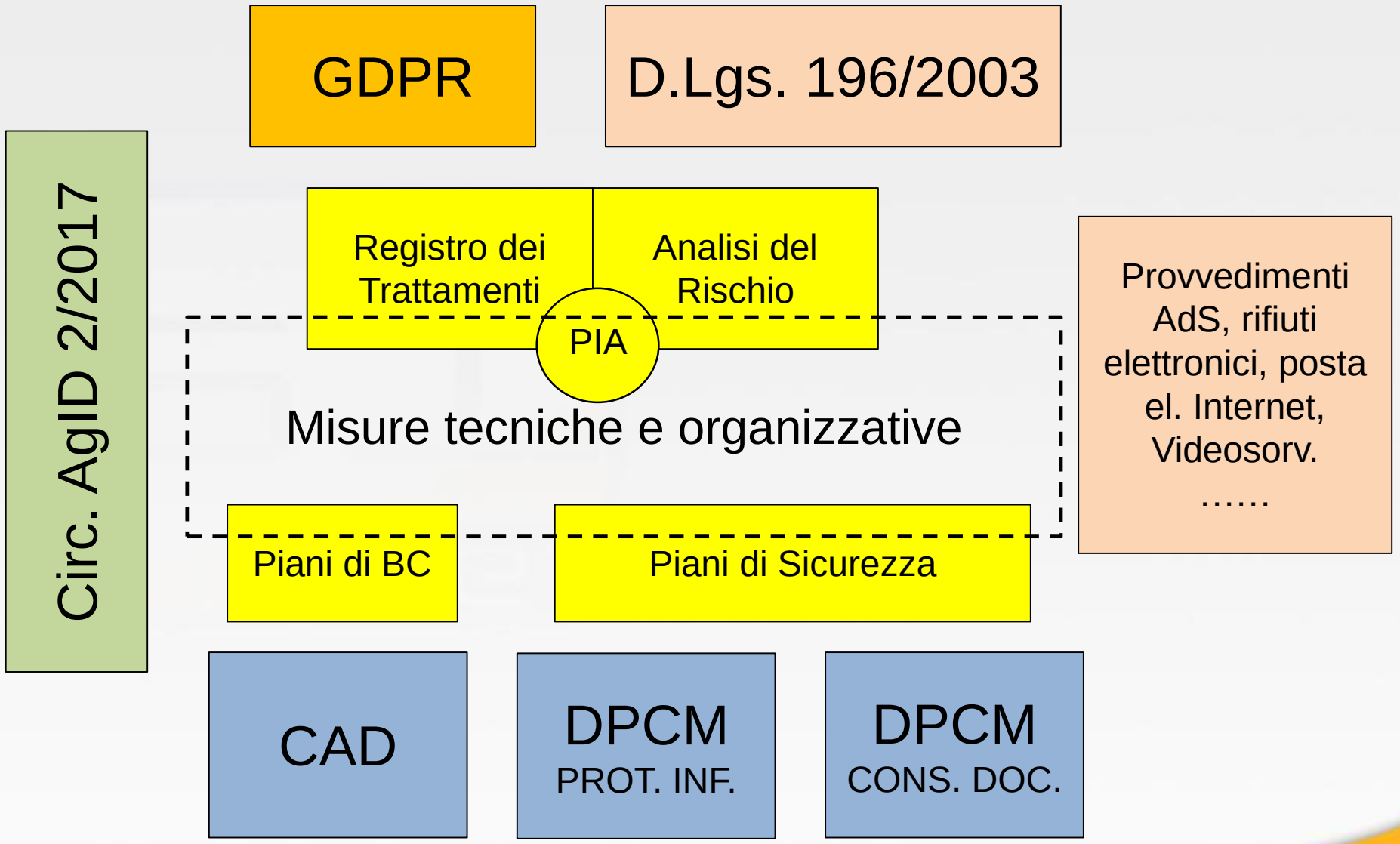
Provvedimenti AdS, rifiuti elettronici, posta el. Internet, Videosorv.
……

CAD

DPCM
PROT. INF.

DPCM
CONS. DOC.

SISTEMA GESTIONE PRIVACY (SGP)



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

IL CONTESTO ICT









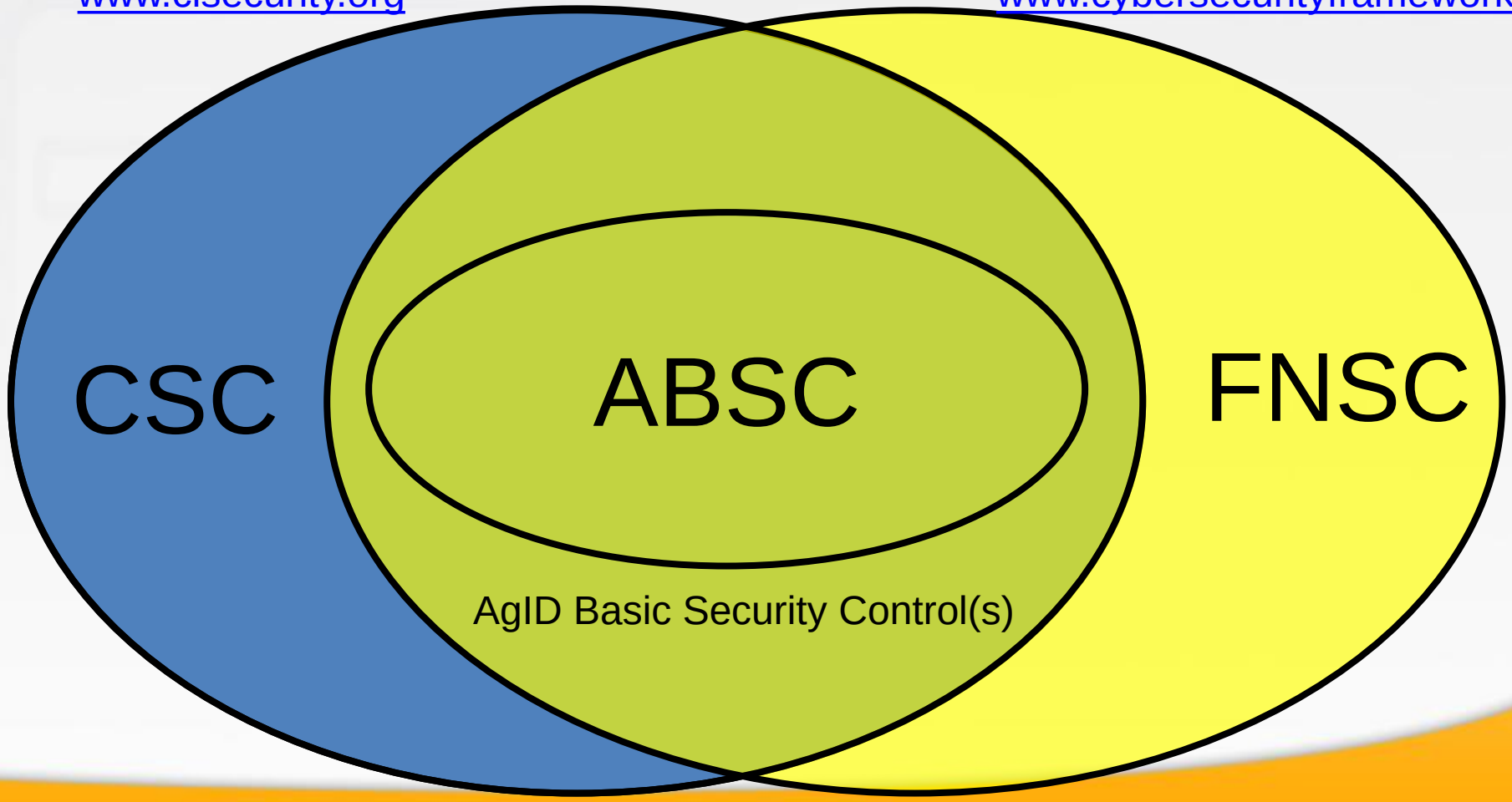




RIFERIMENTI DI SICUREZZA

Critical Security Controls for
Effective Cyber Defense
(Center for Internet Security)
www.cisecurity.org

Framework Nazionale
Sicurezza Cibernetica
(CIS La Sapienza)
www.cybersecurityframework.it



CLASSI DI MISURE DEI CONTROLLI

ABSC 1: INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI

ABSC 2: INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI

CLASSI DI MISURE DEI CONTROLLI

ABSC 3: PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER

ABSC 4: VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ

CLASSI DI MISURE DEI CONTROLLI

ABSC 5: USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

ABSC 8: DIFESE CONTRO I MALWARE

CLASSI DI MISURE DEI CONTROLLI

ABSC 10: COPIE DI SICUREZZA

ABSC 13: PROTEZIONE DEI DATI

GDPR – violazione dati personali

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.

GDPR – violazione dati personali

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.

COSA E' DATA BREACH?

DATA BREACH E'…

PROVV. SU DATA BREACH [7400401]

Attacco informatico ai danni di piattaforma tecnologica di cui si è evidenziata la debolezza delle misure di sicurezza.

L'elemento di maggiore criticità di tale procedura è risultata la potenziale debolezza della password scelta in fase di registrazione (è infatti risultato possibile scegliere password di lunghezza inferiore agli otto caratteri).

PROVV. SU DATA BREACH [7400401]

ACCERTAMENTI ISPETTIVI

Ruoli di titolare e responsabile

Al riguardo, si evidenzia che la **mancata designazione delle società xyz1 e xyz2 quali responsabili del trattamento** dei dati personali degli utenti …. configura l'**illiceità del trattamento** medesimo in ragione della **comunicazione dei dati a soggetti terzi, in mancanza del consenso degli interessati**; pertanto, questa Autorità, si riserva di verificare, con autonomo procedimento, la sussistenza dei presupposti per l'eventuale contestazione delle sanzioni amministrative di cui all'art. 162, comma 2bis del Codice.

PROVV. SU DATA BREACH [7400401]

ACCERTAMENTI ISPETTIVI

Verifiche tecnologiche

a) il portale web e parte della piattaforma sono stati realizzati avvalendosi di un **prodotto software**… versione … affetta da **indiscutibile obsolescenza tecnica** (il prod. individuava nel 2013 la "fine vita")

b) la registrazione delle **password** avveniva **in chiaro**

c) il portale **non realizzava policy efficaci sulla qualità delle password**, ammettendo l'uso di password **banali**, facilmente esposte alla **decifrazione e ad attacchi di tipo brute force** anche in modalità interattiva online

PROVV. SU DATA BREACH [7400401]

ACCERTAMENTI ISPETTIVI

Verifiche tecnologiche

d) i **vulnerability assessment** commissionati dal titolare hanno evidenziato una serie di criticità cui sarebbe stato possibile porre rimedio avvalendosi di una metodologia di sviluppo del software maggiormente strutturata (c.d. approccio basato sulla "Data protection by design ")

e) *[**Informazioni di rilevanza politica, ndr**]…* associato a un numero telefonico corrispondente

[pseudonimizzazione, ndr]

PROVV. SU DATA BREACH [7400401]

ACCERTAMENTI ISPETTIVI

Verifiche tecnologiche

f) la possibilità di tracciare a ritroso il voto espresso dagli interessati non risulta neppure bilanciata, per esempio, da un robusto **sistema di log degli accessi** e delle **operazioni svolte da persone dotate dei privilegi di amministratore della piattaforma** che consenta, almeno, di condurre a posteriori azioni di auditing sulla liceità dei trattamenti attuati dal detentore dell'archivio elettronico

PROVV. SU DATA BREACH [7400401]

ACCERTAMENTI ISPETTIVI

Profili di carattere generale

a) **Informativa** (specifica che i dati non verranno comunicati a terzi, mentre invece non ci sono nomine di responsabile esterno alle società manutentrici)

b) **Consenso esplicito** e separato dal resto per attività di carattere promozionale e pubblicitaria

PROVV. SU DATA BREACH [7400401]

PRESCRIZIONE MISURE E ACCORGIMENTI NECESSARI

Profili di carattere generale

a) adeguate azioni di **vulnerability assessment** attuate precedentemente alla messa in esercizio

b) sistema di autenticazione informatica (password min 8 caratteri e controllo automatico di qualità che impedisca l'uso di password "deboli«)

c) protocolli di rete *https*

d) conservazione delle password degli utenti siano rafforzate adoperando **algoritmi crittografici robusti**

e) misure di auditing (registrazioni degli accessi e delle operazioni compiute (log) sul database)

Grazie per l'attenzione

Aldo Lupi