Sh@rePro

Privacy: misure minime AgID e strumenti per il GDPR
L'esperienza dell'Università degli Studi di Torino

3 dicembre 2020

PROCEDamus
PROCEDIMENTIAMMINISTRATIVIDELLEUNIVERSITA'DEGLISTUDI
progetto di formazione-intervento per le università e gli enti di ricerca

L'applicazione del GDPR e delle misure minime AgID

L'Ateneo ha attivato una serie di azioni per l'applicazione delle previsioni normative sulla tutela dei dati personali europee (GDPR 2016/679) e nazionali sulla sicurezza (Misure minime AgID) muovendosi su alcune direttrici:

- ✓ *Organizzative*
- ✓ *Strumentali e tecniche*
- ✓ *Comportamentali*

Applicazione GDPR - Misure organizzative

Gli interventi sull'organizzazione si sono concretizzati in:

- ✓ *Nomina DPO*
- ✓ *Definizione di uno Staff di risorse dedicate a supporto del DPO*
- ✓ *Approvazione Regolamento interno di applicazione del GDPR che ha disegnato un modello partecipato assegnando al DPO un ruolo consulenziale, di monitoraggio e supporto nella gestione degli adempimenti*
- ✓ *Referenti privacy individuati per ogni Direzione/Dipartimento/Scuola/Centro quali soggetti di raccordo tra strutture e DPO*

Applicazione GDPR - Misure strumentali e tecniche

- ✓ *Template: registro trattamenti, registro data breach, accordo di contitolarità, accordo per nomina a responsabile esterno, informativa per il trattamento dei dati*
- ✓ *Flusso operativo data breach*
- ✓ *Condivisione DPIA elaborata dal Comitato europeo per la protezione dei dati - EDPB*
- ✓ *Definizione di un questionario per avvio progetti di ricerca*
- ✓ *Software per la gestione del flusso dati e documentale (in corso system test in ambiente di preproduzione)*

Applicazione GDPR - Misure strumentali e tecniche

- ✓ *Analisi e valutazione per porting di alcuni servizi su piattaforme in Cloud*

- ✓ *Next Generation Firewall → firewall 'intelligenti' che partendo dall'applicazione in uso consente di introdurre regole più puntuali, ha componenti software integrative che fanno uso di algoritmi intelligenza artificiale e machine learning*

- ✓ *Analisi dei log → implementazione e configurazione di soluzioni SIEM- Security Information and event management*

- ✓ *Protocollo per il controllo dell'accesso alla rete (802.1x) l'accesso alla rete sarà oggetto di filtro a soli utenti o dispositivi autorizzati*

- ✓ *Introduzione di nuove soluzioni per consentire aggiornamenti automatici dei software e dei sistemi operativi sia sulle postazioni di lavoro che sui server*

Applicazione GDPR - Misure comportamentali

La sensibilizzazione sulla tutela dei dati personali parte necessariamente dalla consapevolezza: gli interventi sui comportamenti si sono concentrati prioritariamente sull'asse ***formativo/informativo***

- ✓ *Formazione a tutto il personale*
- ✓ *Allestimento pagina informativa intranet*
- ✓ *Formazione specifica per i Referenti privacy*

intranet
L'UNIVERSITÀ DI TORINO ON LINE

Applicazione Misure Minime sulla Sicurezza AgID – Misure organizzative

Le azioni sull'applicazione delle Misure minime AgID si sono articolate in:

Staff Sicurezza ICT e Identità Digitale

- ✓ Presidio organizzativo specifico → inserimento in organigramma della Direzione Sistemi Informativi di uno Staff con competenza d'ambito

- ✓ Amministratori di sistema → censimento, formalizzazione nomina, formazione specifica

- ✓ Accordo con Polizia Postale → per adottare procedure di intervento e di scambio di informazioni utili a prevenire efficacemente i crimini informatici, l'indebita sottrazione di informazioni o qualsiasi ulteriore attività illecita conseguenti al tentativo di attacco informatico con finalità di interruzione dei servizi di pubblica utilità.

- ✓ Policy → approvazione di policy «**dedicate**» in materia di sicurezza che sistematizzano gli ambiti ICT (identità, rete, postazioni, servizi informatici)

PROCEDamus
PROCEDIMENTIAMMINISTRATIVIDELLEUNIVERSITA'DEGLISTUDI
progetto di formazione-intervento per le università e gli enti di ricerca

Sh@rePro

Applicazione Misure Minime sulla Sicurezza AgID – Misure strumentali e tecniche

- ✓ Registro degli incidenti
- ✓ Aggiornamento misure minime AgID
- ✓ Assessment di sicurezza su ambito definito (autenticazione)
- ✓ Previsione di estensione di assessment di sicurezza su altri ambiti

Misure minime di sicurezza ICT per le pubbliche amministrazioni

Applicazione Misure Minime sulla Sicurezza AgID – Misure strumentali e tecniche

- ✓ Adozione di soluzione avanzate per prevenire, analizzare, rilevare minacce sulle postazioni di lavoro
- ✓ Adozione di soluzione per la gestione e manutenzione da remoto dei personal computer assegnati al personale in smartworking coerente con la sicurezza informatica necessaria
- ✓ Analisi per autenticazione a due fattori
- ✓ Analisi per adempimento delle previsioni del Decreto Semplificazione: autenticazione con SPID per servizi al cittadino

spid

Applicazione Misure Minime sulla Sicurezza AgID – Misure comportamentali

La sensibilizzazione sulla sicurezza parte necessariamente dalla consapevolezza: gli interventi sui comportamenti si sono concentrati pertanto prioritariamente sull'asse formativo/informativo

- ✓ Organizzazione di un corso base sulla sicurezza informatica rivolto a tutto il personale e fruibile on demand su istanza Moodle

- ✓ Formazione specifica sul tema rivolta al personale d'ambito

- ✓ Definizione di Procedure operative di sicurezza informatica (identità digitale, rete, wifi, voip, postazione di lavoro, posta elettronica, hosting, licenze software, aule informatizzate, posta elettronica)

intranet
L'UNIVERSITÀ DI TORINO ON LINE

- ✓ Pagina informativa intranet

PROCEDamus
PROCEDIMENTIAMMINISTRATIVIDELLEUNIVERSITA'DEGLISTUDI
progetto di formazione-intervento per le università e gli enti di ricerca

Sh@rePro

GDPR e Sicurezza – Gli interventi durante la fase emergenziale

La fase emergenziale ha offerto un'opportunità di introdurre soluzioni tecnologicamente avanzate per coprire i fabbisogni, accelerando la fase di analisi dei prerequisiti per la tutela dei dati personali e della sicurezza

- ✓ Presidio tecnico e informativo sui servizi digitali per garantire la continuità amministrativa e gestionale dell'Ateneo
- ✓ Organizzazione della didattica, della ricerca scientifica e della terza missione 'alternativa'
- ✓ Supporto Organi Collegiali centrali e periferici per organizzazione sedute telematiche
- ✓ Definizione di procedure e protocolli per la gestione dei casi sospetti e confermati COVID

GDPR e Sicurezza – Gli interventi durante la fase emergenziale

- ✓ Sistemi di tracciamento ingressi e rilevazione della temperatura con strumentazione dedicata (telecamere termosensibili, termoscanner)
- ✓ Distribuzione di personal computer al personale collocato in lavoro agile con configurazioni gestite centralmente
- ✓ Fornitura di VPN – virtual private network
- ✓ Abilitazione servizio di portabilità degli interni telefonici
- ✓ Formazione on line per il personale sugli strumenti di collaboration

Problemi riscontrati

- ✓ Modello partecipato poco funzionale per realtà complessa, articolata e multicentrica
- ✓ Difficoltà nell'introduzione di soluzioni tecnologicamente avanzate
- ✓ Difficoltà nella gestione dell'analisi del rischio sui progetti di ricerca, studi clinici

Problemi riscontrati

- ✓ Rapporto organizzativamente complesso con la rete degli ospedali del territorio con cui è co-gestita la formazione in ambito medico (corso di laurea a ciclo unico in medicina e chirurgia, corsi di laurea professioni sanitarie, scuole di specializzazione area medica)

- ✓ Scarsa sensibilità sul trattamento dati/sicurezza nella componente docente/ricercatore → tema è percepito come 'inutile burocrazia'

- ✓ Presenza di trattamenti nell'ambito medico/sanitario che comportano la gestione di categorie particolari di dati personali

Sh@rePro

Ing. Angelo Saccà
direzione.ict@unito.it

sh@rePro

***Caso di studio*: la privacy nelle sedute di laurea in emergenza sanitaria**

L'esperienza dell'Università degli Studi del Sannio

C.Riccardi – Responsabile Sistemi Applicativi e componente del Team Privacy

3 dicembre 2020

Sedute di laurea

Ante

Post

Pubblicità

Disposizioni giuridiche

Regio Decreto del 4 giugno 1938, Art.43.
Regolamento Didattico di Ateneo, Art. 29, comma 9.

"La prova finale è pubblica."

Esigenze sociali

La partecipazione all'evento della seduta di laurea come espressione della necessità di socialità, soprattutto negli eventi che segnano momenti importanti nella vita universitaria.

Pubblicità in emergenza sanitaria

Come contemperare le esigenze di Privacy con la Pubblicità di una prova finale svolta a distanza?

Il nuovo impegno per gli atenei, tutti, ha avuto inizio con il susseguirsi della normativa emergenziale.

Le line guida del Garante hanno aiutato a fare chiarezza ma hanno dato origine a nuove sfide per un piccolo ateneo come Unisannio, in particolare per le esigue risorse a disposizione (professionali ed economiche).

Sedute di Laurea: review del processo

L'Università degli Studi del Sannio in piena emergenza sanitaria ha affrontato la revisione del processo per contemperare i diversi interessi.
Il team del DPO ha contribuito ad affrontare questa sfida grazie alle diverse “anime” che lo compongono.

Si è cercato di:

- Armonizzare Diritto e e Tecnologia
- Contemperare Pubblicità e Privacy
- Ridefinire il Trattamento
- Individuare i Rischi
- Valutare le potenzialità dei Sistemi Informatici a supporto

Scenari

Accessibilità consentita	Strumenti	Considerazioni	Privacy Vs Pubblicità
Solo ai candidati	Sistema di videoconferenza	Esigenze sociali compresse Risorse con competenze digitali	**Massima tutela della Privacy Pubblicità fortemente limitata**
Solo ai candidati e ad un numero fissato e censito di interessati esterni	Sistema di videoconferenza	Esigenze sociali limitatamente soddisfatte Maggiori risorse con adeguate competenze digitali	**Tutela Privacy garantita Pubblicità ridotta (limiti delle tecnologie utilizzabili)**
Accesso limitato ai candidati Accesso indifferenziato agli interessati esterni subordinato all'autorizzazione del candidato	Sistema di videoconferenza Canale social	Esigenze sociali sufficientemente soddisfatte Risorse con competenza digitali	**Tutela Privacy garantita Pubblicità consentita**
Accesso limitato ai candidati Accesso indifferenziato subordinato alla richiesta di pubblicazione del candidato	Sistema di videoconferenza Canale social	Esigenze sociali sufficientemente soddisfatte Risorse con competenza digitali	**Tutela Privacy garantita Pubblicità consentita**
Accesso limitato ai candidati Accesso indifferenziato	Sistema di videoconferenza Canale social	Esigenze sociali sufficientemente soddisfatte Risorse con competenza digitali	**Tutela Privacy fortemente limitata Pubblicità pienamente consentita**

Scelta dell'Ateneo

L'Ateneo viene autorizzato esplicitamente dal laureando all'utilizzo delle proprie immagini per realizzazione di video e materiali multimediali, realizzati e utilizzati esclusivamente per finalità promozionali e divulgative anche mediante pubblicazione sui portali istituzionali e sui canali social ufficiali di Ateneo.

(*fonte: Informativa per il trattamento dei dati personali per la realizzazione di video e materiale multimediale promozionale e divulgativo; Liberatoria per utilizzo del ritratto/riprese audio-video)*

Le sedute di laurea sono organizzate sulla piattaforma Webex con tutti i laureandi e, contemporaneamente, in diretta, viene trasmessa anche sul canale ufficiale YouTube dell'Ateneo, previa acquisizione del consenso del candidato, al fine di consentire la partecipazione all'evento anche a congiunti e amici.

Quesito

Dove si deve attestare il rapporto tra Privacy e Pubblicità?

Qual è lo strumento più adeguato?

… problematiche aperte

Le problematiche ancora aperte e sulle quali il confronto è auspicabile per vivere in mondi condivisi (e Sh@rePRO ne è un esempio), lascia spazio in diversi ambiti, come:

- privacy by design (tech, social, …);
- protezione dei dati ambientali;
- definizione di vincoli comportamentali;
- sensibilizzazione sui temi della sicurezza;
- garanzia degli strumenti di pubblicità;
- vincoli di territorialità (Ue ed extra UE);
- risorse limitate (riforma ad invarianza della spesa) ;
- ampliamento delle competenze digitali;
- digital divide;
- …

Sh@rePro

Grazie e buon Sh@rePRO a tutti

teamprivacy@unisannio.it

caterina.riccardi@unisannio.it

Sh@rePro

Privacy: l'altra faccia della medaglia.
Il processo di adozione dell'ISO 27001 all'Università di Verona

Giovanni M. Bianco CIO Univr – **Gianluca Lombardi** DPO Univr

3 dicembre 2020

Trattamenti dati: l'impressione di chi lavora nell'IT

Obiettivi

1. È possibile approfondire «l'altro lato della medaglia» della Privacy? (Ovvero, cosa ne è del Sistema Informativo?)

2. Ci sono adeguate «misure tecniche ed organizzative» che possono supportarci nel trattamento dati?

3. È possibile mettere le mani su un'esperienza vera?

"Before I write my name on the board, I'll need to know how you're planning to use that data."

1) È possibile approfondire «l'altro lato della medaglia» della privacy? (ovvero, cosa ne è del sistema informativo?)

In maniera abbastanza sorprendente il concetto di «sistema informativo» non è tra i concetti esplicitamente sviluppati nel GDPR

Eppure tutti noi ormai diamo per scontato che la grandissima parte dei trattamenti avvenga con strumenti elettronici

GDPR: le 50 parole più ricorrenti

Showing top 50 of 1463 possible words

accordance (134) application (114) appropriate (115) article (508) authority (562) board (128) body (111) case (109) commission (113) concerned (157) controller (524) country (119) data (1250) decision (150) ensure (120) establishment (129) including (191) information (229) interest (139) international (116) law (214) legal (128) measures (156) member (372) natural (183) necessary (122) organisation (116) paragraph (178) particular (170) personal (804) processing (718) processor (264) protection (317) provide (220) public (209) purposes (261) pursuant (154) referred (238) regard (121) regulation (326) relating (146) request (113) rights (179) rules (111) specific (121) state (322) subject (508) supervisory (449) third (123) union (221)

Una sola occorrenza di «sistema d'informazione»

(49) Costituisce legittimo interesse del titolare del trattamento interessato trattare dati personali relativi al traffico, in misura strettamente necessaria e proporzionata per garantire la sicurezza delle reti e dell'informazione, vale a dire la capacità di una rete o di un sistema d'informazione di resistere, a un dato livello di sicurezza, a eventi imprevisti o atti illeciti o dolosi che compromettano la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati personali conservati o trasmessi e la sicurezza dei relativi servizi offerti o resi accessibili tramite tali reti e sistemi da autorità pubbliche, organismi di intervento in caso di emergenza informatica (CERT), gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT), fornitori di reti e servizi di comunicazione elettronica e fornitori di tecnologie e servizi di sicurezza. Ciò potrebbe, ad esempio, includere misure atte a impedire l'accesso non autorizzato a reti di comunicazioni elettroniche e la diffusione di codici maligni, e a porre termine agli attacchi da «blocco di servizio» e ai danni ai sistemi informatici e di comunicazione elettronica.

(49) The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems.

GDPR: «Misure tecniche» e «Misure organizzative»

La ragione per cui il GDPR non parla di Sistema Informativo è che più generalmente si riferisce a «misure tecniche», mettendo subito in chiaro, alla nota 15, che

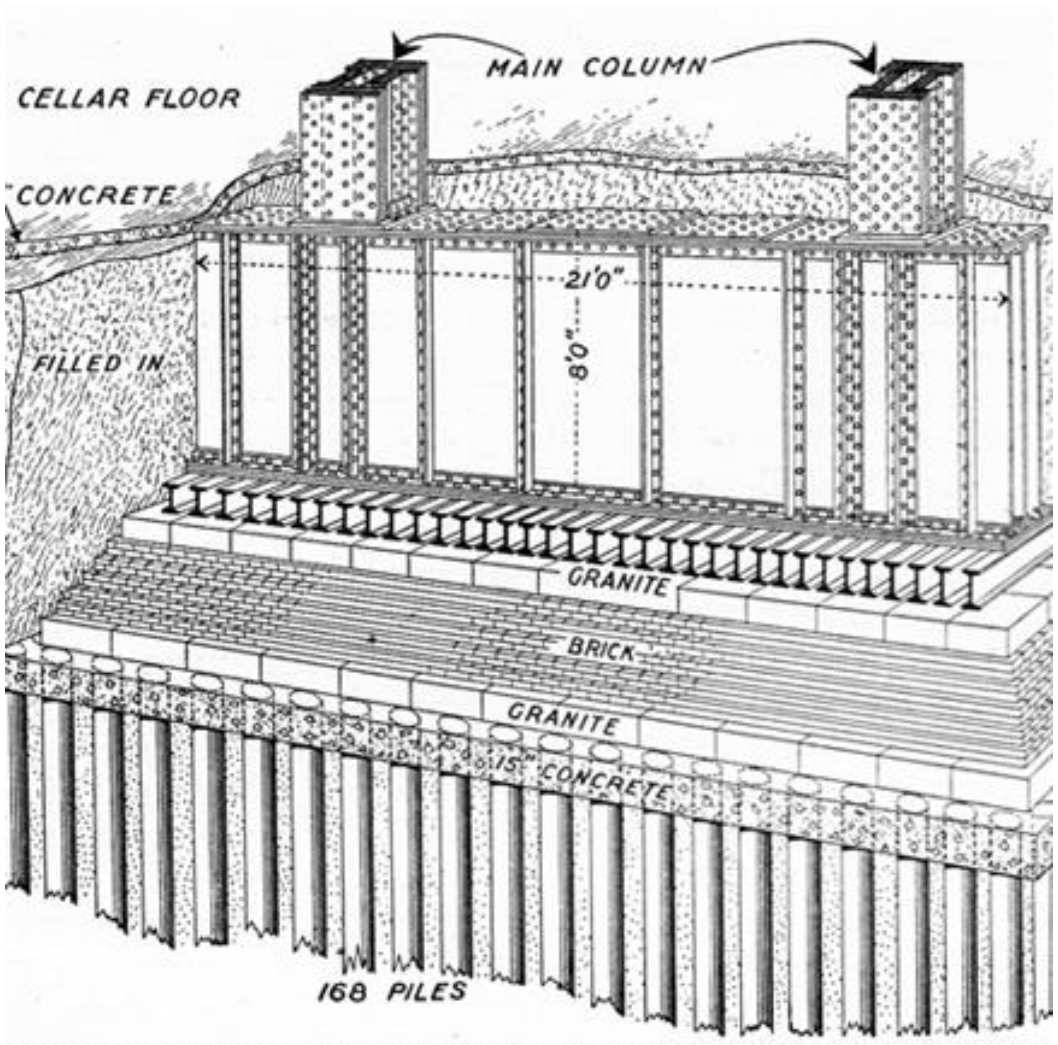
«Al fine di evitare l'insorgere di gravi rischi di elusione, la protezione delle persone fisiche dovrebbe essere neutrale sotto il profilo tecnologico e non dovrebbe dipendere dalle tecniche impiegate»

Il GDPR ci aiuta con le «misure tecniche»?

Articolo 24

Responsabilità del titolare del trattamento

1. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, <u>il titolare del trattamento mette in atto misure tecniche e organizzative adeguate</u> per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.
2. ...
3. **L'adesione** ai codici di condotta di cui all'articolo 40 o **a un meccanismo di certificazione** di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento.

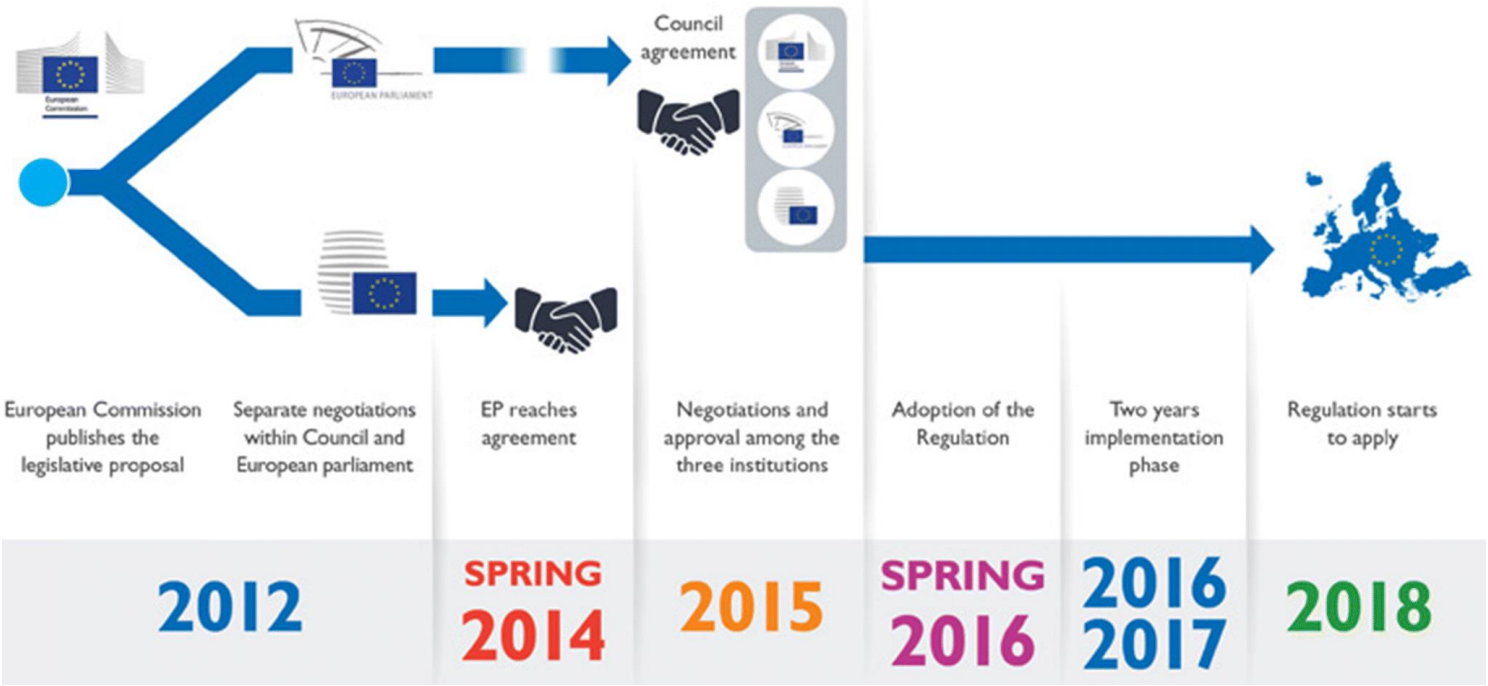


LE FOUNDATIONS IN DEEP WET SAND, WITH MASSIVE CONCRI
AND STEEL PIERS, FOR THE HUGE COLUMN GIRDERS IN
PARK ROW BUILDING, NEW YORK CITY

Misure tecniche: «il titolare deve»

La ragione per cui il GDPR non norma le misure tecniche (ve lo ricordate l'Allegato B?) è essenzialmente una:

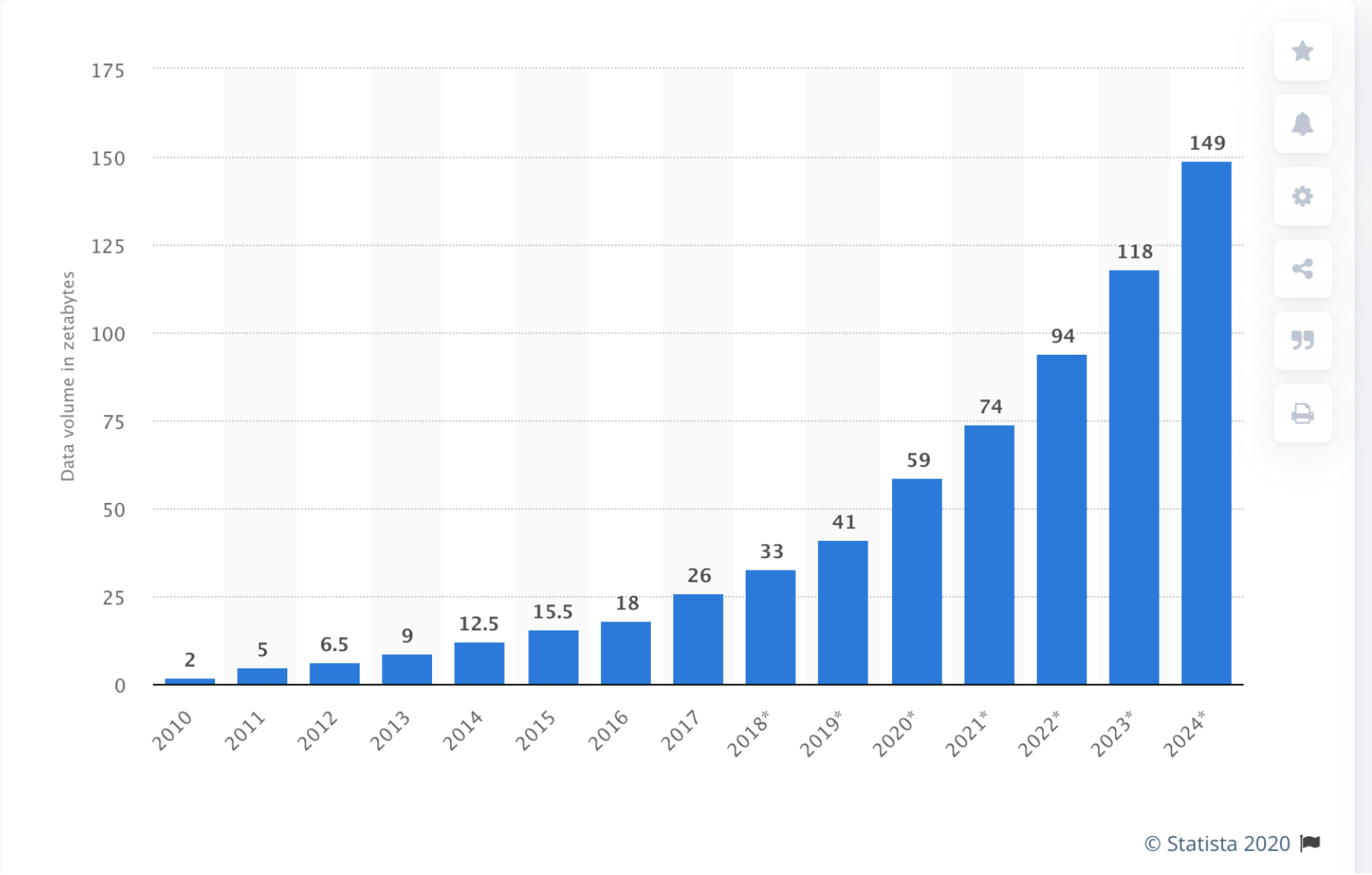
La rapidità con cui i trattamenti e i sistemi di trattamento evolvono ***non è compatibile*** *con l'evoluzione temporale di una norma*



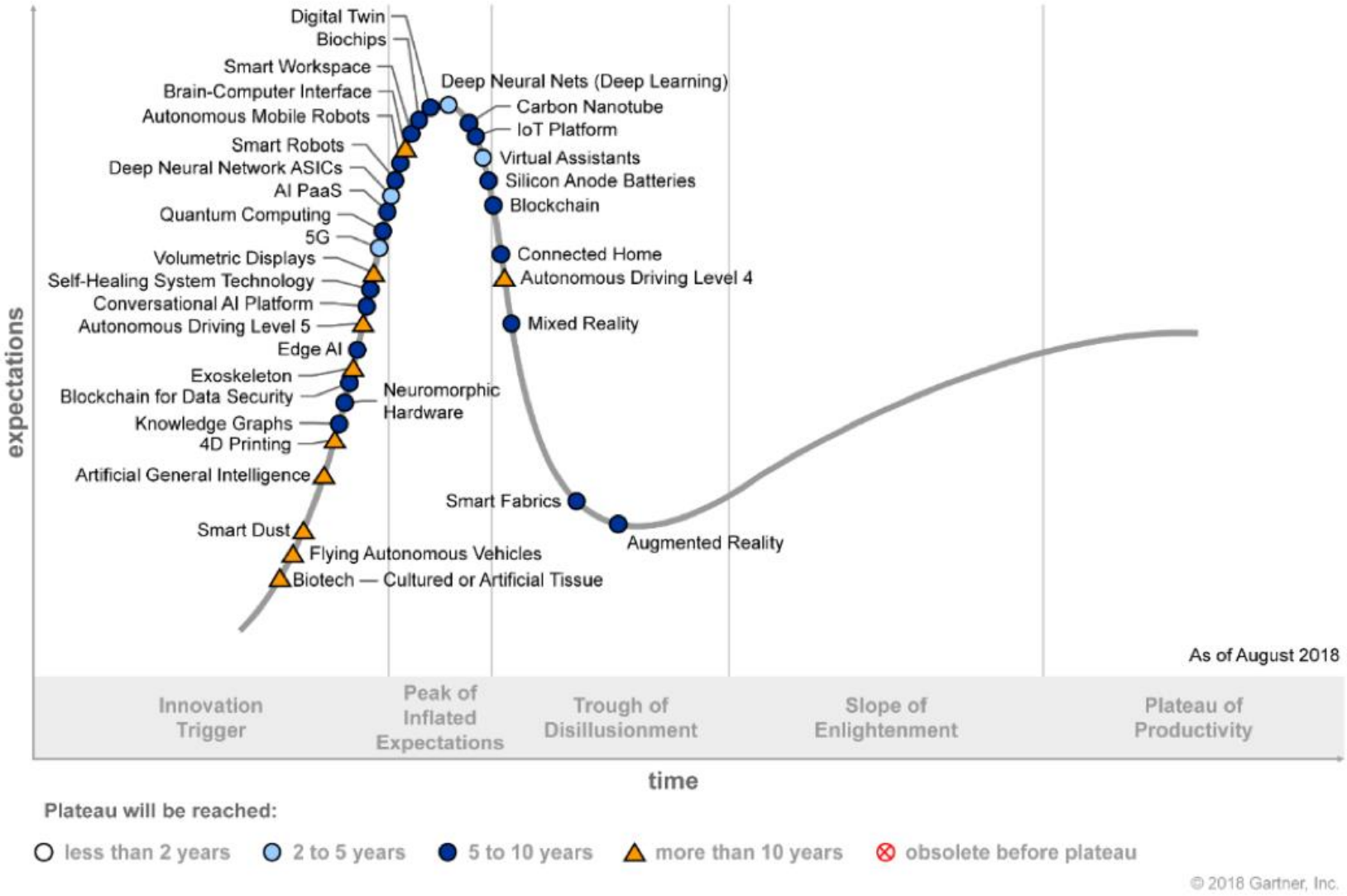
Lopes, I.M., Guarda, T. & Oliveira, P. General Data Protection Regulation in Health Clinics.J Med Syst 44, 53 (2020)
https://doi.org/10.1007/s10916-020-1521-0

Volume of data/information worldwide from 2010 to 2024

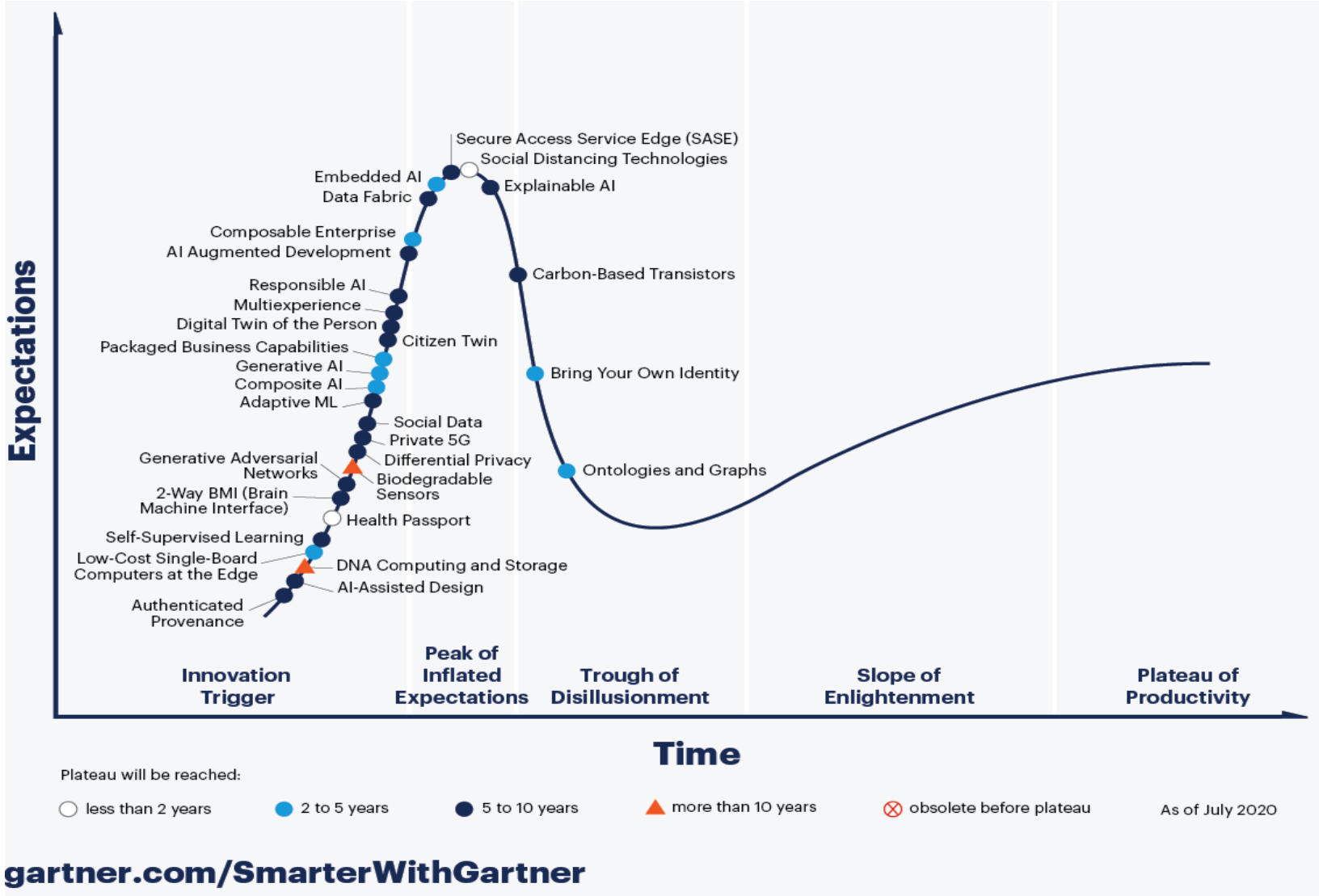
(in zettabytes)

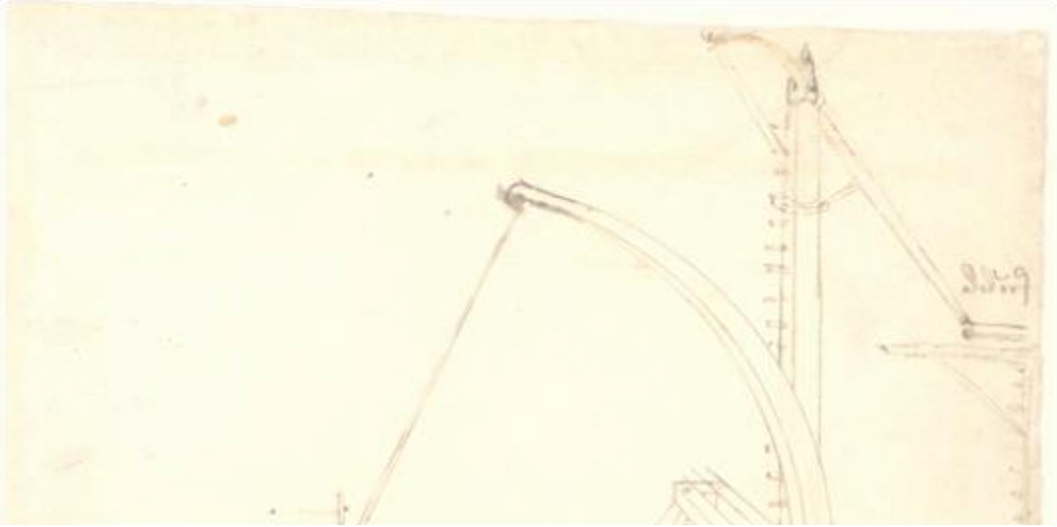


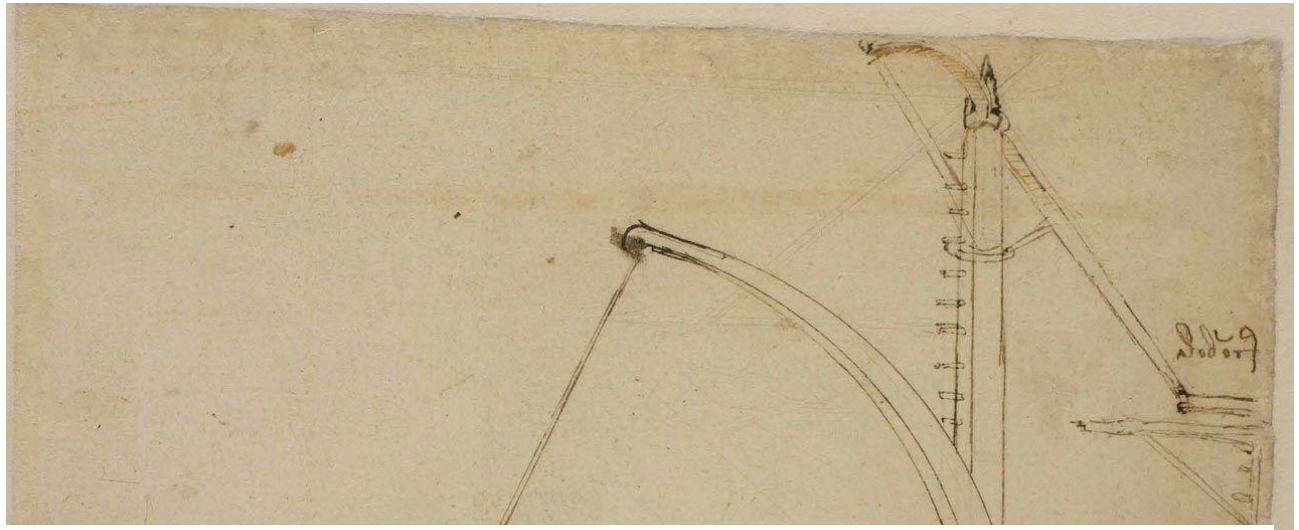
2018 - Si può rincorrere normativamente la «tecnica»?



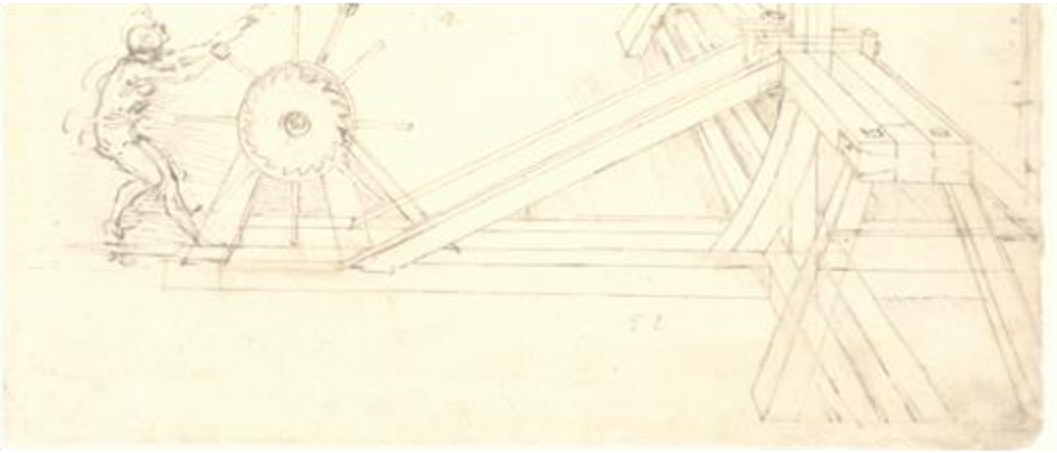
2020 - Si può rincorrere normativamente la «tecnica»?

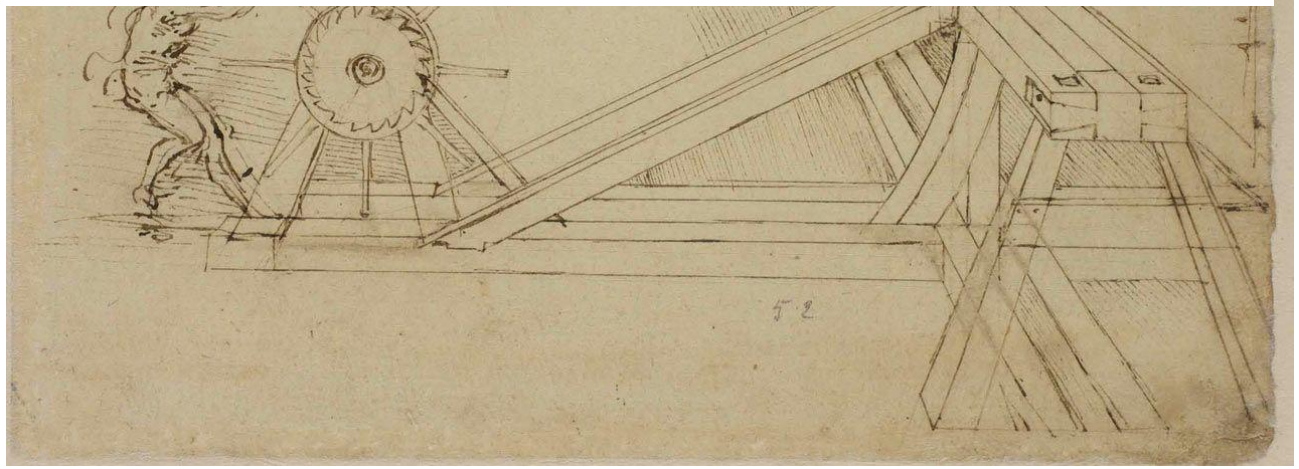






2) Ci sono adeguate «misure tecniche e organizzative» che possono supportarci nel trattamento dati?

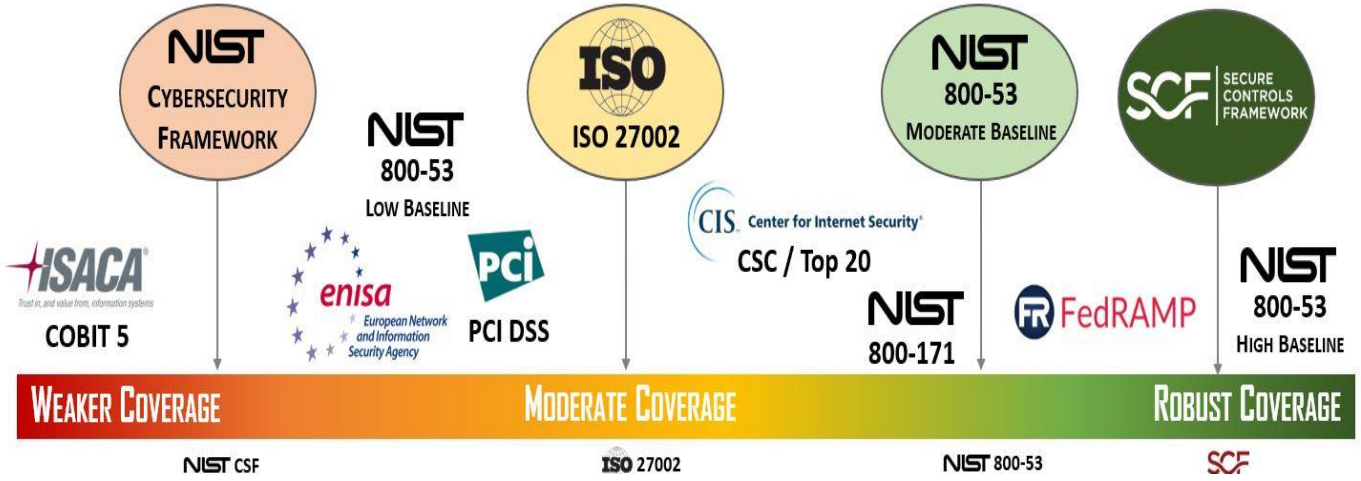




Cosa stiamo cercando

Ci servirebbe una misura «tecnica ed organizzativa» per i Sistemi Informativi in grado di:

- *Affrontare le sfide di un contesto in continuo rapidissimo cambiamento*
- *Ottenere fiducia nella capacità di fornire prodotti e servizi conformi alle attese*
- *Essere omnicomprensiva dei diversi aspetti*

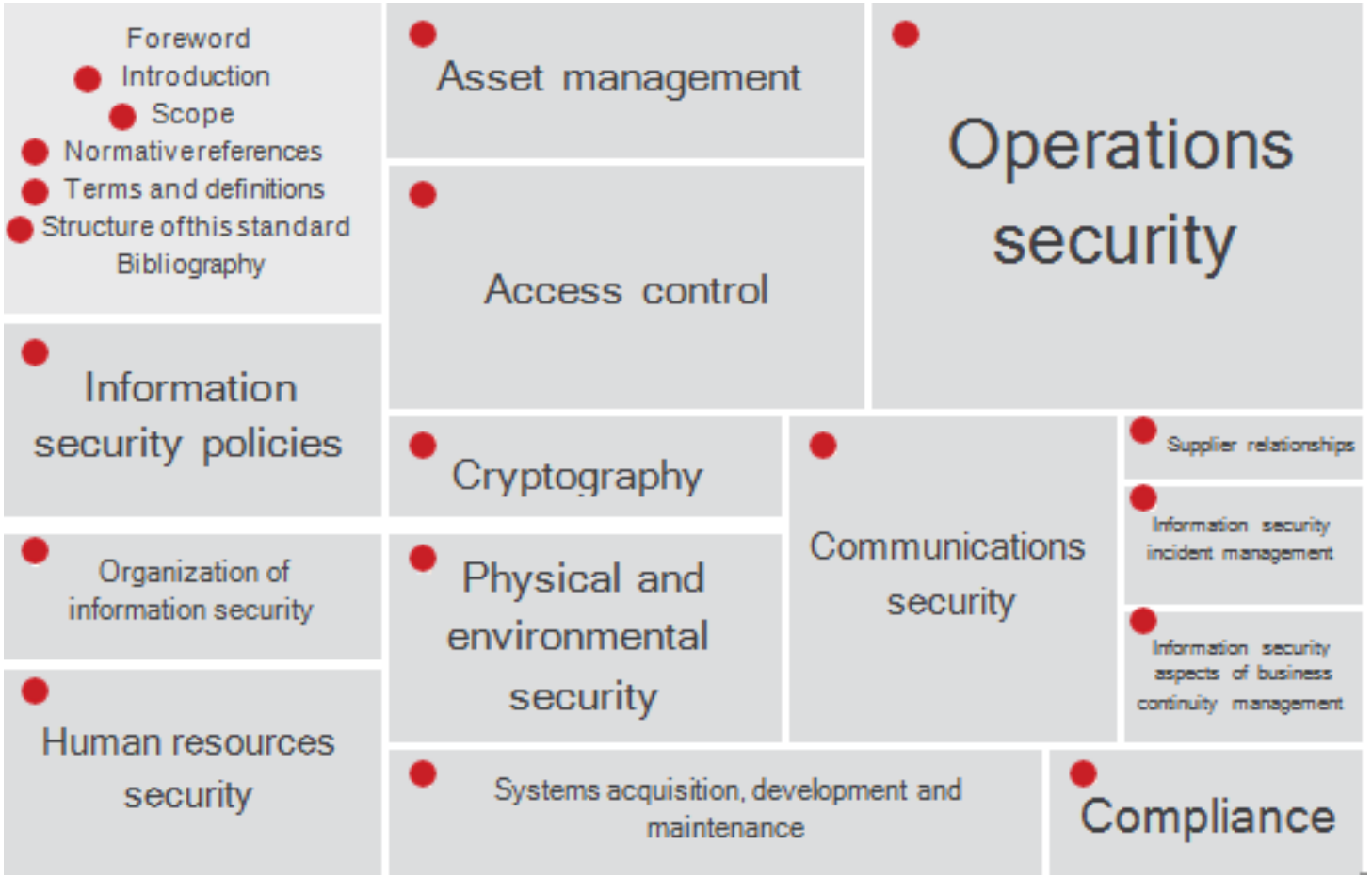


Cosa è la ISO2700x

Lo standard **ISO/IEC 27001** è un sistema di gestione («norma») a livello internazionale certificabile che contempla **requisiti per la sicurezza** delle Informazioni, pensata ed ideata per prevedere controlli di sicurezza <u>adeguati</u> e <u>proporzionati</u>

La «ISO 270xx family»

27001 Requirements
27002 Code of Practice
27003 Impl. Guidance
27005 IS Risk Management
27017 Cloud Computing
27018 Public Cloud Computing
27032 Cyber Security
27033 Network Security
27034 Application Security
27040 Storage Security
…



3) È possibile mettere le mani su un’esperienza vera?

Sh@rePro

Giovanni M. Bianco
Università degli studi di Verona

Sh@rePro

Privacy: l'altra faccia della medaglia.
Il processo di adozione dell'ISO 27001 all'Università di Verona

Giovanni M. Bianco CIO Univr – **Gianluca Lombardi** DPO Univr

3 dicembre 2020

3) È possibile mettere le mani su un’esperienza vera?

Ing. Gianluca Lombardi – DPO Università di Verona

Maestro PROTEZIONE DATI & DATA PROTECTION DESIGNER®	**Maestro della Protezione Dati & Data Protection Designer® IIP** https://www.istitutoitalianoprivacy.it/albo-maestri-iip/
aicq sicev Sistema di Certificazione e Valutazione	**DPO ex UNI 11697 (Cert. N. 005)** **Valutatore PRIVACY ex UNI 11697 (Cert. N. 026)** https://portal.aicqsicev.it/public/certified-persons
TÜV SÜD	**Privacy Officer e Consulente della Privacy (N. CDP 038)** https://www.tuvsud.com/it-it/risorse/ricerca-certificati/professionisti
ISO-27001 Lead Auditor	**Lead Auditor ISO 27001**

Obiettivi

1. Quali sono le differenze ed i punti di contatto tra il GDPR e la ISO 27001 ?

2. Perché implementare un sistema ISO 27001 in università per rispondere anche al GDPR ?

3. Come prepararsi ad un processo di certificazione ISO 27001 in università ?

QUALI SONO LE DIFFERENZE ED I PUNTI DI CONTATTO TRA IL GDPR E LA ISO 27001

Differenze

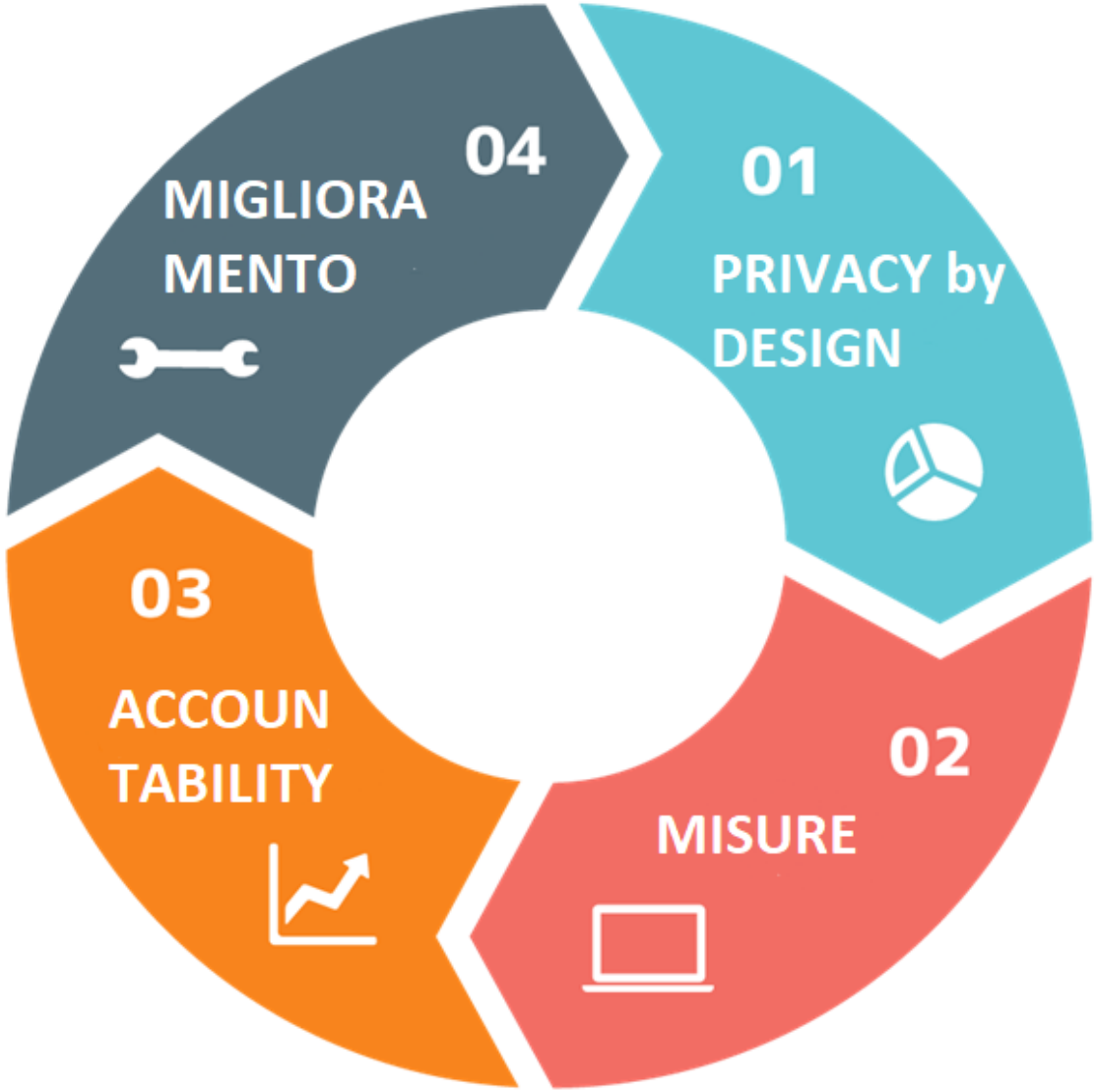
ARGOMENTO	ISO 27001	GDPR
CHI PROTEGGE ?	I dati aziendali, in particolare quelli legati al business aziendale	I dati degli interessati che forniscono le loro informazioni al Titolare.
QUALI MISURE DI SICUREZZA ?	In base all'importanza dei dati per il business aziendale	In funzione dell'impatto che un evento negativo può avere sugli interessati
MODALITA' DI TRATTAMENTO ?	I dati sono trattati nel modo in cui l'azienda lo ritiene corretto per perseguire il proprio business	I dati devono essere trattati in modo lecito, corretto e trasparente e conosciuto da parte dell'interessato.
FINALITA' DI TRATTAMENTO ?	Nessun vincolo rispetto le finalità	Finalità determinate, esplicite e legittime
MINIMIZZAZIONE ?	Nessun vincolo	Raccogliere solo i dati minimi necessari per l'erogazione del servizio

Differenze

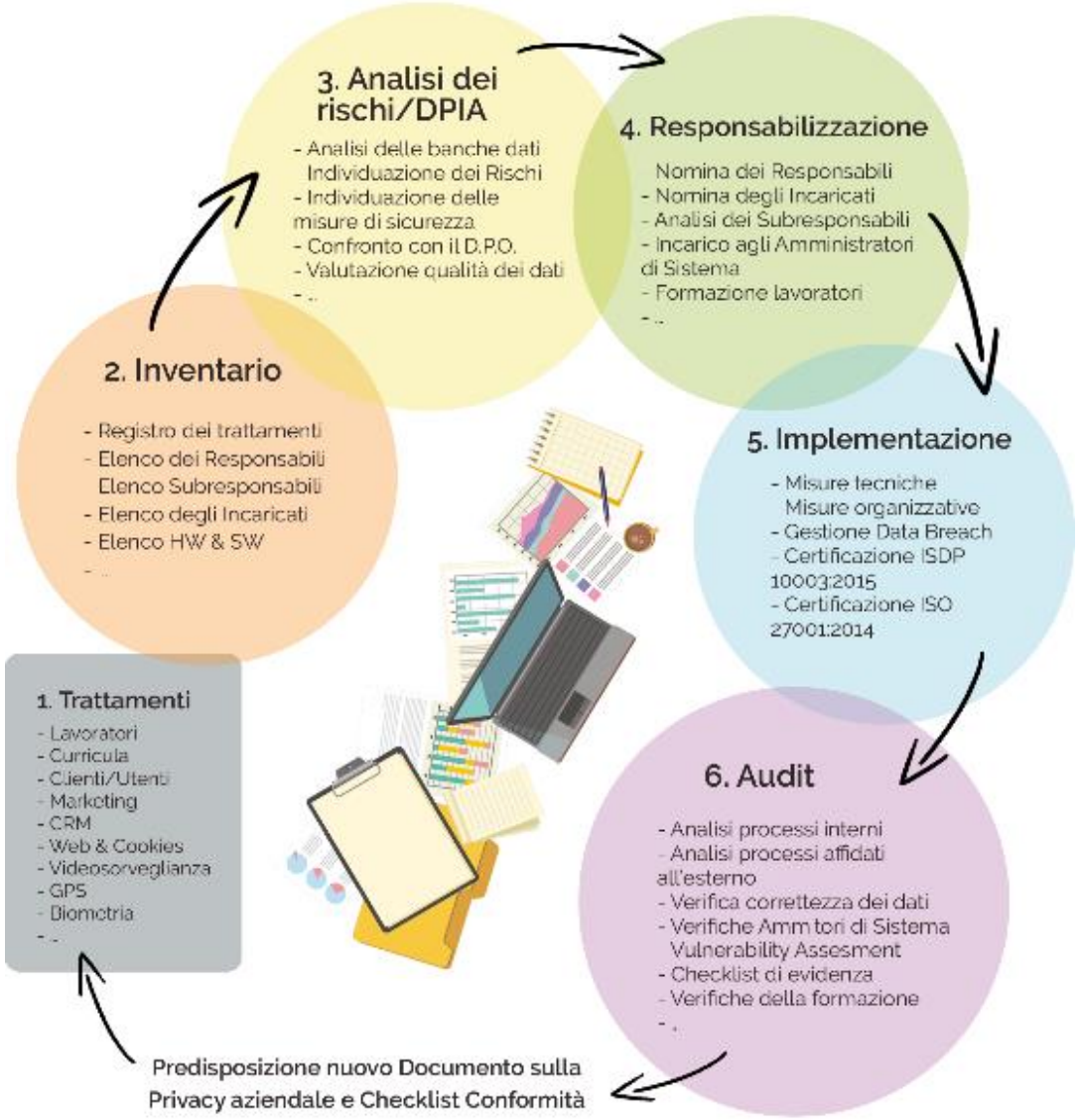
ARGOMENTO	ISO 27001	GDPR
ESATTEZZA ?	Nessun Vincolo	I dati devono essere esatti ed aggiornati
TEMPO DI CONSERVAZIONE ?	Nessun vincolo	Solo per il tempo necessario al trattamento
RESPONSABILIZZAZIONE ?	Nessun vincolo	Art. 5.2 Accountability
SANZIONI ?	Nessuna	Fino a 20.000.000 €
DATA BREACH ?	Nessuno	Segnalazione al Garante ed agli interessati se necessario
ESERCIZIO DEI DIRITTI ?	Nessuno	Procedure per garantire l'accesso ai diritti da parte degli interessati
MISURE TECNICHE ED ORGANIZZATIVE	Previste e da documentare (114 controlli)	Previste ma oggetto di valutazione del rischio da parte del Titolare

Punti di contatto

Alla base del GDPR



Circolo virtuso del GDPR:



Alla base della 27001

PERCHE' IMPLEMENTARE UN SISTEMA ISO 27001 IN UNIVERSITA' PER RISPONDERE ANCHE AL GDPR ?

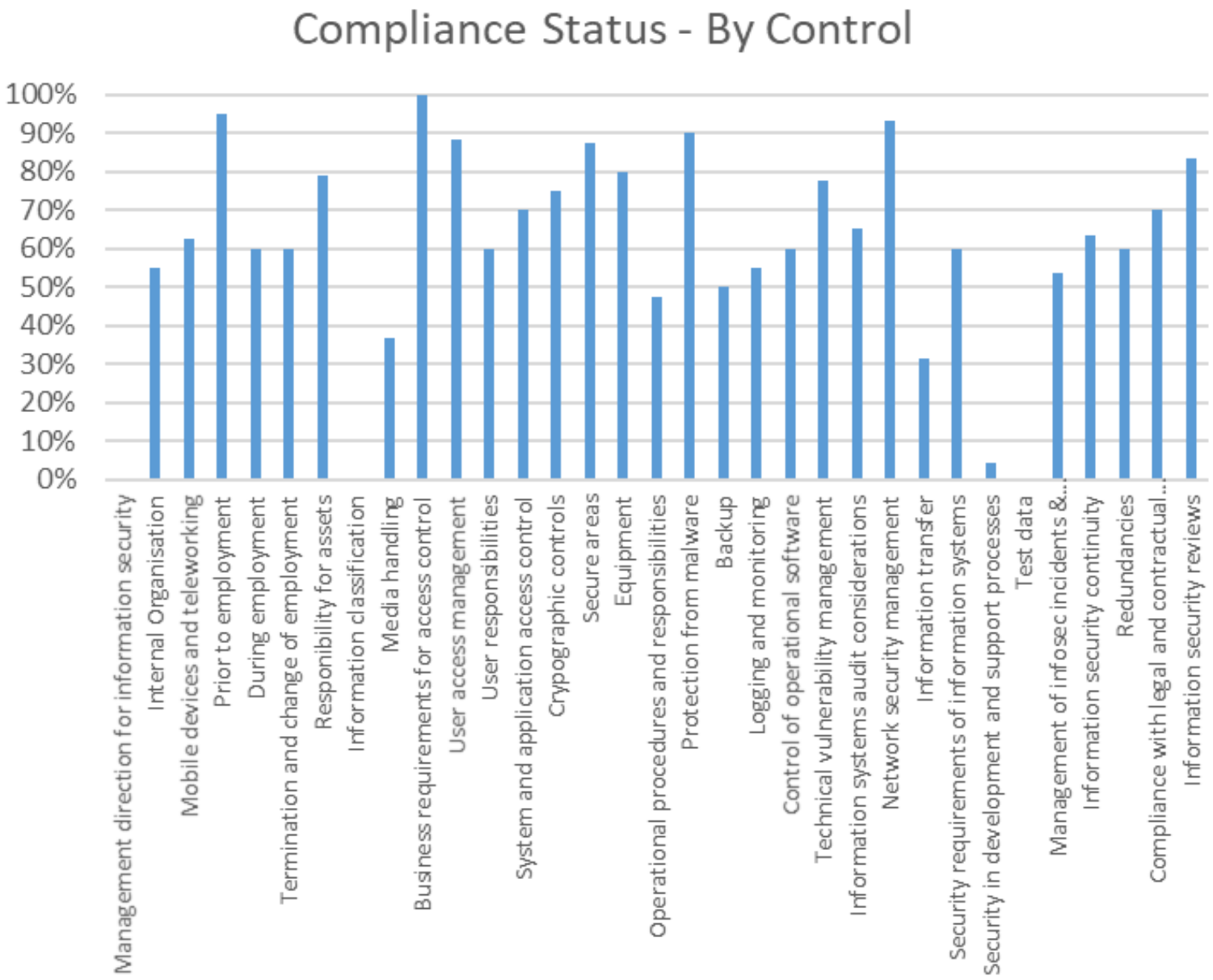
Scenario di riferimento

1. Numero elevato di trattamenti
2. Distribuzione dei trattamenti all'interno dei vari dipartimenti
3. Trattamenti caratterizzati da alta dinamicità
4. Trattamenti basati significativamente su sistemi informatici
5. Ruolo chiave della DSIT nell'erogazione di servizi
6. Alta professionalità dei vari protagonisti del sistema
7. Attività svolte in base all'esperienza dei singoli
8. Insufficiente rendicontazione e dimostrazione delle attività svolte

Assesment iniziale

- Due giorni intensa di confronto con i vari operatori
- Analisi delle attività con un occhio esterno
- Analisi dei sistemi tenendo conto di:
  - CYBERSECURITY
  - GDPR
  - MISURE MINIME AGID
  - ISO 27001
- Elaborazione di una checklist finale di conformità

Assesment iniziale



PROCEDamus
PROCEDIMENTIAMMINISTRATIVIDELLEUNIVERSITA'DEGLISTUDI
progetto di formazione-intervento per le università e gli enti di ricerca

Assesment iniziale

Standard	Section	Status
A.5.1	Management direction for information security	0%
A.6.1	Internal Organisation	55%
A.6.2	Mobile devices and teleworking	63%
A.7.1	Prior to employment	95%
A.7.2	During employment	60%
A.7.3	Termination and change of employment	60%
A.8.1	Responibility for assets	79%
A.8.2	Information classification	0%
A.8.3	Media handling	37%
A.9.1	Business requirements for access control	100%
A.9.2	User access management	88%
A.9.3	User responsibilities	60%
A.9.4	System and application access control	70%
A.10.1	Crypographic controls	75%
A.11.1	Secure areas	88%
A.11.2	Equipment	80%
A.12.1	Operational procedures and responsibilities	48%
A.12.2	Protection from malware	90%
A.12.3	Backup	50%
A.12.4	Logging and monitoring	55%
A.12.5	Control of operational software	60%
A.12.6	Technical vulnerability management	78%
A.12.7	Information systems audit considerations	65%
A.13.1	Network security management	93%
A.13.2	Information transfer	31%
A.14.1	Security requirements of information systems	60%
A.14.2	Security in development and support processes	4%
A.14.3	Test data	0%
A.16.1	Management of infosec incidents & improvements	54%
A.17.1	Information security continuity	63%
A.17.2	Redundancies	60%
A.18.1	Compliance with legal and contractual requirements	70%
A.18.2	Information security reviews	83%

Assesment iniziale

PROCEDamus
PROCEDIMENTIAMMINISTRATIVIDELLEUNIVERSITA'DEGLISTUDI
progetto di formazione-intervento per le università e gli enti di ricerca

Assesment iniziale

Standard	Section	Status
A.5	Information Security Policies	0%
A.6	Organisation of information security	57%
A.7	Human resources security	72%
A.8	Asset management	43%
A.9	Access control	81%
A.10	Cryptography	75%
A.11	Physical and environmental security	83%
A.12	Operations security	59%
A.13	Communications security	58%
A.14	System acquisition, development and maintenance	18%
A.15	Supplier relationships	82%
A.16	Information security incident management	54%
A.17	Information security aspects of business continuity management	63%
A.18	Compliance	75%

Assesment iniziale

Target:	Direzione Informatica Università di Verona			
Date Audit:	22 e 23 Novembre 2019			
Auditors:	Gianluca Lombardi e Maria Grec			
	Lead Auditors 27001			
Referenti interni:	Bianco Giovanni			
	Dal Monte Marco			
Overall Compliance:			**59%**	

Assenza di una politica della sicurezza → Privacy by Design

A.5	Information Security Policies			
A.5.1	**Management direction for information security**			
A.5.1.1	Policies for information security	1. Do Security policies exist? 2. Are all policies approved by management? 3. Are policies properly communicated to employees?	Manca una politica della sicurezza delle informazioni. Di conseguenza è assente una sua approvazione ed una sua diffusione (es. metterla sul sito internet e/o diffusa sulla intranet ziendale/bacheca).	0%
A.5.1.2	Review of the policies for information security	1. Are security policies subject to review? 2. Are the reviews conducted at regular intervals? 3. Are reviews conducted when circumstances change?	Manca una procedura per la revisione della politica da parte della Direzione. La revisione della politica è necessaria in caso di cambio delle condizioni al contorno o in caso di cambiamento dei servizi erogati. Inoltre deve essere comunque rivista almeno una volta l'anno.	0%

Gestione incidenti → Data Breach

A.16	Information security incident management			
A.16.1	**Management of information security incidents and improvements**			
A.16.1.1	Responsibilities and procedures	Are management responsibilities clearly identified and documented in the incident management processes?	Segnalazione di mancanza di un servizio ed attivazione di un'unità di crisi ad hoc (non formalizzata). Presenza di un piano di disaster recovery. Reperibilità su base volontaria.	60%
A.16.1.2	Reporting information security events	1. Is there a process for timely reporting of information security events? 2. Is there a process for reviewing and acting on reported information security events?	Incidenti sui client --> gestione dei ticket. Sui server presente Nagios. Viene effettuata un'analisi degli eventi per migliorare la situazione. Apertura ticket su kaspersky.	75%
A.16.1.3	Reporting information security weaknesses	1. Is there a process for reporting of identified information security weaknesses? 2. Is this process widely communicated? 3. Is there a process for reviewing and addressing reports in a timely manner?	Libera iniziativa. Non presente una procedura definita.	50%
A.16.1.4	Assessment of and decision on information security events	Is there a process to ensure information security events are properly assessed and classified?	Presente prassi consolidata ma assenza di procedure	50%
A.16.1.5	Response to information security incidents	Is there an incident response process which reflects the classification and severity of information security incidents?	Necessario formulare una procedura di risposta all'incidente e di data breach	40%
A.16.1.6	Learning from information security incidents	Is there a process or framework which allows the organisation to learn from information security incidents and reduce the impact / probability of future events?	Mancanza di debriefing formalizzato	40%
A.16.1.7	Collection of evidence	1. Is there a forensic readiness policy? 2. In the event of an information security incident is relevant data collected in a manner which allows it to be used as evidence?	Gestito sulle richieste dell'autorità giudiziaria.Gestione dei log ?	60%

PROCEDamus
PROCEDIMENTIAMMINISTRATIVIDELLEUNIVERSITA'DEGLISTUDI
progetto di formazione-intervento per le università e gli enti di ricerca

COME PREPARARSI AD UN PROCESSO DI CERTIFICAZIONE ISO 27001 IN UNIVERSITA' ?

Modalità di lavoro

- Delimitazione campo di applicazione
- Forte commitment della Direzione
- Definizione capo progetto interno e supporto esterno
- Definizione del gruppo di lavoro interno
  - Sistemi
  - Infrastrutture
  - Amministratori di Sistema
  - Sviluppo software ...
- Registrazione delle sessioni di lavoro
- Definizione della Road Map

Predisposizione documentazione e procedure

- Definizione dei modelli

- Definizione della documentazione di sistema:
  - Documenti
  - Procedure
  - Modulistica
  - Allegati

Predisposizione documentazione e procedure

- Utilizzo degli strumenti esistenti:
  - Wiki – intranet, Teams, …
  - Consolle di controllo presenti

- Implementazione nuovi sistemi di verifica e controllo

- Definizione delle attività da controllare e modalità

CONCLUSIONI

Risultati attuali a metà strada

- Modelli di azione ben definiti
- Concetto di procedure e sistemi di controllo assimilati
- Verifiche sui sistemi informatici interni, valutazione delle criticità ed implementazione di nuove soluzioni effettuate
- Fornite numerose risposte all'ufficio privacy ed al D.P.O.
- Gestione di eventi negativi efficiente e collaborativa
- Definite le modalità di gestione degli AdS
- Rinnovato il Disciplinare di utilizzo degli strumenti elettronici

Ulteriori risultati attesi a breve

- Miglioramento della gestione dello sviluppo sicuro interno e di quanto fatto sviluppare all'esterno
- Miglioramento Disaster Recovery e Business continuity
- Gestione dei processi documentata ed indipendente dai soggetti che li implementano
- Report periodici sui sistemi e sui processi (accountability)
- Migliore gestione dei diritti degli interessati
- Maggior permeabilità del GDPR all'interno dei dipartimenti

Ing. Gianluca Lombardi

https://www.linkedin.com/in/gianlucalombardi/

Tel. 348-2345012
Mail: info@glconsulting.com

MONDO 27001

www.mondo27001.it

MONDO PRIVACY

www.mondoprivacy.it

PROCEDamus
PROCEDIMENTIAMMINISTRATIVIDELLEUNIVERSITA'DEGLISTUDI
progetto di formazione-intervento per le università e gli enti di ricerca

Sh@rePro

Sh@rePro

PROCEDamus
PROCEDIMENTIAMMINISTRATIVIDELLEUNIVERSITA'DEGLISTUDI
progetto di formazione-intervento per le università e gli enti di ricerca