UNITYFVG
United Universities of FVG
Technology Transfer

SISSA

UNIVERSITÀ
DEGLI STUDI DI TRIESTE

UNIVERSITÀ
DEGLI STUDI
DI UDINE
hic sunt futura

SISSA + UNITS + UNIUD vs. (N.I.S.) + GDPR + CAD

Incontro di “sensibilizzazione” Dipartimenti in funzione degli adempimenti “privacy” (e altro) -> 25 maggio 2018

Dott. Avv. FEDERICO COSTANTINI
Professore aggregato di Informatica giuridica
DISG / UNIUD

Università degli Studi di Udine
Aula multimediale (Rizzi)
10 maggio 2018

Riprendendo una frase da una famosa citazione televisiva «the winter is coming» (Il trono di Spade), si può anche dire che «GDPR is coming»

https://www.facebook.com/VaronisSystems/photos/pb.125005500878837.-2207520000.1508767539./1549165935129446/?type=3&theater

Ed ecco ben rappresentata la reazione del nostro legislatore
(che ben ci rappresenta) …

RISERVATEZZA

Il regolamento Ue sostituisce il codice di tutela privacy

–di Antonello Cherchi

(Marka)

VIDEO

Perché la truffa del fondo brucia risp
in Italia non potrebbe accadere

I PIÙ LETTI DI NORME & TRIBUTI

1. CONTRATTI PUBBLICI
Statali, aumenti a tempo. Nel 2019
paga più bassa

2. DICHIARAZIONI
Nuovo modello per la liquidazione

http://www.ilsole24ore.com/art/norme-e-tributi/2018-03-21/il-regolamento-ue-sostituisce-codice-tutela-privacy-211242.shtml?uuid=AEZLcELE

Ed ecco ben rappresentata la reazione del nostro legislatore
(che ben ci rappresenta) …

PRIVACY

Gdpr, approvato lo schema di decreto: questi i punti sul tavolo

Home > Sicurezza Digitale > Privacy

Approvato in via preliminare lo schema di decreto legislativo per adeguare il quadro normativo nazionale alle disposizioni del regolamento UE 2016/679 GDPR. Ecco perché è un passo importante e quali sono i principali dossier in esame

4 giorni fa

Alessandro Longo

https://www.agendadigitale.eu/sicurezza/privacy/gdpr-approvato-lo-schema-di-decreto-questi-i-punti-sul-tavolo/

E la reazione di coloro i quali possono eventualmente sottrarsi all'applicazione della norma (uscendo dal mercato europeo…

https://www.impresacity.it/news/19746/per-alcune-aziende-usa-il-gdpr-e-troppo-difficile.html

... E anche il legislatore italiano ci mette del suo…

Diritto dei Media

La convergenza tra televisione, nuove tecnologie e telecomunicazioni ha prospettato l

di Fulvio Sarzana

nòva

Scienza | Tecnologie | Creatività | Social Innovation | Dossier | Blog

Il Decreto di attuazione del regolamento Privacy #GDPR: sconfessati i principi della prima bozza.

6 maggio 2018 | Fulvio Sarzana | GDPR General Data Protection Regulation - Regolamento europeo n. 2016/679

La Presidenza del Consiglio dei Ministri ha inviato alla ragioneria generale dello Stato il **Decreto di adeguamento al Regolamento Europeo sulla privacy (GDPR)**, in una bozza molto diversa da quella originariamente presentata.

La Ragioneria generale ne ha vistato la conformità e si attendono ora i necessari passi successivi.

Prima di commentare brevemente le nuove disposizioni una avvertenza: le bozze circolate in queste ore sono incomplete e non tengono conto delle modifiche apportate, soprattutto dal punto di vista economico, all'ultimo, ai fini della bollinatura da parte della Ragioneria

http://fulviosarzana.nova100.ilsole24ore.com/2018/05/06/il-decreto-di-attuazione-del-regolamento-privacy-gdpr-sconfessati-i-principi-della-prima-bozza/

,.. Tanto rumore per nulla?

Artif Intell Law (2017) 25:429–443
DOI 10.1007/s10506-017-9206-9

CrossMark

Using artificial intelligence to support compliance with the general data protection regulation

John Kingston[1]

Published online: 1 September 2017

<Index>

(1) Un «caso» concernente la protezione dei dati personali

Presentazione di uno scenario tratto dall'esperienza lavorativa quotidiana

(2) Introduzione: il contesto

Descrizione del quadro giuridico di riferimento

(3) «focus» sugli aspetti problematici

- **(3.1) Sicurezza informatica**, Direttiva UE 1146/2016 «N.I.S.» e «resilienza»
- **(3.2) Dati personali**, adempimenti *ex* Regolamento UE 679/2016
- **(3.3) Amministrazione digitale**, adempimenti *ex* D. Lgs. 82/2005

(4) Metodo adottato

Modalità di azione adottata

(5) Attività

Iniziative programmate: linee guida, sensibilizzazione, formazione

(6) Valutazioni finali

Conclusioni, domande, discussione

<Index/>

Tizia, in qualità di docente, viene a conoscenza del fatto che lo studente Caio soffre di un disturbo medico per il quale può essere soggetto a improvvise crisi.
Si pone il problema di far sapere ai colleghi come comportarsi qualora una crisi si verifichi in sede di lezione o esame.

Cosa **può** fare (in punto di fatto)?
Cosa **deve** fare (in punto di diritto?
Cosa **non deve** fare (in punto di diritto)?
Perché?
(segue breve discussione)

</>

Tizia, impiegata presso una segreteria studenti, un giorno riceve una telefonata da una persona che chiede di ricevere informazioni concernenti la carriera universitaria dello studente Caio, rappresentando di esserne il genitore.
L'interlocutore è molto insistente e rappresenta un quadro di notevoli difficoltà personali e familiari.

Cosa **può** fare (in punto di fatto)?
Cosa **deve** fare (in punto di diritto?
Cosa **non deve** fare (in punto di diritto)?
Perché?
(segue breve discussione)

</>

Tizio una mattina passando per un corridoio trova sul pavimento un foglio di carta su cui sono riportate delle credenziali di accesso ad uno degli applicativi di Ateneo.
Il foglio non è suo, ma il proprietario delle credenziali è individuabile.

Cosa **può** fare (in punto di fatto)?
Cosa **deve** fare (in punto di diritto?
Cosa **non deve** fare (in punto di diritto)?
Perché?
(segue breve discussione)

</>

L'introduzione di **nuove tecnologie** (e il loro rapido susseguirsi) crea **conflitti** culturali e sociali …

Tecnologia = «strumento di salvezza»

2001: A Space Odyssey (1968) (Stanley Kubrick)

SCIENTISMO

SCETTICISMO

Tecnologia = «strumento del demonio»

Galileo (1945) (Bertolt Brecht)

… mentre il mezzo tecnologico tende a «sterilizzare» l'interazione che abbiamo con gli altri, diminuendo la percezione degli effetti della nostra stessa condotta.

«il problema del vecchio mandarino»

«*ricordi quel passo in cui [Rousseau, n.d.r.] domanda al lettore che cosa farebbe se potesse arricchirsi uccidendo in Cina, con un semplice atto di volontà, un vecchio mandarino, senza muoversi da Parigi?*».

Huffington Post

-> HONORÈ DE BALZAC, *Le père Goriot*, tr. it. di Giorgio Cingoli, *Papà Goriot* (I narratori del realismo; 35), 1961 (1834), pp. 126-127 [Domanda di Eugène de Rastignac all'amico Horace Bianchon]

-> HENNING RITTER, *Nahes und fernes Unglück. Versuch über das Mitleid*, tr. it. di Marco Rispoli, *Sventura lontana. Saggi sulla compassione*, Milano, Adelphi (Saggi. Nuova serie; 55), 2007 (2004)

In questo contesto, l'Unione Europea si è posta un obiettivo politico preciso: creare un «mercato unico digitale»

"The Digital Single Market strategy aims to open up digital opportunities for people and business and enhance Europe's position as a world leader in the digital economy"

"data economy" = 257 miliardi € (2014) = 1,85% PIL della UE
= 272 miliardi € (2015) = 1,87% PIL della UE
= 643 miliardi € (2020) = 3,17% PIL della UE (stima)

Oggi **l'informazione è l'unico valore** (in quanto dato, ovvero organizzazione sociale, ovvero *asset* economico)

Floridi, Luciano (a cura di), *The Onlife Manifesto. Being Human in a Hyperconnected Era*, Cham, Springer International Publishing (Open Access, 2015. https://ec.europa.eu/digital-agenda/en/onlife-manifesto.
EAG Report 2018 25/01/2018 Report by the EDPS (European Data Protection Supervisor) Ethics Advisory Group
https://edps.europa.eu/sites/edp/files/publication/18-01-25_eag_report_en.pdf

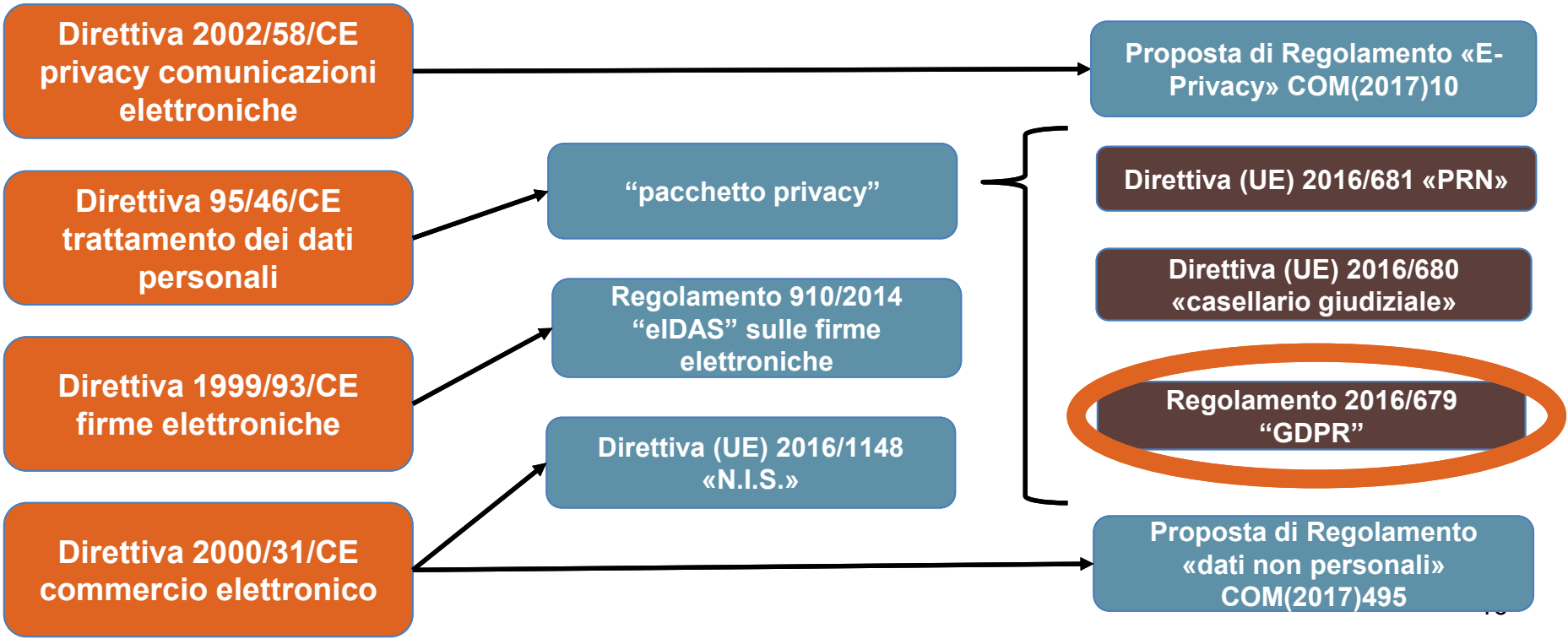
"[…] *Le tecnologie dell'informazione e della comunicazione (TIC) non costituiscono più un settore a sé stante, bensì sono la base stessa di tutti i sistemi economici e delle società innovativi e moderni*. […]".

Considerando (1), Proposta di Regolamento UE relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione Europea, COM(2017) 495 final del 13.9.2017.

https://ec.europa.eu/jrc/en/science-area/information-society

https://ec.europa.eu/commission/index_en

Nell'ambito dell'Unione Europea di recente si è assistito ad una consistente integrazione di norme preesistenti in tema di **sicurezza** dell'informazione e **protezione** dei dati personali.



Da ciò alcune **importanti scadenze**

31/12/2017: attuazione Circolare 18 aprile 2017 AgID
-> Misure minime di sicurezza P.A. (per ulteriori approfondimenti vedasi oltre)

9/5/2018: adeguamento Direttiva UE 2016/1148 «N.I.S.» da parte dell'Italia
-> rientrano tra gli «operatori di servizi essenziali» (art. 4 c. 1 n.4) anche «prestatori di assistenza sanitaria ex art. 3 lett. g) DIR. 2011/24/UE» (allegato II, n. 5, DIR. 2016/1148/UE)

25/5/2018: **adempimenti Regolamento UE 679/2016 «GDPR»**
-> diversi adempimenti (per ulteriori approfondimenti vedasi oltre)

Queste innovazioni normative determinano modifiche su corpus normativi preesistenti nel nostro ordinamento.
In particolare:

- il **D. Lgs. 30 giugno 2003, n. 196**, Codice in materia di protezione dei dati personali;

- il **D. Lgs. 7 marzo 2005, n. 82**, Codice dell'amministrazione digitale;

- il **D. Lgs.14 marzo 2013, n. 33**, Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni

Ad aumentare la difficoltà della situazione vi è l'estrema «complessità» del contesto giuridico di riferimento, nel quale interagiscono tra loro:

- Convenzioni e tribunali internazionali (CEDU)
- Norme e giurisprudenza dell'Unione Europea
- Norme statali (legislazione, regolamento)
- C.D. «soft law» (provvedimenti Garante, linee guida WP29 su Sanzioni, DPO …)
- Regolamenti interni (provvedimenti M.R., Dir. Gen.)
- Standard tecnici (ISO)
- Codici deontologici professionali e di autoregolamentazione (Medicina, Statistica)

-> Direttiva UE: vincola negli obiettivi non nelle misure (di regola) quindi richiede recepimento (es: L. 167/2017, in particolare art. 24 conservazione traffico telefonico 72 mesi)

-> Regolamento UE: immediatamente vincolante (anche se «per comodità» (es: L. 163/2017) delega al Governo per recepimento

</>

In questa sede prendiamo in considerazione separatamente i tre aspetti accennati in precedenza:

(3.1) Sicurezza informatica, Direttiva UE 1146/2016 «N.I.S.» e «resilienza»

(3.2) Dati personali, adempimenti *ex* Regolamento UE 679/2016

(3.3) Amministrazione digitale, adempimenti *ex* D.Lgs. 82/2005

(3.1) Sicurezza informatica, Direttiva UE 1146/2016 «N.I.S.» e «resilienza»

Il riferimento alla Direttiva UE «Network Information Security» serve per delineare **l'approccio complessivo** adottato dalle Istituzioni europee al quale conviene perlomeno ispirarsi.

Si considera brevemente:

(1) Il concetto di sicurezza informatica

(2) Le implicazioni che riguardano le «organizzazioni complesse»

(3) L'approccio previsto dalla UE

(3.1) Sicurezza informatica, Direttiva UE 1146/2016 «N.I.S.» e «resilienza»

(1) Il concetto di «sicurezza informatica»

Noi tutti siamo abituati a pensare alla sicurezza in termini **assoluti** …

Fort Knox (Kentucky)

…ma **non è concepibile** un sistema informatico che sia **sempre** «sicuro» …

… sicché la «sicurezza informatica» oggi può essere configurata **solo** in termini di **«gestione del rischio informatico»**

<(3) «focus» sugli aspetti problematici>

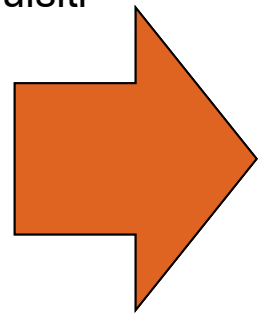
(3.1) Sicurezza informatica, Direttiva UE 1146/2016 «N.I.S.» e «resilienza»

(1) Il concetto di «sicurezza informatica»

"CIA TRIAD"

(1) Confidenzialità (Confidentiality)
(2) Integrità (Integrity)
(3) Disponibilità (Availability)

.. E la nozione si è **evoluta** nel tempo (seguendo le tecnologie) aggiungendo ulteriori requisiti



"Information Assurance and Security (IAS) octave"

(4) "responsabilizzazione" (Accountability)
(5) "monitoraggio" (Auditability)
(6) "autenticità / fiducia" Authenticity/Trustworthiness
(7) "non-ripudiabilità" (Non-repudiation)
(8) Riservatezza (legale) (Privacy)

-> J. H. Saltzer e M. D. Schroeder, The protection of information in computer systems, in «Proceedings of the IEEE», 63 n. 9 (1975), pp. 1278-1308.

-> Barbara Guttman e Edward A. Roback, An Introduction to Computer Security: The Nist Handbook, , Washington, Diane Publishing, 1995.

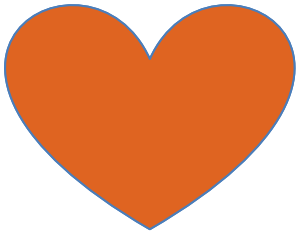
-> YULIA CHERDANTSEVA E JEREMY HILTON, *A Reference Model of Information Assurance and Security*, Eight International Conference on Availability, Reliability and Security (ARES 2013), IEEE (ed.), 2013, pp. 546-555.

(3.1) Sicurezza informatica, Direttiva UE 1146/2016 «N.I.S.» e «resilienza»

(2) Implicazioni che riguardano le «organizzazioni complesse»

Sono **diversi ed eterogenei** i fattori da considerare della sicurezza informatica delle organizzazioni sociali

(1) information (dati, in generale)
(2) people
(3) business processes (procedure)
(4) hardware
(5) software
(6) reti



-> Alter, Steven, *Defining information systems as work systems: implications for the IS field*, in «European Journal of Information Systems», 17 n. 5 (2008), pp. 448-469

(3.1) Sicurezza informatica, Direttiva UE 1146/2016 «N.I.S.» e «resilienza»

(2) Implicazioni che riguardano le «organizzazioni complesse»

Bisogna notare che in tutti i modelli teorici **l'elemento umano** è sempre presente

(A) Decisioni aziendali in tema di sicurezza

(B) **Pratica** dei dipendenti, precauzioni effettivamente adottate

(C) **Coinvolgimento** dei dipendenti da parte del management

(D) «policy» di sicurezza informativa stabilita dal management ed applicata da tutto il personale

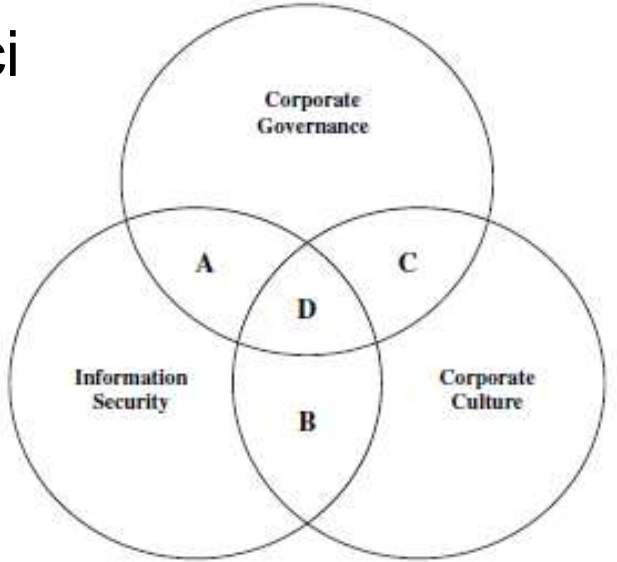


Figure 1 The relationships between information security, corporate governance and corporate culture.

-> Thomson, Kerry-Lynn e Rossouw von Solms, *Information security obedience: a definition*, in «Computers & Security», 24 n. 1 (2005), pp. 69-75

<(3) «focus» sugli aspetti problematici>

(3.1) Sicurezza informatica, Direttiva UE 1146/2016 «N.I.S.» e «resilienza»

(3) L'approccio previsto dalla UE

RESILIENZA

«la capacità di un materiale di autoripararsi dopo un danno o di una comunità (o sistema ecologico) di **ritornare al suo stato iniziale** dopo essere stata sottoposta a una **perturbazione** che l'ha allontanata da quello stato»

Wikipedia

- Drettiva "NIS" (UE) 2016/1148 del 6 luglio 2016 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione
- Raccomandazione del 13.9.2017, C(2017) 6100 final, programma per una risposta coordinata a crisi di cibersicurezza su vasta scala (azioni coordinate tra ENISA, CSIRT nazionali, CERT-UE)
- Risoluzione del Parlamento europeo del 3 ottobre 2017 sulla lotta alla criminalità informatica (2017/2068(INI))
- Council Conclusions on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU - Council conclusions (20 November 2017)

(3.2) Dati personali, adempimenti *ex* Regolamento UE 679/2016

Il riferimento al Regolamento Generale sulla Protezione dei Dati Personali si inserisce in un contesto già ricco di istanze e di complessità.
Vale la pena accennare ad alcuni aspetti specifici:

(1) Quadro concettuale preliminare: privacy / riservatezza / dati personali

(2) Novità del GDPR in sintesi

(3) Implicazioni e problematiche in ambito universitario

(3.2) Dati personali, adempimenti *ex* Regolamento UE 679/2016

(1) Quadro concettuale preliminare: privacy / riservatezza / dati personali

«privacy», «riservatezza», e «protezione dei dati personali» non sono sinonimi

Privacy = «diritto di essere lasciati soli»

-> Nel nostro ordinamento **non** esiste la privacy come **«diritto» assoluto**

-> Warren, Samuel D., and Louis D. Brandeis. "The Right to Privacy." *Harvard Law Review* 4, no. 5 (1890): 193-220.

Samuel D. Warren

Louis Brandeis

(3.2) Dati personali, adempimenti *ex* Regolamento UE 679/2016

(1) Quadro concettuale preliminare: privacy / riservatezza / dati personali

«privacy», «riservatezza», e «protezione dei dati personali» non sono sinonimi

Riservatezza = mancanza di un interesse pubblico giuridicamente apprezzabile a conoscere dettagli della vita privata della persona

-> Nel nostro ordinamento è un **diritto di matrice giurisprudenziale** (Cassazione 2129/1975) concepito «in negativo» rispetto al titolare (oggetto di valutazione è l'interesse altrui a conoscere, non l'intimità in sè)

Soraya Esfandiary Bakhtiari

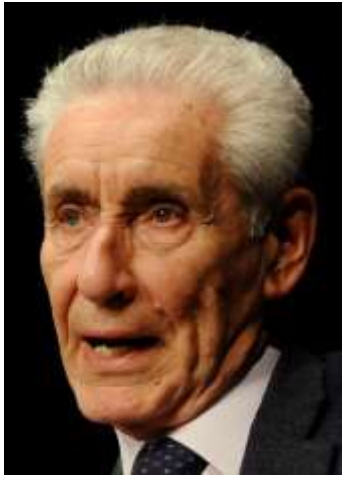
(3.2) Dati personali, adempimenti *ex* Regolamento UE 679/2016

(1) Quadro concettuale preliminare: privacy / riservatezza / dati personali

«privacy», «riservatezza», e «protezione dei dati personali» non sono sinonimi

Dati personali = dati che si riferiscono al soggetto «interessato»

-> nel nostro ordinamento la protezione dei dati personali **non è un «diritto» perfetto** ma solo un interesse giuridicamente qualificato, infatti si qualifica come «interessato» il soggetto a cui i dati si riferiscono

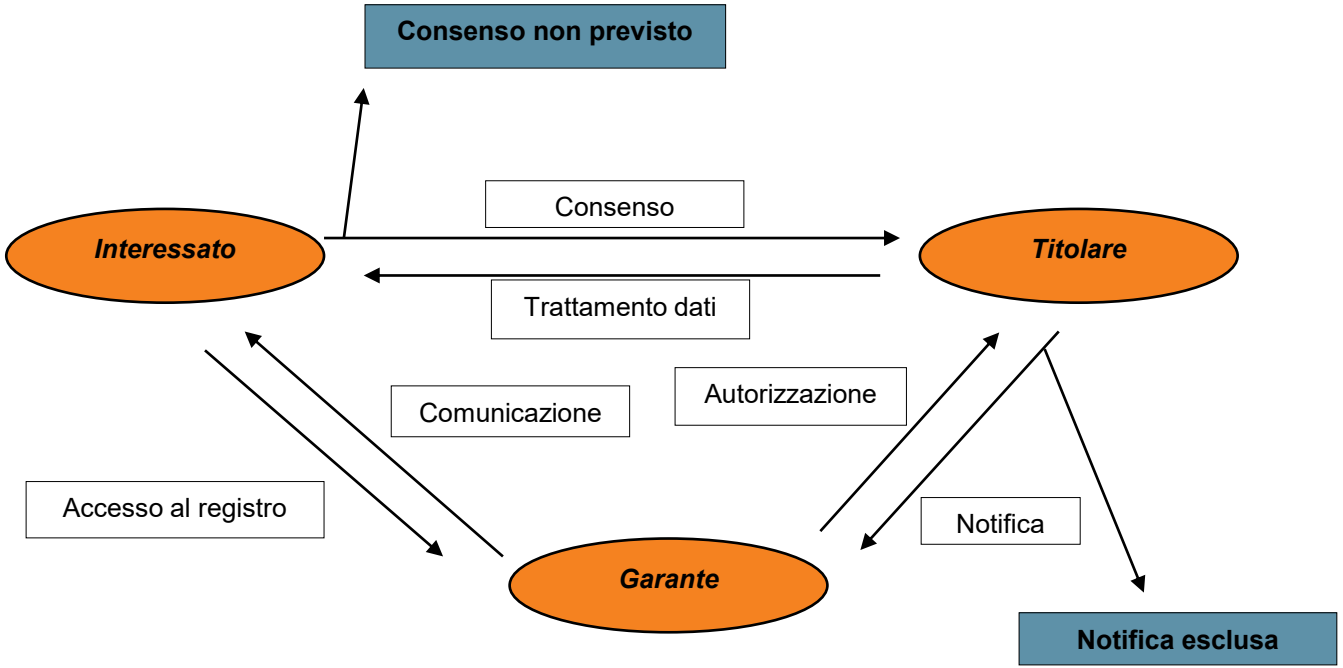


Stefano Rodotà

(3.2) Dati personali, adempimenti *ex* Regolamento UE 679/2016

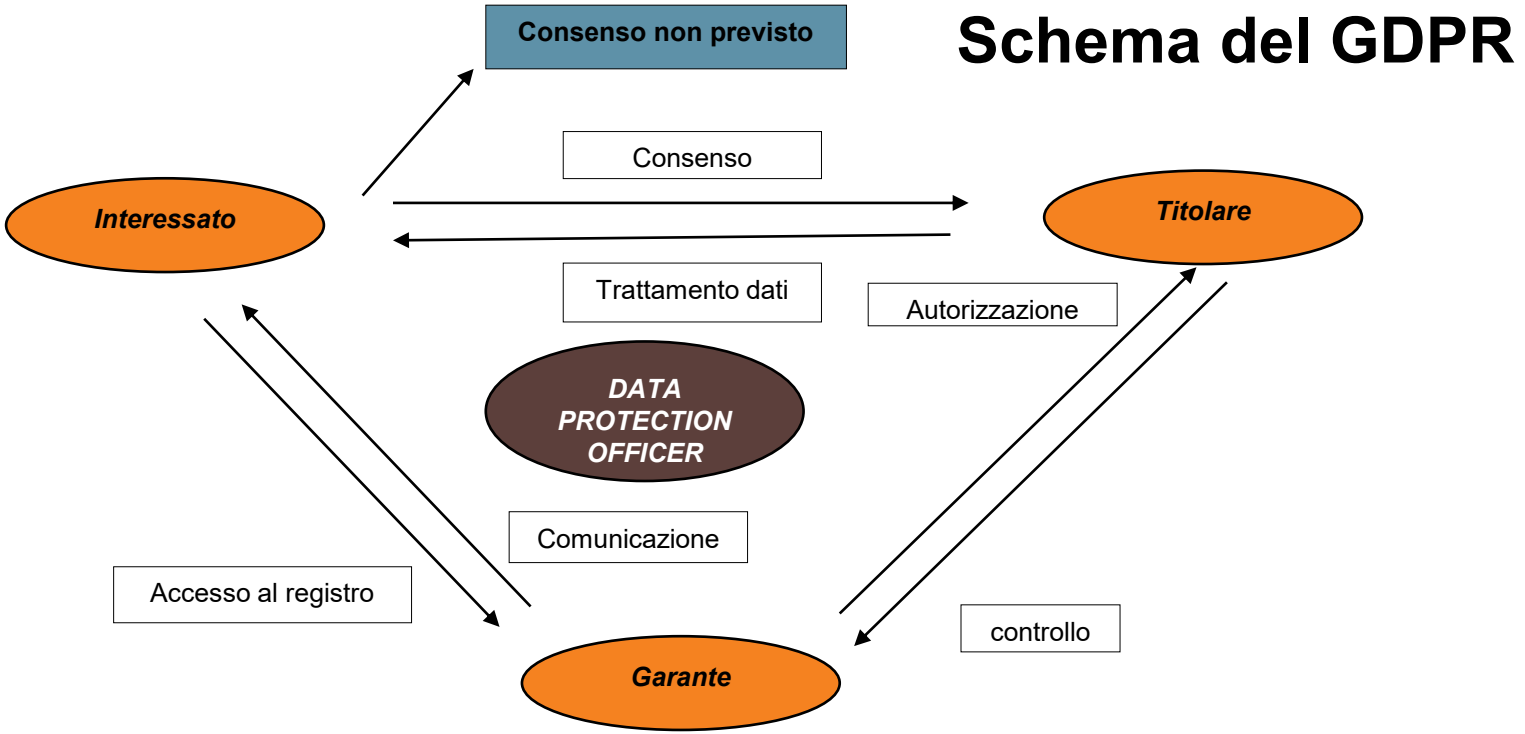
(2) Novità del GDPR in sintesi

Schema del D.Lgs. 196/2003



(3.2) Dati personali, adempimenti *ex* Regolamento UE 679/2016

(2) Novità del GDPR in sintesi



(3.2) Dati personali, adempimenti *ex* Regolamento UE 679/2016

(2) Novità del GDPR in sintesi

(1) Previsione espressa del «diritto all'oblio»

(2) Trasparenza -> GUIDELINES WP29 260

(3) Portabilità dei dati personali (cambio di provider)

(4) Diritto di notifica in caso di «data breach» (72 ore)

(5) «valutazione di impatto» per dati di particolare importanza -> GUIDELINES WP29 248

(6) Privacy by design / by default

(7) Data Protection Officer («competenze» > «titoli») -> GUIDELINES WP29 243, FAQ

(8) Titolare / responsabile del trattamento dei dati

(9) Codici di autodisciplina / certificazioni delle misure di sicurezza

(10) Sanzioni (molto elevate)

(3.2) Dati personali, adempimenti *ex* Regolamento UE 679/2016

(2) Novità del GDPR in sintesi

(1) **<u>Sanzioni amministrative pecuniarie (GDPR)</u>** (artt. 83 anche in aggiunta alle misure art. 58)

(2) **<u>Altre sanzioni stabilite dagli Stati membri</u>** (art. 84) -> Sanzioni penali D.Lgs. 196/2003

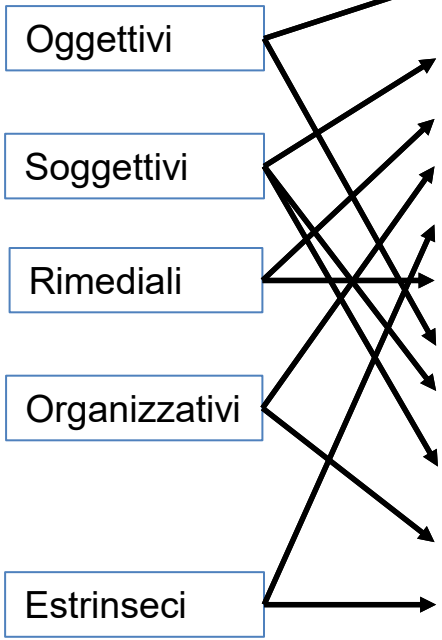
Le sanzioni amministrative pecuniarie sono disciplinate in modo «composito», distinguendosi:

(1) Criteri
(2) Prescrizioni
(3) Sanzioni

(3.2) Dati personali, adempimenti *ex* Regolamento UE 679/2016

(2) Novità del GDPR in sintesi

(1) Criteri (oltre che «effettive», «proporzionate», «dissuasive»)



a) la natura, la gravità e la durata della **violazione** tenendo in considerazione la natura, l'oggetto o la **finalità** del trattamento in questione nonché il **numero di interessati** lesi dal danno e il **livello del danno** da essi subito;

b) il carattere **doloso o colposo** della violazione;

c) le **misure** adottate dal titolare del trattamento o dal responsabile del trattamento **per attenuare** il danno subito dagli interessati;

d) il grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle **misure tecniche e organizzative** da essi messe in atto ai sensi degli articoli 25 e 32;

e) eventuali **precedenti violazioni** pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento;

f) il grado di **cooperazione con l'autorità di controllo** al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;

g) le **categorie di dati personali** interessate dalla violazione;

h) la maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento **ha notificato la violazione**;

i) qualora siano stati **precedentemente disposti provvedimenti** di cui all'articolo 58, paragrafo 2, nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti;

j) l'adesione ai **codici di condotta** approvati ai sensi dell'articolo 40 o ai **meccanismi di certificazione** approvati ai sensi dell'articolo 42; e

k) eventuali **altri fattori aggravanti o attenuanti** applicabili alle circostanze del caso, ad esempio i **benefici** finanziari conseguiti o le **perdite** evitate, direttamente o indirettamente, quale conseguenza della violazione.

(3.2) Dati personali, adempimenti *ex* Regolamento UE 679/2016

(2) Novità del GDPR in sintesi

(2) Prescrizioni e (3) Sanzioni

(§.4) a) gli **obblighi** del titolare del trattamento e del responsabile del trattamento a norma degli articoli 8, 11, da 25 a 39, 42 e 43;
b) gli obblighi **dell'organismo di certificazione** a norma degli articoli 42 e 43;
c) gli obblighi **dell'organismo di controllo** a norma dell'articolo 41, paragrafo 4;

(§. 4) sanzioni amministrative pecuniarie fino **a 10 000 000 EUR**, o per le imprese, fino **al 2 % del fatturato** mondiale totale annuo dell'esercizio precedente, se superiore

(§. 5) a) i **principi** di base del trattamento, comprese le condizioni relative al **consenso**, a norma degli articoli 5, 6, 7 e 9;
b) i **diritti** degli interessati a norma degli articoli da 12 a 22;
c) i **trasferimenti** di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale a norma degli articoli da 44 a 49;
d) **qualsiasi obbligo ai sensi delle legislazioni** degli Stati membri adottate a norma del capo IX;
e) **l'inosservanza di un ordine**, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo ai sensi dell'articolo 58, paragrafo 2, o il negato accesso in violazione dell'articolo 58, paragrafo 1.

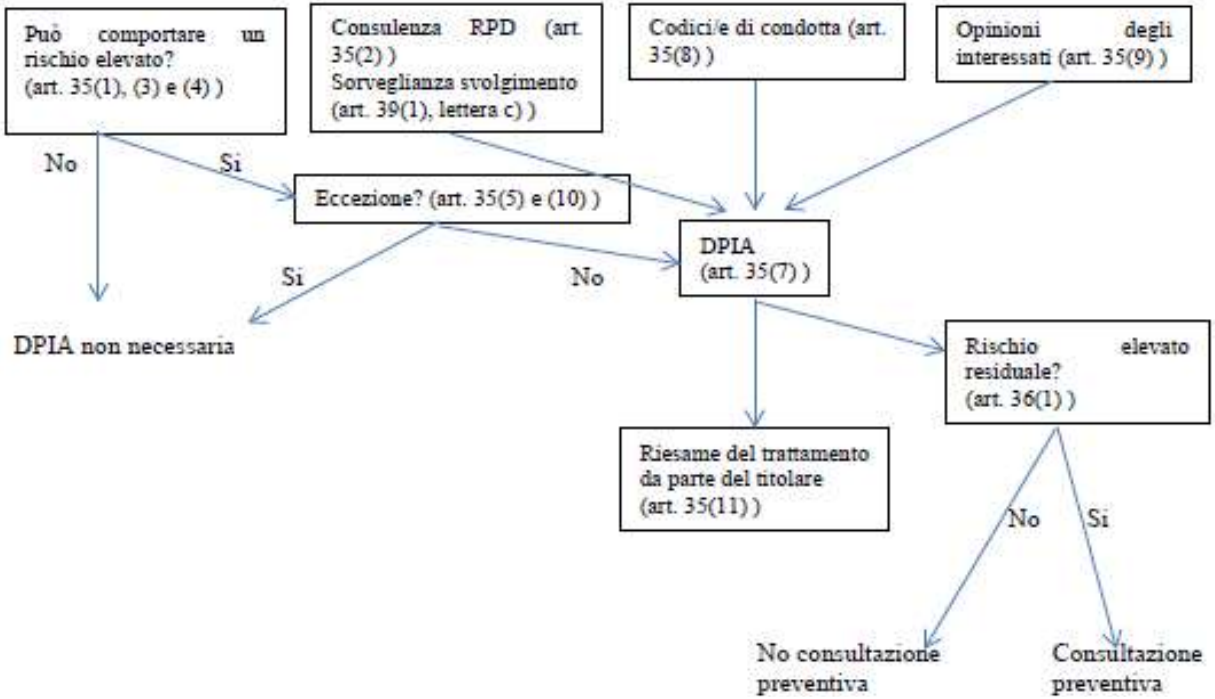
(§. 6) sanzioni amministrative pecuniarie **fino a 20 000 000 EUR**, o per le imprese**, fino al 4 % del fatturato** mondiale totale annuo dell'esercizio precedente, se superiore

(§. 6) l'inosservanza di un **ordine da parte dell'autorità di controllo** di cui all'articolo 58, paragrafo 2,

(§. 7) estensione alle istituzioni pubbliche

(3.2) Dati personali, adempimenti *ex* Regolamento UE 679/2016

(2) Novità del GDPR in sintesi -> la «valutazione di impatto» (art. 35 GDPR)



Schema processo DPIA

Linee guida WP29, pag. 6

<(3) «focus» sugli aspetti problematici>

(3.2) Dati personali, adempimenti *ex* Regolamento UE 679/2016

(2) Novità del GDPR in sintesi -> la «valutazione di impatto» (art. 35 GDPR)

ATTENZIONE!

«Lo svolgimento della DPIA **è un processo continuativo** e non un'attività *una tantum*».

Linee guida WP29, pag. 14

-> WRIGHT, D., Making Privacy Impact Assessment More Effective, in «Information Society», 29 n. 5 (2013), pp. 307-315

Linee guida WP29, pag. 16

(3.2) Dati personali, adempimenti *ex* Regolamento UE 679/2016

(3) Implicazioni in ambito universitario –> esempio: UNIUD

1 Applicativi didattica e ricerca:
1.1 Esse3
1.2 Elearning - Materiale didattico
1.3 Orario di ricevimento
1.4 Primo
1.5 Verbali dottorato
1.6 PICA
1.7 OpenUniud
1.8 IRIS
1.9 Kosmos
1.10 U-WEB Timesheet
1.11 U-WEB Missioni
2 Applicativi del personale
2.1 CSA
2.2 Concorsi docenti/ricercatori
2.3 Concorsi TA
2.4 Prestazioni esterne
2.5 Perform
2.6 Presenze
2.7 Candidature PEO
2.8 Documenti online
2.9 Titulus
2.10 Titulus organi/Archivio delibere
3 Applicativi di contabilità
3.1 UGOV (contabilità/PJ/Pian. e contr.)
3.2 Budget
3.3 Archivio Contratti
4 Applicativi comuni
4.1 Web
4.2 Helpdesk informatico
4.3 Posta elettronica e applicativi 365
4.4 Valutazioni online
4.5 InviaMail
4.6 Prenotazione risorse di Ateneo

Complessità del «registro dei trattamenti»

≠ domini
≠ interessati
≠ responsabili
≠ funzioni
≠ dispositivi HW
≠ sistemi SW

-> cfr. gruppo di lavoro CODAU, *Linee guida Privacy e GDPR, versione dicembre 2017*

(3.3) Amministrazione digitale, adempimenti *ex* D.Lgs. 82/2005

In questa sede vale la pena concentrarsi sugli aspetti più significativi

(1) Brevi cenni introduttivi

(2) Le più importanti innovazioni recenti

(3) Le implicazioni per l'università

(3.3) Amministrazione digitale, adempimenti *ex* D.Lgs. 82/2005

(1) Brevi cenni introduttivi

IL PRIMO PROBLEMA DI FONDO DEL C.A.D.:

IL TESTO E LE RIFORME DEL C.A.D.!

D.Lgs. 4 aprile 2006, n. 159,
Legge 24 dicembre 2007, n. 244,
Legge 28 gennaio 2009 n. 2,
Legge 18 giugno 2009, n. 69,
Legge 3 agosto 2009, n. 102,
D.Lgs. 30 dicembre 2010, n. 235,
Legge n. 221/2012 (Agenda Digitale)
Legge n. 98/2013 (decreto «del fare»)
D.Lgs. n. 179 del 26 agosto 2016 (riforma Madia)
D. Lgs. N. 217 del 13 dicembre 2017, in G.U. 12/01/2018

(3.3) Amministrazione digitale, adempimenti *ex* D.Lgs. 82/2005

(1) Brevi cenni introduttivi

IL SECONDO PROBLEMA DI FONDO DEL C.A.D.:

(TALVOLTA) VIENE APPLICATO!

«Va **condannata** la p.a. che non abbia adempiuto alla **pubblicazione** sulla pagina iniziale del proprio sito web **dell'indirizzo di posta elettronica certificata**, così come previsto dall'art. 54 comma 2 ter d.lg. n. 82 del 2005 (codice dell'amministrazione digitale), **ad adottare tutti gli atti amministrativi necessari a garantire l'effettiva possibilità per gli utenti di comunicare con la Regione attraverso la posta elettronica certificata** (PEC), nel rispetto del combinato disposto di cui **agli art. 3** e 6 dello stesso codice che prevedono il diritto dei cittadini e degli utenti a comunicare con tecnologie telematiche con le pubbliche amministrazioni».

T.A.R. Potenza Basilicata sez. I 23 settembre 2011 n. 478 in Publica 2011

(3.3) Amministrazione digitale, adempimenti *ex* D.Lgs. 82/2005

(2) Le più importanti innovazioni recenti

(1) SPID, ANPR, domicilio digitale
(2) Dematerializzazione
(3) Firme elettroniche -> Regolamento eIDAS (1° luglio 2016)
(4) Disaster recovery (art. 50 bis CAD)
(5) Trasparenza amministrativa (segue)
(6) «Regole tecniche» ministeriali -> «Linee guida» AgID
(7) Misure minime di sicurezza (segue)
(8) Responsabilità dirigenziale per perseguimento della «digitalizzazione»

-> **Regolamento (UE) n. 910/2014** del Parlamento europeo e del Consiglio, del 23 luglio 2014 , in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE, in OJ L 257, 28.8.2014, p. 73–114
-> **Decisione di esecuzione (UE) 2015/1506** della Commissione, dell'8 settembre 2015, che stabilisce le specifiche relative ai formati delle firme elettroniche avanzate e dei sigilli avanzati che gli organismi del settore pubblico devono riconoscere, di cui all'articolo 27, paragrafo 5, e all'articolo 37, paragrafo 5, del regolamento (UE) n. 910/2014, in OJ L 235, 9.9.2015, p. 37–41
-> **Decisione di esecuzione (UE) 2016/650** della Commissione, del 25 aprile 2016, che stabilisce norme per la valutazione di sicurezza dei dispositivi per la creazione di una firma e di un sigillo qualificati a norma dell'articolo 30, paragrafo 3, e dell'articolo 39, paragrafo 2, del regolamento (UE) n. 910/2014, in OJ L 109, 26.4.2016, p. 40–42

(3.3) Amministrazione digitale, adempimenti *ex* D.Lgs. 82/2005

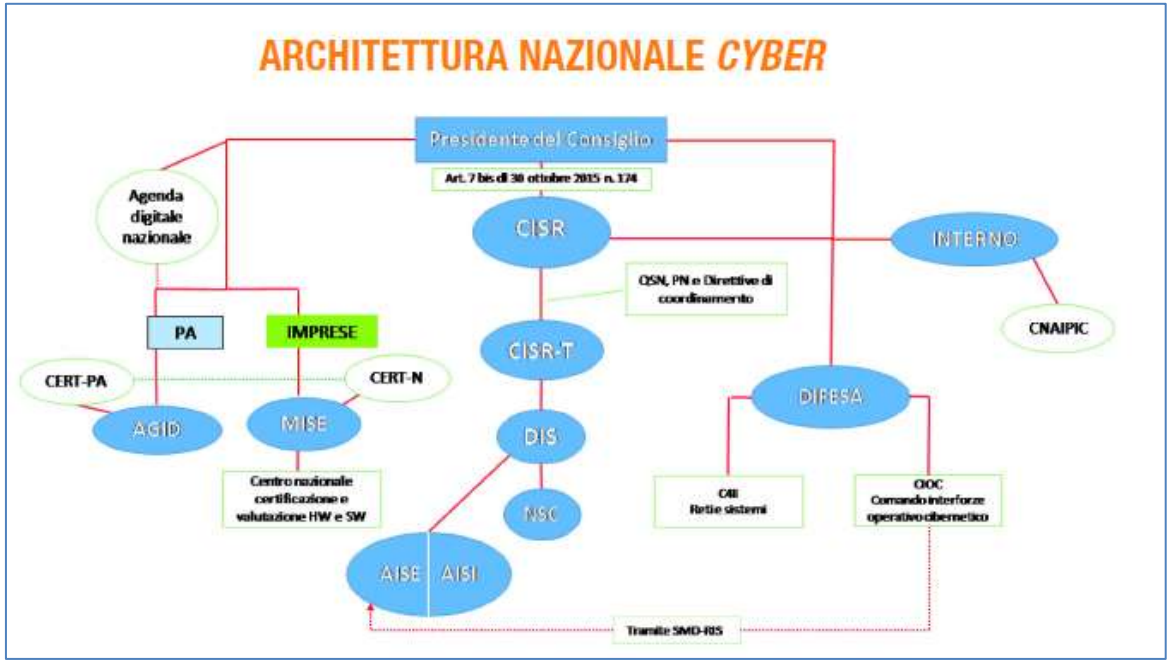
(2) Le più importanti innovazioni recenti

In particolare: le misure minime di sicurezza

Fonti giuridiche:

- L. 3 agosto 2007, n. 124, Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto,
- Direttiva P.C.M. 1° agosto 2015
- D.P.C.M. 17 febbraio 2017, Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali,
- Piano nazionale per la protezione cibernetica e la sicurezza informatica (marzo 2017)
- Circolare AgID 18 aprile 2017 «Misure minime di sicurezza ICT per le P.A.»

Standard tecnici
Controlli SANS20 -> CIS 6.0 (ottobre 2015)



(3.3) Amministrazione digitale, adempimenti *ex* D.Lgs. 82/2005

(2) Le più importanti innovazioni recenti

In particolare: la «trasparenza» amministrativa

Fonti giuridiche:

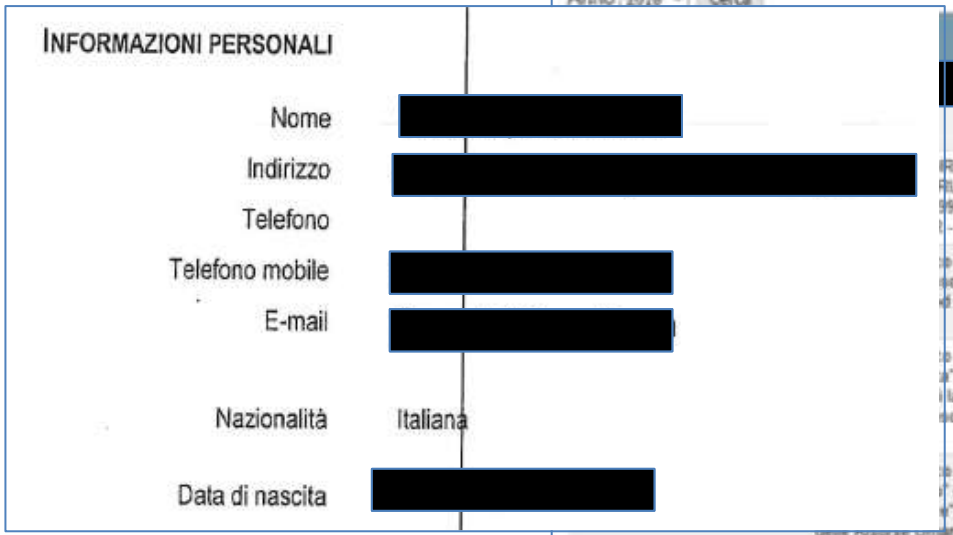
- D. Lgs.14 marzo 2013, n. 33, Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicita', trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni

- Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati -> Testo Linee Guida

(3.3) Amministrazione digitale, adempimenti *ex* D.Lgs. 82/2005

(3) Le implicazioni per l'Università

… Troppa trasparenza?



INFORMAZIONI PERSONALI

Nome [redacted]

Indirizzo [redacted]

Telefono

Telefono mobile [redacted]

E-mail [redacted]

Nazionalità Italiana

Data di nascita [redacted]

Incarichi di collaborazione e consulenza affidati a soggetti esterni

Relativamente agli incarichi per i quali è avvenuta la verifica dell'insussistenza, anche potenziale, di conflitto di interesse.

Anno 2018 Cerca

Incarico	Estremi atto	Data atto	Compenso	Inizio	Fine
[redacted] 01/2018 al 15/01/2019 FSEHEAD	1	12/12/2018	20382.00 €	16/01/2018	15/01/2019
RITTO COMMERCIALE (GI0288) - Corso di RUDENZA (337) - Percorso: PERCORSO 999) - A.A. 2017/2018 - Ore 15 - CFU 9 - - Incarico di didattica integrativa retribuito		18/10/2018	375.00 €	01/10/2017	30/09/2018
o di natura seminariale dal titolo "Il potere so il Master di I livello in Gestione delle d Organizzazione del lavoro - a.a.	58	30/01/2018	630.52 €	02/02/2018	02/02/2018
o di natura seminariale dal titolo "I contratti a" e "Il licenziamento collettivo dal punto di lavoro" " presso il Master di I livello in sorse Umane ed Organizzazione del lavoro	41	23/01/2018	576.92 €	27/01/2018	03/02/2018
o di natura seminariale dal titolo "I contratti " e "Il licenziamento collettivo dal punto di " presso il Master di I livello in Gestione ane ed Organizzazione del lavoro - a.a. 2017/2018	40	23/01/2018	576.92 €	27/01/2018	10/02/2018

</>

Descrizione sommaria del metodo prospettato

In linea di principio, il processo di riorganizzazione potrebbe svolgersi molto semplicemente come segue:

(1) TECNOLOGIA -> (2) ORGANIZZAZIONE -> (3) PERSONE

In altri termini, configurare tre fasi essenziali:
(1) Innovazione tecnologica;
(2) Modifica delle procedure amministrative;
(3) Formazione del personale;

… ma …

Questo approccio sarebbe **sostenibile** (ed efficace a lungo termine)? NO
Sarebbe **condiviso** dalle persone coinvolte? NO
È davvero **conforme** agli obiettivi del GDPR? NO

Descrizione sommaria del metodo prospettato:

Si è ritenuto opportuno procedere tenendo in maggiore considerazione il «fattore umano»:

OBIETTIVO:

creare una **«comunità di interesse»** intorno ai **problemi** concernenti la protezione dei dati personali e la digitalizzazione dei processi amministrativi in generale

Indirizzo generale delle attività prospettate

(1) Coordinamento delle azioni
-> «cabina di regia»;

(2) centralità del «fattore umano»
-> favorire un consapevole adempimento delle misure adottate.

<(5) Attività prospettate>

Descrizione sommaria delle attività proposte:

Si prospetta la possibilità di adottare iniziative a **diversi «livelli»:**

(1) Attività preliminare di «**sensibilizzazione**» con distinzione dei destinatari in tre gruppi:

(1) Direzione;
(2) Amministrazione;
(3) Docenti / ricercatori;

(2) Predisposizione di **«Linee guida» generali** per consentire di orientarsi autonomamente nel contesto in rapida evoluzione;

(3) Creazione di una **piattaforma comune** di «approfondimento» (F.A.Q., webinars, dispense);

(4) **Integrazione** reciproca e coordinata delle modifiche tecnologiche e organizzative;

(5) Possibilità di effettuare «**segnalazioni**» individuali tramite il sito www.unityfvg.it: «*non ti carichiamo un ulteriore problema, ti aiutiamo a risolvere quelli che incontri nella tua esperienza quotidiana*»)

(6) **Formazione** specifica distinta per aree di competenza

</>

Descrizione sommaria delle attività proposte:

Principi generali delle «Linee guida»

(1) Principio di immedesimazione personale.
Il principio si traduce in una forma di **rispetto personale** dell'interessato al trattamento dei dati e si può esprimere come risposta ad una semplice domanda: **"come vorrei che i miei dati fossero trattati"?**

(2) **Principi generali relativi al trattamento dei dati**. Questi criteri sono contemplati in via generale anche dalla vigente normativa in tema di tutela dei dati personali. Vengono qui riportati **nella formulazione del GDPR** (art. 5):
a. I dati devono essere trattati con **liceità, correttezza, trasparenza**;
b. I dati devono essere trattati con **finalità** determinata, esplicita, legittima;
c. I dati devono essere trattati se e in quanto **necessario** alle finalità previste;
d. I dati devono essere **esatti, aggiornati e tempestivamente rettificati**;
e. I dati devono essere **conservati** per il tempo strettamente necessario al loro utilizzo e successivamente **eliminati**;
f. I dati devono essere trattati in modo che siano **protetti** da perdita o accesso abusivo;
g. I soggetti che trattano dati devono essere in grado di **dimostrare** il rispetto dei principi sopra indicati.

</>

TAKE AWAY

(1) La «sicurezza» non esiste, esiste «l'incerto»;

(2) La «privacy» non esiste, esiste il controllo dell'informazione (e la protezione dei dati personali);

(3) Nella sicurezza informatica il fattore umano è importante come quello tecnologico.

(4) Non esiste più la distinzione tra «ciò che devo fare» e la «privacy»

(5) Keep calm and … GDPR!

DOMANDE / DISCUSSIONE

?!

RINGRAZIAMENTI

Grazie per l’attenzione!

federico.costantini[@]uniud.it