



GDPR - General Data Protection Regulation

RGPD - Regolamento Generale sulla Protezione dei Dati

Regolamento Privacy Unione Europea (2016/679) relativo al trattamento dei dati personali dei cittadini della Comunità Europea

Renato Narcisi – NetSense S.r.l.

Contesto normativo di riferimento

1995	Direttiva U.E. 94/46/CE
Dicembre 1995	Legge 675/96 che recepisce la direttiva
1999	D.P.R. 318/1999 (misure minime di sicurezza da adottare per il trattamento dei dati personali)
01-01-2004	Va in vigore il Codice in materia di protezione dei dati personali (D.Lgs. 196/2003) altrimenti detto "Testo unico sulla privacy"
2004	Provvedimento sulla videosorveglianza
27-11-2008	Viene definito il ruolo degli Amministratori di Sistema
08-04-2010	Secondo provvedimento sulla videosorveglianza che sostituisce quello del 2004
04-05-2016	Viene pubblicato sulla G.U. Dell'U.E. Il General Data Protection Regulation (GDPR) – Regolamento UE 2016/679 o Regolamento Generale sulla Protezione dei Dati (RGPD)
2016-2018	Linee Guida Gruppo Articolo 29
25-05-2018	Il GDPR trova piena attuazione e nasce il Comitato europeo per la protezione dei dati
19-09-2018	Entra in vigore il decreto di attuazione del RGPD, D.Lgs. 101/2018



Era davvero necessaria?

ERRORE TIPICO: obiettare che non si ha nulla da nascondere.

E se i dati che non nascondiamo passassero di mano in mano e fossero male interpretati?

ESEMPIO: CARD NOMINATIVE DEI SUPERMERCATI



minimarket familiare → catene supermercati → fondi di investimenti

RISULTATO:

Miei comportamenti si potrebbero riflettere nelle richieste di mutui/servizi assicurativi

Non è fantascienza: In UK è successo proprio questo alle catene di PUB

Negligenti con le nostre mail?

Mia mail



INVIATO	DATA	ORA	DESTINATARIO	STATO	CONTENUTO
1	10/10/2010	10:00	10000000000000000000	OK	TESTO DEL MIO PRIMO MESSAGGIO
2	10/10/2010	10:05	10000000000000000000	OK	TESTO DEL MIO SECONDO MESSAGGIO
3	10/10/2010	10:10	10000000000000000000	OK	TESTO DEL MIO TERZO MESSAGGIO
4	10/10/2010	10:15	10000000000000000000	OK	TESTO DEL MIO QUARTO MESSAGGIO
5	10/10/2010	10:20	10000000000000000000	OK	TESTO DEL MIO QUINTO MESSAGGIO
6	10/10/2010	10:25	10000000000000000000	OK	TESTO DEL MIO SESTO MESSAGGIO
7	10/10/2010	10:30	10000000000000000000	OK	TESTO DEL MIO SETTIMO MESSAGGIO
8	10/10/2010	10:35	10000000000000000000	OK	TESTO DEL MIO OTTAVO MESSAGGIO
9	10/10/2010	10:40	10000000000000000000	OK	TESTO DEL MIO NONO MESSAGGIO
10	10/10/2010	10:45	10000000000000000000	OK	TESTO DEL MIO DECIMO MESSAGGIO



tutti i documenti che sono transitati negli anni dalla mail:

- CI / CF
- estratti conto bancari (IBAN / ecc)
- conti telefonici e numeri di SIM



POTENZIALE FURTO DELLA MIA IDENTITA', CLONAZIONI SIM, ALTRO

- ricatti
- furti di account più importanti
- ecc.

Errore tipico che genera vulnerabilità

Secondo Esempio :
REGISTRAZIONE NEI VARI SITI UTILIZZANDO SEMPRE LA STESSA MAIL



E' capitato a me? <https://haveibeenpwned.com>



The screenshot shows the homepage of the 'Have I Been Pwned' website. At the top is a dark navigation bar with links: Home, Notify me, Domain search, Who's been pwned, Passwords, API, About, and Donate. The main content area has a blue background with a large white rounded rectangle containing the text ';-have i been pwned?'. Below this is a subtitle: 'Check if you have an account that has been compromised in a data breach'. A search bar with the placeholder 'email address' and a 'pwned?' button is present. A 1Password advertisement is shown below the search bar. The bottom section features statistics on pwned websites, accounts, pastes, and paste accounts, followed by sections for 'Largest breaches' and 'Recently added breaches'.

Home Notify me Domain search Who's been pwned Passwords API About Donate

;-have i been pwned?

Check if you have an account that has been compromised in a data breach

email address pwned?

Generate secure, unique passwords for every account [Learn more at 1Password.com](#)

Why 1Password?

346	6,931,949,148	90,564	111,659,504
pwned websites	pwned accounts	pastes	paste accounts

Largest breaches

772,904,991 Collection #1 accounts

Recently added breaches

40,960,499 ShareThis accounts

<https://haveibeenpwned.com>



The screenshot shows the homepage of the 'Have I Been Pwned' website. At the top is a dark navigation bar with links: Home, Notify me, Domain search, Who's been pwned, Passwords, API, About, and Donate. The main heading is '';--have i been pwned?' with the subtitle 'Check if you have an account that has been compromised in a data breach'. A search bar contains the email 'rnarcisi@gmail.com' and a 'pwned?' button. The result section, on a dark red background, states 'Oh no — pwned!' and 'Pwned on 3 breached sites and found no pastes (subscribe to search sensitive breaches)'. Below this is a section titled '3 Steps to better security' with a 'Start using 1Password.com' button. The bottom features three yellow cards: the first shows a password 'CUV6U4!GU', the second shows a person at a computer, and the third shows a person with a mail icon.

Home Notify me Domain search Who's been pwned Passwords API About Donate

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

rnarcisi@gmail.com pwned?

Oh no — pwned!

Pwned on 3 breached sites and found no pastes (subscribe to search sensitive breaches)

3 Steps to better security Start using 1Password.com

CUV6U4!GU

COSA FARE?

- Cambiare password nella propria mail.
- Utilizzare una mail SOLO per le cose importanti e una seconda per le altre

MA SOPRATTUTTO:

Imparare che la password è importante quanto le chiavi di un oggetto materiale.

La responsabilità di furti di dati / perdita di privacy /ecc. ricadrà sull'addetto al trattamento, se il dispositivo non era protetto da password, o se la password era troppo debole.

GDPR - General Data Protection Regulation

RGPD - Regolamento Generale sulla Protezione dei Dati

DEFINIZIONI E PRINCIPI GENERALI

Perchè una nuova normativa?

Uniformare le normative dei vari stati membri

Aggiornare la normativa agli ultimi sviluppi tecnologici e, allo stesso tempo non vincolarla allo stato attuale della tecnologia

Prevedere delle **sanzioni pecuniarie** che siano «**effettive, proporzionate e dissuasive**» per i trasgressori

A chi si rivolge il GDPR?

A tutte le organizzazioni (enti pubblici, associazioni, imprese e studi professionali) **che hanno una presenza fisica in almeno uno Stato dell'Unione Europea**

A tutte le organizzazioni (enti pubblici, associazioni, imprese e studi professionali) **straniere che processano o memorizzano dati personali di cittadini europei**

GDPR coinvolge privacy e protezione dei dati

TUTELA DELLA PRIVACY:

riservatezza nell'uso delle informazioni personali di terzi

PROTEZIONE DEI DATI:

obblighi relativi alle misure di sicurezza nella gestione informatica dei dati

Art. 4 - Definizioni

«**dato personale**»: qualsiasi informazione riguardante una **persona fisica identificata o identificabile**; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

«**dati genetici**»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

«**dati biometrici**»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

«**dati relativi alla salute**»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;



Art. 4 - Definizioni

«**trattamento**»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;



Art. 5 - I principi da rispettare (tutto nasce da qui)

I dati personali sono:

- a) **Trattati in modo lecito, corretto e trasparente** nei confronti dell'interessato (principio di «liceità, correttezza e trasparenza»);
- b) **Raccolti per finalità determinate, esplicite e legittime** e successivamente trattati in un modo non incompatibile con quelle finalità (principio di «limitazione della finalità»);
- c) **Adeguati, pertinenti e limitati a quanto necessario** rispetto alle finalità per le quali sono trattati (principio di «minimizzazione dei dati»);
- d) **Esatti**: devono essere adottate tutte le misure per cancellare o rettificare tempestivamente i dati inesatti (principio di «esattezza»);
- e) **conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità** per le quali sono trattati (principio di «limitazione della conservazione»);
- f) **trattati in maniera da garantire un'adeguata sicurezza dei dati personali**, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali (principio di «integrità e riservatezza»).



Art. 5 - I principi da rispettare (tutto nasce da qui)

I dati personali sono:

a) **Trattati in modo lecito, corretto e trasparente** nei confronti dell'interessato (principio di «liceità, correttezza e trasparenza»);

b) **Raccolti per finalità determinate, esplicite e legittime** e successivamente trattati in un modo non incompatibile con quelle finalità (principio di «limitazione della finalità»);

c) **Adeguati, pertinenti e non eccessivi** rispetto alle finalità per le quali sono trattati (principio di «adeguatezza»);

d) **Esatti**; devono essere accurati e aggiornati; non devono essere trattati dati inesatti (principio di «accuratezza»);

e) **conservati in un formato che consenta l'accesso, l'uso e la comunicazione per un arco di tempo non superiore al conseguimento delle finalità** per le quali sono trattati (principio di «limitazione della conservazione»);

f) **trattati in maniera da garantire un'adeguata sicurezza dei dati personali**, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali (principio di «integrità e riservatezza»).

..... LECITO.....

Quale è la base giuridica?

CONSENSO SI / CONSENSO NO

Art. 5 - I principi da rispettare (tutto nasce da qui)

I dati personali sono:

- a) **Treatati in modo lecito, corretto e trasparente** nei confronti dell'interessato (principio di «liceità, correttezza e trasparenza»);
- b) **Raccolti per finalità determinate, esplicite e legittime** e successivamente trattati in un modo non incompatibile con quelle finalità (principio di «limitazione della finalità»);
- c) **Adeguati, pertinenti e limitati a quanto necessario** rispetto alle finalità per le quali sono trattati (principio di «minimizzazione»);
- d) **Esatti**; devono essere conservati in forma esatta e non inesatti (principio di «accuratezza»);
- e) **conservati in un arco di tempo non superiore al necessario** per le finalità per le quali sono trattati (principio di «limitazione della conservazione»);
- f) **trattati in maniera da garantire un'adeguata sicurezza dei dati personali**, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali (principio di «integrità e riservatezza»).

.... FINALITA' DETERMINATE ED ESPLICITE...

cambia la finalità?

Si deve definire un nuovo trattamento

Art. 5 - I principi da rispettare (tutto nasce da qui)

I dati personali sono:

- a) **Treatati in modo lecito, corretto e trasparente** nei confronti dell'interessato (principio di «liceità, correttezza e trasparenza»);
- b) **Raccolti per finalità determinate, esplicite e legittime** e successivamente trattati in un modo non incompatibile con quelle finalità (principio di «limitazione della finalità»);
- c) **Adeguati, pertinenti e limitati a quanto necessario** rispetto alle finalità per le quali sono trattati (principio di «minimizzazione dei dati»);
- d) **Esatti**: devono essere adottate tutte le misure per cancellare o rettificare tempestivamente i dati inesatti (principio di «accuratezza»);
- e) **conservati in un arco di tempo non superiore a quello necessario** allo scopo della conservazione (principio di «limitazione della conservazione»);
- f) **trattati in maniera da garantire la protezione**, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali (principio di «integrità e riservatezza»).

..... LIMITATI.....

devo chiedere ciò che mi necessita.

Tema caldo: professione dei genitori e INVALSI



Art. 5 - I principi da rispettare (tutto nasce da qui)

I dati personali sono:

- a) **Treatati in modo lecito, corretto e trasparente** nei confronti dell'interessato (principio di «liceità, correttezza e trasparenza»);
- b) **Raccolti per finalità determinate, esplicite e legittime** e successivamente trattati in un modo non incompatibile con quelle finalità (principio di «limitazione della finalità»);
- c) **Adeguati, pertinenti e limitati** rispetto alle finalità per le quali sono raccolti e trattati (principio di «adeguatezza, pertinenza e limitazione»);
- d) **Esatti**: devono essere adottate tutte le misure per cancellare o rettificare tempestivamente i dati inesatti (principio di «esattezza»);
- e) **conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al necessario per scopi per i quali i dati sono stati raccolti e trattati** (principio di «limitazione della conservazione»);
- f) **trattati in maniera da garantire un'adeguata sicurezza dei dati personali**, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali (principio di «integrità e riservatezza»).

no comment



Art. 5 - I principi da rispettare (tutto nasce da qui)

I dati personali sono:

- a) **Trattati in modo lecito, corretto e trasparente** nei confronti dell'interessato (principio di «liceità, correttezza e trasparenza»);
- b) **Raccolti per finalità determinate, esplicite e legittime** e successivamente trattati in un modo non incompatibile con quelle finalità (principio di «limitazione della finalità»);
- c) **Adeguati, pertinenti e limitati** rispetto alle finalità per le quali sono trattati (principio di «proporzionalità»);
- d) **Esatti**: devono essere adottate tutte le misure necessarie per assicurare l'accuratezza dei dati inesatti (principio di «esattezza»);
- e) **conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità** per le quali sono trattati (principio di «limitazione della conservazione»);
- f) **trattati in maniera da assicurare la loro sicurezza**, compresa la protezione, mediante adozione di misure tecniche e organizzative adeguate, contro l'accesso non autorizzato o l'uso non autorizzato, la divulgazione non autorizzata o l'eliminazione non autorizzata, l'alterazione non autorizzata o la distruzione non autorizzata, l'illecezione e dalla perdita, dalla distruzione o dal danno accidentali (principio di «integrità e riservatezza»).

no comment



Art. 5 - I principi da rispettare (tutto nasce da qui)

I dati personali sono:

- a) **Trattati in modo lecito, corretto e trasparente** nei confronti dell'interessato (principio di «liceità, correttezza e trasparenza»);
- b) **Raccolti per finalità determinate, esplicite e legittime** e successivamente trattati in un modo non incompatibile con quelle finalità (principio di «limitazione della finalità»);
- c) **Adeguati, pertinenti e limitati** alla finalità per la quale sono trattati (principio di «limitazione della finalità»);
- d) **Esatti**: devono essere esatti e non devono essere dati inesatti (principio di «accuratezza»);
- e) **conservati in un formato che consenta l'accesso, la consultazione e l'uso** per il tempo necessario alla finalità per la quale sono trattati (principio di «limitazione della conservazione»);
- f) **trattati in maniera da garantire un'adeguata sicurezza dei dati personali**, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali (principio di «integrità e riservatezza»).

.... ADEGUATA SICUREZZA....

impone l'adozione di misure di sicurezza tecniche ed informatiche a protezione dei dati

Art. 5 e C.74 : introduzione Accountability nel RGPD

Il regolamento pone con particolare enfasi l'accento sulla **responsabilizzazione** (*accountability* - "dover rendere conto del proprio operato") del titolare e dei responsabili del trattamento.

Sintesi dell'art.5 e del Considerando 74:

Il Titolare del trattamento è il soggetto competente a garantire (e comprovare) il rispetto dei principi posti dalla disciplina in tema di trattamento dei dati personali:

- liceità,
- correttezza e trasparenza,
- limitazione delle finalità,
- minimizzazione,
- esattezza,
- limitazione della conservazione,
- integrità,
- riservatezza.

Accountability: uno dei principi base del RGPD

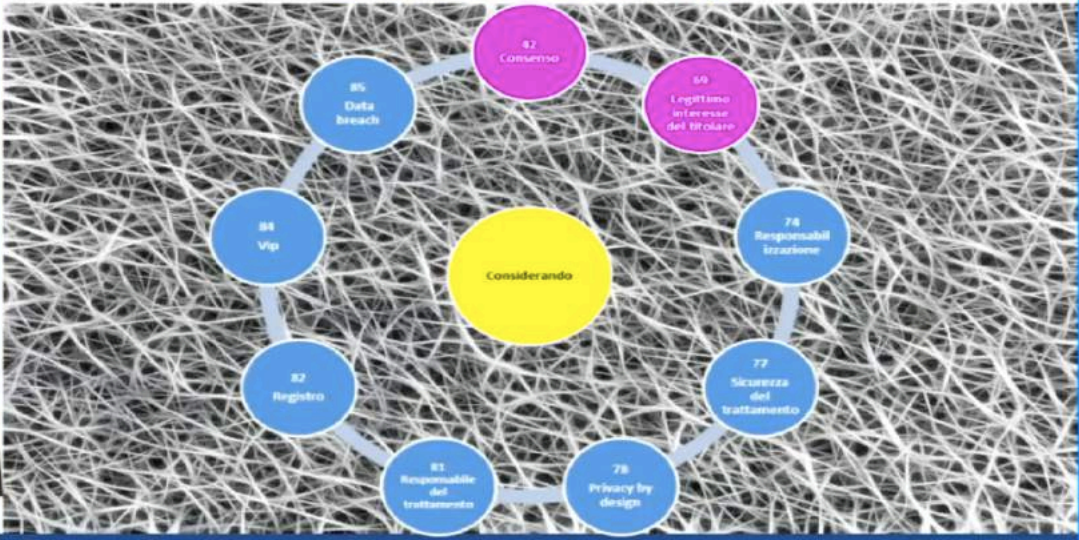
Approccio del tutto nuovo che **demanda ai titolari il compito di decidere autonomamente le modalità e i limiti del trattamento dei dati** alla luce dei criteri specifici indicati nel Regolamento.

Regolamento UE. Il Garante privacy incontra la Pa (Bari, 15/01/18) - 3) ACCOUNTABILITY: F. MODAFFERI

Il nuovo regolamento UE in materia di protezione dei dati personali
Sviluppi e impatti per i soggetti pubblici

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

La trama dell'accountability



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

Francesco Modafferi
Dirigente del Dipartimento
Libertà pubbliche e sanità

Francesco Modafferi

24:31 / 44:51

fonte slide:
Garante
incontra le PA –
Bari 15/01/2018

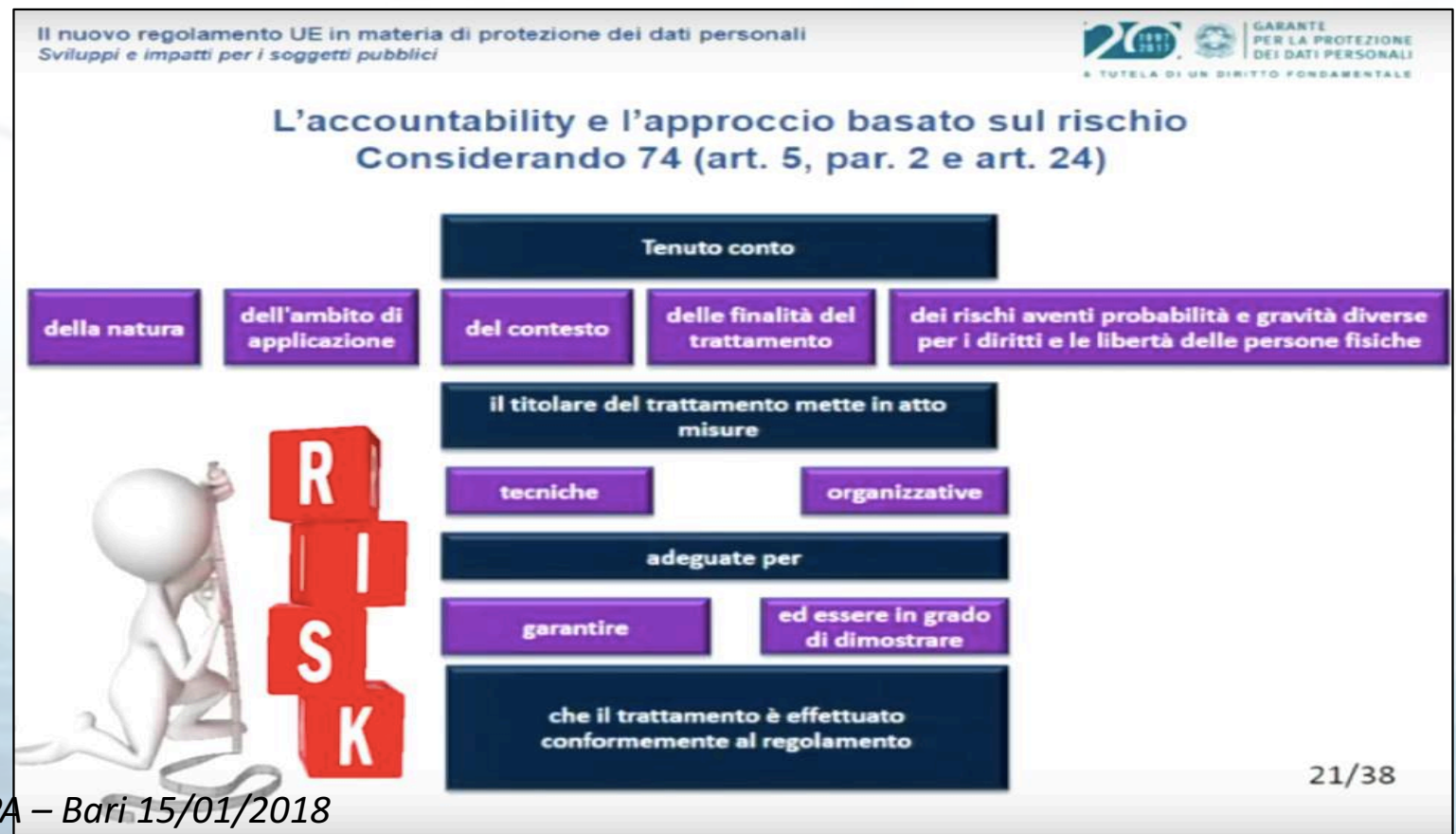
Accountability -> misure a discrezione del Titolare

Onere di porre in essere una serie di adempimenti che rendano i **principi posti dal GDPR verificabili nei fatti e non più soltanto obblighi giuridici esistenti sulla carta.**

Sulla base di quali:

- parametri di riferimento?
- regole?
- certificazioni?
- codici di condotta?

NULLA di ben definito



Accountability: uno dei principi base del RGPD

Disegno del regolamento ancora incompiuto: mancano ancora pezzi fondamentali che si definiranno nel prossimo periodo.

Il RGPD incoraggia gli stati membri a:

- definire Codici condotta. Art. 40
- definirne i monitoraggi. Art. 41
- definire Certificazioni: Art. 42
- definire organismi di certif.: Art. 43

Si attende tutto ciò, oltre che linee guida del (futuro) Comitato



COSA EVITARE? il Data Breach (art. 33, C85, C87, C88)



Per Data Breach si intende la violazione degli standard di sicurezza adottati per la protezione dei dati personali che può comportare “accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l’accesso ai dati personali trasmessi, memorizzati o comunque trattati”.

Violazione dei dati personali → necessaria la comunicazione all’autorità di vigilanza:

Nel caso di Data Breach, i Titolari del trattamento sono tenuti a informare adeguatamente le autorità di controllo “senza indebito ritardo e, ove possibile, **entro e non oltre 72 ore dopo esserne venuti a conoscenza**”. Qualora la notifica non venga effettuata entro tale termine, si rende necessario fornire una “giustificazione motivata” per tale ritardo.

Data Breach (art. 33, C85, C87, C88)

- Accesso non autorizzato a risorse informatiche
- Cancellazione totale o parziale di archivi
- Furto di identità
- Diffusione volontaria o involontaria di dati sensibili
- Accesso a siti web non consentiti
- Alterazione di database
- Intrusione fisica in strutture ad accesso riservato
- Installazione di software potenzialmente dannosi
- Utilizzo di risorse aziendali per cyber attacchi a sistemi di terzi
- Violazione di copyright
- Denial of service

→ Attenzione alle linee guida emanate dall'AGID (circolare 2/2017)



Le sanzioni con il RGPD – art. 83, C148, C150-C152

Il nuovo **sistema sanzionatorio** introdotto dal GDPR prevede **due fasce di sanzioni pecuniarie**:

1. fino a 10 milioni di Euro o fino al 2% del fatturato globale annuo dell'azienda, se superiore
2. fino a 20 milioni di Euro o fino al 4% del fatturato globale annuo dell'azienda, se superiore

Nel caso di violazioni di minore gravità è ammesso un ammonimento (art. 58), in luogo della sanzione pecuniaria.

Le sanzioni con il RGPD – art. 83, C148, C150-C152

Ogni autorità di controllo provvede affinché le sanzioni amministrative pecuniarie inflitte siano in ogni singolo caso **effettive, proporzionate e dissuasive**.

Al momento di infliggere una sanzione pecuniaria e di determinare l'ammontare della stessa, si tiene conto di vari elementi:

- la natura, la gravità e la durata della violazione, nonché il numero di interessati lesi dal danno e il livello del danno da essi subito;
- il carattere doloso o colposo della violazione;
- le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati;
- eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento;
- il grado di cooperazione con l'autorità² di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;



Le sanzioni con il RGPD – art. 83, C148, C150-C152

Sanzioni fino a 10 milioni di Euro o fino al 2% del fatturato globale annuo dell'azienda, se superiore si applicano per violazioni riguardanti:

- Consenso richiesto ai minori;
- Violazione dei principi di «privacy by design» e «privacy by default»;
- Violazione delle disposizioni sui Responsabili del trattamento;
- Violazioni sui registri delle attività di trattamento;
- Data breach;
- Valutazione di impatto sulla protezione dei dati;
- Violazioni sulla designazione, la valutazione e sui compiti del DPO.



Le sanzioni con il RGPD – art. 83, C148, C150-C152

Le Sanzioni fino a 20 milioni di Euro o fino al 4% del fatturato globale annuo dell'azienda, se superiore si applicano per violazioni riguardanti:

- Violazione dei principi applicabili al trattamento dei dati personali (liceità, correttezza, trasparenza, minimizzazione dei dati, esattezza dei dati, limitazione della conservazione, integrità e riservatezza dei dati;
- Informativa e Consenso;
- Violazioni relative a particolari tipologie di dati (sensibili – giudiziari);
- Diritto di accesso, di rettifica, diritto all'oblio, portabilità dei dati, diritto di opposizione;
- Profilazione degli interessati;
- Trasferimento di dati verso paesi terzi;



GDPR - General Data Protection Regulation

RGPD - Regolamento Generale sulla Protezione dei Dati

FIGURE E RUOLI DELLA NORMATIVA

Art. 4 - Figure e ruoli previsti dalla normativa

DEFINIZIONE ITALIANA	DEFINIZIONE INGLESE
Titolare del trattamento	Data controller
Interessato	Interessato
Addetto al trattamento	Data handler
Responsabile del trattamento	Data processor
Responsabile della protezione dei dati	Data Protection Officer (DPO)

Da normative precedenti ma non espressamente indicate dal GDPR

Amministratore di sistema / di rete / di database

Scompare l'incaricato del Trattamento

Il Titolare del trattamento (Data Controller)

La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.

quindi:

IL DIRIGENTE SCOLASTICO in co-titolarietà con il MIUR

L'Interessato al trattamento (Data subject)

L'interessato (*data subject*) al trattamento è la persona fisica a cui si riferiscono i dati personali, quindi «il proprietario» dei suoi dati

quindi: famiglie, alunni, dipendenti, personale esterno, ecc.

Diritti degli interessati

- Diritto di accesso ai dati (modulo predisposto dal Garante)
- Il titolare deve rispondere entro 1 mese dalla richiesta.
- Se i dati presentano degli errori o delle anomalie, l'interessato può esercitare il diritto alla rettifica.
- Diritto di rettifica (art. 16, C65)
- Diritto all'oblio (art. 17, C65 e C66 – no per esercizio pubblici poteri)
- Diritto di limitazione al trattamento (art.18, C67)
- Diritto alla portabilità dei dati (art.20, C68 – no per esercizio pubblici poteri)

L'Addetto al trattamento (Data handler)

L'addetto al trattamento è colui che tratta dati personali sotto l'autorità del Titolare.

quindi: DOCENTI – ATA – DSGA

E' obbligo del Titolare **istruire l'addetto al trattamento.**

Ad esempio, a scelta e senza nessuna priorità specifica:

- Consegna di manuali,
- Formazione in e-learning;
- Formazione in aula;
- Eccetera.

Il Responsabile del Trattamento (Data Processor)

La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

Responsabile interno o esterno?

Il ruolo del responsabile del trattamento di cui al regolamento europeo è chiaramente riservato ad un soggetto esterno all'azienda, con riferimento ai fornitori di servizi (anche evidenziato con parere 1/2010 del Gruppo Articolo 29).

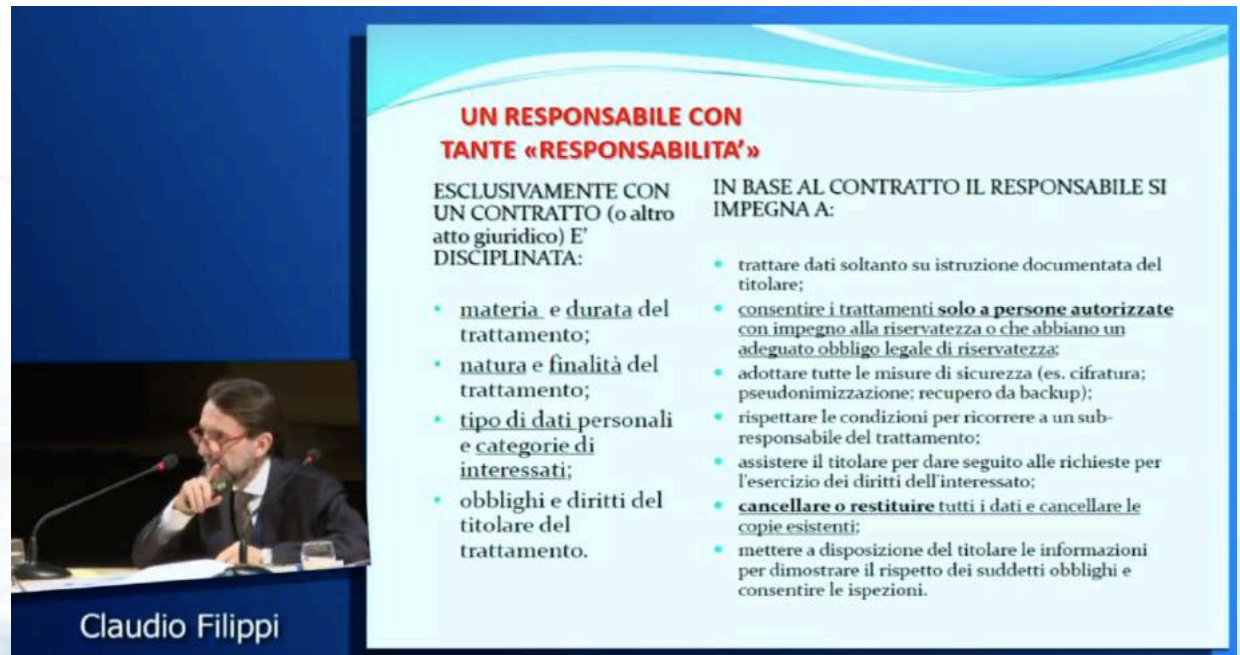
Quindi:

- **Società per registro informatico / segreterie digitali**
- **Azienda di assicurazioni**
- **Tecnici/aziende di consulenza per amministrazione di sistema**
- **Azienda di Web Host (sito internet) e consulenti**
- **Formatori / professionisti esterni**
- **eccetera**

Designazione responsabile del trattamento (art.28)

Obbligo di **predisporre un contratto** per la designazione delle responsabilità a carico del Responsabile del Trattamento

- Titolare sempre responsabile delle attività dei RdT.
- Normati i Sub-Responsabili (responsabilità sempre “a salire” sui Responsabili)



UN RESPONSABILE CON TANTE «RESPONSABILITA'»

<p>ESCLUSIVAMENTE CON UN CONTRATTO (o altro atto giuridico) E' DISCIPLINATA:</p> <ul style="list-style-type: none"> • <u>materia e durata</u> del trattamento; • <u>natura e finalità</u> del trattamento; • <u>tipo di dati personali e categorie di interessati</u>; • <u>obblighi e diritti</u> del titolare del trattamento. 	<p>IN BASE AL CONTRATTO IL RESPONSABILE SI IMPEGNA A:</p> <ul style="list-style-type: none"> • trattare dati soltanto su istruzione documentata del titolare; • consentire i trattamenti solo a persone autorizzate con impegno alla riservatezza o che abbiano un adeguato obbligo legale di riservatezza; • adottare tutte le misure di sicurezza (es. cifratura; pseudonimizzazione; recupero da backup); • rispettare le condizioni per ricorrere a un sub-responsabile del trattamento; • assistere il titolare per dare seguito alle richieste per l'esercizio dei diritti dell'interessato; • cancellare o restituire tutti i dati e cancellare le copie esistenti; • mettere a disposizione del titolare le informazioni per dimostrare il rispetto dei suddetti obblighi e consentire le ispezioni.
--	---

Claudio Filippi

fonte slide: Garante incontra le PA – Bari 15/01/2018

Obblighi del Responsabile del Trattamento

- Trasparenza (mettere a disposizione del titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi)
- Garantire la sicurezza e riservatezza dei dati (adottare criteri privacy-by-default e privacy-by-design nonché le misure di sicurezza di cui all'art.32)
- Vincolare i dipendenti,
- Informare il titolare delle violazioni avvenute,
- Occuparsi della cancellazione dei dati alla fine del trattamento
- Tenere il registro dei trattamenti (art.30)

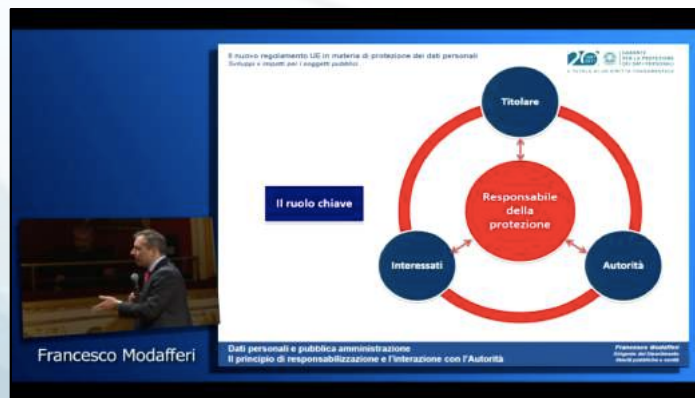


Art. 37 - Responsabile della Protezione dei Dati (RPD / DPO)

Per il Titolare: un referente e un facilitatore in materia di protezione dei dati

Per gli interessati: un punto di contatto con il titolare

Per l'ente Garante: il punto di contatto con il Titolare in caso di incidenti.



- Artt. 37-38-39 RGPD
- Considerando 97 RGPD
- WP 243 rev. 01 (linee guida sui responsabili della protezione dei dati) del "GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI"

fonte slide: Garante incontra le PA – Bari 15/01/2018

Il video, pubblicato su YouTube, mostra una presentazione del ruolo strategico del Responsabile della Protezione dei Dati (RPD) nel nuovo sistema di governance dei dati. La slide principale, intitolata "Il RPD: un ruolo strategico ...", presenta il RPD come la "Figura chiave nel nuovo sistema di governance dei dati". Al centro della slide c'è un'illustrazione di un personaggio con un cappello da laurea che siede su una pila di libri. Da questo personaggio partono linee che lo collegano a quattro ovali blu: "Titolare", "Personale che tratta dati", "Interessati" e "Autorità di controllo". In basso a sinistra, un video in anteprima mostra Anna Carla Meloni. Sotto il video, il titolo è "Regolamento UE. Il Garante privacy incontra la Pa (Bari, 15/01/18) - 6) RPD: C. MELONI".

Art. 37 - Responsabile della Protezione dei Dati (RPD / DPO)



L'RPD (anche chiamato DPO) è un professionista o una società di consulenza con conoscenze specialistiche della normativa, dell'organizzazione del Titolare e delle tecnologie informatiche e di sicurezza adottate o adottabili dallo stesso.

linee guida sui responsabili della protezione dei dati:

WP 243 rev. 01 del "GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI"

Deve essere designato obbligatoriamente dal titolare nei seguenti casi:

- **Quando il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico** (ad eccezione delle autorità giurisdizionali nell'esercizio delle loro funzioni);
- Quando i trattamenti consistono e richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
- Quando il trattamento riguarda, su larga scala, dati sensibili o giudiziari.



Designazione RPD (DPO)

L'RPD (DPO) può essere selezionato tra i dipendenti del titolare del trattamento oppure può essere un soggetto esterno e autonomo, ingaggiato in base a un contratto di servizi.



fonte slide: Garante incontra le PA – Bari 15/01/2018

In ogni caso, i suoi dati di contatto devono essere pubblicati e resi noti agli interessati oltre ad essere comunicati all'autorità di controllo competente.



Art. 39 – Compiti minimi del RPD (DPO)

- a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
- b) sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
- c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;
- d) cooperare con l'autorità di controllo;
- e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.



L'amministratore di sistema – la storia

- Disciplina di protezione dei dati (pre 2003): *“soggetto al quale è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di banca dati e di consentirne l'utilizzazione”*(art. 1, comma 1, lett. c) d.P.R. 318/1999)
- DLgs 196/2003: scompare il riferimento
- Provvedimenti formali (Novembre 2008 e Giugno 2009) del Garante della Privacy: viene nuovamente introdotta, assieme ad una puntuale indicazione di ruoli e professionalità
- GDPR: manca una espressa enunciazione di tale figura, lasciando completa carta bianca al Titolare nell'organizzazione tecnica del proprio Istituto (**accountability**).

CHE FARE A SCUOLA?

Interpretazione più diffusa:

il provvedimento del Garante del 2009 non è in contrasto con il GDPR

→ AMMINISTRATORE SI

L'amministratore di sistema – un po' di chiarezza

La figura professionale dell'amministratore di sistema è suddivisa in vari profili specifici, (normativa UNI-11506 – UNI-11621-2).

- **System Administrator** (*quello della vecchia accezione "Amministratore di Sistema"*).
Opera su: hardware, sistemi operativi come Windows o Linux, sistemi di gestione credenziali e diritti di accesso a risorse, applicativi specifici.
Svolge: azioni di installazione, configurazione, monitoraggio e risoluzione di interruzioni del funzionamento e di problemi (ossia le cause dei malfunzionamenti).
- **DBA (DataBase Administrator)** (*ruolo sempre più scollegato dalla vecchia accezione*)
Opera su: DBMS, ossia i sistemi di gestione dei dati e degli insiemi di dati.
Svolge: ottimizza il funzionamento e garantisce le prestazioni ottimali dei database, risolve problematiche ed errori che si possono verificare sui dati stessi durante le normali operazioni; realizza strumenti di reportistica o integrazione fra basi dati diverse;

L'amministratore di sistema – un po' di chiarezza

La figura professionale dell'amministratore di sistema" è suddivisa in vari profili specifici, (normativa UNI-11506 – UNI-11621-2).

- **Network Administrator** *(ruolo sempre più scollegato dalla vecchia accezione)*
Opera su: strumenti di rete, dai firewall, router agli switch.
Svolge: garantisce la separazione dei domini di rete interni (direzione/aree rete server/reti WiFi), applica le politiche di autenticazione all'accesso ad Internet, ottimizza il funzionamento e garantisce le prestazioni ottimali della navigazione e dell'accesso ad Internet, stabilisce gli accordi con i fornitori di connettività dati/fonia, è responsabile dei firewall e gestisce – in ultima istanza - anche i sistemi di cavi .

L'amministratore di sistema – un po' di chiarezza

E a scuola?

- **System Administrator:** l'azienda (o il professionista) che gestisce e fornisce assistenza su PC / server / cartelle condivise / backup / NAS.
- **DBA (DataBase Administrator) :** Argo / Axios / Spaggiari / eccetera
- **Network Administrator:** l'azienda (o il professionista) che gestisce e fornisce assistenza su navigazione in rete, autenticazione alla rete e firewall.

NOTA: spesso la NetSense, in seno al servizio NetSecurity, prende l'incarico di Network Administrator (Amministratore di Rete).

Art. 38 – Posizione del RPD (DPO) e incompatibilità

Il lavoro dell'RPD (DPO) deve svolgersi in **assoluta autonomia e indipendenza**: nessuno può dargli alcuna istruzione circa l'esecuzione dei suoi compiti.

NON può svolgere altre mansioni o compiti in conflitto di interessi con il Titolare.

e a scuola?

Tipicamente incompatibili DPO - System Administrator e Database Administrator (le attività di questi ultimi dipendono molto dalle scelte organizzative del Titolare e interessano una gran mole di dati personali).

DPO compatibile con Network Administrator (l'attività dell'amministratore di rete è indipendente dalle scelte organizzative del Titolare, non tratta quasi mai dati personali e i tracciati di servizio non sono mai cedibili al Titolare ma solo alle Autorità giudiziali).

GDPR - General Data Protection Regulation

RGPD - Regolamento Generale sulla Protezione dei Dati

MISURE GENERALI INDICATE DAL REGOLAMENTO

consenso, informative, registro, DPIA, misure di sicurezza

PRIMA DI TUTTO : BASE GIURIDICA

prima ancora di come e a quali condizioni

Quale **base giuridica** rende lecito il trattamento?

CONSENSO SI O CONSENSO NO? E IN QUALI CASI?



Art. 5 – Base giuridica (principio di leicità)

Il trattamento è lecito solo se ricorre almeno una delle seguenti condizioni (C40):

- a. **l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità (C42 e C43);**
- b. **il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso (C44);**
- c. **il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento (C45);**
- d. **il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica (C46);**
- e. **il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento (C45 e C46);**
- f. **il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore. (C47–C50)**



Lettera f non per autorità pubbliche nell'esercizio delle loro funzioni.

Base giuridica – in sintesi a scuola consenso o no?

Il Dirigente può trattare i dati senza consenso:

- quando il trattamento interessa l'esecuzione di un contratto di cui l'interessato è parte (fornitori, esperti esterni, eccetera)
- per tutte le attività che è obbligato per legge ad effettuare,
- quando il trattamento è necessario alle finalità istituzionali (es. attività entro PTOF).

Per il tutti gli altri trattamenti : NECESSARIO CONSENSO

Esempio:

- Trattamento foto / video
- Trasmissione dati per scopo di inserimento in scuole di ordine superiore
- Attività di allocazione post-diploma
- Attività progettuali non riportate nel PTOF

Consensi acquisiti con la “vecchia” 196/2003

Acquisire nuovamente se:

- Il modello utilizzato per la raccolta **non rispetta il requisito di inequivocabilità** e quindi potrebbero esserci delle incertezze sul fatto che l'interessato abbia acconsentito al trattamento dei suoi dati;
- Il titolare del trattamento **ha considerato come consenso il silenzio o l'inattività dell'interessato**, oppure abbia adottato la preselezione delle caselle, oppure ancora il consenso sia richiesto solamente per una delle diverse finalità del trattamento dei dati;
- La formula del consenso **non è chiaramente distinguibile**, non essendo contenuta in una clausola specifica separata dalle altre clausole del contratto o da altri contenuti;
- La formula del consenso non è evidente e infatti **mancano degli elementi, di contenuto o di forma**, che permettano di capire immediatamente che in quel punto si stia parlando del diritto di acconsentire o meno;
- La formula del consenso **non utilizza un linguaggio semplice e chiaro** e quindi non è comprensibile da parte di qualunque interessato;
- Non è espresso che **il consenso possa essere revocato in modo incondizionato** né sono indicate le modalità in cui tale revoca possa avvenire (che devono essere semplici come la stessa manifestazione del consenso);
- **Non sono indicate l'identità** del titolare del trattamento dei dati **e le finalità** del trattamento.



Consenso dei minori nella società dell'informazione

Per quanto riguarda l'offerta diretta di servizi della società dell'informazione ai minori, il trattamento di dati personali del minore è lecito ove il minore abbia almeno 16 anni. Ove il minore abbia un'età inferiore ai 16 anni, tale trattamento è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale. Gli Stati membri possono stabilire per legge un'età inferiore a tali fini purché non inferiore ai 13 anni.

Il titolare del trattamento si adopera in ogni modo ragionevole per verificare in tali casi che il consenso sia prestato o autorizzato dal titolare della responsabilità genitoriale sul minore, in considerazione delle tecnologie disponibili.

L'informativa sulla privacy con il RGPD

L'interessato va informato riguardo tutti i trattamenti dei suoi dati.

Artt. 13 e 14 del RGPD.

Cambia l'informativa. Non più lunga, piena di parole legali o troppo tecniche che l'utente medio non è in grado di comprendere.

L'informativa deve avere **forma concisa, deve essere chiara, facilmente accessibile ed intellegibile** (anche da minori).

Il RGPD indica i **contenuti minimi e le modalità**.

STUDENTI E FAMIGLIE INFORMATE

Tutte le scuole – sia quelle pubbliche, sia quelle private – hanno l'obbligo di far conoscere agli "interessati" (studenti, famiglie, professori, etc.) come vengono trattati i loro dati personali. Devono cioè rendere noto, attraverso un'adeguata informativa, quali dati raccolgono, come li utilizzano e a quale fine.



TRATTAMENTO DEI DATI NELLE ISTITUZIONI SCOLASTICHE PUBBLICHE

Le istituzioni scolastiche pubbliche possono trattare solamente i dati personali necessari al perseguimento di specifiche finalità istituzionali oppure quelli espressamente previsti dalla normativa di settore. Per tali trattamenti, non sono tenute a chiedere il consenso degli studenti. Alcune categorie di dati personali degli studenti e delle famiglie – come quelli sensibili e giudiziari – devono essere trattate con estrema cautela, nel rispetto di specifiche norme di legge, verificando prima non solo la pertinenza e completezza dei dati, ma anche la loro indispensabilità rispetto alle "finalità di rilevante interesse pubblico" che si intendono perseguire.

L'informativa sulla privacy con il RGPD

L'informativa ai sensi dell'art. 13 del GDPR deve contenere i seguenti elementi:

1. l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
2. i dati di contatto del responsabile della protezione dei dati (DPO), se nominato;
3. le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
4. qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
5. gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
6. ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo;
7. il periodo di conservazione dei dati personali;
8. i diritti che competono all'interessato;
9. il diritto di proporre reclamo a un'autorità di controllo;
10. se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
11. l'esistenza di un processo decisionale automatizzato, compresa la profilazione.



L'informativa sulla privacy con il RGPD

L'informativa ai sensi dell'art. 14 del GDPR deve contenere i seguenti elementi, in aggiunta a quelli previsti dall'art. 13:

1. la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico;

L'informativa deve essere data all'interessato entro un termine ragionevole dall'ottenimento dei dati personali, ma **al più tardi entro un mese**



Il registro dei trattamenti – Art. 30 , C82

Il registro dei trattamenti, è uno strumento indispensabile per ogni valutazione e analisi del rischio (principio di accountability).

L'onere della tenuta del registro è a carico del titolare e dei responsabili del trattamento. Il registro deve essere tenuto in forma scritta, anche in formato elettronico e deve essere esibito su richiesta al Garante.

Nel registro devono essere indicati una lista di contenuti obbligatori elencati in art.30.

Il paragrafo 2 dell'articolo 30 del GDPR prevede che anche i responsabili del trattamento debbano tenere un registro simile in relazione alle attività svolte per conto del titolare.

Ci sono cause di esenzione ma numerosi pareri indicano l'opportunità di mantenere il registro in OGNI CASO per dimostrare la propria “accountability”.

Il Registro dei trattamenti Art. 30

Il titolare del trattamento deve dimostrare di aver concretamente adottato le misure finalizzate ad assicurare l'applicazione del GDPR.

Il registro dei trattamenti, quindi, è uno **strumento indispensabile per ogni valutazione e analisi del rischio** (principio di accountability).

Il registro deve essere tenuto in forma scritta, anche in formato elettronico e deve essere esibito su richiesta al Garante. Nel registro devono essere indicati una lista di contenuti obbligatori:

- il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
- le finalità del trattamento;
- una descrizione delle categorie di interessati e delle categorie di dati personali;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
- Gli eventuali trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale;
- I termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- Una descrizione generale delle misure di sicurezza tecniche e organizzative.



Il Registro dei trattamenti Art. 30

La tenuta del registro dei trattamenti è obbligatoria per tutti gli organismi con più di 250 dipendenti, ma anche per coloro che effettuano trattamenti che possano presentare “un rischio per i diritti e le libertà dell’interessato, o il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all’articolo 9, paragrafo 1 (dati personali che rivelino l’origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l’appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all’orientamento sessuale della persona) o i dati personali relativi a condanne penali e a reati.

Anche se non si rientra tra i soggetti obbligati, è comunque preferibile adottare ugualmente un registro dei trattamenti



La valutazione di impatto (DPIA)

Art. 35 , C84, C89-C93, C95

La DPIA è una procedura prevista dall'articolo 35 del GDPR che mira a **descrivere un trattamento di dati** per valutarne la necessità e la proporzionalità nonché i relativi rischi, allo scopo di approntare misure idonee ad affrontarli.

Una DPIA può riguardare un singolo trattamento oppure più trattamenti che presentano analogie in termini di natura, ambito, contesto, finalità e rischi.

In generale la DPIA riguarda il trattamento di dati ad alto rischio o trattati con strumenti tecnologici avanzati.

La valutazione di impatto (DPIA)

Quando fare la DPIA?

La DPIA deve essere condotta **prima** di procedere al trattamento. Dovrebbe comunque essere previsto un **riesame continuo della DPIA, ripetendo la valutazione a intervalli regolari.**

Chi deve fare la DPIA?

La **responsabilità della DPIA spetta al titolare, anche se la conduzione materiale** della valutazione di impatto può essere affidata a un altro soggetto, interno o esterno all'organizzazione. Il titolare **ne monitora lo svolgimento consultandosi** con il **responsabile della protezione dei dati (DPO) e acquisendo** - se i trattamenti lo richiedono - il parere di esperti di settore, del **responsabile della sicurezza dei sistemi informativi e del responsabile IT.**

DPIA – casi di obbligatorietà



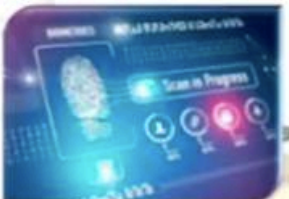
fonte: Garante incontra le PA – Bari 15/01/2018

DPIA – casi di obligatorietà

Il nuovo regolamento UE in materia di protezione dei dati personali
Sviluppi e impatti per i soggetti pubblici

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

art. 35, comma 3. ... casi espressi DPIA **obbligatoria**
trattamenti su larga scala di particolari categorie di dati

		
DATI GENETICI	CONVINZIONI RELIGIOSE(o filosofiche)	OPINIONI POLITICHE
		
DATI SULLA SALUTE	ORIGINE RAZZIALE O ETNICA	APPARTENENZA SINDACALE
		
DATI BIOMETRICI	VITA O ORIENTAMENTO SESSUALE	CONDANNE PENALI E REATI

fonte: Garante incontra le PA – Bari 15/01/2018

DPIA – casi di obbligatorietà

Il nuovo regolamento UE in materia di protezione dei dati personali
Sviluppi e impatti per i soggetti pubblici

20
GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI
A TUTELA DI UN DIRITTO FONDAMENTALE

art. 35, comma 3. ... casi espressi DPIA **obbligatoria**



fonte: Garante incontra le PA – Bari 15/01/2018

DPIA – casi di obligatorietà

Il nuovo regolamento UE in materia di protezione dei dati personali
Sviluppi e impatti per i soggetti pubblici

2019
GARANTE PER LA PROTEZIONE DEI DATI PERSONALI
A TUTELA DI UN DIRITTO FONDAMENTALE

ALTRI CASI DI DPIA OBBLIGATORIA

principio di carattere generale
RISCHIO ELEVATO

PIÙ CHE CRITERI SONO DEGLI INDICI O INDIZI

1. Trattamenti valutativi o di scoring
2. Decisioni automatizzate che producono significativi effetti giuridici o di analoga natura
3. Monitoraggio sistematico
4. Dati sensibili o dati di natura estremamente personale
5. Trattamenti di dati su larga scala
6. Combinazione o raffronto di insiemi di dati
7. Dati relativi a interessati vulnerabili
8. Utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative
9. Trattamenti che, di per sé, "impediscono [agli interessati] di esercitare un diritto o di avvalersi di un servizio o di un contratto"



WP248 del Gruppo Articolo 29
9 criteri.

Obbligatorietà: almeno 2

Si attendono indicazioni
specifiche da Garante
nazionale e dal legislatore

fonte: Garante incontra le PA – Bari 15/01/2018

Misure di Sicurezza del trattamento – Art. 32 , C83

L'art. 32 deputato alla messa in atto di misure tecniche ed organizzative.

Il Regolamento europeo non parla neanche di misure tecniche minime, ma si esprime solamente in **termini di adeguatezza**.

Elenco esemplificativo e non esaustivo di misure tecniche ed organizzative di sicurezza:

- a) la pseudonimizzazione e la cifratura dei dati personali;*
- b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;*
- c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;*
- d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento”.*

Sicurezza del trattamento – Art. 32 , C83

Non esiste una lista puntuale come quella dell'allegato B del vecchio Codice Privacy.

Ciò in linea con il **principio dell'accountability** su cui si basa l'intero RGPD:
Titolare e responsabile del trattamento devono responsabilizzarsi e mettere in atto misure di sicurezza adeguate alla loro realtà aziendale.

Art. 25 - Privacy by design e privacy by default

privacy by design:

La privacy come elemento **di progettazione delle misure tecniche ed organizzative** (*privacy by design*), anche prima che il trattamento inizi.

Chiaramente si dovrà tenere conto anche del tipo di dati trattati.

privacy by default:

Per impostazione predefinita i Titolari dovrebbero trattare solo i dati personali nella misura necessaria e sufficiente per le finalità previste e per il periodo strettamente necessario a tali fini. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

Nota: eventuali (future) certificazioni saranno comprovanti della conformità a tali principi.



GDPR - General Data Protection Regulation

RGPD - Regolamento Generale sulla Protezione dei Dati

POSSIBILI MISURE DI CARATTERE GENERALE PER LA SCUOLA

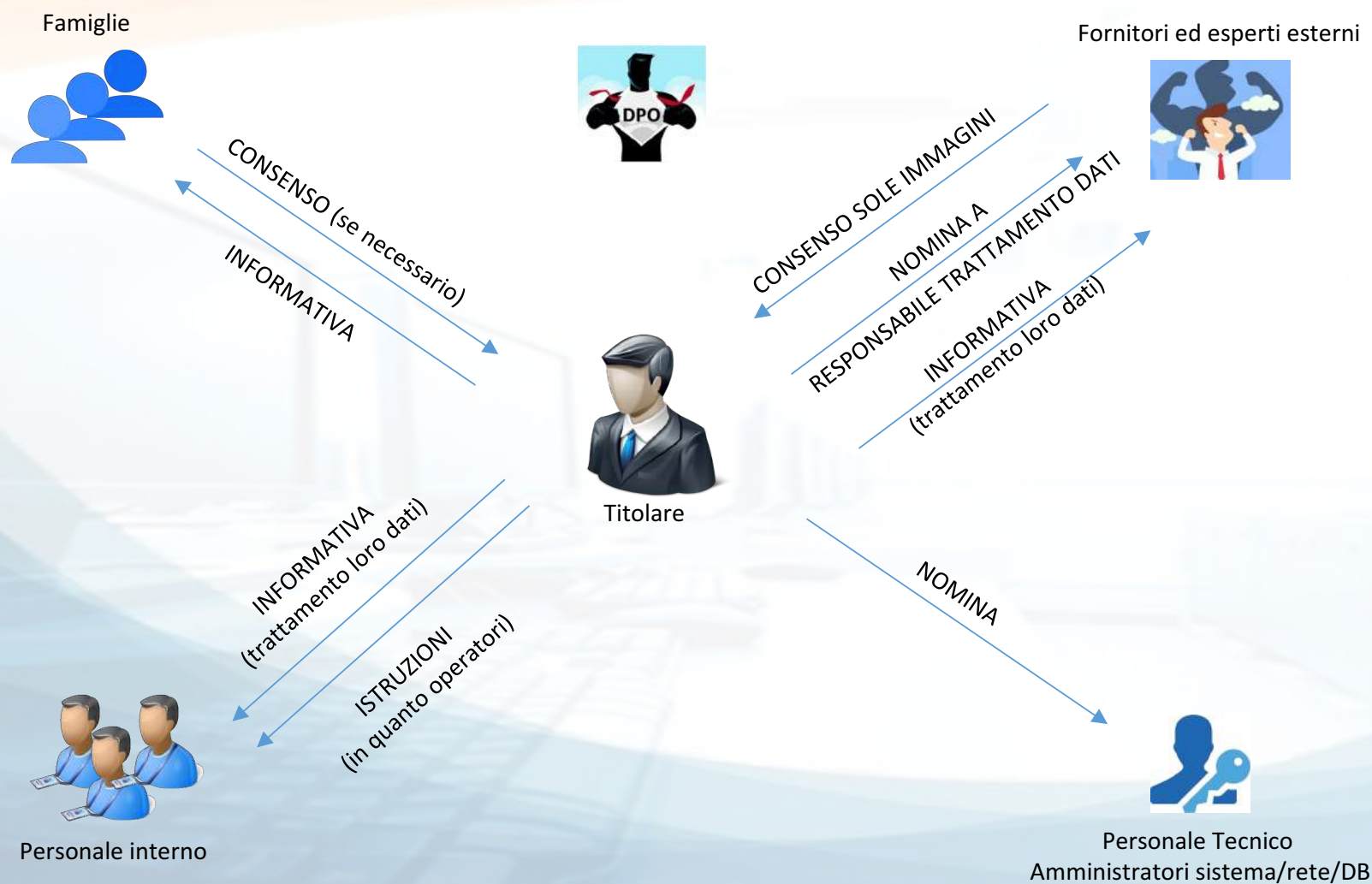
MISURE DA ADOTTARE

- A) MISURE AMMINISTRATIVE
- B) MISURE DI CAUTELA (FOTO / PASSWORD / DOCUMENTI)
- C) MISURE TECNICHE – RETE DATI
- D) MISURE TECNICHE – PC AULE E LABORATORI
- E) MISURE TECNICHE – PC E SISTEMI SEGRETERIA



niente paura ...

SINTESI



MISURE AMMINISTRATIVE DA ADOTTARE

A) MISURE AMMINISTRATIVE

1. Mantenere il sito aggiornato con modulistica, informative, istruzioni e dati DPO
2. FAMIGLIE
 - iscrizione: modulo consensi per il trattamento generico a tutte le famiglie
(*modulo all'ultima pagina informativa famiglia area pubblica*)
 - in itinere: consensi relativi a trattamenti specifici
3. DIPENDENTI (ANCHE SUPPLENTI BREVI):
 - Modulo di ricevuta istruzioni
(*modulo all'ultima pagina informativa docenti area pubblica*)
 - Se si fanno foto: richiesta consenso
4. FORNITORI (solo quelli che trattano dati per conto del titolare):
 - nomina a Responsabile del Trattamento (usare fac-simile area modulistica)
 - Se si fanno foto: richiesta consenso

Consiglio: In segreteria “didattica” mantenere una copia dell’informativa ai genitori.
Al “personale” mantenere una copia dell’informativa ai dipendenti e delle istruzioni

MISURE DI CAUTELA : FOTO / VIDEO

Realizzarli senza primi piani (foto di gruppo) oppure sfumate / oscurate



MISURE DI CAUTELA : FOTO / VIDEO (caso genitori)

NOTA PRIVACY

LINEE GUIDA DEL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

LE FOTO ED I VIDEO RIPRESI DURANTE LE RECITE ED ALTRE INIZIATIVE SCOLASTICHE POSSONO ESSERE UTILIZZATI SOLO PER FINI PERSONALI E DESTINATI AD UN AMBITO FAMILIARE O AMICALE.

LA DIFFUSIONE DI TALI FOTO E VIDEO ATTRAVERSO CANALI SOCIALI (FACEBOOK / ECC.), WEB O QUALSIASI ALTRO MEZZO DI COMUNICAZIONE VIOLA LE NORMATIVE VIGENTI IN MATERIA.

MISURE CAUTELA : PASSWORD

CHIARO RIFERIMENTO: (Gestionali e Registro Elettronico)

Perché rispettare le prescrizioni del Codice nella scelta delle password?

Se qualcuno accede ad un computer o ad un servizio WEB potrà impossessarsi di dati personali e aziendali.

La responsabilità di questa sottrazione ricadrà sull'addetto al trattamento, se il dispositivo non era protetto da password, o se la password era troppo debole.

Il 90% dei furti di identità sono riconducibili ad un uso non responsabile delle password

La password

Suggerimenti per creare una password sicura (tratto dal sito della polizia postale):

- Creare una password di minimo dieci caratteri, contenente almeno una maiuscola, almeno una minuscola, almeno un numero e almeno un carattere speciale tra quelli elencati: ! \$? # = * + - . , ; :
 - Includere caratteri dall'apparenza simili in sostituzione di altri caratteri (ad esempio il numero "0" per la lettera "O" o il carattere "\$" per la lettera "S").
 - Creare un acronimo univoco (ad esempio "PDRM" per "Piazza Delle Repubbliche Marinare").
- Includere sostituzioni fonetiche o grafiche (ad esempio "6 arrivato" per "Sei arrivato" o "Arrivo + tardi" per "Arrivo più tardi").

Da evitare:

- Non utilizzare le stesse password per più account.
- Non usare una password già utilizzata in un esempio di come si sceglie una buona password.
- Non utilizzare una password contenente dati personali (nome, data di nascita, ecc.).
- Non usare parole o acronimi che si possono trovare nel dizionario.
- Non usare sequenze di tasti sulla tastiera (asdf) o sequenze di numeri (1234).
- Non creare password di soli numeri, di sole lettere maiuscole o di sole lettere minuscole.
- Non usare ripetizioni di caratteri (aa11).

Suggerimenti per tenere al sicuro la password:

- Non comunicare a nessuno la password (inclusi partner, compagni di appartamento, colleghi, ecc.).
- Non lasciare la password scritta in posti facilmente raggiungibili da altri.
- Non inviare mai la password per email.
- Verificare periodicamente la password corrente e cambiarla con una nuova.



La password - Le linee guida del NIST

Password complesse?

Dalla ricerca del NIST è emerso che gli utenti, quando venivano costretti a scegliere dei simboli o dei numeri, si affidavano quasi sempre agli stessi: i più usati sono i numeri 1,2 e 3 e il punto esclamativo.

Gli hacker, conoscendo questa tendenza, sono spesso riusciti a rubare password, anche complesse.

CONSIGLIO: UTILIZZARE APP O SOFTWARE PORTACHIAVE



APP o Software portachiave

Sono software nei quali memorizzare tutte le proprie password.

- saranno crittografate
- accessibili solo da noi attraverso una masterpassword
- la masterpassword è protetta attraverso una “autenticazione a due vie”
- altro (in base al tipo di software scelto)
- **Consiglio: LastPass, sia Free che Premium (30 Euro /anno)**

FACEBOOK / ALTRI SOCIAL NETWORK

Facebook ricorda che utilizzando il social network l'utente accorda all'azienda di Zuckerberg *"licenza non esclusiva, trasferibile, che può essere concessa come sottolicensa, libera da royalty e valida in tutto il mondo, che consente l'utilizzo dei contenuti (...) pubblicati su Facebook o in connessione con Facebook"*.

In altre parole, **Facebook si dichiara libera di utilizzare le foto e gli altri contenuti conferiti dall'utente ovunque lo ritenga opportuno e senza versare un centesimo in termini di royalty**. I contenuti, foto comprese, restano quindi di proprietà dell'utente ma Facebook non dovrà versare alcun corrispettivo economico se vorrà riutilizzarle. Eventuali società con cui Facebook abbia stretto un accordo, potranno a loro volta - sulla base di un'apposita licenza - riutilizzare lo stesso materiale.

CONCLUSIONE : NO PUBBLICAZIONE FOTO SU SOCIAL NETWORK

solo informazioni o foto anonimizzate

POSSIBILI MISURE TECNICHE DA ADOTTARE – RETE DATI

B) MISURE TECNICHE – RETE DATI (rete WIFI, rete aule e laboratori e rete segreteria)

FIGURA COINVOLTA: AMMINISTRATORE DI RETE

- verificare la separazione fisica (o con VLAN) delle tre rete
- autorizzare l'uso della rete a personale autorizzato con l'uso di credenziali personali (user e password individuali!)
- mantenere tracciati di navigazione anonimi (quale PC dall'interno ha generato un certo traffico verso Internet)
- mantenere altri tracciati (DHCP, accessi in rete, ecc.)
- rispettare le indicazioni AGID (circolare 2/2017(su DPCM 01/08/2015 relativo a misure minime sicurezza ICT

Esigenza funzionale: su più linee Internet, implementare meccanismi di failover (spostare le varie reti sulle linee di uscita più performanti)

POSSIBILI MIS. TECNICHE DA ADOTTARE – PC AULE E LAB

C) MISURE TECNICHE – PC AULE E LABORATORI

FIGURA COINVOLTA: AMMINISTRATORE DI SISTEMA

Problema: spesso documenti riservati (es. relazioni attività con soggetti BES o password di registro informatico) vengono dimenticati nei PC ad uso “promiscuo”.

Problema2 : nelle scuole esiste normalmente un parco macchine esteso (tanti PC)

Soluzione che mette d'accordo esigenze tecniche (basso costo manutenzione) e GDPR:

- UTILIZZO SOFTWARE DI CONGELAMENTO DELLA CONFIGURAZIONE SU TUTTI I PC (reboot and restore RX / deep freeze / ecc.)

La password di congelamento e scongelamento: all'amministratore di sistema

POSSIBILI MIS. TECNICHE DA ADOTTARE – SEGRETERIA

D) MISURE TECNICHE – PC E SISTEMI SEGRETERIA

FIGURA COINVOLTA: AMMINISTRATORE DI SISTEMA

Obiettivo1: nessuno deve leggere dati da Hard Disk, anche sottratti dalla segreteria

Obiettivo2: nessun dato deve perdersi, anche a seguito di danno o furto

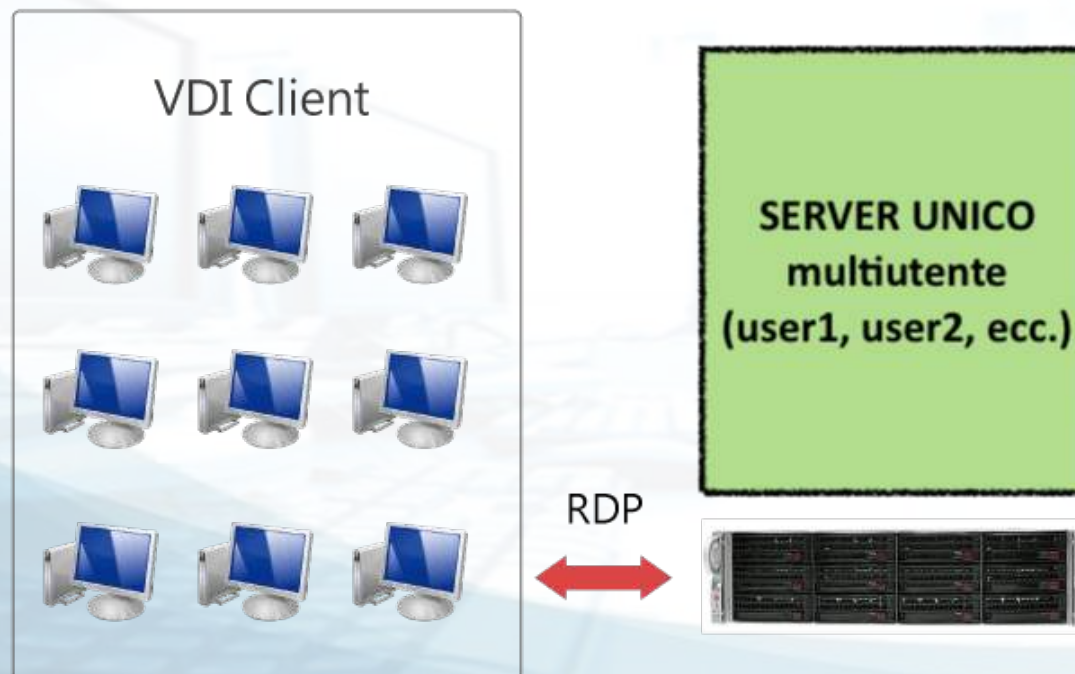
Soluzione 1 :

- UTILIZZO SOFTWARE FREE DI CRITTOGRAFIA PER GLI HARD DISK (BitLocker / File Vault)
- UTILIZZO DI SISTEMI FREE DI SINCRONIZZAZIONE DEI FILE PROPRI (owncloud / nextcloud) Attenzione: no dropbox, gdrive, eccetera.
- UTILIZZO DI SISTEMI DI BACKUP AUTOMATICI DELL'INTERO SISTEMA (ACRONIS ecc.)

POSSIBILI MIS. TECNICHE DA ADOTTARE – SEGRETERIA

Soluzione avanzata che mette d'accordo basso costo manutenzione e GDPR:

- segreteria in un'unica macchina server e postazioni di segretr. veri e propri terminali



Data Breach (art. 33, C85, C87, C88)

ATTENZIONE alle **chiavette USB** e agli **Hard Disk portatili**



L'enorme diffusione di questi dispositivi, nonché la loro praticità e semplicità di utilizzo può comportare problemi anche gravi ai dati aziendali contenuti.

Nella stragrande maggioranza dei casi, i dati contenuti in questi dispositivi non sono protetti. Lo smarrimento, quindi, dovrebbe portare alla notificazione di data breach al Garante sulla Privacy.

Una soluzione semplice e poco costosa potrebbe essere quella di usare dei software di crittografia sui dispositivi USB forniti dall'azienda.

I trattamento dei dati cartacei

ATTENZIONE alla carta riciclata!

ATTENZIONE alle stampe che si lasciano!

Se la stampante è condivisa con altri utenti o è fuori dal campo visivo evitare di lasciare le stampe per troppo tempo, perché degli utenti non autorizzati potrebbero visualizzarle o asportarle.

I trattamento dei dati cartacei

Per eliminare dati sensibili cartacei utilizzare il distruggi documenti.

Il livello di sicurezza di un distruggi documenti è dettato dalla norma DIN 66399:

Livello di sicurezza 1: Documenti di carattere generale devono essere invalidati o resi illeggibili.

Livello di sicurezza 2: Documenti interni che devono essere invalidati o resi illeggibili.

Livello di sicurezza 3: **Supporti dati con dati sensibili**, riservati e personali che richiedono una maggiore protezione.

Livello di sicurezza 4: Supporti dati con dati particolarmente sensibili e riservati nonché dati personali che richiedono una maggiore protezione.

Livello di sicurezza 5: Supporti dati con informazioni strettamente segrete di rilevanza per l'esistenza di una persona, azienda o istituzione.

Livello di sicurezza 6: Supporti dati con documenti strettamente segreti, quando è necessario.

Livello di sicurezza 7: Per dati strettamente segreti, per cui necessario adottare le misure di prevenzione di massima sicurezza.

Il GDPR e i servizi in CLOUD

SI CONOSCE QUALI SIANO LE MISURE DI SICUREZZA ADOTTATE DAL FORNITORE PER PROTEGGERE I DATI?

Il Titolare del trattamento **ha sempre l'obbligo di indicare le misure di sicurezza e verificare che siano rispettate dai propri fornitori**. Pertanto, è necessario chiedere dettagliate informazioni al fornitore del servizio su questo punto.

DOVE SI TROVANO FISICAMENTE I SERVER DOVE RISIEDONO I DATI?

In Italia: il trattamento dei dati non richiede nessun adempimento;

In un paese della Comunità Europea:

vale il trattato di Schengen, ribadito dal nuovo Regolamento Europeo, che permette la libera circolazione dei dati, ma si deve comunicare agli interessati che i loro dati usciranno dall'Italia;

Il GDPR e i servizi in CLOUD

In un paese extraeuropeo:

la soluzione è sconsigliata. Per scegliere questa soluzione è necessario che **siano assicurate dal fornitore misure di sicurezza pari o superiori a quelle che si avrebbero nei paesi europei.**

Per prima cosa bisogna vedere se il paese extraeuropeo è nella lista dei paesi considerati affidabili, quindi bisogna **verificare se vengono adottate le misure previste dalla Commissione Europea.**

Verificato che sia tutto in regola, **rimangono due ulteriori obblighi:**

1. comunicare agli interessati che i loro dati usciranno dai confini europei;
2. provvedere alla notifica al Garante.



Il GDPR e i servizi in CLOUD

È STATO VALUTATO L'IMPATTO AZIENDALE CHE SI AVREBBE SE I DATI SUL CLOUD ANDASSERO PERSI O DISTRUTTI?

I dati non sono da noi. Se il fornitore o uno della filiera fallisse? Se fosse attaccato da un pirata informatico? Se avesse dei problemi legati ad un evento fisico (terremoto, incendio, alluvione, ...). I dati delle aziende hanno un valore elevatissimo ed è meglio **predisporre adeguate misure di backup** con varie tipologie di frequenza (per maggiori garanzie temporali) e vari punti di stoccaggio (per delocalizzare sul territorio il rischio).

ESISTONO GARANZIE DI RISERVATEZZA PER I NOSTRI DATI NEL CASO IN CUI UN CONCORRENTE CONDIVIDA GLI STESSI SERVIZI CLOUD?

Chi offre un servizio alla mia azienda in cloud, offrirà lo stesso servizio anche ai miei concorrenti. **Quali sono le logiche a garanzia della sicurezza dei miei dati aziendali?** Chi e come gestisce i criteri di accesso e le politiche di password? Vi è possibilità di accedere facilmente alla mia password?



Il GDPR e i servizi in CLOUD

LA TECNOLOGIA UTILIZZATA DAL FORNITORE DI CLOUD È DI TIPO “PROPRIETARIO”? I DATI POSSONO ESSERE ESPORTATI FACILMENTE?

Nell'ipotesi in cui un giorno si voglia cambiare fornitore del servizio, i dati caricati fino a quel momento sono facilmente esportabili? Il fornitore garantisce il rispetto del diritto alla portabilità dei dati previsto dal GDPR?

NEL CASO IN CUI SI ACCERTI UNA VIOLAZIONE O LA PERDITA DEI DATI, IL FORNITORE GARANTISCE UN PRONTO RISARCIMENTO DEL DANNO?

Non è più un tema da sottovalutare. Con il nuovo GDPR, ogni violazione dei dati (data breach) deve essere segnalata al Garante e in alcuni casi anche agli interessati. Questo significa almeno due cose: la prima che **devo essere certo che il mio fornitore mi comunichi un data breach in tempi veloci e certi** per adempiere alle richieste del Garante, la seconda che **abbia la capacità economica o assicurativa di rispondere alle richieste di risarcimento.**



Ransomware cos'è?

Il ransomware è un programma informatico dannoso che infetta un dispositivo (PC, Tablet, Smartphone, Smart TV), bloccando l'accesso ai contenuti (foto, video, file) e chiedendo un riscatto (ransom) per «liberarli».

La richiesta di pagamento con le relative istruzioni è presentata in una finestra che appare automaticamente sullo schermo del dispositivo infettato.

L'utente ha pochi giorni per pagare, poi il blocco dei file diventa definitivo.

Ci sono 2 tipi principali di ransomware:

Cryptor: criptano i file contenuti nel dispositivo rendendoli illeggibili;

Blocker: bloccano l'accesso al dispositivo infettato.

Ransomware come si diffonde?

Il ransomware si diffonde soprattutto attraverso messaggi inviati via e-mail, sms o chat o che appaiono su pagine web e social network, che sembrano provenire da soggetti conosciuti e sicuri (corrieri espressi, gestori di servizi (acqua, luce, gas), operatori telefonici, soggetti istituzionali ecc.

Chi li riceve è indotto ingannevolmente ad aprire allegati o a cliccare link o banner collegati a software dannosi.

Il dispositivo infettato può a sua volta «contagiarne» altri, perché il ransomware, impossessandosi della rubrica dei contatti, può utilizzarla per spedire automaticamente messaggi contenenti file dannosi.

Ransomware come difendersi?

La prima difesa dai ransomware è **evitare di aprire messaggi provenienti da soggetti sconosciuti** o con i quali non si hanno rapporti (ad es. un operatore telefonico di cui non si è cliente, un corriere da cui non si aspettano consegne, ecc.) e non cliccare su collegamenti a siti sospetti.

E' utile installare un **antivirus con estensione per malware** sui propri dispositivi e mantenere aggiornato il sistema operativo.

E' fondamentale **effettuare backup periodici dei contenuti**, così, nel caso in cui fosse necessario formattare il dispositivo per sbloccarlo, i dati in esso contenuti non verranno persi.

Ransomware come liberarsene?

Pagare il riscatto è solo apparentemente la soluzione più facile. Oltre al danno economico, si corre infatti il rischio di non ricevere i codici di sblocco, o addirittura di finire in liste di «pagatori», potenzialmente soggetti a periodici attacchi ransomware. L'alternativa è quella di rivolgersi a tecnici specializzati capaci di sbloccare il dispositivo.

Oppure si può formattare il dispositivo, ovviamente se si ha a disposizione un backup. E' consigliabile sempre segnalare o denunciare l'attacco ransomware alla Polizia Postale, anche per aiutare a prevenire ulteriori truffe.



Grazie per l'attenzione

Per qualsiasi informazione contattateci a:

info@netsenseweb.com

095.8996123 / 095.334673