ORDINE DEI DOTTORI COMMERCIALISTI E DEGLI ESPERTI CONTABILI
MILANO

FONDAZIONE COMMERCIALISTI ODCEC di MILANO

Adempimenti privacy per gli studi professionali

PIETRO BERGAMINI

20 gennaio 2023


WEBINAR IL GDPR NEGLI STUDI PROFESSIONALI – PRINCIPALI ADEMPIMENTI

A cura del rag. Pietro Bergamini

AGENDA

- **Nozioni Generali**
  - *Normativa considerata CdP (Dlgs 196/03) GDPR (2016/679)*
- **Le Disposizioni Rilevanti per IT**
  - *Come funzione di supporto*
  - *Come funzione autonoma*
- **L'Outsourcing**
  - *Esternalizzazione di attività*
- **Provvedimenti Garante Rilevanti per IT**
  - *Provvedimento AdS*
  - *Rottamazione*
- ***Legenda***

  New = ***Novità Regolamento UE***

Il Regolamento UE sulla privacy-(2/4)

Entrata in vigore e Applicabilità

- **PUBBLICATO IN GUEE**
  - *4 maggio 2016*
- **ENTRA IN VIGORE**
  - ***Il 24 MAGGIO 2016-*** *20 gg dopo pubblicazione GUEE*
- **SI APPLICA**
  - ***Dal 25 MAGGIO 2018-*** *2 anni dopo la pubblicazione GUEE*

Il Regolamento UE sulla privacy- (3/4)
Conseguenze Normative

- **ABROGA LA DIRETTIVA PRIVACY EU 95/46**
  - *2 anni dopo la pubblicazione in GUCE*
  - *Base del Codice Privacy Italiano (Dlgs 196/03)*

- **NON ABROGA LA DIRETTIVA EU 2002/58**
  - *Recepita da Codice Privacy: Comunicazioni elettroniche*
  - *Riguarda: Marketing non richiesto, pubblicità , marketing telefonico e postale*
  - *Norme specifiche per il Consenso al trattamento dei dati*
  - *Protegge sia persone fisiche sia persone giuridiche*

Quadro di Riferimento Normativa Privacy-Business

IN EUROPA

REGOLAMENTO UE

- ***Riguarda*** *la protezione dei dati delle* ***Persone fisiche***
- ***Esclude*** *i dati delle* ***Persone giuridiche***

«DIRETTIVA» COMUNICAZIONI ELETTRONICHE 58/2002

- ***Include*** *protezione dei dati delle Persone* ***fisiche e giuridiche***

IN ITALIA

REGOLAMENTO UE

- *Idem*

CODICE PRIVACY

- *Include anche la Direttiva Comunicazioni 2002*

PROVVEDIMENTI GARANTE (c.10)

Il Regolamento UE sulla privacy

Quadro Generale

- ***IN SINTESI***
  - ☐ *Conferma dei principi generali*
    - ➢ *Modifiche di precedenti norme*
      - ➢ *Norme del tutto nuove*

DUE ANNI DI TEMPO PER ADEGUARSI

- ➢ *fino al 24 maggio 2018*

Il Regolamento UE sulla privacy
Principali CONFERME vs Codice Privacy

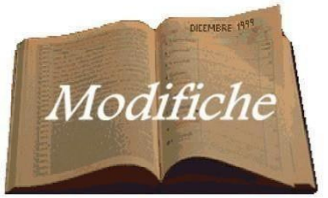
Principi GENERALI del Codice Privacy
Ripresentati dal Reg UE nell'art 5

- ***NECESSITA'/MINIMIZZAZIONE:*** *(ex art 3 cdp)*
- ***TRASPARENZA:*** *informativa (ex art 13 cdp)*
- ***LICEITA':*** *Legge, Consenso, Legittimo interesse (ex art 23 cdp)*
- ***PROPORZIONALITA':*** *finlità vs mezzi utilizzati (ex art 11 cdp)*
- ***PERTINENZA E NON ECCEDENZA*** *(ex art 11 cdp)*
- ***CONSERVAZIONE:*** *cancellazione esaurito lo scopo (ex art 11 cdp)*
- ***SICUREZZA/INTEGRITA'*** *(ex art 31 segg cdp)*

Il Regolamento UE sulla privacy

New

Principali **MODIFICHE** a norme del Codice Privacy

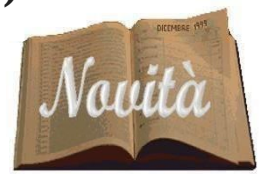


- ***INFORMATIVA** (art 12 segg.)*
- ***CONSENSO** (art 7)*
- ***DIRITTI DI ACCESSO DELL'INTERESSATO** (art 15 segg.)*
- ***RESPONSABILITA' TITOLARE vs RESPONSABILE PER OUTSOURCING** (art 28)*
- ***ANALISI RISCHI E MISURE DI SICUREZZA** (art 32)*
- ***SANZIONI** (art 82 segg.)*

Il Regolamento UE sulla privacy

Principali NORME DEL TUTTO NUOVE (1/3)

New



- ***RAFFORZAMENTO DIRITTO ALL'OBLIO*** ***(art 17)***
  - *Diritto a ottenere la cancellazione dei dati esaurito lo scopo*

- ***DIRITTO ALLA PORTABILITÀ DEI DATI*** ***(art 20)***
  - *Diritto a ottenere il trasferimento dei dati da un fornitore all'altro*

- ***ACCOUNTABILITY*** ***(art 24)***
  - *Responsabilizzazione e obbligo di prova*

- ***PRIVACY BY DESIGN E BY DEFAULT*** ***(art 25)***
  - *Obbligo di proteggere i dati fin dalla progettazione e garantire la privacy con impostazioni pre-definite*

Il Regolamento UE sulla privacy

Principali NORME DEL TUTTO NUOVE (2/3)

New

- ***REGISTRO DEI TRATTAMENTI*** *(art 30)*
  - *Obbligo di tenere un registro dei trattamenti svolti*
- ***DATA BREACHES*** *(art 33)*
  - *Obbligo di notifica delle violazioni all'interessato e al Garante*
- ***VALUTAZIONE DI IMPATTO*** *(art 35)*
  - *Obbligo di valutare preliminarmente l'impatto dei trattamenti sulla privacy*

Il Regolamento UE sulla privacy

Principali NORME DEL TUTTO NUOVE (3/3)

New

- ***DATA PROTECTION OFFICER (art 37)***
  - *Nuova figura di Garanzia all'interno delle organizzazioni*
- ***CERTIFICAZIONE /MARCHI (art 42)***
  - *Riconoscimento di conformità al Regolamento*
- ***RAFFORZAMENTO DELLE SANZIONI PECUNIARIE (art 83 segg)***
  - *Aumento dell'importo delle sanzioni fino al 4% fatturato*

NOZIONI DI BASE

- **DATO PERSONALE**
  - *Differenti categorie di dati*
- **TRATTAMENTO**
- **PROFILAZIONE**

DATO PERSONALE art 4,1

"QUALSIASI INFORMAZIONE RIGUARDANTE UNA PERSONA FISICA IDENTIFICATA O IDENTIFICABILE … (Art. 4,1)
- "INTERESSATO" –

N.B. anche persone giuridiche, enti , assoc per Mktg (art. 130 Cdp)

- ***DEFINIZIONE AMPIA***
  - ✓ *Nome, dati anagrafici*
  - ✓ *Dati relativi all'ubicazione*
  - ✓ *Numero di identificazione (Codice fisc., carta di credito…)*
  - ✓ *Identificativo on line*
  - ✓ *Stato di salute, abitudini*
  - ✓ *Immagine, voce…*
  - ✓ *Dati oggettivi e di origine soggettiva*

CATEGORIE DI DATI PERSONALI (1/2)

- **DATI PARTICOLARI** art 9 — New

Dati che rivelano:

- *- ex Dati Sensibili*
  - ✓ *Origine razziale o etnica*
  - ✓ *Opinioni politiche*
  - ✓ *Convinzioni religiose/filosofiche*
  - ✓ *Appartenenza sindacale*
  - ✓ *Relativi alla salute*
  - ✓ *Relativi alla vita sessuale o all'orientamento sessuale*
- *Dati Genetici* — New
- *Dati Biometrici* — New

- **DATI PENALI** art 10

Dati relativi a:

- *Condanne penali*
- *Reati*
- *Connessi a misure di sicurezza*

CATEGORIE DI DATI PERSONALI (2/2)

- ***DATI CHE PRESENTANO RISCHI*** *art. 35*

  New

  Presentano rischi elevati per liberta'/dignita' della persona e sono assoggettati ad accorgimenti specifici, su base "Valutazione di Impatto" (prior checking).

  Es: Profilazione, Trattamenti su larga scala , Geolocalizzazione, Videosorveglianza …

- ***DATI COMUNI***

  Tutti gli altri dati riconducibili ad una persona

  Es: Anagrafici, indirizzi postali , indirizzi IP, codiciidentificativi, conto corrente , carta di credito , valutazioni ….

- ***DATI ANONIMI***

  Informazioni che non possono essere associate ad un interessato identificato o identificabile.

  A tali dati non si applica il Regolamento

TRATTAMENTO art 4.2

New

"QUALSIASI OPERAZIONE concernente la RACCOLTA, REGISTRAZIONE, ORGANIZZAZIONE, STRUTTURAZIONE, CONSERVAZIONE, ADATTAMENTO, MODIFICA, ESTRAZIONE, CONSULTAZIONE, USO, COMUNICAZIONE, MESSA A DISPOSIZIONE, RAFFRONTO, INTERCONNESSIONE, LIMITAZIONE, CANCELLAZIONE E DISTRUZIONE di dati

DEFINIZIONE AMPIA

- ***Da RACCOLTA***

  a

- ***DISTRUZIONE***

New

PROFILAZIONE art 4.4

" Qualsiasi forma di trattamento <u>automatizzato</u> di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica,

in particolare per analizzare o prevedere aspetti riguardanti

- ✓ *il rendimento professionale,*
- ✓ *la situazione economica,*
- ✓ *la salute,*
- ✓ *le preferenze personali,*
- ✓ *gli interessi,*
- ✓ *l'affidabilità,*
- ✓ *il comportamento,*
- ✓ *l'ubicazione o gli spostamenti*

di detta persona fisica

IL SISTEMA

GARANTE

- SUPPORTO/CHIARIMENTI
- ISPEZIONI E CONTROLLI
- SANZIONI AMMI.VE

AUTORITA' GIUDIZIARIA

- SANZIONI PENALI
- RISARCIMENTO DANNO

Titolare del trattam.

- DOVERE DI ADEGUAMENTO LEGGE

PERSONE

- DIRITTO ALLA PRIVACY

Ruoli importanti

IL TITOLARE DEL TRATTAMENTO

*Il titolare del trattamento (**art. 4** del **GDPR**) è definito come la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità, le condizioni e i mezzi del trattamento sono determinati dal diritto dell'Unione o dal diritto di uno Stato membro, il titolare del trattamento o i criteri specifici applicabili alla sua nomina possono essere designati dal diritto dell'Unione o dal diritto dello Stato membro.*

Nell'ambito dell'organizzazione dell'ente o dell'azienda il titolare del trattamento rimane una figura fondamentale e tale figura assume una rilevanza tale da coincidere con lo stesso concetto di titolare del trattamento di cui al nostro codice. Egli é tenuto ad adottare politiche e attuare misure adeguate per garantire ed essere in grado di dimostrare che il trattamento dei dati personali effettuato è conforme alla normativa.

Il RESPONSABILE 1/3

art 4.8

- ***CHI E'***
  - ***E' il soggetto che tratta dati personali per conto del Titolare – Ruolo importante che approfindiremo durante il webinar***

- ***TIPOLOGIA***
  -
  - **Responsabile "Esterno"** ***(obbligatorio)***

New

New

Il Data Protection Officer

art 37

- *E' la figura di Garanzia del rispetto della legge in Azienda*
- *Nomina Obbligatoria in determinati casi (P.A., Monitoraggio…)*
- *E' nominato dal Titolare o dal Responsabile (artt 37-39)*
- *Possibile un unico DPO di "gruppo"*
- *Deve essere in possesso di competenza e professionalità*
- *Deve essere dotato di risorse umane e finanziarie*
- *Esegue compiti previsti dalla legge: verifiche, pareri,*
- *formazione Riferisce al vertice gerarchico, Opera in autonomia.*
- *Punto di contatto per Interessati e Garante privacy*

CHI, ove necessario, DEVE ESSERE NOMINATO ?

UN DIPENDENTE DI ALTO PROFILO

oppure

UN ESTERNO CON CONTRATTO DI SERVIZIO

New

Contitolarità del trattamento

L'**art. 26** del GDPR parla di contitolari del trattamento quando due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento dei dati personali. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito al rispetto degli obblighi derivanti dal Regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato.

Tale accordo riflette adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati ed il contenuto essenziale dell'accordo è messo a disposizione dell'interessato. Comunque, indipendentemente dalle disposizioni dell'accordo, l'interessato può esercitare i propri diritti ai sensi del regolamento nei confronti di e contro ciascun titolare del trattamento.


ACCOUNTABILITY
IMPRESSION
IMPACT
COMMUNICATION
CASE STUDY
TREND
FORECAST
DIRECTION
POSITIVE
MANAGMENT
UNITY
FEARLESS
REPORT
SALE
INNOVATIVE
SOLUTION
VALUES
RESULTS
PROFIT
TOOL
HUMAN
EXPERIENCE
STRATEGY
CORPORATE
ATTITUDE
DEVELOPMENT

NUOVO
PRINCIPIO GENERALE GUIDA
del Reg. UE

New

L'ACCOUNTABILITY

Artt. 5, 24

- *Responsabilizzazione del Titolare nelle decisioni di tutela della privacy/ misure adeguate*

- *Obbligo di documentare le motivazioni, le scelte e di dimostrare l'adeguamento al Reg. UE*

- *NECESSITA' DI GESTIONE INFORMATICA*
- *"Ove applicable" CREAZIONE DI SITO INTRANET DEDICATO*

New

L'ACCOUNTABILITY

Artt. 5, 24

COSA DOCUMENTARE

esempi

- ***LE NOVITA'***
  - ✓ *Registro dei trattamenti*
  - ✓ *Misure di sicurezza*
  - ✓ *Violazione dei dati/Data breach*
  - ✓ *Privacy by design*
  - ✓ *Valutazioni preventive di impatto,*

- ***LE CONFERME E LE MODIFICHE***
  - ✓ *Rispetto dei Principi Generali*
  - ✓ *Tempo di conservazione dei dati/Data retention*
  - ✓ *Gestione dei Diritti degli Interessati (Informativa, Consensi, Diritto di controllo dei dati)*

GESTIONE DEI DIRITTI DEGLI INTERESSATI

New ➢ *INFORMATIVA*

➢ *CONSENSO*

New ➢ *CONTROLLO DEI DATI*

L' INFORMATIVA (1/2)

Art 13

Principio di TRASPARENZA

- **COS'E'**
  - *Dichiarazione del Titolare all' Interessato*
- **SCOPO**
  - *Mettere in grado l'Interessato di conoscere le intenzioni del Titolare*
  - *Consentirgli di valutare le conseguenze*
  - *Poter accettare o rifiutare il Trattamento*
  - *Controllare il seguito dei suoi dati*
- **QUANDO E' NECESSARIA**
  - *...sempre, anche se non deve essere richiesto il consenso*

L' INFORMATIVA (2/2)

New

L'Accountability

- ***ONERE DELLA PROVA***
  - *Revisione delle vecchie Informative*
  - *Registrazione della data di conferimento*
  - *Gestione varie Tipologie*
  - *Visibilità agli Incaricati, dei testi delle Informative*
  - *File Storico*

IL CONSENSO (1/2)

Art 7

Condizione di LICEITA'

COS'E'

- *E' la condizione necessaria per poter trattare i dati in modo lecito, in assenza di una delle altre condizioni previste dalla legge (es. esecuzione contratto, obbligodi legge ...)*
- *Deve essere richiesto in chiusura dell'Informativa*
- *Risposta dell'interessato all'Informativa*

SCOPO

- *Autorizzare o negare l'uso dei dati*

CONDIZIONI DI VALIDITA'

- ***INFORMATO** invalido se non preceduto da informativa*
- ***SPECIFICO,** richiesto in modo chiaro e distinguibile dal resto*
- New ***LIBERO** svincolato da costrizioni . es. l'esecuzione del contratto non deve essere subordinata al rilascio del Consenso per l'invio di pubblicità*
- New ***CONSAPEVOLE E INEQUIVOCABILE,** basato su dichiarazione o azione positiva - <u>No caselle pre-barrate</u>*

IL CONSENSO (2/2)

Art 7

- **LA PLURALITA' DEI CONSENSI**
  - ***Diritto di esprimere Consenso per una o più finalità***
  - ***Esempi di finalità aggiuntive:***
    - ✓ *Profilazione,*
    - ✓ *Invio di pubblicità non richiesta,*
    - ✓ *Comunicazione a terzi diversi da Responsabile e Incaricati ,*
    - ✓ *Trasferimento dati extra UE*
    - ✓ *…..*
- **GRANULARITA'**
  - ***Richiesta Consenso distinto e separato per ciascuna finalità***

- ***GESTIONE GRANULARITA'***
- ***VISIBILITA' DEI CONSENSI E DELLE REVOCHE***

IL DIRITTO DI CONTROLLO SUI PROPRI DATI

Artt 15-22

- **SCOPO**
  - *Dominio sui dati e Verifica di correttezza*

- **COSA COMPRENDE**
  - *DIRITTO DI ACCESSO*
  - *DIRITTO DI RETTIFICA*
  - New *DIRITTO ALL'OBLIO*
  - New *DIRITTO DI LIMITAZIONE DEL TRATTAMENTO*
  - New *DIRITTO ALLA PORTABILITA' DEI DATI.*

DISPOSIZIONI COMUNI
ai Diritti di Controllo
Art 12

- **RICHIESTA DELL'INTERESSATO**
  - *Inoltrata senza formalità*
- **DOVERE DEL TITOLARE**
  - *Obbligo di verificare l'identità dell'Interessato*
- **RISPOSTA ALL' INTERESSATO (art. 12)**
  - *Senza giustificato ritardo*
  - *Entro 1 mese + 2 mesi di proroga se complessa - (CdP 15+15)*
  - *Comunque informare l'Interessato entro 1 mese*
  - *Mancata risposta: Ricorso a Garante o Aut. Giudiziaria.*

New

IL DIRITTO DI CONTROLLO

OBBLIGHI DI GESTIONE

- **Gestione dei tempi di risposta**
- **Creazione di "Robinson List " per Mktg**
  - *Revoche del consenso, cancellazioni…*
- **Gestione Portabilità dei dati**
- **Gestione Limitazione del trattamento**
  - *In caso di dati inesatti, fino alla rettifica,In caso di contestazione, fino a chiarimento, Su richiesta, in alternativa alla cancellazione*
  - *Definire modalità di gestione*
    - ✓ *Es:Trasferire i dati ad altro sistema*
    - ✓ *Rendere i dati inaccessibili*
    - ✓ *Rimuovere temporaneamente i dati*
    - ✓ *Congelare i dati*
    - ✓ *In ogni caso, identificarli nel sistema*

LA PROTEZIONE DEI DATI

LE MISURE DI SICUREZZA

(Art. 32 RegUE)

LE MISURE DI SICUREZZA- art 32

Destinatari e Responsabilità

- **DESTINATARI DELLA NORMA**
  - *Titolare*
  - *Responsabile*
  - *Incaricato*

- **RESPONSABILITA'**
  - ***TITOLARE E RESPONSABILE***
    - ✓ *Individuare e adottare le Misure di Sicurezza*
    - ✓ *Fornire agli Incaricati istruzioni/formazione al riguardo*
    - ✓ *Vigilare su efficacia*
  - ***INCARICATI***
    - ✓ *Trattare i dati secondo le istruzioni ricevute*
    - ✓ *Comportamento consapevole dei rischi*

SICUREZZA DELLE INFORMAZIONI (Estratto da un Modello Organizzativo Privacy)

Il patrimonio informativo da tutelare è costituito dall'insieme delle informazioni trattate nell'espletamento delle procedure istituzionali e aziendali, rispetto alle quali l'ente assicura l'integrità e la protezione e consente l'accesso esclusivamente ai ruoli e alle funzioni necessarie e preventivamente autorizzate.

La mancanza di adeguati livelli di sicurezza può infatti comportare il danneggiamento dell'immagine aziendale, la mancata soddisfazione degli iscritti, il rischio di incorrere in sanzioni legate alla violazione delle leggi vigenti nonché altri danni di natura economica e finanziaria.

Per conseguire sempre l'allineamento normativo e aumentare la capacità di controllo l'ente ha istituito e mantiene aggiornato un registro delle attività di trattamento.

L'ente identifica, quando ritenuto necessario a seguito delle risultanze dell'analisi dei rischi connessi al trattamento dei dati personali, le ulteriori esigenze di sicurezza tramite la valutazione di impatto sulla protezione dei dati che consente di acquisire un livello aggiuntivo di consapevolezza sul livello di esposizione a minacce dei propri sistemi di gestione dei dati.

La valutazione del rischio, eseguita su tutti i trattamenti in essere o previsti, permette di valutare le potenziali conseguenze e i danni che possono derivare dalla mancata applicazione delle misure di sicurezza al sistema informativo e in generale all'intera organizzazione oltre a indicare quale sia la probabilità che le minacce identificate trovino reale attuazione. I risultati di questa valutazione determinano le azioni necessarie per individuare le corrette e adeguate misure di sicurezza e i meccanismi per garantire la protezione dei dati personali.

LE MISURE DI SICUREZZA

Qualità delle misure

ADEGUATE

non predefinite

SPECIFICHE

Ad hoc

Vincolanti

MINIME

predefinite

Vincolanti

Origine

Individuate dal Titolare

In base alla ***valutazione dei rischi***

Individuate dal Garante

Predefinite, incluse nei Provvedimenti Generali o ad hoc

Allegato B del Codice Privacy

New

Non più previste da Reg UE

LE MISURE DI SICUREZZA

Obblighi di verifica e scadenze

☐ *Controlli periodici di efficacia e adeguatezza*
(art 29 Cdp/ Accountability GDPR)

☐ *Verifica periodica dei profili di autorizzazione, su base almeno annuale (p.to 14 MMS/ Accountability GDPR)*

➢ *Verifica periodica dell'attività degli Amm.di Sistema su base almeno annuale (Provv. Gar.)*

➢ *Verifica periodo conservazione dati (art 4 GDPR , Aut.Gen dati sensibili, videosorveglianza….)*

☐ *Verifica periodica del Registro dei trattamenti e delle istruzioni*

LE MISURE DI SICUREZZA

Le violazioni della privacy

Il sistema sanzionatorio art 77 segg

New

SANZIONE AMMINISTRATIVA
Fino al 4% del fatturato

RISARCIMENTO DANNI
Materiali e morali

SANZIONE PENALE
Disposte dai singoli Stati

New

DANNO DI IMMAGINE
Notifica data breach

L’ANALISI DEI RISCHI
e
LE MISURE DI SICUREZZA

(Art. 32 Reg UE)

Principi della sicurezza dei dati

Sicurezza informatica: salvaguardia dei sistemi informatici da potenziali rischi e/o violazioni dei dati. I principali aspetti di protezione del dato sono **confidenzialità**, **integrità** e **disponibilità**.

Confidenzialità

Proprietà che le informazioni non siano rese disponibili o divulgate a persone non autorizzate, entità o processi

Integrità

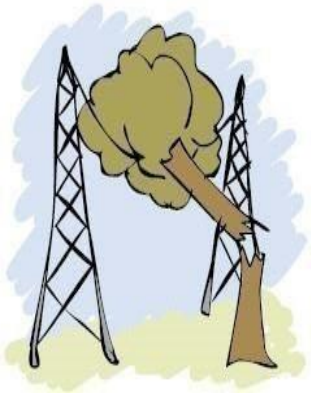
Proprietà di proteggere l'accuratezza e lacompletezza delle informazioni

Disponibilità

Proprietà di rendere il dato accessibile e utilizzabile su richiesta da parte di unentità autorizzata

Minacce alla Sicurezza dei Dati

EVENTI NATURALI
(terremoti, alluvioni, etc.)



INCIDENTI ALLE TECNOLOGIE
(malfunzionamento e rottura tecnologie, interruzione servizi informativi, etc.)

INCIDENTI AMBIENTALI
(incendi, blackout, etc.)

Dati

ATTACCHI AL PATRIMONIO
(furti, frodi, sabotaggio, etc.)

ATTACCHI INFORMATICI
(virus, spam, phishing, etc.)

ERRORI UMANI

COSA SI INTENDE PER MISURE DI SICUREZZA INFORMATICHE?

Ci si riferisce a tutte quelle misure tecniche e organizzative atte a garantire un livello di sicurezza proprozionato al rischio, così da salvaguardare la riservatezza l'integrità e la disponibilità delle informazioni gestita da un'organizzazione, una difesa non solo da attacchi diretti ma anche da fenomeni come calamità naturali oppure da problemi accidentali. Per poter individuare le misure idonee di sicurezza ogni azienda dovrà strutturare un processo continuo di valutazione del rischio e individuazione dei rimedi. Tutto questo è regolamentato dal GDPR.

Quali sono le funzioni di un antivirus?

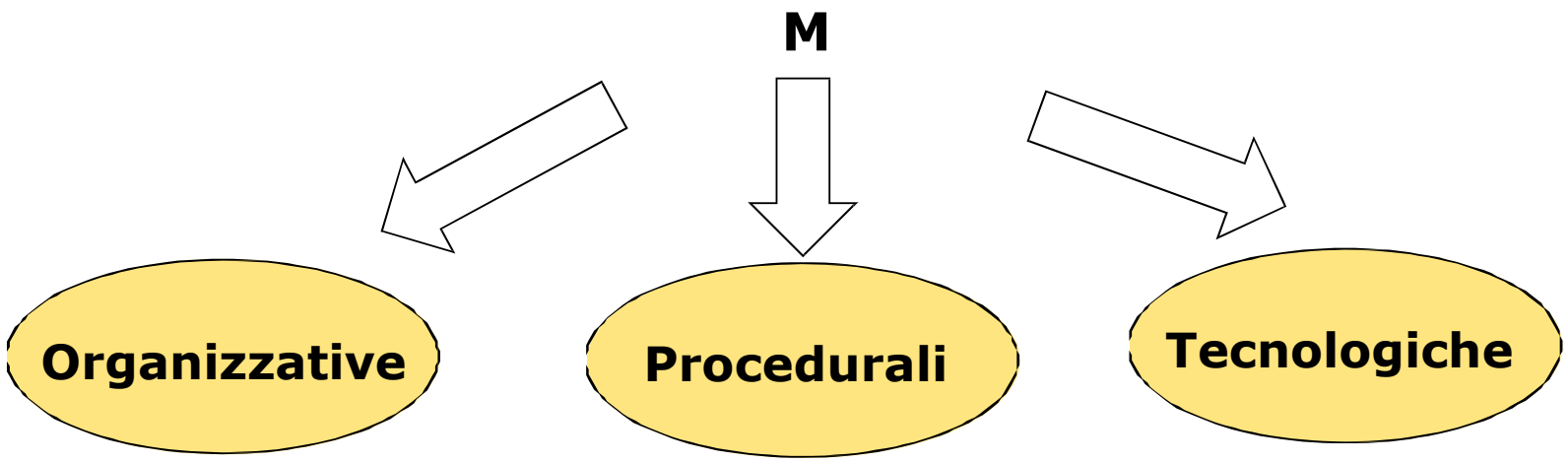
L’antivirus è tipicamente un’applicazione in grado di verificare la presenza di virus nei file memorizzati sui vari supporti,in memoria o nel settore di avvio. In caso venga trovato un virus sconosciuto è normalmente possible procedure all’eliminazione o alla pulizia del file. Gli antivirus hanno anche una funzione preventiva, cioè rimangono sempre attivi per impedire l’accesso dei virus nel Sistema. Devono essere periodicamente aggiornati per avere una protezione efficace.

Finalità delle misure di sicurezza e privacy

Proteggere i dati personali da:
possibili attacchi (interni o esterni) o eventi (accidentali o indesiderati)
che potrebbero provocare danni
alla ***libertà e ai diritti dell'interessato,***

compromettendo

la riservatezza, ***l'integrità,*** ***la disponibilità*** *dei dati personali*
e
i principi privacy *(es. scelta e consenso, limitazione dei trattamenti, etc.)*



Quando si può affermare che una password sia robusta?

Numeri di telefono,indirizzi, codici di pagamento, abbonamenti e altre informazioni sensibili sono protette da una password. Dai metodi usati per violare le password si può capire come difendersi. Una Password "robusta" deve avere almeno otto o più caratteri, evitando però di scegliere parole o termini "prevedibili" come nome, data di nascita, indirizzo e altre informazioni facilmente reperibili sul vostro conto. La password deve avere caratteri speciali, essere alfanumerica e deve contenere lettere maiuscole e minuscole.

LE MISURE DI SICUREZZA

"ADEGUATE"

- *Il Titolare ha l' Obbligo di adottare misure " adeguate" (art32 DPGR)*
  - ✓ *obbligo esistente anche nel CdP: addizionali alle "minime" (art.31 Cdp)*
- *Si tratta di misure in continua evoluzione*
- *Devono essere Individuate dal Titolare valutando più fattori*
- *L'obbligo di adottare misure adeguate riguarda anche il Responsabile "esterno" (art 28)*

New

  - ✓ *In caso di outsourcing*

LE MISURE DI SICUREZZA (11/17)

Il Livello della Sicurezza

- **QUALITA' DELLE MISURE**
  - ***Livello di protezione"ADEGUATO"***
  - ***Tenuto conto di***
    - *Stato dell'arte e sviluppi tecnici*
    - *Natura dei dati,*
    - *Contesto e strumenti adottati*
    - *Probabilità e gravità dei rischi.*
    - *Bilanciamento costi vs rischi*

New

- **MONITORAGGIO**
  - *Livello di "adeguatezza" è in continua evoluzione*
  - *Revisione Periodica delle misure adottate*
  - *Tenendo conto anche dell'esperienza acquisita*

LE MISURE DI SICUREZZA (12/17)

Copertura: tempo

- **PRIMA DI INIZIARE IL TRATTAMENTO**

- **DURANTE TUTTE LE OPERAZIONI DI TRATTAMENTO**

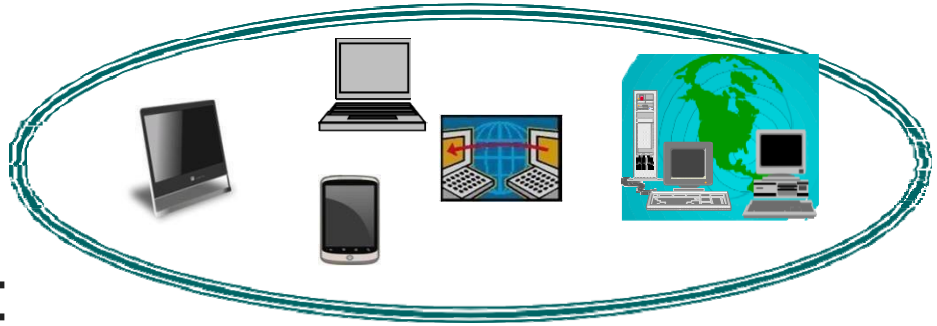
  (Cfr Definizione art 4)

  - *Raccolta,*
  - *conservazione,*
  - *trasmissione,*
  - *elaborazione …*

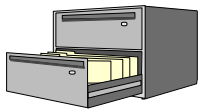
LE MISURE DI SICUREZZA (13/17)

Copertura: Strumenti e modalità'

- **ELETTRONICI:** *server centralizzati, cloud, informatica individuale, smartphone, tablet, etc…*



- **CARTACEI**



- ***ALTRO:*** *fax, stampanti …* 

Cosa si intende per "Backup"?

Il Backup è una copia di sicurezza di un hard disk, di una parte dell'hard disk o di uno o più file effettuata su supporti di memorizzazione diversi da quello in uso. L'operazione è il modo migliore per gli utenti privati e aziende di tutelarsi da qualsiasi evenienza. In caso di malfunzionamento o Guasti, furti oppure attacchi da parte dei cybercriminali o, anche da errori umani, avere una copia di backup può salvare dati e informazioni preziose.

Il comportamento dei dipendenti

- **PREVENIRE ILLECITA DIVULGAZIONE**
  - *A Terzi*
  - *Scrivania sgombra*
- **PROTEGGERE DATI vs STRUMENTI**
  - *Segretezza e robustezza Psw, utilizzo PIN, Screen saver …*
  - *Controllo e custodia degli strumenti,*

- **PROTEGGERE DATI vs LUOGHI/ACQUISIZIONI INVOLONTARIE**
  - *Distanze di cortesia/ Open Space/Aree chiuse*
  - *Presidio Stampanti, Copiatrici, Fax …*
  - *Separazione dati sensibili da dati comuni, Armadi chiusi a chiave*
  - *Distruggi documenti*
- **AZIONI PREVENTIVE.** Es:
  - *Codifica voci su cedolino, Consegna diretta dei documenti/invio plichi chiusi*

  ✓ ***ISTRUZIONI/CONSAPEVOLEZZA/FORMAZIONE***
  ✓ ***SITO PRIVACY IN INTRANET***
  ✓ ***"PRIVACYZZARE" I PROCESSI***

GLI AUTORIZZATI *AL TRATTAMENTO*

CHI? Dipendenti, Collaboratori, Stagisti/e, Praticanti, Segretari/e ecc..

Il regolamento europeo non prevede espressamente la figura dell'**incaricato**, ma non ne esclude la nomina, facendo riferimento a **persone autorizzate** al trattamento dei dati sotto l'autorità diretta del titolare o del responsabile (art. 4, n. 10 GDPR).

Il Codice Privacy novellato dal D. lgs 101/2018, invece, ha introdotto (art. 2 quaterdecies) espressamente la figura del soggetto designato, una persona fisica che opera sotto l'autorità e responsabilità del titolare del trattamento, al quale possono essere delegati specifici compiti e funzioni. Comunque sia definito, Incaricato, designato o autorizzato, è il **soggetto persona fisica che effettua materialmente le operazioni di trattamento sui dati personali**. L'autorizzato può operare alle dipendenze del titolare, ma anche del responsabile se nominato. Ovviamente gli autorizzati possono essere organizzati con diversi livelli di delega.

Designazione e istruzioni operative

Il regolamento europeo non prevede l'obbligo di nomina o designazione espressa, ma è fondamentale **fornire agli autorizzati le istruzioni operative** (art. 29 GDPR), compreso gli obblighi inerenti le misure di sicurezza, e che sia fornita loro la **necessaria formazione**. In caso contrario, infatti, anche in presenza di formali designazioni, queste sarebbero del tutto prive di valore.

I Registri del Trattamento

Registri delle attività di trattamento (Art. 30)

1. Ogni Titolare o il suo rappresentante , ove applicabile, tengono un registro delleattività di trattamento svolte sotto la propria responsabilità.
2. Ogni Responsabile del trattamento o, ove applicabile, il suo rappresentante, tengonoun registro delle attività di trattamento svolte sotto la propria responsabilità.

I Registri **non si applicano alle aziende con meno di 250 dipendenti, a meno che:**

- il trattamento **presenti rischi per l'interessato**
- il trattamento **non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10.**

Registri del Titolare

- ❑ Nome e dati di contatto del Titolare e, se applicabile, del DPO
- ❑ Finalità del trattamento
- ❑ Descrizione delle categorie degli interessati e le categorie di dati personali trattati
- ❑ Categorie di destinatari, inclusi i destinatari di paesi terzi
- ❑ Termini ultimi per la cancellazione dei dati
- ❑ Descrizione generale misure tecniche e organizzative di sicurezza (art. 32)

Registri del Responsabile

- ❑ Nome e i dati di contatto del/dei Responsabili del trattamento, di ogni Titolare del trattamento per cui si agisce e, se applicabile, del DPO
- ❑ Categorie dei trattamenti per conto di ogni titolare
- ❑ Trasferimenti di dati personali verso paesi terzi
- ❑ Descrizione generale misure tecniche e organizzative di sicurezza (art. 32)

LA NOTIFICA DI VIOLAZIONE DATI PERSONALI

(Artt. 33, 34 Reg UE)

La Notifica delle Violazioni dei dati personali

(Data Breach)

Art. 33 - Notifica di una violazione dei dati personali all'autorità di controllo

- **Obbligo di notifica al Garante**, senza ingiustificato ritardo, **entro 72 ore** dal momento in cui ne è venuto a conoscenza, a meno che non sia in grado di dimostrare, in conformità con il principio di responsabilità, che la violazione non comporti un rischio per i diritti e le liberta' degli interessati
  - Natura della violazione, categorie e numero di interessati
  - Riferimenti del Responsabile Protezione Dati o altra figura
  - Probabili conseguenze della violazione dei dati personali
  - Misure adottate per porre rimedio alla violazione e per attenuarne i possibili effetti negativi

Art. 34 - Comunicazione di una violazione dei dati personali all'interessato

- **Obbligo di comunicazione <u>anche</u> agli Interessati**, senza ritardo
  - In caso di **rischio elevato** (es. discriminazione, furto di identità, perdite finanziarie etc..) per i diritti e le liberta' delle persone fisiche
  - Per disposizione del Garante .

Non è richiesta la comunicazione all'interessato se:

- il titolare del trattamento ha attuato misure tecniche e organizzative adeguate di protezione tali da rendere i dati incomprensibili (Cifratura)
- la comunicazione richiederebbe sforzi sproporzionati (puo' essere sostituita da una comunicazione pubblica)

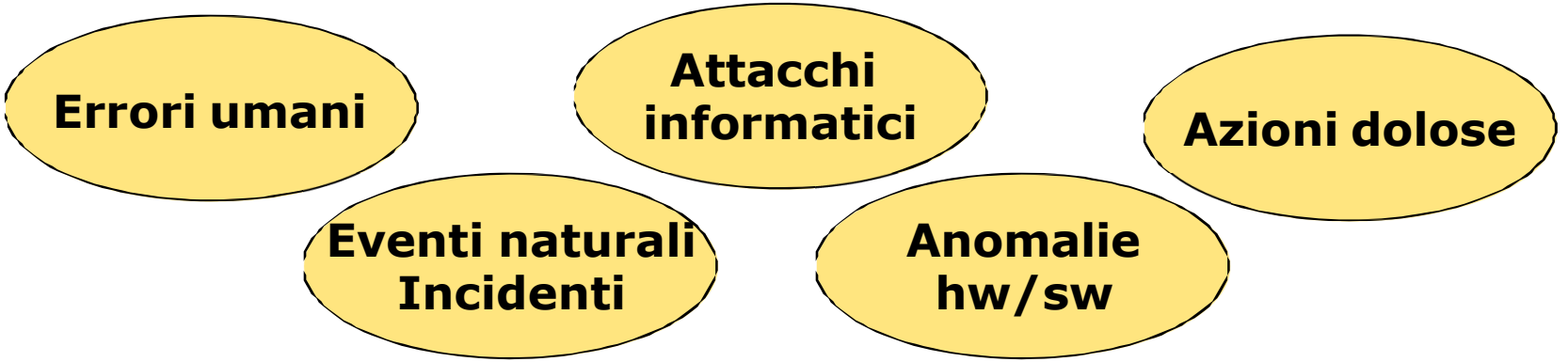
Quando si configura un caso di Violazione di Dati Personali

Violazione di dati personali (data breach): eventi (incidenti di sicurezza) che, per incuria (**colpa**), intenzionali (**dolo**) o accidentali (es. eventi naturali, terremoto) comportano:

- perdita
- distruzione
- modifica
- diffusione non autorizzata
- accesso ai dati personali trasmessi, memorizzati o comunque elaborati, con strumenti elettronici e/o in formato cartaceo,

con possibili **danni per la libertà e i diritti degli interessati**

Cause di data breach



CRITTOGRAFIA STRUMENTO INDISPENSABILE

La crittografia rappresenta uno strumento fondamentale nella lotta contro il cybercrimine. La crittografia è la conversione dei dati da un formato leggibile in un formato codificato che può essere letto o elaborato solo dopo che è stato decriptato. Impiegata sia dai singoli utenti che dalle grandi aziende, la crittografia è ampiamente utilizzata su Internet per tutelare le informazioni inviate fra il browser e il server. Tali informazioni potrebbero includere tutto, dai dati di pagamento alle informazioni personali.

La crittografia si basa sui concetti di algoritmo di cifratura e "chiave". Le informazioni inviate vengono cifrate mediante un algoritmo e possono essere decodificate alla destinazione solo con la chiave appropriata. La chiave può essere memorizzata nel sistema ricevente oppure trasmessa insieme ai dati criptati.

L'algoritmo oggi più diffuso utilizzato in crittografia è chiamato Advanced Encryption Standard (AES). Fu sviluppato alla fine degli anni '90 e divenne uno standard pubblico alla fine del 2001. Nel 2003 la National Security Agency statunitense ha approvato l'AES a 128 bit per proteggere tutte quelle informazioni governative classificate come secret e l'AES a 192 e 256 bit per i documenti cosiddetti top secret.

La criptazione dei dati nelle operazioni di backup è una delle caratteristiche più importanti che i software dedicati a questi processi devono tenere in considerazione, non solo perché risulta ormai essere una misura precauzionale necessaria, ma anche perché ci sono delle leggi da rispettare.

La criptazione dei dati è usata anche dalle reti VPN, infatti riescono a crittografare il traffico tra i server VPN sicuri e il proprio computer in modo che non possa essere letto da terzi, ad esempio il provider di servizi internet o l'operatore Wi-Fi locale.

LINEE GUIDA

Linee guida in materia di notifica delle violazioni di dati personali (data breach notification) - WP250, definite in base alle previsioni del Regolamento (UE) 2016/679

Adottate dal Gruppo di lavoro Art. 29 il 3 ottobre 2017
Versione emendata e adottata il 6 febbraio 2018

La Videosorveglianza negli ambienti di lavoro

REGOLAMENTO UE 2016/679
DIRETTIVA 680/2016 – D.LGS 51/2018

D.LGS 196/2003 come modificato D.Lgs 101/2018

STATUTO DEI LAVORATORI – L. n.300/1970

Provv. Generale 08 aprile 2010, doc. webn. 1712680.

LE FONTI (Videosorveglianza

Il legittimo comportamento del Titolare del trattamento

Considenrando che il GDPR conferma che ogni trattamento deve trovare il proprio fondamento in un'idonea base giuridica e che I fondamenti di liceità del trattamento sono quelli che vengono citati nell'art.6 del GDPR, diventa necessario per il Titolare del trattamento conoscere la base giuridica sulla quale si basa il trattamento dei dati dei propri clienti.
Il seguente elenco comprende esempi di interessi legittimi per il professionista che possono costituire una base giuridica lecita del trattamento, interessi legittimi a condizione che non prevalgono sugli interessi o sui diritti e le libertà fondamentali dell'interessato. Interessi legittimi:

- Quando l'interessato è un cliente del titolare;
- Quando l'interessato è alle dipendenze del Titolare del trattamento;
- Quando I dati dell'interessato sono trattati ai fini strettamente necessari ai fini di prevenzioni delle frodi.

Quando un trattamento dei dati può essere considerate lecito?

- Quando l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
- 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.
- Il trattamento è necessario per adempiere a un obbligo legale al quale è soggetto il titolare del trattamento.


Pause

PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE E PROTEZIONE PRE-DEFINITA

(Art 25 Reg UE)

Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita (Privacy by design e by default)

Art. 25 - Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

1. Il Titolare mette in atto **misure tecniche e organizzative adeguate**, tenendo conto dei **rischi per i diritti e le libertà delle persone**, sia al **momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso,** quali la **pseudonimizzazion**e, volte ad attuare in modo efficace i principi di protezione dei dati, quali la **minimizzazione**, …

2. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per **garantire che siano trattati**, **per impostazione predefinita, solo i dati personali necessari ….**

3. Possibilità di utilizzo di **certificazione** (articolo 42) per dimostrare la conformità ai requisiti del Regolamento.

Il concetto di Privacy by design

- **Privacy by Design** è un **approccio innovativo** che va utilizzato in ogni occasione e contesto in cui sia necessario **garantire** la protezione dei datipersonali

- E' un "caposaldo" fondamentale del Regolamento, in quanto "**garanzia"** di rispetto nel tempo dei diritti degli interessati da parte dei Titolari dei trattamenti di dati personali

- Qualsiasi progetto va realizzato considerando **dalla progettazione (by design**):
  - il rispetto dei Principi di Protezione dei dati
  - la presenza di misure di sicurezza dei dati (**non solo tecnologiche**ma anche organizzative, procedurali) adeguate ai rischi dei trattamenti·

- Applicato non solo nello sviluppo di **nuovi processi di trattamento** di dati personali, ma anche nel caso di **cambiamenti ai processi esistenti**,o a fronte di incidenti. Fondamentali:
  - l'adozione di **processi e strumenti**
  - il **coinvolgimento del DPO/ Delegato Privacy** sin
  - dall'origine.


0100101
01

L’ OUTSOURCING

Esternalizzazione di Attività

(Art 28 Reg UE)

L' OUTSOURCING

COS' E'

- *L' esternalizzazione di una attività da parte di una Organizzazione ad un soggetto "esterno"*

- *L'attività, che comporta trattamento di dati personali, viene svolta dal soggetto esterno «per conto» di un altro soggetto*

  Esempi:

  - ✓ *predisposizione cedolini, archiviazione …*
  - ✓ *Gestione sistema informativo, Cloud; Rottamazione…*
  - ✓ *call center*
  - ✓ *agenti*
  - ✓ *gestione eventi*
  - ✓ *…*

L' OUTSOURCING
La normativa: Art 28

- **QUESITO**
  - *Cosa prevede il Regolamento UE in caso di outsourcing?*

- **RISPOSTA**
  - *Chi svolge attività "per conto di…" è obbligatoriamente un Responsabile privacy -"esterno"*

GESTIONE DI ATTIVITA' PERCONTO DI ALTRI

ESTERNALIZZAZIONE
Da Azienda a Società esterna

L'Azienda commissiona il servizio a una Società esterna (es: un Servizio IT)

- *L'Azienda è il Titolare del tratt.*
- *La Società esterna che svolge attività "per conto dell'azienda" assume il ruolo di Responsabile del trattamento*
- *Il dipendente della Società esterna che svolge l'attività per conto dell'Azienda ha il ruolo di Incaricato (dalla Soc. esterna- Responsabile)*

➢ **OBBLIGHI :**

New

1. ***Contratto scritto (o atto equipollente)***
2. ***Ruolo di Resp "esterno" con assegnazione compiti di cui art 28 Reg. UE (+ eventuali altri di cui a Provv Garante)***

New

OUTSOURCING
OBBLIGHI CONTRATTUALI DI CUI ALL'ART 28 DEL REG. UE

IL CONTRATTO DI SERVIZIO DEVE ESSERE INCLUDERE I SEGUENTI OBBLIGHI PRIVACY (minimi)

- **Deve disciplinare**
  - *la materia esternalizzata, la durata, la natura e finalità del trattamento, il tipo di dati le categorie di interessati, gli obblighi e i diritti del Titolare*

- **Deve includere i seguenti obblighi per il Responsabile esterno:**
  - *Trattare i dati soltanto su istruzioni documentate del Titolare, anche in caso di trasferimento extra Ue*
  - *Garantire che gli incaricati siano obbligati al rispetto della privacy*
  - *Adottare misure di sicurezza adeguate*
  - *Assistere il Titolare nelle risposte da fornire all' interessato in caso di esercizio del diritto di "controllo dei dati"*
  - *Assistere il Titolare nel garantire il rispetto degli obblighi di Sicurezza, Data Breach, Valutazione preventiva di impatto, Prior checking col Garante*
  - *Divieto di sub-appalto senza accordo preventivo del Titolare*
  - *Cancellare i dati o restituirli al titolare alla fine del servizio*
  - *Consentire attività di verifica, controllo, e ispezione del Titolare*
  - *Informare il Titolare dei casi di violazione della privacy*

RIVEDERE E INTEGRARE I CONTRATTI DI OUTSOURCING

IL RESPONSABILE

"Esterno"- sintesi

- *Soggetto che tratta dati per conto del Titolare*
- New *Ruolo "obbligatorio" in caso di esternalizzazione di attività (es: predisposizione cedolini, gestione sistema informativo, call center, agenti…)*
- *Puo' essere persona fisica o giuridica*
- *Deve presentare adeguate garanzie di rispetto del Regolamento- culpa in eligendo del Titolare*
- New *I trattamenti esternalizzati devono essere disciplinati da un contratto (o atto giuridico) scritto, sottoscritto per accettazione*
- New *Il contratto deve prevedere una serie di vincoli prestabiliti:art28*

CHI E' ALL' ESTERNO DELL' AZIENDA

CIASCUN OUTSOURCER

OBBLIGHI: *1. Contratto scritto (o atto equipollente)*
2.Assegnazione compiti/responsabilità di cui art 28 Reg UE
3.Assegnazione compiti /responsabilità prescritti da Provv Garante

I PROVVEDIMENTI DEL GARANTE

E

LE RICADUTE SULLA SICUREZZA

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

SCOPO

- ***Quadro unitario***
- ***Chiarimenti e Prescrizioni***
- ***Valore di legge***

ESEMPI
DI PROVVEDIMENTI DEL GARANTE

- *Fidelity card (24/2/2005)*
- *Tracciamento posiz geografica/ RFID (9/3/2005**)***
- *Rapporto di lavoro (23/11/2006)*
- *Uso e-mail e Internet sul lavoro (1/3/2007)*
- *Gestori Telefonici (15/12/05-1/2/08)*
- ***Rottamazione (13/10/08)***
- *Semplificazione delle misure di sicurezza in particolari circostanze(27/11/2008)*
- ***L' Amministratore di sistema (27/11/2008)***
- *Videosorveglianza (8/4/10)*
- *Marketing Telefononico e Registro opposizioni (19/1/2011)*
- *Biometria (23/11/2006 e 12/11/2014)*
- *Cookies (8-23/5/2014)*
- ***……***

ROTTAMAZIONE

Fonti:

-P.G. : 13/10/2008- Rifiuti di apparecchiature elettroniche e Misure di Sicurezza

-PG: 5/12 2008 - Come rottamare il Pc

-Documento 12/12/ 2008- Istruzioni pratiche per una cancellazione sicura

LA ROTTAMAZIONE

- **Misure Tecniche Preventive**
  - *Proteggere i file con password di cifratura*
  - *Memorizzare i dati su hard disk/supporti magnetici con sistemi di cifratura automatica al momento della scrittura*
- **Misure Tecniche di cancellazione sicura**
  - *Usare programmi di riscrittura che provvedono una volta eliminati i file (es: nel cestino)a scrivere ripetutamente nelle aree vuote*
  - *Usare sistemi di formattazione a basso livello o di demagnetizzazione*
- **Smaltimento Rifiuti**
  - *Per hard disk e supporti non riscrivibili, utilizzare punzonatura, deformazione meccanica o distruzione fisica*

L’ AMMINISTRATORE DI SISTEMA (AdS)

Provv. Gen. : 27/11/2008

L’ AMMINISTRATORE DI SISTEMA

ORIGINE

- *FIGURA ESPRESSAMENTE PREVISTA NEL DPR 318/99 - “VECCHIA” LEGGE SULLA PRIVACY*

- *SCOMPARSA NEL “NUOVO” DISCIPLINARE TECNICO – all B del Codice della PRIVACY*

- *RIPRESENTATA A SEGUITO DI DENUNCE/ISPEZIONI*

Contenuto del Provvedimento

- **FINALITA'**
  - *DARE RISALTO / RESPONSABILIZZARE FIGURA "CHIAVE"NELLA GESTIONE DEI PROCESSI AZIENDALI*
  - *RESPONSABILIZZARE LA SCELTA DEI CANDIDATI AdS*
  - *PREVENIRE ACCESSI NON CONSENTITI*
  - *ACCERTARE ABUSI*
- **PRESCRIZIONI**
  - *ADOZIONE DI MISURE TECNICHE E ORGANIZZATIVE" SPECIFICHE"*
  - *OBBLIGATORIE*

Le Prescrizioni del Provvedimento

- **DESTINATARI**
  - *TUTTI I TITOLARI DEL TRATTAMENTO*
  - *SONO ESENTATI COLORO CHE RIENTRANO NELL'AMBITO DI APPLICAZIONE DEL REGIME DI SICUREZZA SEMPLIFICATO (Provv. 27/11/08 sulle semplificazioni)*

- **OGGETTO DELLE PRESCRIZIONI**
  - *NUOVE MISURE DI SICUREZZA OBBLIGATORIE*
  - *ADEMPIMENTI TECNICI E ORGANIZZATIVI*


DATA
RETENTION

La fonte dell'obbligo di cancellazione dei dati personali è, oggi, l'art. 5, paragrafo 1, lettera e) del GDPR, cioè la norma che detta il principio di limitazione della conservazione: «*I dati sono 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*.

Il riferimento è all'art. 11, paragrafo 1, lettera e) del Codice Privacy (prima dell'abrogazione *ex* D.Lgs. 101/2018): «*I dati personali oggetto di trattamento sono conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati*».

INDIVIDUAZIONE DEI TEMPI DI CONSERVAZIONE NELLE VARIE E MOLTEPLICI NORMATIVE DI SETTORE.

PRIVACY POLICY ***(Informazioni e note legali relative ai servizi online e alle condizioni contrattuali praticate).***

CORRETTA GESTIONE DEI COOKIES E LATRI STRUMENTI DI TRACCIAMENTO (Provv. del Garante del 10 Giugno 2021)

NAVIGAZIONE SICURA "PROTOCOLLO DI RETE SSL"


KEEP
CALM
AND
GRAZIE
PER L'ATTENZIONE

Riferimenti

Ragioniere Pietro Bergamini
DPO ODCEC LATINA
ragbergamini@gmail.com