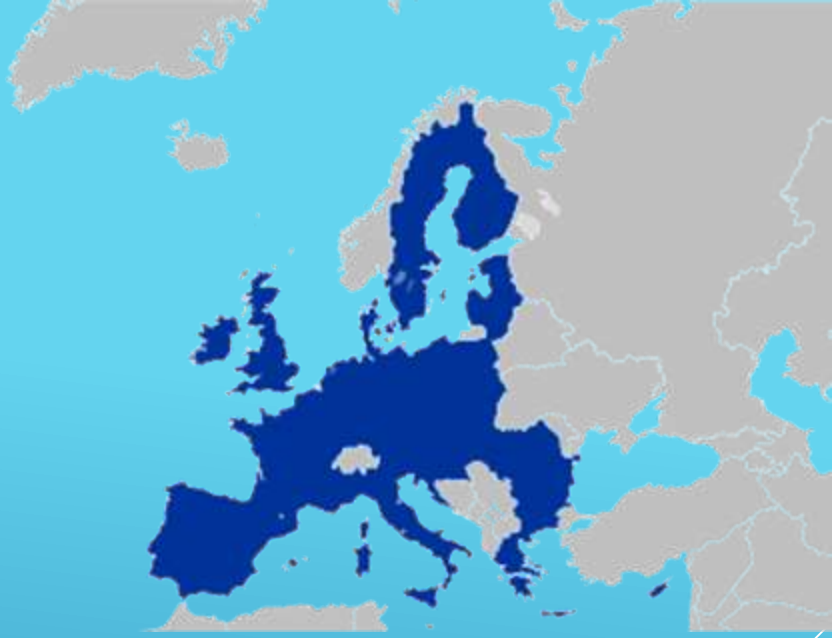
GDRP
IL NUOVO REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI PERSONALI

Dott. Carmine De Simone – DPO CAF Confsal S.r.l.

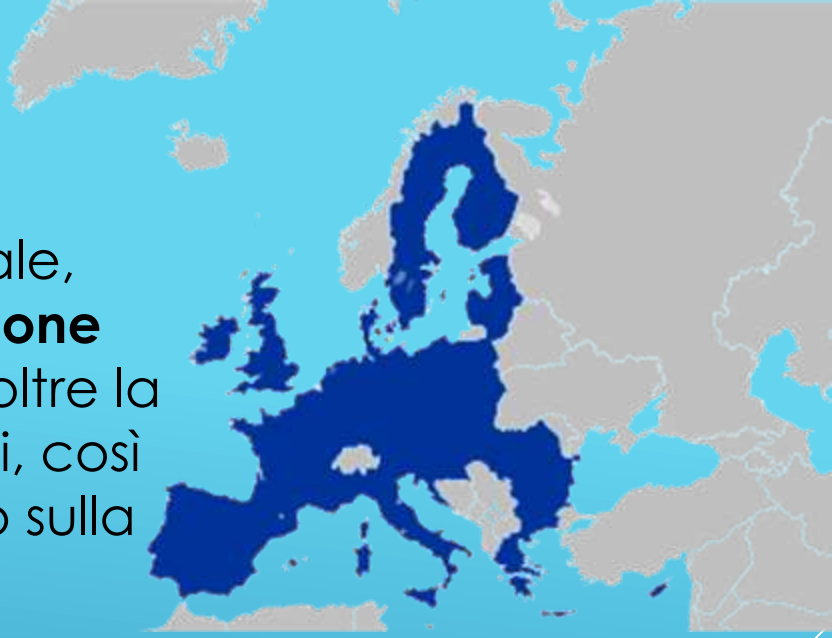
- ~~Direttiva 95/46/CE~~
  - ~~Legge 675/1996~~
  - ~~Altre normative introdotte nel corso del tempo~~
  - ~~D. Lgs. 196/2003~~
  - ~~Allegato B~~
- Provvedimenti vari? Es. Amministratori di Sistema
- Regolamento generale sulla sulla protezione dei dati (GDPR)
  - Reg. UE 679/2016
  - In vigore dal 25/05/2016
  - Si applicherà dal 25/05/2018

LA NORMATIVA E SUA EVOLUZIONE

CAF confsal



PRINCIPI FONDAMENTALI

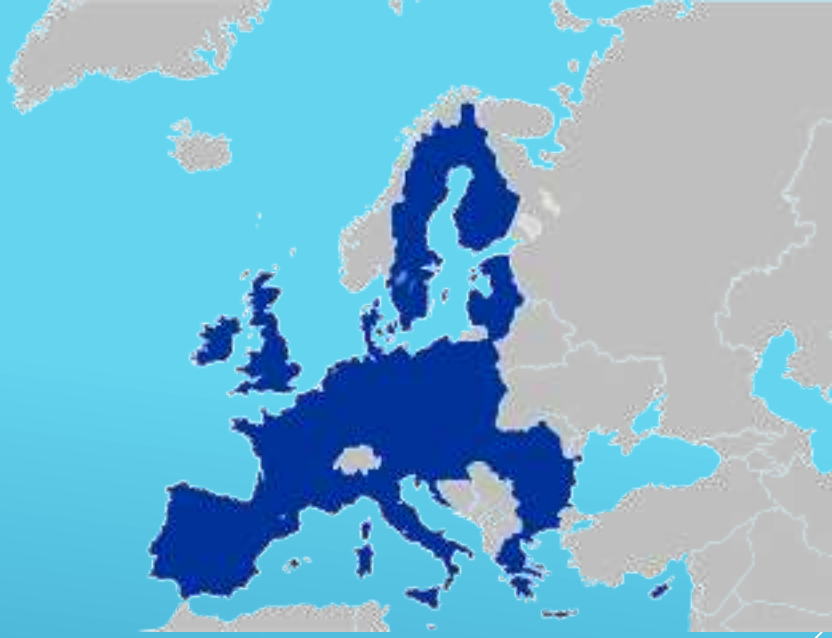


- Mentre la **privacy** rappresenta una sorta di diritto individuale, che tutela il singolo nella sua solitudine, il **diritto alla protezione dei dati personali**, invece, estende la tutela dell'individuo oltre la sfera della vita privata e in particolare nelle relazioni sociali, così garantendo l'autodeterminazione decisionale e il controllo sulla circolazione dei propri dati.
- Rientra tra i diritti fondamentali della persona (Convenzione Europea dei diritti dell'uomo - CEDU, art. 8.1 e Trattato Fondativo Unione Europea -TFEU art. 16.1)
- Ogni persona detiene il diritto alla protezione dei dati di carattere personale che lo riguardano

PRINCIPI FONDAMENTALI

CAF confsal

In **grassetto bianco** sono evidenziate le novità e le specificazioni del GDPR

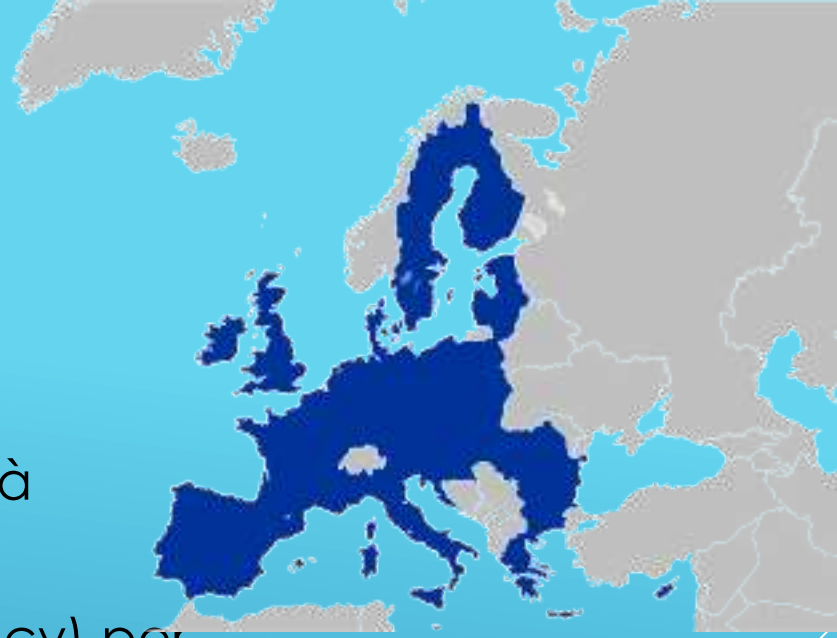


- Liceità, correttezza **e trasparenza**
- Trattamenti solo per scopi determinati, espliciti e legittimi **(limitazione della finalità)**
- Principio di necessità **(minimizzazione dei dati)**
  - conservati solo per il tempo strettamente necessario **(limitazione della conservazione)**
- Dati esatti e aggiornati **(esattezza dei dati)**

PRINCIPI FONDAMENTALI

CAF confsal

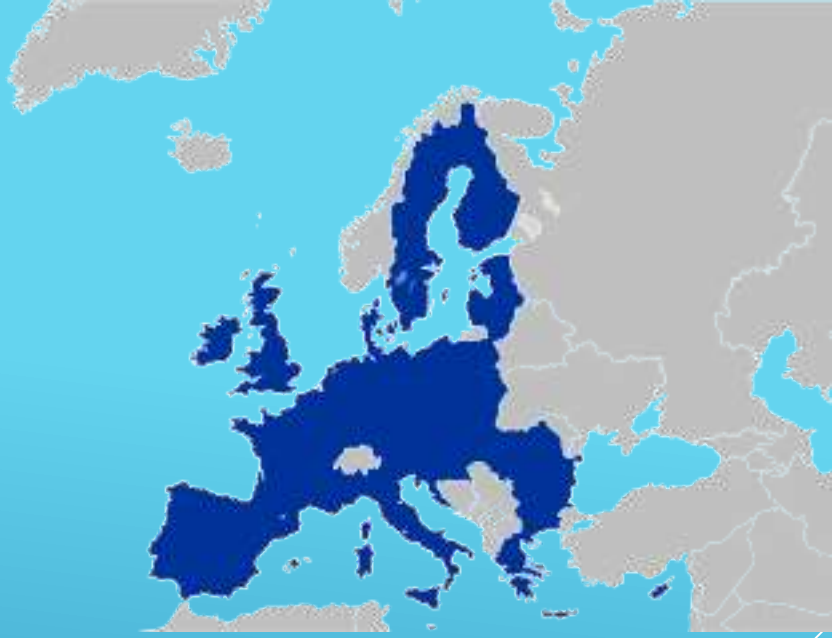
In **grassetto bianco** sono evidenziate le novità e le specificazioni del GDPR



- Obblighi di sicurezza vs. distruzione, perdita, accesso non autorizzato, trattamento illecito o non conforme alle finalità **(integrità e riservatezza)**
- ~~Intervento ex ante dell'Autorità di controllo (Garante Privacy) per autorizzare/verificare preventivamente determinati tipi di trattamenti~~ **(accountability)**

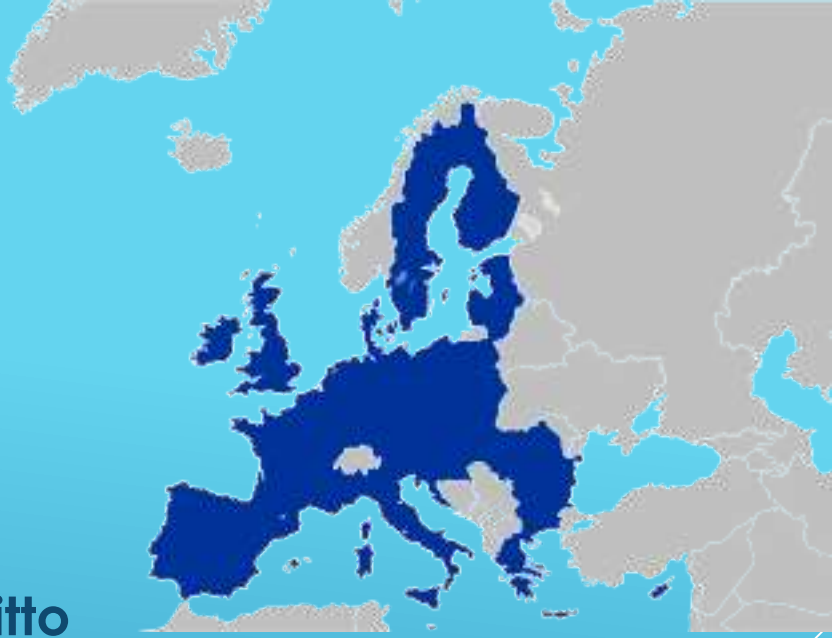
PRINCIPI FONDAMENTALI

In **grassetto bianco** sono evidenziate le novità e le specificazioni del GDPR



I DIRITTI DELL'INTERESSATO

In **grassetto bianco** sono evidenziate le novità e le specificazioni del GDPR



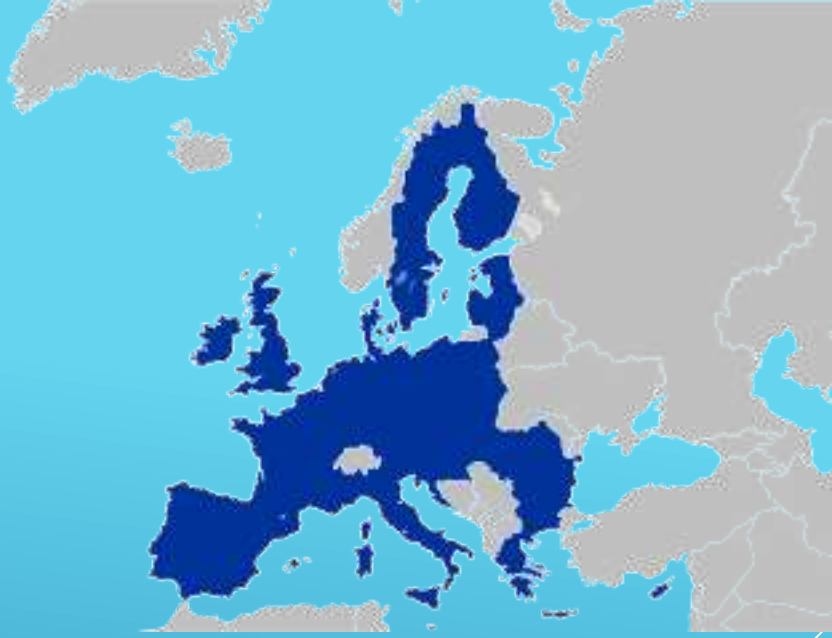
I Diritti dell'interessato

Il Regolamento 679/2016 ha da un lato ribadito e dall'altro introdotto tutta una serie di diritti in capo all'interessato.
Se per un verso sono stati ripresi e rafforzati il **diritto alla trasparenza del trattamento , il diritto di accesso ai dati, il diritto di rettifica dei dati personali e il diritto alla limitazione nonché di opposizione al trattamento**, **dall'altro verso le introduzioni del diritto all'oblio e del diritto alla portabilità** sono le previsioni di maggior rilievo volte a garantire una sempre più ampia tutela dell'interessato.

I DIRITTI DELL'INTERESSATO

CAF confsal

In **grassetto bianco** sono evidenziate le novità e le specificazioni del GDPR



Diritto all'Oblio - Art. 17

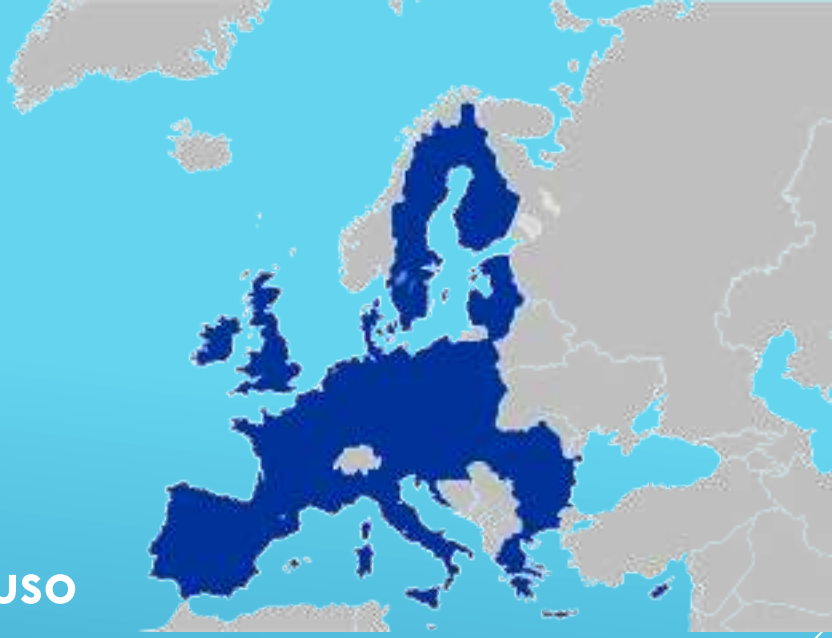
L'interessato ha diritto di ottenere la cancellazione senza ingiustificato ritardo quando:

- **I dati non siano più necessari rispetto alle finalità per le quali erano stati raccolti**
- **Il consenso al trattamento venga revocato**
- **L'interessato si opponga al trattamento**
- **I dati siano trattati illecitamente**
- **I dati debbano essere cancellati per legge**

I DIRITTI DELL'INTERESSATO

CAF confsal

In **grassetto bianco** sono evidenziate le novità e le specificazioni del GDPR



Portabilità dei dati - Art. 20

L'interessato ha diritto di ricevere in un formato strutturato di uso comune e leggibile da dispositivo automatico i dati che lo riguardano e di trasmettere tali dati ad un altro titolare senza impedimenti da parte del titolare che li ha forniti

I DIRITTI DELL'INTERESSATO

CAF confsal

In **grassetto bianco** sono evidenziate le novità e le specificazioni del GDPR

LE TIPOLOGIE DI DATI

CAF confsal

In **grassetto bianco** sono evidenziate le novità e le specificazioni del GDPR

- **"dato personale":** qualunque informazione relativa a persona fisica identificata o identificabile (ad es. tramite riferimento ad altre informazioni)
- **"dati sensibili":** dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a ~~partiti~~, sindacati, ~~associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale~~, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale **e i dati genetici e biometrici (art. 9 e C10 del GDPR)**
- **"dati giudiziari":** ……relativi a indagini, procedimenti e condanne penali

LE TIPOLOGIE DI DATI

CAF confsal

In **grassetto bianco** sono evidenziate le novità e le specificazioni del GDPR

I SOGGETTI

In **grassetto bianco** sono evidenziate le novità e le specificazioni del GDPR

- **"interessato":** la persona fisica cui si riferiscono i dati personali
- **"titolare":** il soggetto (anche non persona fisica) cui competono le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza (possibile la contitolarità, **previo specifico accordo sulla responsabilità**)
- **"responsabile"** il soggetto (anche non persona fisica) preposto (per iscritto) dal titolare al trattamento dei dati personali; **possibile la nomina di sub-responsabili**
- **"incaricato":** persona fisica autorizzata(per iscritto?) a compiere operazioni di trattamento dal titolare o dal responsabile **(non espressamente previsto ma comunque contemplato dal GDPR – art. 4.10)**
- **DPO = Data Protection Officer ("Responsabile" della Protezione dei Dati: ma non lo è!!): il problema dell'obbligatorietà (enti pubblici, oppure attività "principale" che comporta il monitoraggio degli interessati o il trattamento di dati sensibili o giudiziari su "larga scala")**

I SOGGETTI

CAF confsal

In **grassetto bianco** sono evidenziate le novità e le specificazioni del GDPR

INFORMATIVA

In **grassetto bianco** sono evidenziate le novità e le specificazioni del GDPR

- Deve essere preventiva ed includere (salvo informazioni già note all'interessato)
  - finalità, modalità e **base giuridica** (consenso, contratto, interessi vitali della persona interessata o di terzi, obblighi di legge dl titolare, interesse pubblico, interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati) del trattamento;
  - la natura obbligatoria o facoltativa del conferimento dei dati (con le conseguenze di un eventuale rifiuto a conferirli)
  - i soggetti o le categorie di soggetti che possono venirne a conoscenza e l'ambito di diffusione;
  - I diritti dell'interessato (accesso, rettifica, cancellazione, opposizione, **portabilità dei dati, ecc.) ➔ nell'informativa successiva all'ottenimento dei dati;**
  - gli estremi del titolare e, se designato del responsabile, nonché del **DPO**;
  - **se i dati sono trasferiti all'estero e attraverso quali strumenti. (eventuali BCR, ecc.)**

INFORMATIVA

In **grassetto bianco** sono evidenziate le novità e le specificazioni del GDPR

- **Informativa successiva (una volta ottenuti i dati), deve includere, oltre a quanto indicato nella precedente slide, (e salvo informazioni già note all'interessato):**
  - **Periodo di conservazione dei dati**
  - **Diritto di presentare un reclamo all'autorità di controllo**
  - **Eventuale trattamento mediante processi decisionali automatizzati (es: profilazione), indicando logica e conseguenze**
- Se i dati non sono raccolti presso l'interessato, ma presso terzi , l'informativa deve essere fornita presso l'interessato **entro un termine ragionevole (max 1 mese) oppure** al momento della registrazione o comunicazione dei dati a terzi e **deve indicare la fonte dei dati e la categoria a cui essi appartengono.**

INFORMATIVA

CAF confsal

In **grassetto bianco** sono evidenziate le novità e le specificazioni del GDPR

- **L'informativa deve essere concisa, trasparente, intellegibile e facilmente accessibile, ed avere un linguaggio chiaro e semplice**
- **Può anche essere fatta con pittogrammi o icone (si sta valutando un unico sistema europeo di icone)**
- **L'informativa è data, in linea di principio, per iscritto e preferibilmente in formato elettronico**

INFORMATIVA

CAF confsal

In **grassetto bianco** sono evidenziate le novità e le specificazioni del GDPR

CONSENSO

In **grassetto bianco** sono evidenziate le novità e le specificazioni del GDPR

- Deve essere libero, specifico, informato e inequivocabile
  - No tacito o presunto (solo dichiarazione o azione positiva)
  - No caselle pre-spuntate sul modulo
- Per i dati personali «semplici», deve essere ~~documentato per iscritto~~ **dimostrabile dal titolare**
- Per i dati sensibili, deve essere ~~in forma scritta~~ **esplicito (Il consenso è l'unica base giuridica utile per il trattamento dei dati sensibili.**
- **La richiesta di consenso deve essere chiaramente distinguibile (ad es: nella modulistica), in forma comprensibile, semplice e chiara**
- Ci sono casi in cui il consenso non è obbligatorio…

CONSENSO

CAF confsal

- Necessaria l'autorizzazione del Garante per il trattamento dei dati sensibili
  - Autorizzazione generale n. 2/2016 al trattamento dei dati idonei a rilevare lo stato di salute e la vita sessuale (anche) agli esercenti le professioni sanitarie (compresi gli psicologi)
- Notificazione del tra
  - Dati genetici, bion
  - Dati idonei a rivel […] prestazioni di servizi sanitari per via telematica relativi a banche di dati o alla fornitura di beni o alla fornitura di beni, […] rilevazione di malattie mentali, infettive e diffusive, sieropositività […]
  - Dati sensibili per finalità di selezione del personale conto terzi
  - […]
  - Verifica preliminare del Garante in caso di trattamenti di dati non sensibili o giudiziali ma che presentano rischi specifici (es: videosorveglianza)

Principio accountability

ALTRI ADEMPIMENTI PRIMA DI INIZIARE IL TRATTAMENTO

CAF confsal

In **grassetto bianco** sono evidenziate le novità e le specificazioni del GDPR

OBBLIGHI DI SICUREZZA

In **grassetto bianco** sono evidenziate le novità e le specificazioni del GDPR

- Misure di sicurezza
  - Informatiche ed organizzative
- Per ridurre al minimo i rischi di
  - Distruzione o perdita
  - Accesso non autorizzato
  - Trattamento non consentito o non conforme alle finalità
- Per preservare l'integrità e la disponibilità dei dati e il loro trattamento secondo le finalità e le modalità stabilite

OBBLIGHI DI SICUREZZA

CAF confsal

- Sono previste delle misure minime di sicurezza per tutti i titolari (artt 33-35 e All. B D.lgs. 196/03) e delle misure aggiuntive per gli esercenti le professioni sanitarie (art.22.6-7, All. B artt. 20-24 e 28-29)
  - Autenticazione informatica, con procedure di gestione delle credenziali, password cambiate ogni sei mesi (tre mesi per i dati sensibili e giudiziari)
  - Profili di autorizzazione degli incaricati, con aggiornamento periodico del trattamento consentito ai singoli incaricati e agli addetti ICT
  - Protezion ti periodici sistemi operativ
  - Sistemi c
  - Procedu
  - Tratta me
    - Conservazione separate e trattamento disgiunto dei dati sensibili – cifratura o codici identificativi
    - Obblighi in materia di supporti removibili
    - Disaster recovery entro 7gg.
    - Accesso controllato agli archivi cartacei, controllo e custodia di atti e documenti da parte degli incaricati

Principio accountability, ma comunque…….

OBBLIGHI DI SICUREZZA

In **grassetto bianco** sono evidenziate le novità e le specificazioni del GDPR

- **Data protection by design and by default (a monte)**
  - **Se rischi specifici**
    - **Privacy impact assessment (PIA)**
    - **Consultazione preventiva (opzionale) del Garante**
- **Dovere di notificazione al Garante (e di comunicazione all'interessato) le violazioni subite**
  - **Salvo improbabilità di un rischio per i diritti e le liberta delle persone**
- ~~**DPS (era già stato abolito nel 2012)**~~

Registro delle attività dei trattamenti art. 30 (molto più di un DPS ➔ accountability)

- **Il problema dell'obbligatorietà ➔ più di 250 dipendenti, oppure rischio per i diritti e le liberta dell'interessato oppure il trattamento non sia occasionale oppure trattamento di dati sensibili o giudiziari**

- **Nomina del DPO**
- **Opzionali codici di condotta e certificazioni**

OBBLIGHI DI SICUREZZA

CAF confsal

In **grassetto bianco** sono evidenziate le novità e le specificazioni del GDPR

- **Privacy by design e by default – Art. 25**
  - **Privacy by design: protezione prevista fin dalla progettazione di un processo aziendale (ad es. nuova applicazione)**
  - **Privacy by default (impostazione predefinita dell'organizzazione aziendale)**
    - **necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili per soddisfare i requisiti del regolamento e tutelare i diritti degli interessati**
    - **Analisi preventiva e documentata e impostazione a monte del trattamento stesso**
    - **valutazione dei rischi noti ed evidenziati e costruzione dei processi di trattamento conseguente**

OBBLIGHI DI SICUREZZA

CAF confsal

In **grassetto bianco** sono evidenziate le novità e le specificazioni del GDPR

- **Registri dei trattamenti – Art. 30**
  - **Redazione a carico del Titolare e del Responsabile (sono differenti l'uno dall'altro)**
  - **Dovrà contenere**
    - **i dati dei soggetti coinvolti (titolare, contitolare, rappresentante, responsabili, DPO)**
    - **Finalità del trattamento**
    - **Descrizione delle categorie di interessati e delle categorie di dati trattati**
    - **Elenco dei destinatari dati (anche in Paesi terzi)**
    - **Descrizione dei trasferimenti extra UE**
    - **Indicazione dei termini ultimi di cancellazione, ove possibile**
    - **Descrizione delle misure di sicurezza tecniche ed organizzative**

- **Non obbligatorio per imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9 (sensibili), paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10.**

OBBLIGHI DI SICUREZZA

CAF confsal

In **grassetto bianco** sono evidenziate le novità e le specificazioni del GDPR

- **Obbligo Notifica e Comunicazione in caso di Data Breach**
  - **Per violazione dei dati personali (data breach) si intende la divulgazione (intenzionale o non), la distruzione, la perdita, la modifica o l'accesso non autorizzato ai dati trattati da aziende o pubbliche amministrazioni.**
  - **Termine brevissimo: 72 ore (dalla scoperta)**
  - **Deve indicare almeno la natura della violazione, le categorie e il numero degli interessati e di registrazioni coinvolti, le probabili conseguenze, le misure adottate per porre rimedio alla violazione**
  - **Se la violazione è suscettibile di presentare un rischio elevato per i diritti e le liberta degli interessati è obbligatorio comunicare agli stessi la violazione senza giustificato ritardo, salvo che i dati fossero stati resi incomprensibili (ad es. cifratura) siano adottate misure per scongiurare il rischio di lesione ovvero la comunicazione richieda uno sforzo sproporzionato (ma allora è necessaria una comunicazione pubblica o similare)**

Eccezione: non è obbligatorio se improbabile che la violazione dei dati presenti un rischio per i diritti e le libertà delle persone

OBBLIGHI DI SICUREZZA

CAF confsal

In **grassetto bianco** sono evidenziate le novità e le specificazioni del GDPR

- **Valutazione d'impatto – Art. 35**
  - **Necessaria quando un trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone soprattutto se effettuato con nuove tecnologie**
  - **E' richiesta se c'è:**
    - **Valutazione sistematica e globale di aspetti personali, basata su trattamento automatizzato, compresa la profilazione**
    - **Trattamento su larga scala di dati sensibili e giudiziari**
    - **Sorveglianza sistematica su larga scala di aree accessibili al pubblico**
  - **Preventiva**
  - **Autorità di controllo può richiedere elenco delle tipologie di trattamenti per i quali è necessaria la valutazione d'impatto**
  - **Deve contenere almeno la descrizione sistematica dei trattamenti previsti e la finalità (compreso il legittimo interesse del titolare) la valutazione di necessità e proporzionalità del trattamento rispetto alla finalità, la valutazione dei rischi per i diritti e le libertà degli interessati, le misure per affrontare i rischi**

OBBLIGHI DI SICUREZZA

CAF confsal

In **grassetto bianco** sono evidenziate le novità e le specificazioni del GDPR

- **Misure tecniche adeguate/idonee – Art. 35**

  E' necessario mettere in atto misure tecniche ed organizzative adeguate a garantire un livello adeguato al rischio, quali ad esempio:

  - **Pseudonimizzazione**
  - **Cifratura**
  - **Capacità di assicurare su base permanente riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi di trattamento**
  - **Capacità di ripristinare tempestivamente disponibilità e accesso ai dati in caso di incidente fisico o tecnico**
  - **Implementazione di una procedura di test dell'efficacia delle misure**

OBBLIGHI DI SICUREZZA

CAF confsal

In **grassetto bianco** sono evidenziate le novità e le specificazioni del GDPR

- **Data Protection Officer – Art. 37**
  - **Obbligatoria la nomina per Pubbliche Amministrazioni e organismi pubblici, per chi opera monitoraggio sistematico degli interessati su larga scala, quando il trattamento si svolge su larga scala su dati sensibili e giudiziari**
  - **Deve avere conoscenze specialistiche**
  - **Deve essere coinvolto nelle questioni riguardanti il trattamento dei dati personali**
  - **Deve essere autonomo e indipendente**
  - **Deve disporre di un budget di spesa**
  - **Deve essere documentata la scelta con la quale viene nominato o non nominato il DPO (sia lato Titolare che lato Responsabile) linee guida WP29**

OBBLIGHI DI SICUREZZA

CAF confsal

In **grassetto bianco** sono evidenziate le novità e le specificazioni del GDPR

- Sanzioni civili 2050 cc (attività pericolosa, bisogna aver adottato tutte le misure idonee ad evitare il danno)
- Sanzioni amministrative ad esempio:
  - Omessa o incompleta informativa da €6.000 a €36.000
  - Omessa adozione delle misure minime di sicurezza: da €10.000 a €120.000
- Sanzioni penali (reclusione, nelle ipotesi più gravi fino a tre anni – con possibilità di estinzione del reato in via amministrativa)
- **Controlli anche tramite la GdF (ispezione in sede)**
- **Nuova sanzione fino a 10 o 20 ml di Euro e fino al 4% del fatturato mondiale**

PRIVACY: SANZIONI E CONTROLLI

CAF confsal

Thank You

CAF confsal