Ordine degli Psicologi
Regione Abruzzo

Regolamento 679/2016

ARGOCONSULT
passione d'impresa

21 Febbraio 2019

Ordine degli Psicologi
Regione Abruzzo

Programma

- Introduzione al Regolamento 679/2016
- I principi del nuovo regolamento
- La responsabilizzazione
- Concetti di base: definizioni
- Le categorie dei dati personali e il Registro dei trattamenti
- Informative e consensi
- Nomine: responsabile trattamento e DPO
- Privacy by design
- Privacy by default
- L'analisi dei rischi
- La valutazione di impatto
- Il data breach
- Modalità operative di intervento: il rispetto della privacy negli studi di
- Il rispetto del regolamento negli studi professionali

Introduzione normativa

Cosa è successo negli ultimi 10 anni?

Esplosione dei dati generati, raccolti, trattati

- ➔ Dati conservati per periodi indefiniti, molto lunghi, spesso “per sempre”
- ➔ Dati acquisiti e poi successivamente utilizzati per finalità completamente differenti da quelle dichiarate
- ➔ Tecnologie sempre più invasive (cloud computing, smartphone, gesolocalizzazione, biometria, …)
- ➔ Minacce sempre più frequenti alla sicurezza e alla privacy

Regolamento UE 679/2016

173	**Considerando**
99	**Articoli**

- Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE
- ***GDPR: General Data Protection Regulation***

Vantaggi

- Unificando il quadro normativo in materia di protezione dei dati personali, si potrebbero risparmiare **2,3 MILIARDI di Euro / Anno** in termini di semplificazione degli oneri amministrativi e degli adempimenti
- I dati personali dei 500 milioni di cittadini UE valgono circa l'8% del PIL Europeo

Applicazione Materiale e Territoriale

Il GDPR stabilisce le norme relative alla protezione delle **persone fisiche** a prescindere dalla *nazionalità* o dal *luogo di residenza* con riguardo al trattamento dei dati personali

Nonché le norme relative alla **libera circolazione** dei dati personali con la finalità essenziale di **proteggere i diritti e le libertà fondamentali** delle persone fisiche, in particolare il **diritto alla protezione dei dati personali**

Applicazione Materiale e Territoriale

Il GDPR non si applica al trattamento dei dati personali relativi a persone giuridiche

(imprese dotate di personalità giuridica, compresi il nome e la forma della persona giuridica e i dati di contatto di essa)

Ordine degli Psicologi
Regione Abruzzo

Applicazione Materiale e Territoriale

Il GDPR può applicarsi esclusivamente entro l'ambito di applicazione del diritto dell'UE

Non si applica nell'ambito di:
sicurezza nazionale / politica estera e di sicurezza comune dell'Unione

Dati Personali

***Tutte* le informazioni** (*qualsiasi informazione*) **relative a una persona fisica** (l'interessato) al fine di renderla identificata o identificabile

(compresi **i dati personali sottoposti a pseudonimizzazione** i quali possono essere attribuiti a una persona fisica mediante l'utilizzo di ulteriori informazioni)

Dati Personali

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

Principi del Regolamento

- Liceità, correttezza e trasparenza
- Limitazione della finalità
- Minimizzazione dei dati
- Esattezza
- Limitazione della conservazione
- Integrità e riservatezza
- Responsabilizzazione

- **Privacy by Design**
- **Privacy by Default**

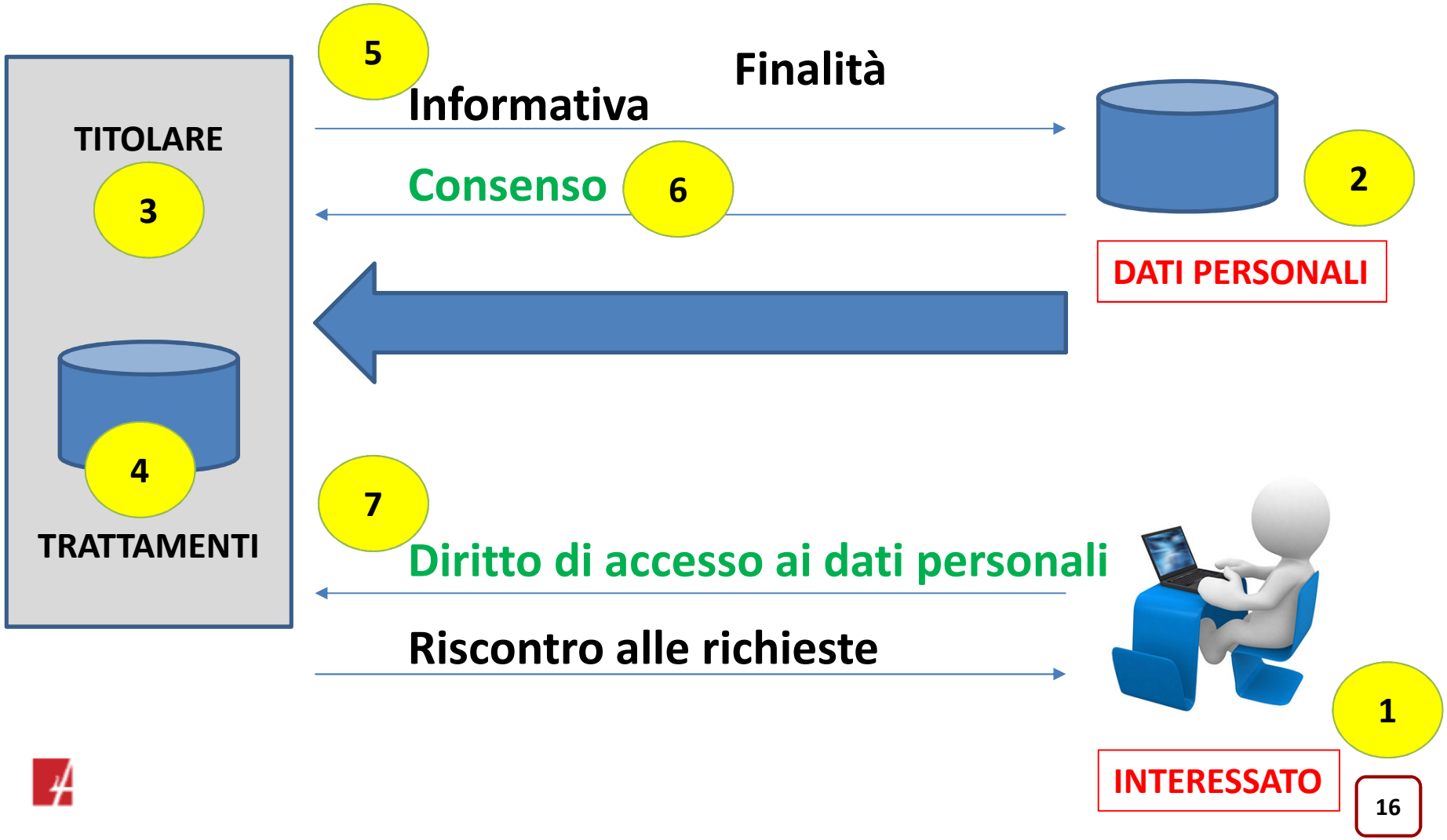
Ordine degli Psicologi
Regione Abruzzo

Base giuridica del trattamento

- Consenso espresso/ esplicito
- Esecuzione di un Contratto
- Obbligo legale
- Salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica
- Esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri
- Perseguimento del legittimo interesse del titolare o di terzi

Diritti dei Cittadini

Trasparenza



I ruoli nella privacy

Ruoli Privacy

- Interessati
- Titolare
- Responsabile del Trattamento (esterno)
- Amministratore di Sistema
- Delegati interni
- **DPO** – Data Protection Officer (Responsabile della Protezione dei Dati)
- «Incaricati»
- Destinatari

Ruoli Privacy

- Per tutti i ruoli di controllo servono nomine/ incarichi **scritti**

Titolare del trattamento

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

Responsabile del trattamento

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

- Il **Responsabile** deve essere in grado di offrire garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto le misure tecniche e organizzative rivolte a garantire che i trattamenti siano effettuati in conformità al GDPR.
- E' consentita la nomina di **sub-responsabili** del trattamento da parte di ciascun responsabile del trattamento per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano il Titolare ed il Responsabile primario
- I trattamenti devono essere eseguite nel rispetto di **istruzioni impartite per iscritto**

DPO

- informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento
- sorvegliare l'osservanza del GDPR
- supportare il titolare del trattamento nella tenuta del registro delle attività di trattamento attenendosi alle specifiche istruzioni impartite
- fornire, se richiesto, un parere in merito alla valutazione d'impatto
- cooperare con il Garante

DPO

- Deve possedere adeguata esperienza, conoscenza della problematica e capacità di effettuare audit approfonditi
- Agisce in totale indipendenza ed autonomia, si interfaccia direttamente con i vertici aziendali
- Può essere un soggetto interno alla struttura, oppure un soggetto esterno assunto in base ad un contratto di servizio

Regole principali

Informativa ⇔ Consenso

Da non confondere!

- Informativa rappresenta le “regole del gioco” del trattamento dei dati
- Deve sempre essere fornita
- Deve essere fornita “previamente” all’interessato
- Un’informativa corretta e completa è presupposto fondamentale per la validità del consenso
- Posso avere un’informativa senza consenso
- Posso avere informativa e consenso
- NON posso avere un consenso che non sia preceduto da idonea informativa

Ordine degli Psicologi
Regione Abruzzo

Registro di Trattamento

- Registro di trattamento del Titolare
- Registro di trattamento del Responsabile

ID	Categorie di interessati	Tipi di dati personali	Trattamento	Area	Finalità	Base giuridica	Database	SW di processamento	Profili autorizzati al trattamento	Informativa	Consenso	Tempi di Conservazione (termini di cancellazione	Misure di sicurezza tecniche e organizzative	Valutazione DPIA (SI/NO)	Destinatari	Responsabili Esterni del Trattamento	Rappresentante del Titolare	Contitolare	Paese terzo o organizzazione internazionale	Garanzie adeguate per il trasferimento
1	Dipendenti	Dati anagrafici e professionali, bancari, contabili/ fiscali, dati relativi alla salute	Gestione buste paga e contenuti contratto di lavoro	Segreteria	Gestione contratto di lavoro	Esercizio obblighi in materia di diritto del lavoro	Fascicoli dipendenti	Office Automation	Presidente Segretario Addetta segreteria Responsabile Qualità Responsabile Anticorruzione	Informativa Dipendenti (IDO)	Modulo Raccolta Consenso	10 anni dopo cessazione del rapporto di lavoro	Armadi chiusi Porta dell'archivio chiusa Credenziali su tutti i PC della sede Firewall Antivirus	NO	Istituti previdenziali, fiscali e assistenziali (INPS, INAIL, ...) Istituti bancari Assicurazioni	Consulente del lavoro (buste paga e dichiarazioni) Studio commerciale Società di formazione Fornitori manutenzione HW/SW	NA	NA	NA	NA
2	Dipendenti	Dati relativi alla salute	Gestione misure di sicurezza, visite mediche	Sicurezza	Gestione della salute e sicurezza sul lavoro	Esercizio obblighi in materia di diritto del lavoro	Archivio cartaceo sicurezza in sala archivio (idoneità sanitaria, certificati per malattie e infortuni)	Nessuno	RSPP Addetta segreteria	Informativa Dipendenti (IDO)	Modulo Raccolta Consenso	10 anni dopo cessazione del rapporto di lavoro	Armadi chiusi Porta dell'archivio chiusa	NO	Medico competente	Consulente sicurezza	NA	NA	NA	NA
3	Presidente Tesoriere Segretario Dipendente segreteria	Dati anagrafici	Comunicazione in poste italiane (postapay) e banca Comunicazione in banca ai fini del rilascio e utilizzo carta di credito (Presidente)	Segreteria	Accreditamento per esecuzione operazioni postali e bancarie	Consenso dell'interessato	Deleghe cartacee approvate dal Presidente archiviate in Segreteria	Nessuno	Presidente Segretario Addetta segreteria Responsabile Anticorruzione	Informativa Consiglieri (ICO)	Modulo Raccolta Consenso	10 anni dopo cessazione dell'incarico	Armadi chiusi Porta dell'archivio chiusa	NO	Banca Poste italiane	Nessuno	NA	NA	NA	NA
4	Iscritti	Dati anagrafici, contabili, certificati casellario giudiziale, dati legati all'istruzione	- Gestione iscrizioni, trasferimenti e cancellazioni dall'albo (Rilascio di delibere/ certificati di iscrizione, di trasferimento e di cancellazione) - Gestione delle attività di pertinenza (verifica casellario giudiziale per valutazione autocertificazione iscritto, ricerca al comune di nascita/ residenza con postalizzazione con insuccesso) - Pagamento quote e controllo stato pagamenti - Gestione comunicazioni agli iscritti (comunicazione a soggetti deputati agli invii massivi cartacei) - Gestione contenziosi - Comunicazione albo a cittadini che lo richiedono - gestione elezioni per il Consiglio dell'ordine	Segreteria	Gestione albo iscritti all'ordine	Obbligo legale	Albo Iscritti cartaceo conservato in sala archivio Albo iscritti elettronico su PC segreteria	Applicazione web-base della Federazione	Presidente Segretario Tesoriere Addetta segreteria Responsabile Qualità Responsabile Anticorruzione	Informatica Iscritti (IIO)	Modulo Raccolta Consenso	Conservazione perenne	Armadi chiusi Porta dell'archivio chiusa Credenziali su tutti i PC della sede Firewall Antivirus Linea di cortesia segreteria	SI	Procura Prefettura NAS ASL Assessorato alla Sanità Enpapi Ministero della Salute Synergo Presidenza della regione FNOPI Tutti gli OPI di Italia AGENAS COGEAPS Cittadini che richiedono accesso ad albo Poste italiane (o altre società di postalizzazione)	Provider per la gestione delle azioni formative Società di manutenzione hardware e software, in relazione alle necessarie manutenzioni, miglioramento etc. delle nostre infrastrutture Studi legali per la gestione di contenziosi	NA	NA	NA	NA

Analisi dei rischi

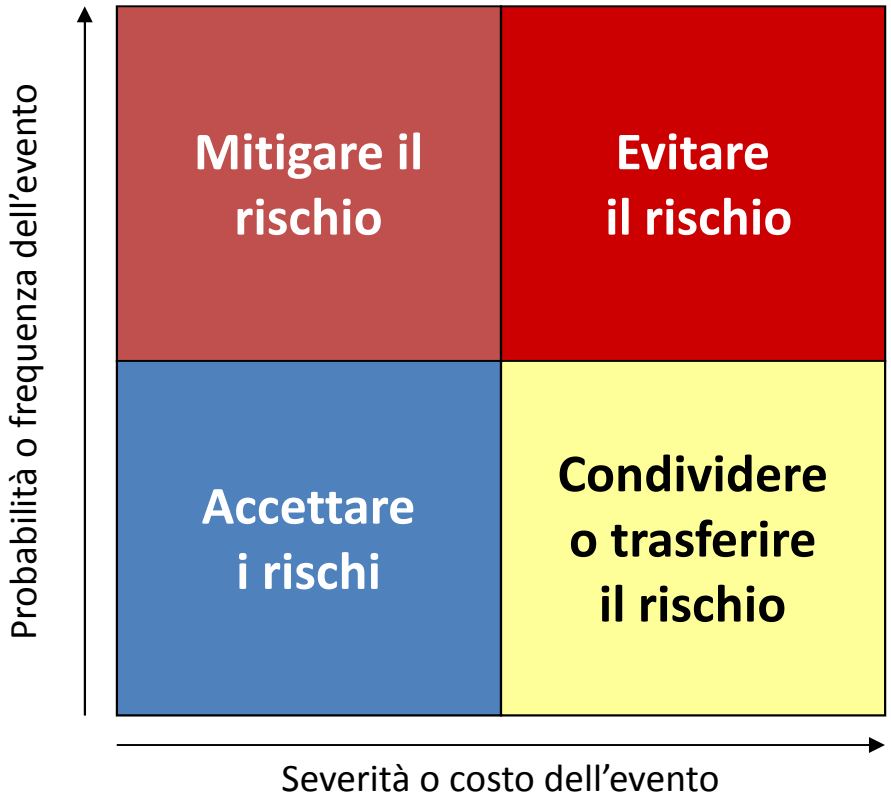
Cos'è un rischio ?

- (ISO GUIDE 73/2002): combinazione della probabilità di un evento e delle sue conseguenze
- (AS/NZS 4360: 2004): la possibilità che accada qualcosa che abbia un impatto sugli obiettivi
- (UNI 11230: 2007): l'insieme della possibilità di un evento e delle sue conseguenze sugli obiettivi
- (UNI ISO 31000: 2018): effetto dell'incertezza sugli obiettivi

Cosa posso fare del rischio ?

- L'organizzazione deve decidere come gestire il rischio.
- Partendo dai risultati dell'analisi del rischio sono identificati i controlli necessari a gestire il rischio. In particolare sono identificate le azioni necessarie a:
  - **Ridurlo**
  - **Evitarlo**
  - **Accettarlo**
  - **Trasferirlo**

La logica del risk management



Le condizioni

Il **RISK MANAGEMENT** deve:

1. essere integrato nella **cultura** dell'organizzazione
2. essere una attività a conduzione direzionale e trovare impiego all'interno della **strategia** dell'organizzazione
3. essere un processo **inclusivo, continuo e graduale** che costruisca un sistema di gestione
4. essere sostenuto da **competenze** tecniche specifiche
5. essere oggetto di **project management**

Sicurezza

SICUREZZA

Riservatezza: accessibile solo a chi è autorizzato, non accessibile a chi non è autorizzato

Integrità: la risorsa deve essere corretta, aggiornata, non corrotta o «falsificata»

Disponibilità: la risorsa deve essere sempre agevolmente disponibile a chi vi può lecitamente accedere

Resilienza: garantire che i sistemi informativi abbiano una continuità operativa

Sicurezza

Riservatezza: accessibile solo a chi è autorizzato, non accessibile a chi non è autorizzato

Integrità: la risorsa deve essere corretta, aggiornata, non corrotta o «falsificata»

Disponibilità: la risorsa deve essere sempre agevolmente disponibile a chi vi può lecitamente accedere

Resilienza: garantire che i sistemi informativi abbiano una continuità operativa

- **Rottura di un hard disk**
- **Virus**
- **Assenza di password**
- **Profili mal configurati**
- **Perdita di chiavetta USB**
- **Furto di PC**
- **Sostituzione di un PC**
- **Assenza dell'incaricato**
- **Comunicazione di password**
- **Modifica di documento protocollato**
- **Furto di documenti**
- **Pubblicazione illecita su Internet**
- **Accesso a dati giudiziari**

Regolamento UE 679/2016

Secondo il GDPR i momenti di valutazione del rischio sono diversi e devono seguire perlomeno due percorsi distinti.

Un insieme base di misure deve essere individuato e stabilito come applicabile **per tutti i trattamenti di dati personali** che si andranno a innescare, indipendentemente dalle loro caratteristiche.

Quelli che rientrano in una serie di condizioni circostanziate nell'**articolo 35** dovranno poi essere soggetti a una **valutazione d'impatto** preliminare alla loro attivazione, subordinandola a un contenimento di eventuali rischi ("rischio accettabile").
Questa valutazione deve inoltre essere riesaminata nel caso cambino le condizioni analizzate.

Responsabilizzazione

Considerando n° 84

A

Per potenziare il rispetto del presente regolamento qualora i trattamenti possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, **il titolare del trattamento dovrebbe essere responsabile dello svolgimento di una valutazione d'impatto sulla protezione dei dati per determinare, in particolare, l'origine, la natura, la particolarità e la gravità di tale rischio**. L'esito della valutazione dovrebbe essere preso in considerazione nella determinazione delle opportune misure da adottare per dimostrare che il trattamento dei dati personali rispetta il presente regolamento. Laddove la valutazione d'impatto sulla protezione dei dati indichi che i trattamenti presentano un rischio elevato che il titolare del trattamento non può attenuare mediante misure opportune in termini di tecnologia disponibile e costi di attuazione, prima del trattamento si dovrebbe consultare l'autorità di controllo.

Gestione del rischio

Considerando n° 90

B

In tali casi, è opportuno che il titolare del trattamento effettui una valutazione d'impatto sulla protezione dei dati prima del trattamento, per valutare la particolare **probabilità e gravità del rischio**, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento e delle fonti di rischio. La valutazione di impatto dovrebbe vertere, in particolare, anche sulle **misure**, sulle **garanzie** e sui **meccanismi** previsti **per attenuare tale rischio** assicurando la protezione dei dati personali e dimostrando la conformità al presente regolamento

Gestione del rischio per la privacy

Il GDPR prevede che i titolari definiscano e gestiscano:

- processi di **assessment** periodici dei trattamenti esistenti
- processi di valutazione di nuovi trattamenti secondo l'approccio "**Privacy by design**"
- **valutazioni periodiche dell'impatto** di specifici trattamenti e dei rischi esistenti in materia di sicurezza
- misure di sicurezza idonee definite sulla base di un approccio "**Risk based**"
- eventuali incidenti "**data breach**" secondo un metodo strutturato
- **audit** periodici dell'effettiva attuazione ed efficacia delle misure di sicurezza in essere
- tutte le eventuali **richieste degli interessati**, con particolare attenzione ai nuovi diritti quali il "diritto all'oblio" e il "diritto alla portabilità" dei dati.

Privacy by Design e by Default

Configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili al fine di tutelare i diritti degli interessati, rispettando il principio di minimizzazione.

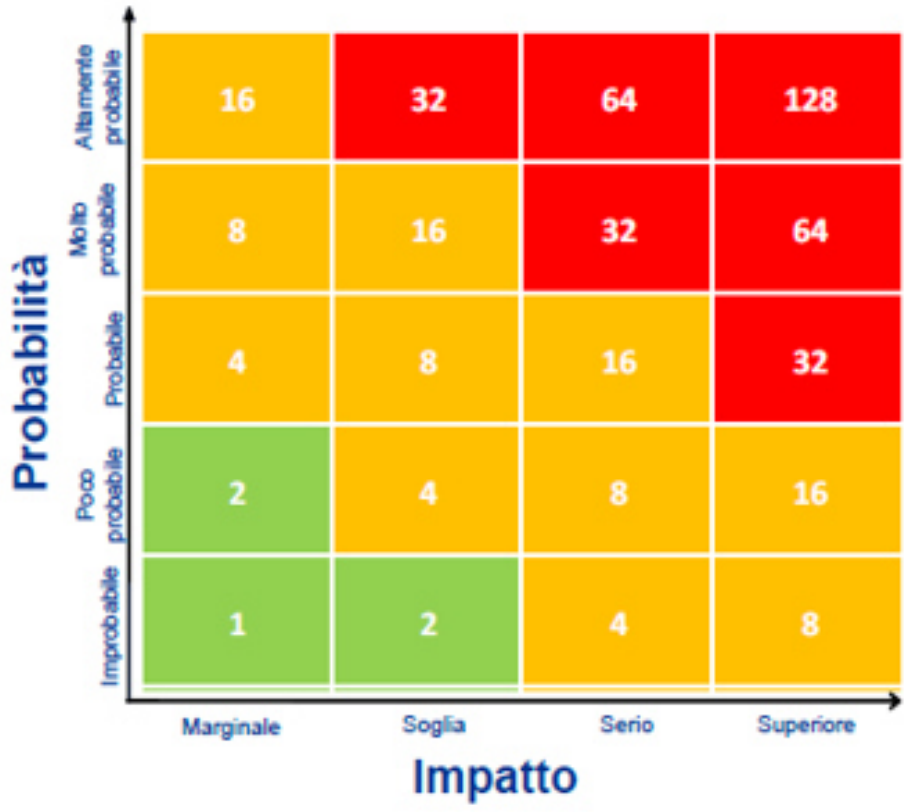
Tutto questo deve avvenire a monte, prima di procedere al trattamento dei dati vero e proprio e richiede, pertanto, un'analisi preventiva e un impegno applicativo da parte dei titolari che devono sostanziarsi in una serie di attività **specifiche e dimostrabili**.

Quali sono i tipi di rischio?

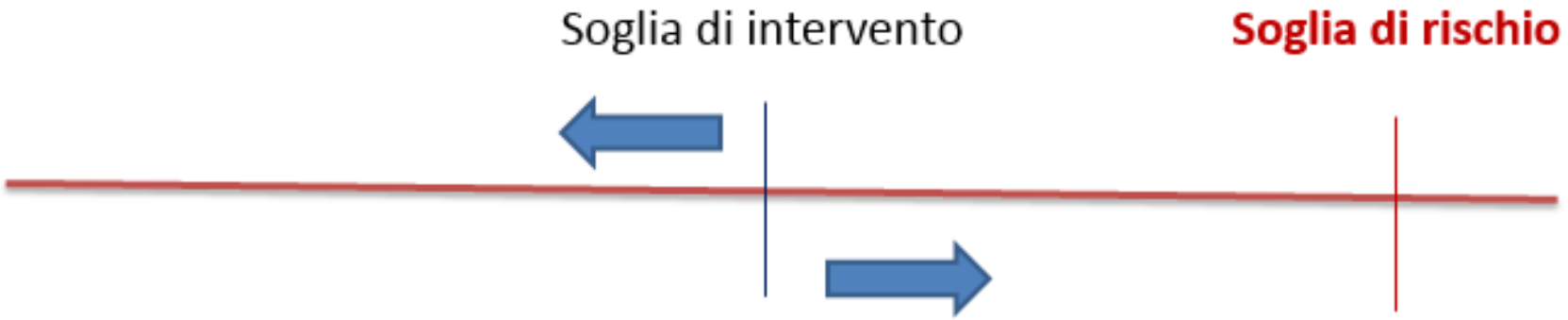
Rischi Privacy

- Distruzione o perdita di dati
- Accesso non autorizzato
- Trattamento non consentito
- Trattamento non conforme alle finalità delle raccolta

Regolamento UE 679/2016



Rischio accettabile



Misure di sicurezza

Misura di sicurezza: "*procedura operativa che prevede di disabilitare un utente all'atto delle dimissioni*"

- Qualcuno la mette in atto questa procedura operativa ?
- Con che frequenza ?
- E' stato individuato chi precisamente deve disabilitare gli utenti ?
- C'è qualcuno che comunica a chi di dovere quali utenti hanno dato le dimissioni ?
- Viene prodotto un resoconto/certificazione delle operazioni effettuate ?
- Come si procede in caso di assenza/indisponibilità di chi deve disabilitare ?

Misure di sicurezza

Misura di sicurezza: "*installazione firewall*"

- Il firewall offre un livello adeguato di protezione perimetrale ?
- Vengono effettuati periodicamente dei "Security Test" per valutare l'adeguatezza della protezione perimetrale ?
- Qualcuno analizza periodicamente i file di log ?
- Che azioni vengono intraprese a fronte dell'analisi dei file di log ?
- Le regole del firewall sono tenute aggiornate ?
- Il firewall è collegato ?
- Il comportamento del firewall è diverso da un filo di rame ?

Misure di sicurezza

Misura di sicurezza: "*archiviazione documentale*"

- Esiste un sistema di controllo documentale per archiviazione e gestione accessi ?
- Il sistema adottato è efficace ?
- Quanti test sono stati condotti per accertarsi della qualità del sistema ?
- Sono stati chiaramente identificati i flussi di gestione ?
- Quale assistenza tecnica serve l'organizzazione ?

Art. 35 – Valutazione d'impatto sulla protezione dei dati

Quando il trattamento, per la sua natura, il suo oggetto, o le sue finalità, presenta rischi specifici per i diritti e le libertà degli interessati, il titolare del trattamento effettua una valutazione d'impatto del trattamento previsto sulla protezione dei dati personali

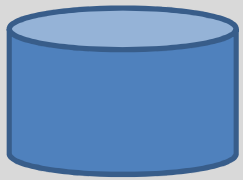
Data Breach

AUTORITA' DI CONTROLLO

Sanzione fino a 1.000.000 di Euro o fino al 2% del fatturato mondiale

Controllo da parte del Responsabile della protezione dei dati

TITOLARE



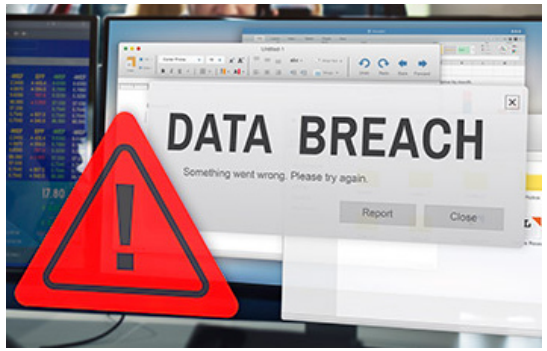
VIOLAZIONE

INTERESSATO

"Violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati o comunque elaborati "

Esempi di violazioni

- Perdita di dati
- Furto di dati (elettronici/ cartacei)
- Alterazione di documenti ufficiali
- Invio di dati all'esterno
- Intercettazione di dati
- Accesso abusivo al sistema



Data Breach

In caso di violazione dei dati personali, il titolare notifica la violazione all'autorità di controllo senza ritardo, ove possibile entro le 72 ore dal momento in cui ne è venuto a conoscenza

Norme per gli Incaricati

Norme per gli Incaricati

INCARICATI

- Uso degli strumenti di trattamento elettronici

Norme per gli Incaricati

- Gli Incaricati sono autorizzati **ad effettuare esclusivamente i trattamenti di dati personali che rientrano nell'ambito di trattamento definito per iscritto** e comunicato all'atto della designazione, con la conseguente possibilità di accesso ed utilizzo della documentazione cartacea e degli strumenti informatici, elettronici e telematici e delle banche dati aziendali che contengono i predetti dati personali

Norme per gli Incaricati

- Il trattamento dei dati personali deve essere effettuato **esclusivamente in conformità alle finalità previste e dichiarate** e, pertanto, in conformità alle informazioni comunicate agli interessati, secondo quanto stabilito dal **Registro dei Trattamenti**

Norme per gli Incaricati

- L'Incaricato del trattamento dei dati personali deve prestare particolare attenzione all'**esattezza** dei dati trattati e, se sono inesatti o incompleti, deve provvedere ad aggiornarli tempestivamente

Norme per gli Incaricati

- Ogni Incaricato del trattamento dei dati personali è tenuto ad osservare tutte le **misure di protezione e sicurezza atte a evitare rischi** di distruzione o perdita anche accidentale dei dati, accesso non autorizzato, trattamento non consentito o non conforme alle finalità della raccolta
- **Archiviazione elettronica** in cartelle con accesso limitato (non su folder comuni)

Norme per gli Incaricati

- Gli Incaricati che hanno ricevuto le **credenziali di autenticazione** per il trattamento dei dati personali, debbono conservare con la **massima segretezza** le componenti riservate delle credenziali di autenticazione (password) e i dispositivi di autenticazione in loro possesso e **uso esclusivo**

Norme per gli Incaricati

- La password deve essere composta da **almeno otto caratteri** oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito
- La componente riservata delle credenziali di autenticazione (password) **non deve contenere riferimenti agevolmente riconducibili all'incaricato**
- La **password va cambiata** con frequenza stabilita dal Regolamento per l'uso degli strumenti informatici (almeno ogni sei mesi)

Norme per gli Incaricati

- Gli incaricati del trattamento non debbono in nessun caso **lasciare incustodito e accessibile** lo strumento elettronico durante una sessione di trattamento dei dati personali
- Attivare lo **screensaver** (dotato di password) prima di allontanarsi dalla postazione di lavoro
- **Non lasciare incustodita la postazione** durante le attività fatte in remoto sulla postazione stessa da ditte esterne autorizzate

Norme per gli Incaricati

INCARICATI

- Uso degli strumenti di trattamento cartacei

Norme per gli Incaricati

- I documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici **non devono essere portati al di fuori dei locali** individuati per la loro conservazione se non in casi del tutto eccezionali, e nel caso questo avvenga, l'asportazione deve essere ridotta al tempo minimo necessario per effettuare le operazioni di trattamento
- Per tutto il periodo in cui i documenti sono al di fuori dei locali individuati per la loro conservazione, l'incaricato del trattamento **non dovrà lasciarli mai incustoditi**
- I documenti non devono essere mai lasciati **incustoditi sul tavolo** durante l'orario di lavoro

Norme per gli Incaricati

- L'incaricato deve controllare che i documenti, composti da numerose pagine o più raccoglitori, siano sempre **completi e integri**
- Al termine dell'orario di lavoro l'incaricato del trattamento deve **riportare tutti i documenti nei locali individuati per la loro conservazione**
- Archiviazione cartacea in armadi/stanze chiuse e relativa gestione possesso chiavi
- **Va definito lo schema di archiviazione per ogni stanza/ funzione →** da decidere unicamente insieme al Responsabile del Trattamento e al DPO

Norme per gli Incaricati

- Si deve adottare ogni cautela affinché ogni persona non autorizzata, non possa venire a conoscenza del contenuto di documenti
- Per evitare il rischio di diffusione dei dati personali, si deve **limitare l'utilizzo di copie fotostatiche**
- Evitare di fare stampe/ fotocopie in **unità centrali** senza poi prelevare i documenti
- E' vietato far uso di **carta riciclata** su documenti cn dati personali
- Particolare cautela deve essere adottata quando i documenti **sono consegnati in originale** a un altro incaricato debitamente autorizzato

Norme per gli Incaricati

- E' proibito discutere, comunicare o comunque trattare dati personali per **telefono**, se non si è certi che il destinatario sia un incaricato autorizzato a potere trattare i dati in questione o quando il telefono è utilizzato in luogo pubblico o aperto al pubblico
- Si raccomanda vivamente di **non parlare mai ad alta voce**, trattando dati personali per telefono, soprattutto utilizzando apparati cellulari, in presenza di terzi non autorizzati, per evitare che i dati personali possano essere conosciuti da terzi non autorizzati, anche accidentalmente

Norme per gli Incaricati

- L'incaricato dovrà osservare scrupolosamente tutte le misure di sicurezza già in atto, o che verranno **comunicate in seguito dal titolare o dal responsabile del trattamento**

Ordine degli Psicologi
Regione Abruzzo

Archivi cartacei

	Regolamento UE 679/2016 Tutela dei dati personali
	Mappa Archiviazione Documenti Cartacei MADC - Rev. 0 del 22/07/2018 Pag. 1 di 1

Funzione:		Responsabile Funzione	

N°	Archivio	Tipologia di documenti/ dati	Interessati	Responsabile archivio	Luogo di archiviazione	Criteri di protezione	Note e criticità

Sanzioni

Sanzioni

- Sanzioni amministrative pecuniarie fino a € 10M o per le imprese fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore. Casi:
  - Art. 8 – Consenso minori
  - Art. 11 – Privacy by design
  - Art. 25 – Privacy by default
  - Art.26-29 – Norme su titolari e responsabili
  - Art. 30 – Registri attività di trattamento
  - Art. 31 – 34 Sicurezza e Data breach
  - Art. 35 e 36 DPIA
  - Art 42 e 43 - Certificazioni

Sanzioni

- Sanzioni amministrative pecuniarie fino a € 20M o per le imprese fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore. Casi:
  - Artt. 5,6,7,9 – Principi base e consenso
  - Artt. 12-22 – Informativa e diritti interessati
  - Artt. 44-49 – Trasferimenti transfrontalieri e inosservanza di ordini dell'autorità

La privacy per lo Specialista Psicologo

Privacy per lo Specialista Psicologo

- Lo psicologo è un professionista che interviene sempre, per definizione, sulla **salute** di individui gruppi e comunità e per tale motivo ogni psicologo nel proprio lavoro entra necessariamente in contatto con **dati comuni (o identificativi)** e con **dati sensibili,** che assieme costituiscono l'insieme dei **dati personali** di un interessato.

Privacy per lo Specialista Psicologo

PRIMA di ogni prestazione professionale, **il professionista psicologo sarà quindi sempre obbligato** a:

- consegnare l'**informativa,** ovvero un documento in cui vengono chiarite tutte le informazioni, in modo adeguate e comprensibile, riguardanti: le modalità di **trattamento dei dati personali** alla luce del Regolamento europeo 2016/679, le prestazioni, le finalità e le modalità delle stesse, nonché circa il grado e i limiti giuridici della riservatezza alla luce del **consenso informato** secondo il Codice Deontologico

Privacy per lo Specialista Psicologo

Dopo la presentazione dell'informativa, dopo aver fornito tutti i chiarimenti necessari e le spiegazioni richieste, assicuratosi di aver adeguatamente informato l'interessato in merito a questioni giuridiche, deontologiche e professionali, lo psicologo deve richiedere esplicitamente e in modo chiaro e dimostrabile o l'opposizione o le **firme**:

- al **consenso informato** (art.24 o art.31 C.D.) e **l'accettazione del preventivo** (L. n.124/2017) → firma 1
- al **consenso al trattamento dei dati personali** (D.Lgs 196 del 2003 / GDPR 679/16) → firma 2

Privacy per lo Specialista Psicologo

DOPO la prestazione professionale, lo psicologo, nell'ambito del campo di applicazione del GDPR, è tenuto a trattare e conservare i dati nel proprio **archivio** secondo indicazioni specifiche e definite in un documento da redigere a cura di ogni professionista, la **valutazione d'impatto**

Privacy per lo Specialista Psicologo

L'archivio dovrà inoltre essere sempre suddiviso fra

- **dati personali del cliente/paziente**, soggetti a tutto quanto previsto dal GDPR e sempre dovuti in caso di richiesta del cliente/paziente, forniti dall'interessato direttamente o osservati e raccolti nella loro forma di dati grezzi generati da un "contatore intelligente" o altri elementi oggettivi di raccolta (ad es. scritti dell'interessato, fotografie, prodotti audio video, i punteggi grezzi di un test, risposte a questionari, i disegni, dati oggettivi di qualsiasi tipo) e
- **dati professionali dello psicologo**, legati alla sua attività, prodotti dal professionista, sempre soggetti a procedure di trattamento secondo il GDPR ma non necessariamente dovuti al cliente/paziente (appunti, relazioni, valutazioni, interpretazioni ecc..).

Privacy per lo Specialista Psicologo

Lo psicologo libero professionista, **dato l'esiguo numero di dati trattati e l'attività di norma svolta in modo individuale, è sempre Titolare del trattamento ma non è strettamente tenuto alla nomina di un DPO**

Come procedere

Progetto

1. Mappatura dei processi
2. Identificazione dati personali
3. Censimento dei trattamenti
4. Censimento e Analisi dei Sistemi Applicativi Informatici
5. Registri di trattamento
6. Informative e consensi
7. Analisi dei rischi
8. Valutazione di impatto
9. Designazione per i ruoli
10. Compliance parti terze
11. Procedure di supporto (gestione incidenti, cambiamenti, comunicazione dati extra UE,…)

Ordine degli Psicologi
Regione Abruzzo

Regolamento 679/2016

ARGOCONSULT
passione d'impresa

21 Febbraio 2019

Grazie