Rödl & Partner

Uno studio globale

IL REGOLAMENTO PRIVACY EUROPEO (GDPR)

I NUOVI ADEMPIMENTI E GLI ADEGUAMENTI ORGANIZZATIVI

Agenda

✓**Introduzione**:

- Il Nuovo Regolamento Privacy Europeo: la nuova rivoluzione culturale
- I nuovi principi del trattamento: l'Accountability
- Perché dimostrare la conformità al Regolamento?
- Come dimostrare l'Accountability? Le fasi dell'Assessment e della Remediation e Implementation

✓**La fase di Assessment**

✓**La fase di Remediation e implementation**

Più nel dettaglio:

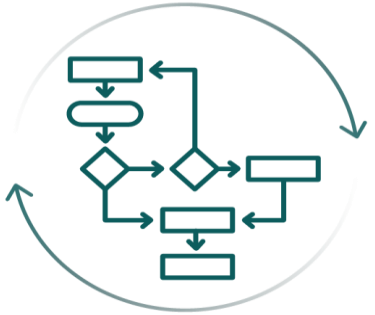
✓ **Cos'è cambiato e cosa fare ora? L'Assessment, la Remediation e Implementation su:**

- Il campo di applicazione del Regolamento
- L'informativa privacy
- Il consenso dell'interessato
- I diritti dell'interessato
- Il Trasferimento dati extra UE

✓ **Le ulteriori prove (e obblighi) dell'Accountability:**

- Misure organizzative adeguate:

- Policy e procedure
- Certificazioni e codici di condotta
- Nomine
- Formazione
- Data Protection Officer
- Data breach
- Registri



Cosa

Introduzione

Il Nuovo Regolamento Privacy Europeo

Il **25 maggio 2016**, dopo anni di trattative, è entrato finalmente in vigore il Nuovo Regolamento Europeo sulla Protezione dei Dati n. 2016/679 ("GDPR o Reg.").

Il GDPR:

- sostituisce dal 25.5.2018 la **Direttiva 95/46/EC** che disciplina il trattamento dei dati e, in larga misura, la normativa nazionale in tema di protezione dati, che ha implementato la direttiva, **introducendo un nuovo complesso di regole applicabili a tutti gli Stati Membri**;
- introduce **massivi cambiamenti alle leggi nazionali**, e quindi anche al D.Lgs.196/2003, impattando in modo significativo su tutte le società ed enti che trattano dati (titolari o responsabili) e su ogni aspetto delle relazioni tra le organizzazioni e il pubblico.

Il mancato adempimento al Regolamento sarà sanzionato a partire dal **25 maggio 2018**.

GDPR: la Rivoluzione Culturale

Introduzione

Il Nuovo Regolamento Privacy Europeo

Il Regolamento cambia integralmente il concetto di privacy, creando un radicale cambio di pensiero, una **rivoluzione culturale**:

- da **forma** (titolari e responsabili sono chiamati ad adempiere ad obblighi, formalità e misure minime di sicurezza **previsti dalla legge** per esimersi da responsabilità):

da … **fare quanto previsto dalla legge**

- a **sostanza** (titolari e responsabili sono chiamati a ridisegnare e ripensare la propria privacy – by design e by default – impostandola sin dall'inizio adottando **le migliori soluzioni adeguate** al loro **caso concreto** e allo specifico **livello di rischio**, per minimizzare il trattamento, solo così esimendosi da responsabilità)

a … **fare quanto valutato dal Titolare/responsabile la soluzione più adatta per il proprio caso concreto**

Introduzione

Il Nuovo Regolamento Privacy Europeo

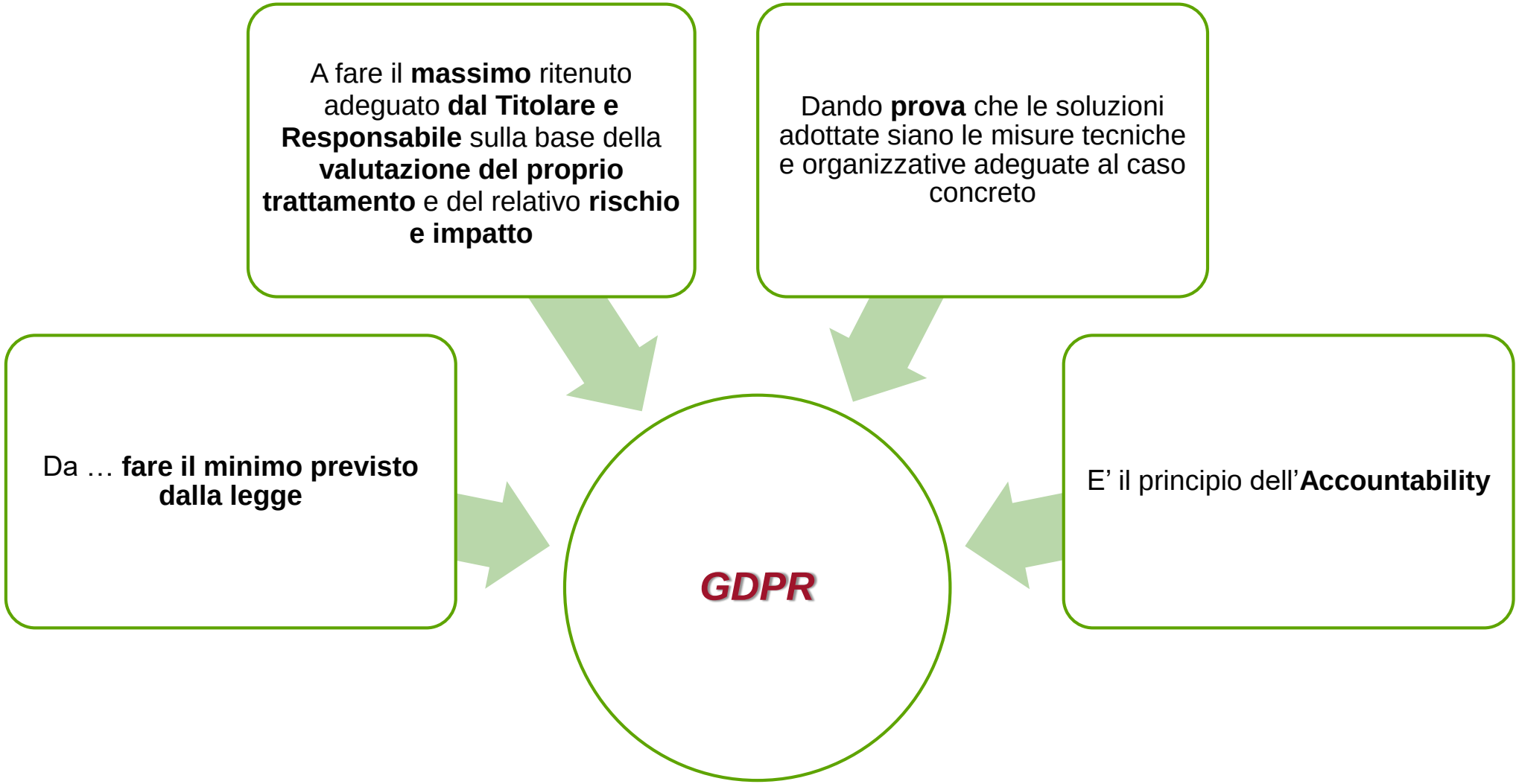
- Non possiamo più sentirci a posto facendo il minimo; **dobbiamo fare il massimo e dimostrare di averlo fatto:**

- **è** il nuovo principio del trattamento, quello di **Accountability, che impone l'obbligo di rispettare il Reg., i suoi principi e di provarlo**

- **SANZIONE FINO AL 4% FATT. MOND. ANNUO GRUPPO**

- Il Principio di Accountability fonda il nuovo VALORE della Privacy: da mera compliance a VALORE **competitivo**, **economico, reputazionale e asset**

Introduzione



Introduzione

D.Lgs. 196/2003	Reg. 2016/679	Conseguenze
Art. 11	Art. 5	
Principio di liceità e correttezza: trattamento secondo legge (es. previo consenso; senza consenso se contratto, obbligo di legge etc)	Idem. E' **principio di liceità, correttezza e trasparenza**	Invariato Sanzioni: **Reg: 83 c. 5 Reg (sanzioni amministrative fino a 20.000.000 eur o 4% fatturato annuo mondiale totale dell'esercizio precedente se superiore) – 83 c. 2** In tutti i casi di oggi: **Sanzioni penali locali** Es.: CP: inutilizzabilità; sanzione penale art. 167 (reclusione fino a 3 anni) **Sanzioni civili** (risarcimento danno imputabile): Il Titolare risarcisce il danno cagionato da trattamento in violazione del Regolamento, se imputabile
Principio di finalità: trattamento per le finalità in informativa	Idem. E' **principio di limitazione della finalità**	Invariato: idem
Principio di esattezza: misure per garantire dati aggiornati	Adozione di **procedure per cancellare e rettificare i dati inesatti**	Idem
Principio di pertinenza e non eccedenza: dati trattati solo pertinenti, completi e non eccedenti rispetto alle finalità, trattati per quanto necessario	Idem. E' il c.d. **principio di minimizzazione**	Fonda la privacy by design – art. 25 Reg
Principio di limitazione della conservazione: conservazione di dati in forma identificativa ammessa solo per tempo non superiore al conseguimento finalità	Idem	Invariato. Fonda la privacy by default - art. 25 Reg

Introduzione

D.Lgs. 196/2003	Reg. 2016/679	Conseguenze
Art. 11	Art. 5	
	Principio di integrità e riservatezza: Obbligo di garantire adeguata sicurezza dei dati mediante **misure tecniche e organizzative adeguate adottate dal Titolare a seconda del caso e del rischio concreto**	**Non bastano più le misure minime.** **Aumento campo e obblighi:** **maggiori obblighi Regolamento per Titolare e Responsabile in tema di garanzia e prova della sicurezza.** Sanzioni: Reg: 83 c. 5 Reg (**sanzioni fino a 20.000.000 eur o 4% fatturato annuo mondiale** totale dell'esercizio precedente se superiore)
	Principio di responsabilizzazione del Titolare e del Responsabile: Rispetto di tutti i precedenti principi e in grado di comprovarlo	**Maggiori Obblighi Regolamento per Titolare e Responsabile in tema di rispetto e relativa prova del rispetto dei principi del trattamento.** ▪ **Titolare e Responsabile hanno entrambi i maggiori obblighi degli artt. 24 – 32 Reg.** ▪ **Sanzione 83 c. 5 Reg**

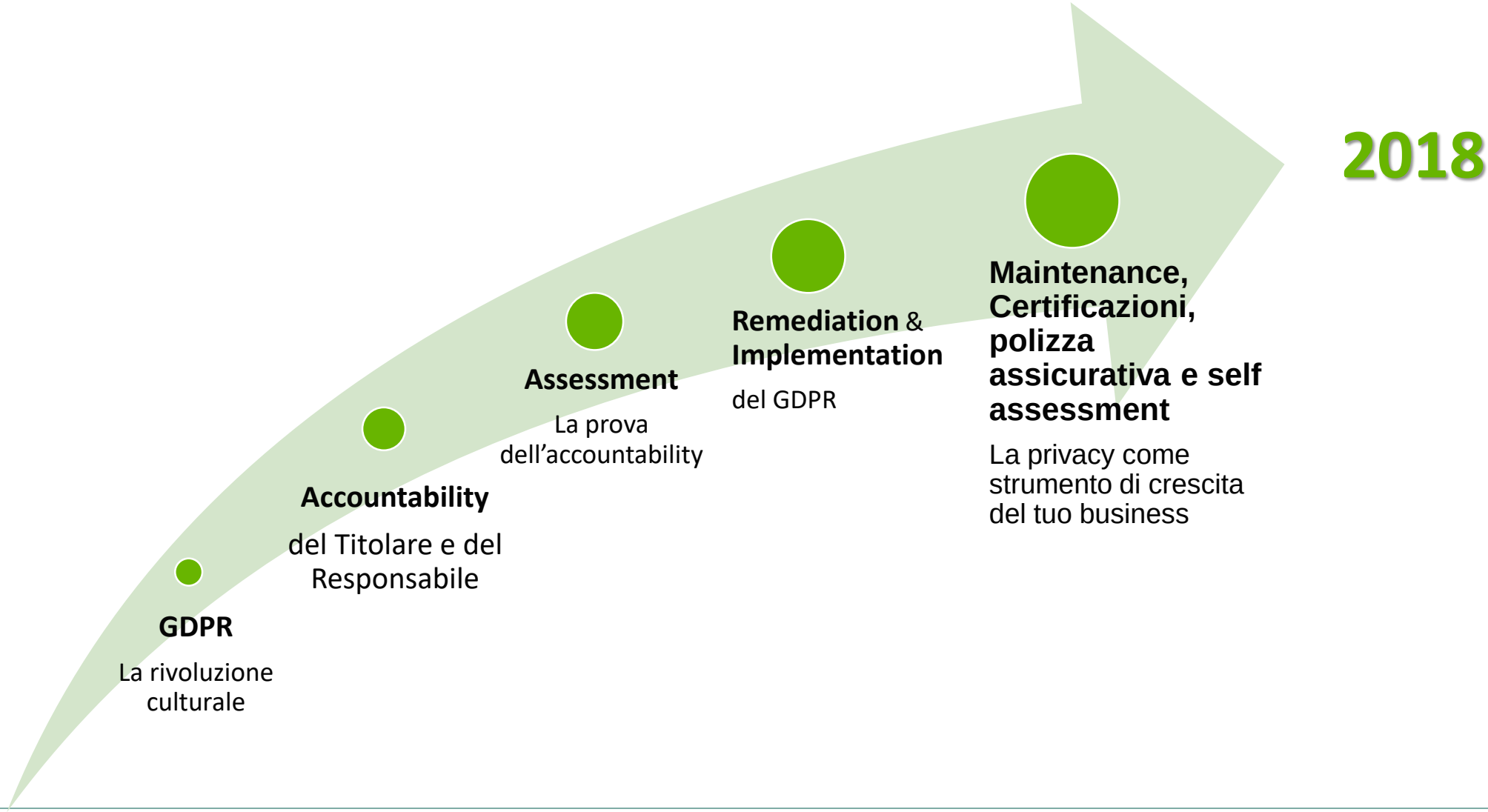
Perché

Perchè adempiere al principio dell'Accountability? Le 7 ragioni

1. **Compliance: evitare sanzioni (fino al *4% del fatturato annuale di gruppo*)**
2. **Sfruttare il valore economico dei big data**
3. **Motivi di business (opportunità di revisione dei processi e loro efficientamento/miglioramento/snellimento, opportunità di marketing e profiling)**
4. **Ottenere vantaggi reputazionali e competitivi**
5. **Ottenere valore etico per l'azienda**
6. **Guadagnare la fiducia del cliente**
7. **Avere maggiore sicurezza dei dati e quindi degli asset strategici**

Come

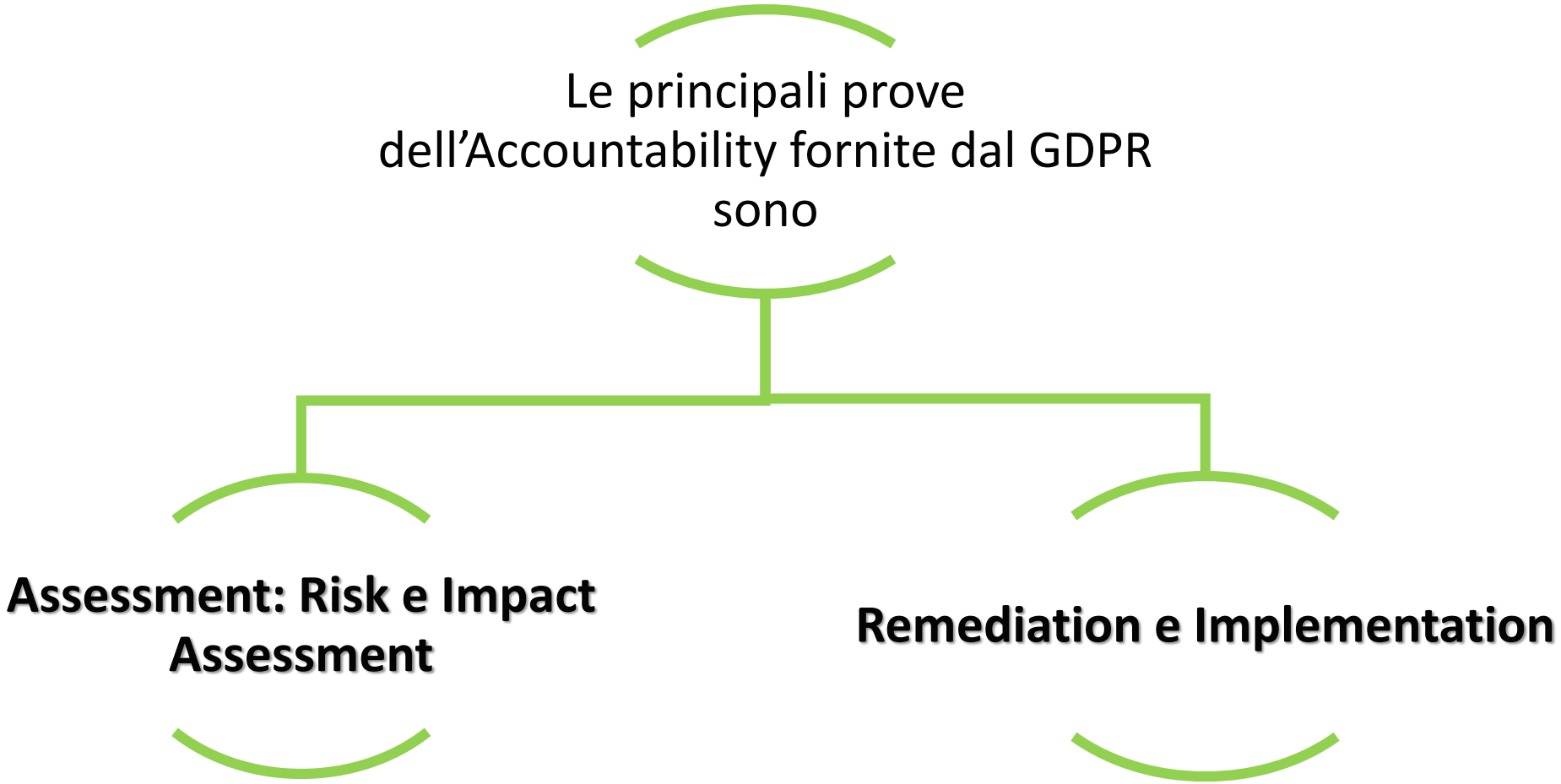
Il nuovo GDPR - Il metodo Rödl & Partner (*)



(*) Method and copyright proprietary

La fase di Assessment

Come provare di essere in linea con il principio dell'Accountability?



L'Assessment - Il metodo Rödl & Partner (*)

Come fare quindi un registro in linea con il GDPR?

1° Fase del Metodo Rödl & Partner: Privacy Assessment secondo la nuova normativa europea e la normativa ISO 27001, 29134, 30000 e ISDP 10003:2015

Risk Assessment

per l'individuazione e la valutazione dei rischi sulla sicurezza dei dati e delle libertà individuali

Privacy Impact Assessment

per la valutazione d'impatto dei trattamenti effettuati sulla protezione dei dati

Data mapping
mappatura dei dati, loro fonte ed uso

Documental Assessment
analisi di tutti i documenti e le procedure privacy (informative, consensi, procedure …)

Verbal Assessment
interviste ai soggetti coinvolti nel trattamento

System Assessment
analisi di tutti i sistemi e di tutte le misure adottate

Valutazione dei rischi
Per la sicurezza dei dati e le libertà individuali

Valutazione di impatto
(Privacy Impact Assessment) del trattamento sulle libertà individuali

Misure
Individuazione delle **misure tecniche e organizzative** adeguate per minimizzare i rischi

Report di Assessment:
Il report finale con la gap analysis tra le risultanze e la norma applicabile

D.Lgs. 196/2003	Reg. 2016/679	Conseguenze
	Art. 35-36	
	Come procedere? RISK ASSESSMENT ⬇ IMPACT ASSESSMENT ⬇ REMEDIATION&IMPLEMENTATION ⬇ ACCOUNTABILITY	

L'Assessment

D.Lgs. 196/2003	Reg. 2016/679	Conseguenze
	Artt. 32 e 35-36 (e Guidelines CNIL 2015, Guidelines ICO 2015, Guidelines WP 2017, ISO 31000, 27001, 29100, 27018, 19600, 21500ISO 29134, ISDP 10003:2015)	
Non è espressamente prevista dal CP, ma es. da: ISDP 10003:2015 UNI EN ISO/IEC 27001, 9001 UNI ISO 31000 (etc)	**Assessment dei rischi sulla sicurezza dei dati e sulle diritti e le libertà delle persone fisiche (art. 32):** ***Risk Assessment*** **Assessment dell' impatto sulla protezione dei dati (art. 35-36) :** ***Impact Privacy Assessment (PIA)*** **Cosa sono?** lo strumento che il GDPR individua quale prova prima per **dimostrare che il Titolare/Responsabile si sta responsabilizzando, sta agendo in modo accountable e lo sta facendo esaminando la propria situazione** (trattamenti, processi e progetti), individuando i rischi e adottando le soluzioni più idonee al caso concreto	Maggiori obblighi Titolare. Sanzioni: Reg: 83 c. 4 Reg (sanzioni fino a 10.000.000 eur o 2% fatturato annuo mondiale totale dell'esercizio precedente se superiore)

L'Assessment

D.Lgs. 196/2003	Reg. 2016/679	Conseguenze
	Art. 35-36	
	In cosa consistono? ***Risk Assessment*** ✓ data mapping (mappatura dati trattati, da chi, dove e come, con flow, procedure, documenti e registri) ✓ descrizione trattamenti previsti (natura, oggetto e contesto) ✓ valutazione necessità trattamenti rispetto a finalità ✓ finalità trattamenti ✓ Individuazione **rischi sulla sicurezza dei dati e sui diritti e le libertà individuali (perdita, modifica illegale, accesso, distruzione)** ***PIA*** *aggiunge* ✓ valutazione impatto dei trattamenti sulla protezione dei dati (i.e. *considerati i rischi* sulla sicurezza e sui diritti e sulle libertà individuali delle persone fisiche, **determinare probabilità e gravità del rischio e quindi l'impatto sulle libertà individuali (es. compressione diritto non discriminazione, libertà di pensiero),** considerando: ❑ Origine, natura, particolarità e gravità del rischio ❑ Natura oggetto e contesto del trattamento ✓ <u>Individuazione misure tecniche e organizzative</u> adottate o da adottare per attenuare i rischi ✓ riesame periodico dell'impatto e delle misure	

L'Assessment

	Reg. 2016/679	
	Art. 35-36	
	Focus sul Risk Assessment: Valutazione di rischio per la sicurezza dei dati e per le libertà individuali **Elenco di rischi** Il rischio (probabilità per gravità) è parametrato alla natura, oggetto, contenuto e finalità del trattamento e include (Cons. 83) ❑ **distruzione accidentale dei dati** ❑ **distruzione illegale** ❑ **perdita** ❑ **modifica** ❑ **rilevazione** ❑ **accesso non autorizzato** Il rischio si concreta se «deriva da trattamenti di dati personali suscettibili di **cagionare danno fisico, materiale o immateriale**» (Cons. 75) – PERICOLO DI DANNO (es. trattamento che possa comportare discriminazione, furto idendità, perdite finanziarie, danno alla reputazione, etc) **Valutazione Probabilità*Gravità rischio = Rischio** **Report di rischio**	

L’Assessment - Tools per il Risk Assessment (art. 32; cons. 74, 75, 76, 83)

Tipologia di trattamento: archivio clienti			
Danno: divulgazione non autorizzata	Probabilità	Gravità	Rischio
Interessi vulnerabili - minori	1	4	4
Trattamento dei Big Data	2	4	8
Trasmissione dei dati in rete e ai servizi di comunicazione	2	4	8

Tipologia di trattamento: archivio clienti			
Danno: divulgazione non autorizzata	Probabilità	Gravità	Rischio
Discriminazione	1	4	4
Furto o usurpazione d’identità	1	3	3
Perdite finanziarie	2	4	8
Pregiudizio della reputazione	2	3	6
Perdita della riservatezza dei dati protetti da segreto professionale	1	4	4
Decifratura non autorizzata della pseudonimizzazione	1	4	4
Qualsiasi altro danno economico o sociale significativo	1	2	2
Perdita dei diritti delle libertà e dell’esercizio del controllo dei dati da parte degli interessati	1	3	3
Trattamento dei dati sensibili	4	4	16

L'Assessment

	Reg. 2016/679	
	Art. 35-36	
	Quando fare un Risk Assessment? Secondo il Reg.: sempre (art. 32)	

L'Assessment – la PIA

D.Lgs. 196/2003	Reg. 2016/679 e WP29 248 del 4 ottobre 2017	Conseguenze
	Art. 35-36 **Focus sul Privacy Impact Assessment**	
	La PIA è **obbligatoria** per legge solo se comporta **un rischio elevato per i diritti dell'interessato, cosa che si verifica** in caso di: **1) Nuove tecnologie (es. cloud, apps, devices, IoT, soluzioni tecnologiche nuove)** **2) Valutazione sistematica e globale di aspetti personali dell'interessato, basata su trattamento automatizzato** : es. comportamento, gusti, abitudini, movimenti, preferenze (es. **profilazione, valutazione scoring comportamentale, match con banca dati, valutazione di dati relativi a soggetti vulnerabili)**	
	3) **Trattamento su larga scala di dati particolar**i o dati giudiziari cliniche, ospedali, tribunali (no medico o avvocato o operatore sanitario singolo)	
	4) **Sorveglianza sistematica su larga scala di zona accessibile al pubblico** ZTL, videosorveglianza in luoghi pubblici (no locali privati) **5) Trattamenti indicati dall'autorità Garante (elenco in attesa entro fine anno)**	

L'Assessment – la PIA

D.Lgs. 196/2003	Reg. 2016/679 e WP29 248 del 4 ottobre 2017	Conseguenze
	Art. 35-36 **Focus sul Privacy Impact Assessment**	
	Altri casi in cui la PIA è **obbligatoria:** **big data e modelling;** **match o combinazione di database e/o di insiemi di dati derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dal consenso iniziale (come avviene, ad esempio, con i Big Data);** **dati relativi a persone vulnerabili (es. minori, soggetti con patologie psichiatriche, richiedenti asilo, anziani, ecc.);** **utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative (es. device Internet of Things, riconoscimento facciale);** **trattamenti valutativi o di scoring;** **trattamenti che, di per sé, potrebbero impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto (es: screening dei clienti di una banca attraverso i dati registrati in una centrale rischi per stabilire la concessione di un finanziamento)**	

L'Assessment – la PIA

D.Lgs. 196/2003	Reg. 2016/679	Conseguenze
	Art. 35-36	
	La PIA contiene almeno: **a)** **una descrizione sistematica dei trattamenti** previsti e delle **finalità** del trattamento, compreso, ove applicabile, **l'interesse legittimo** perseguito dal titolare del trattamento; b) un **assessment** della **necessità** e proporzionalità dei trattamenti in relazione alle finalità; c) un **assessment** dei **rischi** per i diritti e le libertà degli interessati; e d) le **misure previste per mitigare i rischi**, includendo **misure tecniche e organizzative** e per garantire la protezione dei dati personali e dimostrare la compliance col GDPR, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.	

L’Assessment - Come svolgere la PIA: Guidelines del WP29 2017 e CNIL 2015

- identificare i dati
- identificare i trattamenti
- identificare se i trattamenti rispettano i Principi
- identificare chi accede ai dati e a chi vengono comunicati
- identificare i rischi sulla sicurezza dei dati
- identificare i rischi per le libertà individuali
- prevedere i controlli periodici

L’Assessment - Come svolgere la PIA: ISO/IEC 29134

Per ciascuna fase viene descritto:

- Obiettivo
- Input
- Output atteso
- Azioni
- Guida implementativa

L’Assessment - PIA Reports

PIA REPORT

- Executive summary
- ✓ Introduzione
- ✓ Descrizione dell’ambito
- Criteri per la valutazione del rischio
- Requisiti inerenti la privacy
- ✓ Valutazione del rischio
- ✓ Piano di trattamento del rischio
- Conclusioni e decisioni

PIA Public Summary

Aspetti per gli utenti a supporto di un consenso informato

- Tipi di informazioni trattate
- Panoramica del rischio residuo
- Riassunto delle misure di sicurezza e delle azioni attivate
- Informazioni di contatto e supporto

Esempio di PIA e Risk Assessment

Privacy Impact Assessment

Ruoli					Trattamento				Dati
Titolare	Contitolare	Responsabile esterno	Responsabile interno	Struttura del responsabile interno	Nome del trattamento	Descrizione del trattamento	Finalità del trattamento	Necessità e proporzionalità del trattamento	Categorie dei dati

	Soggetti					Extra UE			Cancellazione
Natura dei dati	Categorie degli Interessati	Soggetti interni coinvolti	Ruolo soggetti interni	Soggetti esterni coinvolti	Ruolo soggetti esterni	Trasferimento extra UE	Paese terzo	Garanzie per il trasferimento	Termini ultimi previsti per la cancellazione

Misure			Livello		Rischio			Esito			
Misure tecniche	Misure organizzative	Livello di adeguatezza misure organizzativ	Livello di adeguatezza misure tecniche	Livello medio adeguatezza misure tecnologiche e org.	Rischio per la sicurezza dei dati	Rischio di impatto sulle libertà	Misure previste per mitigare i rischi	Autorizzato da	Non autorizzato da	Da avviare consultazione preventiva Garante	Riesame avvenuto il

L'Assessment

D.Lgs. 196/2003	Reg. 2016/679	Conseguenze
	Art. 35-36	
	Esiti della PIA: **1) No rischio : trattamento effettuabile** **2) Rischio mitigabile: trattamento effettuabile dopo accorgimenti** Se a seguito della valutazione d'impatto sulla protezione dei dati, il titolare del trattamento ritenga che possano essere **adottate misure tecniche e organizzative adeguate** per attenuare il rischio, il trattamento verrà effettuato. **3) Rischio non mitigabile: trattamento non effettuabile (o effettuabile solo dopo autorizzazione Garante)** Se invece, il titolare del trattamento ritenga che non possano essere adottate misure tecniche e organizzative adeguate per attenuare il rischio, il trattamento potrà essere effettuato solo dopo aver preventivamente consultato l'autorità Garante Privacy.	

L'Assessment

	Reg. 2016/679	
	Art. 35-36	
	Quando fare il Privacy Impact Assessment? Secondo il Reg.: **solo in casi specifici (artt. 35-36)** (se il trattamento comporta un alto livello di rischio per i diritti degli interessati) Per provare l'Accountability del Titolare e del Responsabile: **sempre**	

Cosa fare ora

- **Adozione di Procedura/e di Risk e Impact Assessment e aggiornamento**

La fase di Remediation e Implementation

La Remediation e Implementation

A seconda delle risultanze della fase di Assessment:

- ***Remediation***: Revisione/adozione di tutta la documentazione privacy, le procedure e i sistemi
- ***Implementation***: Aggiornamento/Implementazione **misure organizzative adeguate**:
  - Certificazioni e codici di condotta
  - Politiche
  - Nomine
  - Formazione
  - Registri
  - Data breach
  - Data Protection Officer – focus linee guida WP 29

- Aggiornamento/Implementazione **misure tecniche adeguate**:
  - Misure IT
  - Privacy by design
  - Privacy by default

- Aggiornamento/Implementazione **controlli periodici, tools di self assessment** e polizze assicurative

L'Assessment - Il metodo Rödl & Partner (*)

Come provare di essere in linea con il GDPR?

2° Fase del Metodo Rödl & Partner: Remediation e Implementation

Remediation

Aggiornamento documentale, delle procedure e delle misure adottate

Implementation

Assistenza nell'implementazione delle misure tecniche, organizzative e di self-assessment

- **Revisione di tutte le informative, i consensi, le nomine, le procedure e i sistemi**
- Aggiornamento e implementazione delle **misure tecniche IT, Privacy By Default e By Design**
- Revisione e implementazione delle **misure organizzative** (formazione, procedure, nomine, registri…)
- Implementazione di **strumenti per la revisione periodica** (es., tool di Self-Assessment)
- Adozione di **Certificazioni, Codici di Condotta e Polizze** assicurative
- **Formazione** del personale, dei professionisti, C Level e DPO
- Nomina di **Data Protection Officer** (DPO), privacy officer e auditor europei certificati

Cosa è cambiato e cosa fare ora? L'Assessment, la Remediation e Implementation

Assessment, Remediation e Implementation su: Il campo di applicazione del Regolamento - Cosa è cambiato

Rödl & Partner

D.Lgs. 196/2003	Reg. 2016/679	Conseguenze
Art. 5	**Art. 2**	
Trattamento automatizzato e non di dati	Trattamento automatizzato e non di dati contenuti in archivio o destinati a figurarvi (insieme strutturato di dati)	Sostanzialmente invariato
Non effettuato da persona fisica per motivi esclusivamente personali	Idem	Invariato
Effettuato da chiunque è stabilito nel territorio dello Stato	Effettuato da Titolare o Responsabile stabilito nella UE	Riduzione campo: obblighi Regolamento esclusi per incaricati (?)
Art. 5	Art. 3	
Effettuato da chiunque è **stabilito extra UE se usa strumenti siti nella UE** (es. cookies)	Effettuato da Titolare o Responsabile non stabilito nella UE quando : 1) offrono beni e servizi (anche gratis) nell'Unione Europea (indici: *lingua, moneta, ordini in lingua UE*) 2) o effettuino attività di monitoraggio del comportamento di interessati nella UE (cd. *targeting, profilazione, tracciamento navigazione web*). 3) o forniscano di servizi di comunicazione elettronica nell'EU (Prop. E-Privacy 10.1.17)	Aumento campo e obblighi: Obblighi Regolamento estesi anche a titolari e responsabili extra UE **VERSO UNA NORMA UNIVERSALE?**

Assessment, Remediation e Implementation su: Il campo di applicazione del Regolamento - Cosa fare ora

Rödl & Partner

- **Assessment per verificare se si è soggetti al Regolamento**
- **Come? Mappatura dati, trattamenti, finalità, etc**
  - **e redazione procedure**
- **Quindi Remediation e Implementation**

Assessment, Remediation e Implementation su: Il dato personale - Cosa è cambiato

D.Lgs. 196/2003	Reg. 2016/679	Conseguenze
Art. 4	**Art. 4**	
Qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale	Idem. Ma precisa che è identificabile la persona fisica che può essere Identificata con … dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale	Maggiore chiarezza
Dati identificativi (es. nome, cognome, indirizzo, data di nascita, codice fiscale).	Idem. In aggiunta, anche: dati relativi all'ubicazione, un identificativo online	Maggiore chiarezza
Dati sensibili: 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	Ora definiti: Dati particolari: Idem.	Semplificazione obblighi Regolamento per titolari: informativa e consenso esplicito (non necessariamente scritto); nulla si dice su autorizzazione Garante. MA GLI STATI MEMBRI POSSONO DETTARE NG DIVERSE (Cons. 10)

Assessment, Remediation e Implementation su: Il dato personale - Cosa è cambiato

D.Lgs. 196/2003	Reg. 2016/679	Conseguenze
Art. 4	**Art. 4**	
Dati semisensibili: Biometrici	Sono dati particolari	Semplificazione Obblighi Regolamento per titolari: informativa e consenso esplicito (non necessariamente scritto); nulla si dice per prior check. MA GLI STATI MEMBRI POSSONO ADOTTARE NG DIVERSE
Dati giudiziari: idonei a rivelare provvedimenti in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato Sono tali solo i dati afferenti a procedimenti penali.	Idem.	Invariato. Stessi obblighi: Informativa (oltre a nomine e misure)
Art. 4	Art. 11	
Non sono dati soggetti alla normativa i dati anonimi. Non si parla di dati anonimizzati.	Idem. Con la precisazione che non sono dati anonimi i dati prima identificativi, ma poi anonimizzati. In tal caso, c'è trattamento e occorre informativa	Aumento obblighi: obblighi Regolamento titolari estesi per dati anonimizzati (informativa)

Assessment, Remediation e Implementation su: Il dato personale - Cosa è cambiato

D.Lgs. 196/2003	Prop. Reg. E-Privacy – Linee Guida Consiglio Europa 23.1.17	Conseguenze
Art. 4	**Art. 4 e cons 17**	
	Metadati (delle comunicazioni elettroniche): - i dati trattati in una rete di comunicazione elettronica per *trasmettere, distribuire o scambiare il contenuto delle comunicazioni elettroniche* , - i dati usati per *tracciare e identificare la fonte e il destinatario di una comunicazione*, - i dati relativi alla *localizzazione del dispositivo* - i dati generati dal servizio di comunicazione elettronica, es. la data, l'ora, la durata e il tipo di comunicazione.	Aumento obblighi: obblighi Regolamento titolari estesi per metadati e Big Data (risk assessment, PIA, Misure tecniche e organizzative per abbattere i rischi (es. pseudoanonimizzazione), informativa e consenso rinfrescato ogni **6 mesi per le comunicazioni elettroniche (Prop. E-Privacy)**
	Cons. 2: *«I **metadati** includono i numeri chiamati, i siti web visitati, la geolocalizzazione, l'ora, la data e la durata di una chiamata effettuata, ecc., consentendo di trarre conclusioni precise relativamente alla vita privata delle persone coinvolte nella comunicazione elettronica, come le loro relazioni sociali, le loro abitudine e attività quotidiane, i loro interessi, gusti, ecc.»*	
	Linee Guida - Big Data: *« un enorme quantitativo di dati raccolto e analizzato per identificare modelli comportamentali e prevedere il comportamento degli individui»*	

Assessment, Remediation e Implementation su: Il dato personale - Cosa fare ora

- **Assessment per verificare se si trattano dati identificativi, particolari, giudiziari, metadati, big data e dati anonimizzati : fare un Data Mapping**
- **In caso positivo, implementazione Regolamento e determinazione dei necessari adempimenti (remediation e implementation)**
- **Adozione procedure di classificazione dati trattati e gestione dei dati**

Assessment, Remediation e Implementation su: Il trattamento
Cosa è cambiato

Rödl & Partner

D.Lgs. 196/2003	Reg. 2016/679	Conseguenze
Art. 4	Art. 4	
Qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati.	Idem. In aggiunta si precisa che è trattamento anche: - **Profilazione**: trattamento automatizzato per analisi su rendimento professionale, situazione economica, salute, preferenze personali interessi, affidabilità, comportamento, ubicazione e spostamenti persona - **Pseudoanonimizzazione**: Trattamento effettuato in modo tale che i dati personali non possono più essere attribuiti a un interessato, però identificabile con informazioni aggiuntive conservate a parte e protette adeguatamente (distinzione database – cifratura/criptaggio)	**Aumento campo e obblighi :** **ampliamento della nozione di profilazione**

Assessment, Remediation e Implementation su: Il trattamento
Cosa fare ora

Rödl & Partner

- **Assessment per verificare se si pone in essere operazioni di trattamento**
- **In caso positivo, implementazione Regolamento**
- **Come? Mappatura dei trattamenti e redazione procedure e remediation**

Assessment, Remediation e Implementation su: L'informativa privacy - Che cosa è cambiato

D.Lgs. 196/2003	Reg. 2016/679	Conseguenze
Art. 13	**Art. 13**	
Per dati raccolti presso interessato: resa prima dell'inizio del trattamento e prima dell'acquisizione del consenso dell'interessato Per dati non raccolti presso l'interessato: al primo contatto o comunicazione dati	Idem Per dati non raccolti presso l'interessato: al primo contatto o comunicazione dati o entro 1 mese	Sanzioni: Reg: 83 c. 5 Reg (sanzioni fino a 20.000.000 eur o 4% fatturato annuo mondiale totale dell'esercizio precedente se superiore) CP: art. 161 CP (fino 36.000 eur)
Fornita per iscritto o anche solo verbalmente	Idem	Idem
Contiene: • Dati trattati • Finalità • Modalità • Natura obbligatoria o facoltativa del conferimento dati • Conseguenze di un eventuale rifiuto di rispondere • I soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi • diritti di cui all'articolo 7 • Estremi del Titolare e del Responsabile	Idem. In aggiunta: • **Riferimenti Responsabile Protezione Dati (DPO) – email, funzione, telef; no nome** • **Tempo di conservazione dati** • **Nuovi diritti interessato** • **Reclamo autorità di controllo** • **Esistenza di un processo decisionale automatizzato, compresa la profilazione e logica utilizzata nonché i rischi per interessati** • **Se la comunicazione di dati un obbligo legale o contrattuale o un requisito necessario** • **Trasferimento dati extra UE e giustificativo**	Maggiori Obblighi Regolamento per Titolare in tema di informativa. Sanzioni: Reg: 83 c. 5 Reg CP: art. 161 CP

Assessment, Remediation e Implementation su: L'informativa privacy - Cosa fare ora

- **Assessment documentale per raccolta informative (dipendenti, collaboratori, clienti, fornitori, prospect, utenti sito, abbonati)**
- **Gap analysis con norma applicabile**
- **Aggiornamento (o redazione) informative**
- **Adozione procedure per fornitura, gestione e conservazione informative**

Assessment, Remediation e Implementation su: Il consenso dell'interessato - Cosa è cambiato

Rödl & Partner

D.Lgs. 196/2003	Reg. 2016/679	Conseguenze
Art. 23 e 26	Art. 7 e 9; Cons. 42 e 43	
Consenso **dati comuni**: • **espresso** • **libero** (si – no) • espresso **specificamente** in riferimento ad un trattamento chiaramente individuato • **documentato per iscritto** (es. da operatore) • **informato** (con informativa) Consenso **dati sensibili**: • **espresso** • **libero** (si – no) • espresso **specificamente** in riferimento ad un trattamento chiaramente individuato • **scritto** • **informato** (con informativa) • **Autorizzazione Garante**	Consenso analogo sia per dati comuni che sensibili («**dati particolari**»): • espresso • autenticamente **libero** (si – no): **es. check box – no silenzio o caselle precompilate** • espresso **specificamente** in riferimento ad un trattamento chiaramente individuato: **consenso separati**. Consenso per contratto non integrato con quello non contrattuale (es. **marketing; profilazione; big data**) • **Documentabile e non necessariamente scritto** • **informato** • Se scritto, consenso **distinguibile**, facilmente accessibile, linguaggio semplice e **chiaro** • Ammesso consenso da 16enne • Consenso genitore per minore di 16 anni	**Semplificazione obblighi in tema di consenso scritto,** non più richiesto scritto ai fini della validità (dati sensibili). **MA STATI MEMBRI POSSONO PREVEDERE DIVERSAMENTE** (Cons. 10) Sanzioni: Reg: 83 c. 5 Reg (sanzioni fino a 20.000.000 eur o 4% fatturato annuo mondiale totale dell'esercizio precedente se superiore) CP: 167 (reclusione fino a 18 mesi) e 162 (sanzione fino a 120.000 eur)

Assessment, Remediation e Implementation su: il consenso dell'interessato - Cosa è cambiato

Rödl & Partner

D.Lgs. 196/2003	Reg. 2016/679	Conseguenze
	Art. 6 e 9	
Consenso **dati comun**i escluso se: art. 24 Consenso **dati sensibili** escluso se: art. 26	Consenso dati comuni escluso se: - Contratto - Obbligo legale - Interesse vitale - Interesse pubblico - **Interesse legittimo titolare prevalente (es. rapp. Lavoro)** Consenso dati particolari escluso se: - Obblighi legge lavoro, sicurezza - Interesse vitale - Associazioni senza scopo lucro - Esercizio diritto in sede giudiziaria - Dati resi manifestamente pubblici dall'interessato - Interesse pubblico - Medicina preventiva e del lavoro - Sanita pubblica - Scopi scientifici, storici e statistici Cons. 171: ***« non occorre che l'interessato presti nuovamente il consenso, se questo è già stato espresso prima del Reg***.»	**Semplificazione esenzioni.** **MA STATI MEMBRI POSSONO PREVEDERE DIVERSAMENTE** (Cons. 10) Sanzioni: Reg: 83 c. 5 Reg (sanzioni fino a 20.000.000 eur o 4% fatturato annuo mondiale totale dell'esercizio precedente se superiore) CP: 167 (reclusione fino a 18 mesi) e 162 (sanzione fino a 120.000 eur)

Assessment, Remediation e Implementation su: Il consenso dell'interessato - Cosa fare ora

- **Assessment su consensi raccolti**
- **Valutare semplificazione consensi (es. accorpamento consensi per marketing; eliminazione consensi scritti)**
- **Adottare procedure per raccolta e documentazione consensi**

Assessment, Remediation e Implementation su: I diritti dell'interessato - Cosa è cambiato

D.Lgs. 196/2003	Reg. 2016/679	Conseguenze
Art. 7	Art. 15	
1. Diritto di conferma dell'esistenza o meno di dati personali che lo riguardano 2. comunicazione in forma intelligibile. 3. l'indicazione: a) dell'origine dei dati personali; b) delle finalità e modalità del trattamento; c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici; d) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza	Idem. **In più**, indicazione: - Periodo di conservazione - Reclamo autorità di controllo - Esistenza di processo decisionale automatizzato, es. profilazione	Sanzioni: Reg: 83 c. 5 Reg (sanzioni fino a 20.000.000 eur o 4% fatturato annuo mondiale totale dell'esercizio precedente se superiore)

Assessment, Remediation e Implementation su: I diritti dell'interessato - Cosa è cambiato

D.Lgs. 196/2003	Reg. 2016/679	Conseguenze
Art. 7		
4. Diritto di ottenere: a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;	Idem: Art. 16	Invariato. Sanzioni: Reg: 83 c. 5 Reg
b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge.	Art. 17: Diritto all'oblio, ossia di cancellazione dati se, ad esempio: • Non più necessari per finalità • L'interessato revoca il consenso e non esiste altro fondamento giuridico • L'interessato si oppone al trattamento e il Titolare non ha interesse legittimo prevalente • Trattamento illecito Escluso se: • Esercizio diritto in sede giudiziaria • Esercizio diritto di informazione • Adempimento obbligo di legge • Sanità pubblica • Ricerca scientifica e storica	Il Titolare, che ha già trasmesso i dati ad altri titolari, deve informare gli altri titolari, dando elenco destinatari a interessato se richiesto → **SERVE PROCEDURA** Così vale anche per rettificazione o limitazione del trattamento. Sanzioni: Reg: 83 c. 5 Reg

Assessment, Remediation e Implementation su: I diritti dell'interessato - Cosa è cambiato

D.Lgs. 196/2003	Reg. 2016/679	Conseguenze
Art. 7	**Art. 21**	
5) Diritto di opporsi al trattamento, impedendolo in tutto o in parte solo in alcuni momenti: a) per motivi legittimi dell'interessato al trattamento dei dati personali che lo riguardano; b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.	**Diritto generalizzato di opporsi al trattamento in qualsiasi momento,** salvo: - Il Titolare dimostri: • motivi legittimi cogenti e prevalenti sui diritti dell'interessato • o per esercizio o difesa di un diritto in sede giudiziaria **Opporsi alle finalità di marketing o anche di profilazione per fini marketing**	Maggiori Obblighi Regolamento per Titolare Reg: 83 c. 5 Reg (sanzioni fino a 20.000.000 eur o 4% fatturato annuo mondiale totale dell'esercizio precedente se superiore)

Assessment, Remediation e Implementation su: I diritti dell'interessato - Cosa è cambiato

D.Lgs. 196/2003	Reg. 2016/679	Conseguenze
	Art. 18	
	Diritto di limitazione del trattamento: - Se **inesatto** - **Illecito** - **Non necessario per Titolare, ma per interessato** (es. difesa in giudizio) - Opposizione al trattamento, ma pendente verifica di interesse Titolare	Maggiori Obblighi Regolamento per Titolare. Titolare può trattare dati solo per **conservazione, esercizio diritto in sede giudiziaria, interesse pubblico** Reg: 83 c. 5 Reg (sanzioni fino a 20.000.000 eur o 4% fatturato annuo mondiale totale dell'esercizio precedente se superiore)

Assessment, Remediation e Implementation su: I diritti dell'interessato - Cosa è cambiato

D.Lgs. 196/2003	Reg. 2016/679	Conseguenze
	Art. 18 e Linee Guida WP29 13.12.2016	
	Art. 20 (Cons, 68) **Diritto alla portabilità:** Consiste nel diritto dell'interessato di: - ricevere dal Titolare in un formato strutturato interoperabile i propri dati personali: ossia un formato leggibile e riutilizzabile (quindi con i metadati necessari) - conservare il format per usi privati - o trasmetterlo direttamente o farlo trasmettere dal Titolare ad altro Titolare (qualsiasi altro service provider) E' esercitabile se: - trattamento su consenso o contratto e trattamento automatizzato - non se trattamento per adempiere a obbligo legale o interesse pubblico (es. ospedali) - non se dati già cancellati in conformità alle policy di retention Ha ad oggetto: - Dati personali relativi all'interessato: identificativi, sensibili, dati pseudoanonimizzati, no dati anonimi - Dati personali forniti al Titolare dall'interessato	Maggiori Obblighi Regolamento per Titolare (di norma per provider servizi telefonici, energia, etc) Reg: 83 c. 5 Reg

Assessment, Remediation e Implementation su: I diritti dell'interessato - Cosa è cambiato

D.Lgs. 196/2003	Reg. 2016/679	Conseguenze
	- Dati personali forniti al Titolare dall'interessato: ❑ consapevolmente (nome, cognome, email, etc) ❑ inconsapevolmente per l'uso del servizio (es. navigazione web) ➢ Sono solo dati grezzi creati dall'interessato («raw data»): storico delle ricerche web, storico degli acquisti, access log, dati di traffico ➢ Non comprendono i dati creati dal Titolare mediante l'analisi dei dati grezzi fatta dal titolare (es. *dati ottenuti con profilazione o recommendation o analisi statistica basata sui dati grezzi*) – «*inferred and derived data*» La trasmissione può avvenire (SERVE PROCEDURA) : ❑ con download diretto dei dati ❑ o creazione di apposite piattaforme di interazione per la trasmissione diretta tra titolari («Application Programming Interfaces» - API) ❑ o DVD, CD ❑ deve essere protetta (es. cifratura o credenziali autenticazione) Non preclude il diritto dell'interessato di continuare ad avvalersi dei servizi del primo Titolare o di esercitare gli altri diritti (oblio, etc) Non impone la cancellazione dei dati da parte del Titolare prima del tempo della policy retention, salvo esercizio diritti dell'interessato (oblio, etc) Deve essere informato e nell'Informativa vanno indicati i dati portabili	Maggiori Obblighi Regolamento per Titolare Reg: 83 c. 5 Reg
Riscontro all'interessato in **15 giorni**	Riscontro all'interessato «*without undue delay*» e, in ogni caso, entro 30 giorni (o massimo 3 mesi in casi complessi)	Alleggerimento degli Obblighi Regolamento per Titolare

Assessment, Remediation e Implementation su: I diritti dell’interessato - Cosa fare ora

- **Assessment su procedure esercizio dei diritti dell’interessato**
- **Modifica o adozione di procedure con inserimento nuovi diritti**
- **Adozione azioni correttive o di miglioramento**

Le ulteriori prove (e obblighi) dell'Accountability: le misure organizzative

Le procedure

Le ulteriori prove (e obblighi) dell'Accountability: Misure organizzative

D.Lgs. 196/2003	Reg. 2016/679	Conseguenze
	Art. 24	
	Obbligo di adozione di **misure organizzative** adeguate a minimizzare il rischio e di loro aggiornamento, tra cui: a) Politiche adeguate in materia di protezione dei dati: non più misure minime	**Maggiori Obblighi** Regolamento per Titolare e Responsabile: **forte coinvolgimento settore IT e security** Sanzioni: Reg: 83 c. 4 (sanzioni fino a 10.000.000 eur o 2% fatturato annuo mondiale totale dell'esercizio precedente se superiore)
	Esempi di policy da adottare: • Policy privacy • DPS – registri • Regolamento strumenti aziendali – es. per email, pc, smartphone • Procedura PIA • Procedura Privacy by design e by default • Procedura Data Breach • Procedure controllo dati da interessato e cancellazione dati • Procedure data mapping • Procedure gestione informative • procedura per testare, verificare, valutare periodicamente l'efficacia delle misure tecniche e organizzative adottate	

I codici di condotta e le certificazioni

Le ulteriori prove (e obblighi) dell'Accountability: Misure organizzative

D.Lgs. 196/2003	Reg. 2016/679	Conseguenze
	Artt. 40-43 e Consid. 77, 81, 100	
	b) Codici di condotta: sono **elaborati da associazioni di categoria** rappresentanti i titolari (o i responsabili) e approvati dall'autorità Garante competente e indicano come gli aderenti devono comportarsi per essere in linea col regolamento.	**Maggiori Obblighi Regolamento per Titolare** **Azienda etica**
	c) Certificazioni: **sigilli di qualità** e marchi di protezione dei dati per valutare e dimostrare la conformità al Regolamento dei trattamenti effettuati dai titolari (o dai responsabili). **Le certificazioni sono concesse da organismi di certificazione accreditati** (Accredia) per un periodo massimo di 3 anni rinnovabile. ***Unica certificazione oggi esistente in Italia sul Reg.: ISDP 10003:2015*** **Art. 24 c. 3 «*l'adesione ai codici di condotta o a un meccanismo di certificazione può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento*»** **PROVA ACCOUNTABILITY (ART. 5)**	**Sanzioni:** Reg: 83 c. 4 Reg (sanzioni fino a 10.000.000 EUR o 2% fatturato annuo mondiale totale dell'esercizio precedente se superiore) per violazione degli obblighi del titolare (o del responsabile) a norma degli artt. 42-43. Reg: 83 c. 2 lett. j) Per la commisurazione della sanzione **si deve tenere debito conto dell'adesione ai codici di condotta e alle certificazioni di cui agli artt. 40 e 42 Reg.**

Le ulteriori prove (e obblighi) dell'Accountability: Misure organizzative - Cosa fare ora

- **Assessment su procedure, codici di condotta e certificazioni adottate**
- **Adozione azioni correttive o di miglioramento**
- **Procedure di aggiornamento**

Le nomine

Le ulteriori prove (e obblighi) dell'Accountability: Misure organizzative

D.Lgs. 196/2003	Reg. 2016/679	Conseguenze
Art. 30		
d) - **Nomine Incaricati** - **Nomine Ads**	Garante italiano in Gruppo di lavoro Reg. ne conferma l'applicabilità anche post Reg.	Idem
e) **Nomina Responsabile** (art. 29): - Responsabile interno - **Facoltativo** - Con esperienza, capacità e affidabilità - Garantisce protezione dati - **Nomina scritta**	**Art. 28:** - Responsabile esterno: esternalizzazione - **Obbligatorio** - che presenti **garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate** per protezione dati e diritti interessato ***PROVATE DA CODICI DI CONDOTTA E CERTIFICAZIONI*** - **Contratto scritto (o in formato elettronico)**	**Maggiori Obblighi Regolamento per Titolare e Responsabile** Sanzioni: Reg: 83 c. 4 Reg CP: 162: sanzione fino a 120.000 eur

Le ulteriori prove (e obblighi) dell'Accountability: Misure organizzative

D.Lgs. 196/2003	Reg. 2016/679	Conseguenze
Art. 29	**Art. 28**	
	Il contratto col Responsabile (individuale o su base di SCC di Commissione) include: - Operazioni di trattamento assegnate a R - Durata - Istruzioni documentate da T a R - Garanzia del Responsabile che gli incaricati siano vincolati alla riservatezza - Adozione di **misure di sicurezza tecniche e organizzative adeguate** (es. pseudoanonimizzazione, cifratura) da Responsabile - Assistenza del Titolare nel rispetto degli obblighi di misure di sicurezza, data breach e valutazione d'impatto sulla protezione dei dati	**Maggiori Obblighi Regolamento per Titolare e Responsabile** **Sanzioni civili:** **Il Titolare risarcisce il danno cagionato da trattamento in violazione del Regolamento, se imputabile.** **Responsabile risarcisce il danno cagionato da trattamento in violazione degli obblighi imposti al Responsabile dal Regolamento o dalle istruzioni del Titolare, se imputabile.** **Se Titolare e Responsabile sono coinvolti nello stesso trattamento, responsabilità in solido**

Le ulteriori prove (e obblighi) dell'Accountability: Misure organizzative

D.Lgs. 196/2003	Reg. 2016/679	Conseguenze
Art. 29	Art. 28	
	Il contratto col Responsabile include: - Messa a disposizione del Titolare di prove di adempimento a contratto col R - Adozione di registri delle attività del trattamento - Formazione incaricati - Eventuale **autorizzazione scritta del T a R per nomina di sub-Responsabile** - Analoghi obblighi e contratto per sub-Responsabile e **responsabilità esclusiva del Responsabile vs Titolare se sub-Resp inadempiente**	**Maggiori Obblighi Regolamento per Titolare e Responsabile**. Sanzioni amministrative: Reg: 83 c. 4 (sanzioni fino a 10.000.000 eur o 2% fatturato annuo mondiale totale dell'esercizio precedente se superiore) per artt. 24-32 (by design e default, misure, nomine, breach, PIA, PO) 83 c. 5 (sanzioni fino a 20.000.000 eur o 4% fatturato annuo mondiale totale dell'esercizio precedente se superiore) per principi del trattamento, diritti interessati, trasferimenti dati extra EU

Le ulteriori prove (e obblighi) dell'Accountability: Misure organizzative - Cosa fare ora

- **Assessment su nomine incaricati, ads e responsabili e loro aggiornamento**
  - **Adozione di procedure di nomina e aggiornamento nomine**

La formazione

Le ulteriori prove (e obblighi) dell'Accountability: Misure organizzative

D.Lgs. 196/2003	Reg. 2016/679	Conseguenze
	Artt. 29 e 32 c. 4	
Reg. 19 All. B: abrogata con D.L. 5/2012	f) **Formazione**: Formare adeguatamente tutti coloro che trattano i dati e dar prova della formazione (registri)	**Maggiori Obblighi Regolamento per Titolare e Responsabile** Sanzioni: Reg: 83 c. 5 Reg

Le ulteriori prove (e obblighi) dell'Accountability: Misure organizzative - Cosa fare ora

- **Assessment per verificare e aggiornare procedure e documentazione della formazione**

II DPO

Il DPO

g) Il **DPO** è uno degli elementi chiave all'interno del nuovo sistema di ***governance*** dei dati

capace di indirizzare e garantire l'***accountability*** del titolare/responsabile

riducendo il rischio sanzionatorio (fino al 4% del fatturato di Gruppo)

La nomina del DPO

Reg. 2016/679	Conseguenze
Art. 37-39 , Linee Guida WP29 13.12.2016 (emendata il 5.4.2017), Provv. Garante 15.9.17 e 15.12.17	
NOMINA OBBLIGATORIA Titolare e/o Responsabile **devono sempre** nominare il Responsabile per la Protezione (DPO) dei dati se: - Trattamento effettuato da **ente pubblico** (escluso autorità giudiziaria) - Le **attività principali** del Titolare o Responsabile (cioè le operazioni essenziali che sono necessarie al raggiungimento degli obiettivi) comportano trattamenti consistenti nel: **1) Trattamento su larga scala di dati particolari o giudiziari** (es. dati sensibili, salute, vita sessuale, genetici, giudiziari e biometrici): obbligo ad es. per ospedali e cliniche **2) Monitoraggio:** **- regolare degli interessati** : «*costante e periodico, condotto in particolari intervalli di tempo per un periodo particolare, ricorrente o ripetuto a intervalli di tempo regolari*» - **sistematico**: «*pre – organizzato, metodico, parte di una strategia*» - **su larga scala**: « *trattamento che coinvolge ad es. un numero rilevante di soggetti, un volume ingente di diversi dati personali, una significativa durata, un'ampia estensione geografica*»	Reg: 83 c. 4 (sanzioni fino a 10.000.000 eur o 2% fatturato annuo mondiale totale dell'esercizio precedente se superiore)

La nomina del DPO

Reg. 2016/679

Art. 37-39 , Linee Guida WP29 13.12.2016 (emendata il 5.4.2017), Provv. Garante 15.9.17 e 15.12.17

NOMINA OBBLIGATORIA

Il Monitoraggio degli interessati include ad es.

telemedicina

profilazione o tracking (es. con CRM, e-commerce, cookies e log)

connected devices quali contatori intelligenti

l'attività di marketing basata sull'analisi dei dati raccolti

profilazione e scoring per finalità di valutazione del rischio (per esempio, a fini di valutazione del rischio creditizio, prevenzione delle frodi, accertamento di forme di riciclaggio)

tracciamento dell'ubicazione, per esempio da parte di app su dispositivi mobili

programmi di fidelizzazione

pubblicità comportamentale

utilizzo di telecamere a circuito chiuso

La nomina del DPO

Reg. 2016/679	Conseguenze
Art. 37-39 , Linee Guida WP29 13.12.2016 (emendata il 5.4.2017), Provv. Garante 15.9.17 e 15.12.17	
NOMINA FACOLTATIVA Negli altri casi nomina facoltativa (soggetta a queste regole) o di altri soggetti (es. chief privacy officer) non soggetti a queste regole  **NB: DPO STRUMENTO DI GOVERNANCE E ACCOUNTABILITY**	Reg: 83 c. 4 (sanzioni fino a 10.000.000 eur o 2% fatturato annuo mondiale totale dell'esercizio precedente se superiore)

Le competenze del DPO e la posizione

Reg. 2016/679

Art. 37-39 , Linee Guida WP29 13.12.2016 (emendata il 5.4.2017), Provv. Garante 15.9.17 e 15.12.17

Il DPO:

- Deve avere **conoscenza specialistica e giuridica della normativa nazionale** ed europea (es. privacy, diritto del lavoro, diritto sindacale, diritto penale, diritto comunitario, diritto internazionale, etc) proporzionato ai trattamenti di dati effettuati in concreto dal titolare/responsabile, alla complessità e quantità dei dati trattati e alla protezione richiesta per i dati personali oggetto di trattamento.

- Deve avere conoscenza delle **prassi (*processi aziendali, procedure, ISO*) in materia di privacy e del settore di riferimento,** anche in termini di misure tecniche e organizzative

- **Sono richieste competenze specifiche, non attestazioni formali né** l'iscrizione ad appositi albi professionali, ma **la partecipazione a master e corsi di studio e certificazioni personali** (es. TUV, KHC, norma UNI 11697:2017) rappresentano strumento utile per il Titolare e il Responsabile per **valutare il possesso di un livello adeguato di conoscenza**

- Può essere **uno per un unico gruppo imprenditoriale** solo se **facilmente raggiungibile (cioè nella UE)** da ogni stabilimento o uno per ciascuna società del gruppo

- Può essere uno per più enti pubblici o uno per ciascun **ente pubblico**

Le competenze del DPO e la posizione

Reg. 2016/679

Art. 37-39 , Linee Guida WP29 13.12.2016 (emendata il 5.4.2017), Provv. Garante 15.9.17 e 15.12.17

Il DPO:

- Deve garantire **totale autonomia e indipendenza**: a tal fine deve avere **risorse economiche e lavorative** adeguate, non **ricevere istruzioni** da altri soggetti dell'azienda e **rispondere solo al vertice gerarchico** (ad, board)

A tal fine il DPO dovrebbe poter contare su:

- **supporto** attivo della funzione di DPO da parte del senior management;
- **tempo** sufficiente per l'espletamento dei compiti affidati;
- supporto adeguato in termini di **risorse** finanziarie, infrastrutture (sede, attrezzature, strumentazione) e, ove opportuno, di personale;
- **comunicazione** ufficiale della designazione del DPO a tutto il personale;
- **formazione** permanente.

- Può svolgere altre attività, ma non deve agire in situazioni di **conflitto di interesse,** che si verifica in caso di soggetto che **decide finalità e modalità del trattamento:**

Internamente all'azienda, c'è conflitto se il DPO svolge attività di senior management e ha ruoli manageriali di vertice (figure apicali, chief executive, chief financial, head of marketing, head of HR, head of IT, Responsabile servizi informativi, etc)

Le competenze del DPO e la posizione

Reg. 2016/679

Art. 37-39 , Linee Guida WP29 13.12.2016 (emendata il 5.4.2017), Provv. Garante 15.9.17 e 15.12.17

Il DPO :

- Può essere **Interno** (dipendente) solo se riesce a garantire autonomia e indipendenza (almeno **dirigente o alto funzionario che non rivesta altri ruoli apicali e abbia risorse e autonomia di spesa**)

- Può essere **Esterno** (consulente) sulla base di contratto di servizi che ne specifichi bene i compiti

- A seconda della complessità del trattamento, può agire da solo o essere supportato da una **struttura**:

Il DPO può essere coadiuvato da un **team operante sotto la sua autorità**, che costituisca:

una **struttura interna** (composta solo da dipendenti)

esterna (composta solo da autonomi)

o **ibrida** (composta da un DPO esterno e dipendenti interni a supporto)

PRO e CONTRA: Mentre le prime due soluzioni mostrano evidenti limiti (la struttura interna spesso non riesce a garantire indipendenza, autonomia e assenza di conflitto, mentre quella esterna sovente non riesce ad avere la giusta comprensione del business), la terza è senz'altro quella più affidabile, in quanto permette la giusta indipendenza, autonomia e assenza di conflitto, a fronte della piena comprensione dei processi e delle logiche aziendali.

Le competenze del DPO e la posizione

Reg. 2016/679

Art. 37-39 , Linee Guida WP29 13.12.2016 (emendata il 5.4.2017), Provv. Garante 15.9.17 e 15.12.17

Il DPO :

- Ha vincolo di **riservatezza** sulle attività svolte, integrità ed etica professionale
- Non riceve **istruzioni** per quanto riguarda l'esecuzione dei suoi compiti e **non è rimosso o penalizzato** per l'adempimento degli stessi
- Riceve tutto il supporto necessario dal board e delle direzioni interessate (es. HR, IT, Legal)
- **Non è personalmente responsabile della non-compliance al Reg.: tale è solo il Titolare o il Responsabile**

I compiti del DPO

Reg. 2016/679

Art. 37-39 , Linee Guida WP29 13.12.2016 (emendata il 5.4.2017), Provv. Garante 15.9.17 e 15.12.17

Il DPO deve:

- ✓ **informare** sulla normativa e fornire consulenza al titolare o responsabile del trattamento e ai dipendenti sulla normativa applicabile, il Reg e le altre normative applicabili alla protezione dei dati (es. privacy, diritto del lavoro, diritto sindacale, diritto penale, etc)
- ✓ essere **coinvolto** in tutte le questioni di privacy, supportando titolare o responsabile in ogni attività connessa al trattamento dei dati, anche con riguardo alla tenuta dei **registri del trattamento, dei documenti** e **notifiche data breach** (se compito affidatogli espressamente da Titolare o Responsabile)
- ✓ **sorvegliare** l'implementazione e il rispetto del Reg e delle procedure, **valutando i rischi** di ogni trattamento tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento (**Risk Assessment**)
- ✓ **formare e sensibilizzare** il personale, il titolare e i responsabili
- ✓ aiutare il Titolare nel **Privacy Impact Assessment**, dando parere in merito all'esigenza di effettuarla, quali rischi e quali **misure** adottare e sorvegliandone lo svolgimento: n**on ha l'obbligo** di fare PIA né di adottare misure, che invece grava su Titolare e Responsabile
- ✓ **collaborare** con Garante Privacy
- ✓ essere punto di **contatto** per il Garante

Le ulteriori prove (e obblighi) dell'Accountability: Misure organizzative

- **Assessment per verificare necessità di nomina di DPO**
- **Adozione di procedura di nomina e di casistiche di conflitto**

II Data Breach

Le ulteriori prove (e obblighi) dell'Accountability: Misure organizzative

D.Lgs. 196/2003	Reg. 2016/679	Conseguenze
Art. 32 -bis	Art. 33	
Notifica data breach da provider di servizi di comunicazione elettronica entro 72 ore a Garante. Notifica data breach per Dossier sanitario e FSE Comunicazione a interessato se elevato rischio. Art. 37: notificazioni in varie circostanze	h) **Notificazione data breach**: Il Titolare, con assistenza Responsabile e Privacy officer se nominato, notifica violazioni dati a Garante Privacy entro 72 ore dalla scoperta, salvo ingiustificato ritardo e documenta le violazioni. Violazioni = ❑ distruzione accidentale dei dati ❑ distruzione illegale ❑ perdita ❑ modifica ❑ rilevazione ❑ accesso non autorizzato Notifica non necessaria se Titolare prova assenza di rischio per diritti e libertà interessato Notifica include: *descrizione violazione, tipologia e numero di interessati e di dati, conseguenze delle violazioni, misure adottate o da adottare* **Comunicazione a interessato per elevato rischio per i diritti interessato: esclusa se adozione di misure che rendono i dati incomprensibili (es. cifratura, pseudoanonimizzazione)** Abolizione delle altre notificazioni	Maggiori obblighi Titolare. Sanzioni: Reg: 83 c. 4 Reg (sanzioni fino a 10.000.000 eur o 2% fatturato annuo mondiale totale dell'esercizio precedente se superiore

Il Data Breach nel GDPR

Per **Data Breach** si intende nel GDPR «*la violazione di sicurezza che comporta accidentalmente o in modo illecito* ***la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati***» (art. 4, comma 1, n. 12)

Il Data Breach nel Codice Privacy Italiano

Data Breach =

distruzione accidentale dei dati
distruzione illegale
perdita
modifica
rilevazione
accesso non autorizzato

Il Data Breach nel GDPR

Obblighi in caso di Data Breach, anche nel GDPR:

- **Notifica** all'autorità di controllo (art. 33 GDPR)
- **Comunicazione** agli interessati (art. 34 GDPR)
- **Tenuta di registro** dei data breach (art. 33 GDPR)

- In tutti i casi, il **Risk Assessment**

Il Data Breach nel GDPR

Sanzione: art. 83

Fino al **2 % del fatturato mondiale** totale annuo dell'esercizio precedente

I Data Breach e l'Accountability

Reg. 2016/679

Art. 33.5, Linee Guida WP29 3.10.2017 (emendata il 6.2.2018)

Il Titolare ha l'obbligo di tenere un **registro delle violazioni dei dati personali**, che contenga l'indicazione di:

- **tutte le violazioni** dei dati personali che si sono verificate, comprese quelle non notificate all'autorità di controllo e non comunicate agli interessati;
- se non è stata effettuata la notifica all'autorità di controllo, **le motivazioni della mancata notifica**;
- se la notifica all'autorità di controllo è avvenuta dopo le 72 ore dal momento in cui il Titolare ha avuto conoscenza della violazione dei dati personali, l**e motivazioni del ritardo nella notifica**;
- se non è stata effettuata la comunicazione agli interessati, le **motivazioni della mancata comunicazione agli interessati** (i risultati del ***Risk Assessment*** condotto).

Cosa fare ora

Adozione di Procedura di Data Breach e registro

Il Registro dei trattamenti

Il Registro dei trattamenti

D.Lgs. 196/2003	Reg. 2016/679	Conseguenze
	Artt. 30	
Già DPS	i) Obbligo di Adozione **Registri del trattamento (ex DPS):** **- Scritti o in formato elettronico** con dettaglio di: • Nome Titolare o Responsabile e DPO • Finalità e modalità trattamento, • interessati, • dati, • termini di cancellazione dati, • trasferimento extra Ue • descrizione misure tecniche e organizzative adottate • destinatari della comunicazione di dati - Sono **due**: dei trattamenti del titolare e di quelli del Responsabile. - Quelli del Responsabile includono anche*: tutti i titolari, i trattamenti per ogni titolare, le misure per ogni titolare* - Sono **protetti**: psw o chiave - Sono realizzati a seguito della **PIA**	**Maggiori Obblighi Regolamento per Titolare e Responsabile** **Obbligo per titolari e responsabili** • **con + 250 dipendenti** • **se trattamento di dati particolari (art. 9)** • **o rischio per libertà fondamentali (es. profilazione su larga scala)** Sanzioni: Reg: 83 c. 4 Reg Suggerimento: **adottarli sempre e tenerli aggiornati annualmente a prova dell'Accountability -> FOTOGRAFIA DINAMICA**

Il registro dei trattamenti: come redigerlo?

I principali step

Assessment

Redazione del Registro dei trattamento

Redazione Registro rischi

Redazione Manuale di Trattamento Rischio

Come procedere?

ASSESSMENT

DRAFT REGISTRI (AS-IS)

VALUTAZIONE RISCHI e REGISTRO RISCHI

PIANO DI TRATTAMENTO RISCHIO

REGISTRI FINAL → ACCOUNTABILITY

Il 1° step: La fase di Assessment

L'Assessment - Il metodo Rödl & Partner (*)

Come fare quindi un registro in linea con il GDPR?

1° Fase del Metodo Rödl & Partner: Privacy Assessment secondo la nuova normativa europea e la normativa ISO 27001, 29134, 30000 e ISDP 10003:2015

Risk Assessment

per l'individuazione e la valutazione dei rischi sulla sicurezza dei dati e delle libertà individuali

Privacy Impact Assessment

per la valutazione d'impatto dei trattamenti effettuati sulla protezione dei dati

Data mapping
mappatura dei dati, loro fonte ed uso

Documental Assessment
analisi di tutti i documenti e le procedure privacy (informative, consensi, procedure …)

Verbal Assessment
interviste ai soggetti coinvolti nel trattamento

System Assessment
analisi di tutti i sistemi e di tutte le misure adottate

Valutazione dei rischi
Per la sicurezza dei dati e le libertà individuali

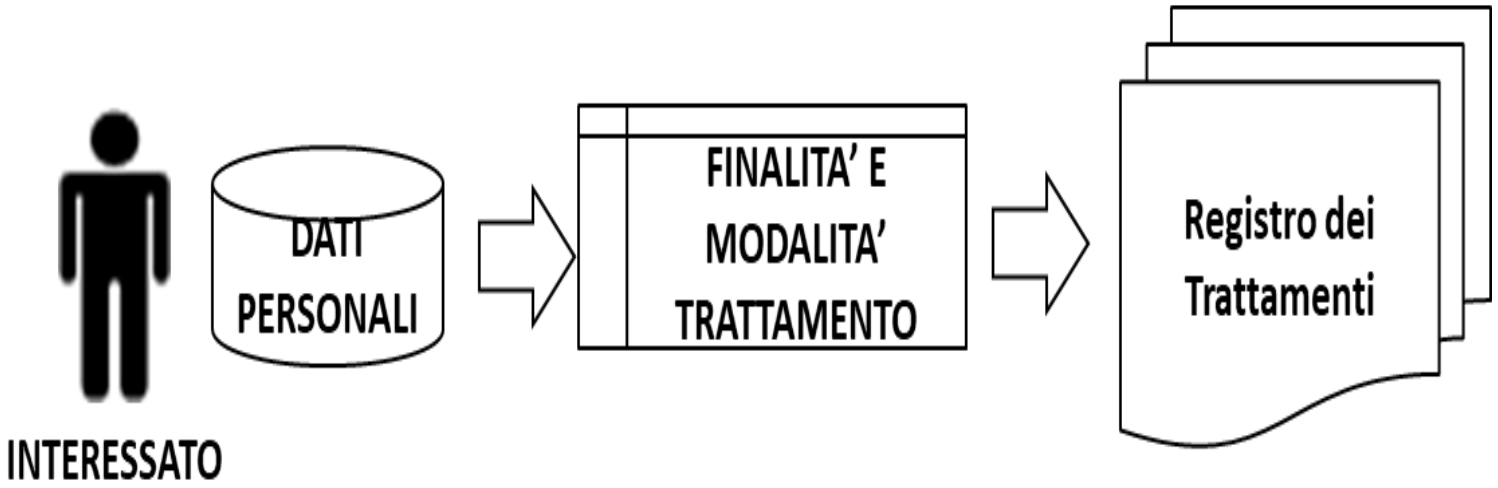
Valutazione di impatto
(Privacy Impact Assessment) del trattamento sulle libertà individuali

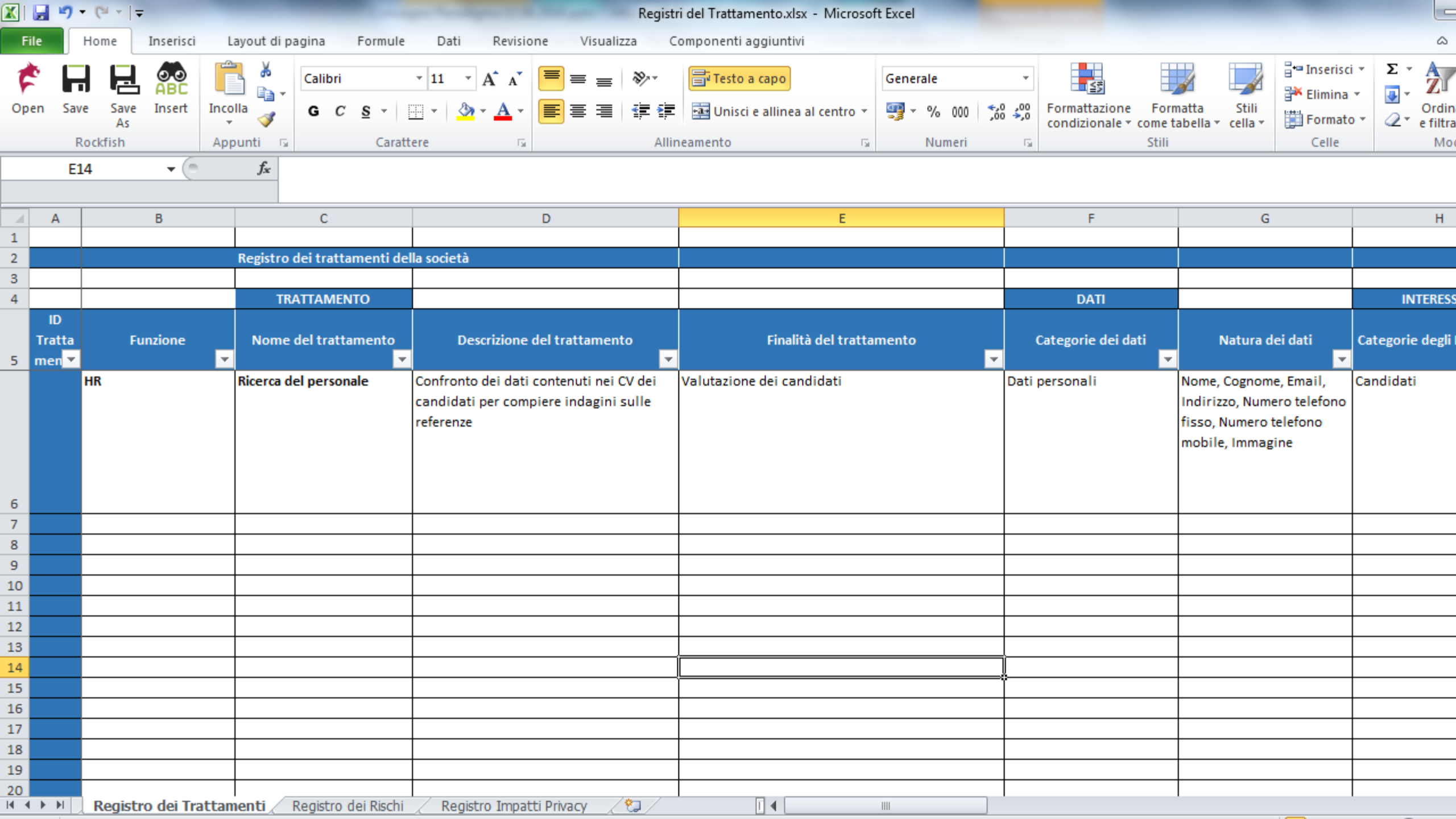
Misure
Individuazione delle **misure tecniche e organizzative** adeguate per minimizzare i rischi

Report di Assessment:
Il report finale con la gap analysis tra le risultanze e la norma applicabile

II 2° step: La redazione del Registro dei trattamenti (as-is)

La redazione dei registri





Registri del Trattamento.xlsx - Microsoft Excel

File | Home | Inserisci | Layout di pagina | Formule | Dati | Revisione | Visualizza | Componenti aggiuntivi

Open | Save | Save As | Insert | Incolla | Calibri | 11 | Testo a capo | Generale | Unisci e allinea al centro | Formattazione condizionale | Formatta come tabella | Stili cella | Inserisci | Elimina | Formato | Ordina e filtra

Rockfish | Appunti | Carattere | Allineamento | Numeri | Stili | Celle

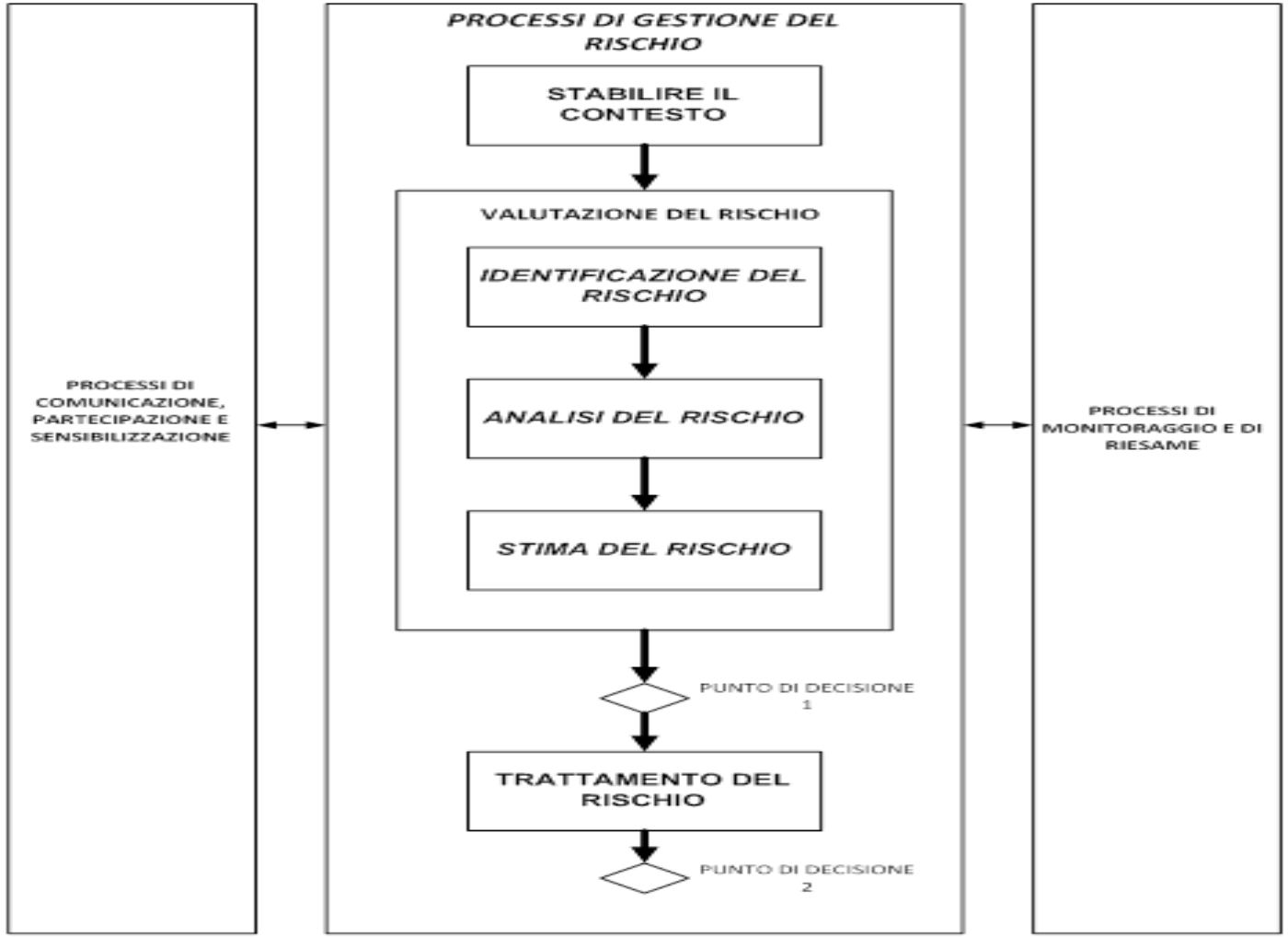
E14

	A	B	C	D	E	F	G	H
1								
2		Registro dei trattamenti della società						
3								
4			TRATTAMENTO			DATI		INTERESS
5	ID Tratta men	Funzione	Nome del trattamento	Descrizione del trattamento	Finalità del trattamento	Categorie dei dati	Natura dei dati	Categorie degli
6		HR	Ricerca del personale	Confronto dei dati contenuti nei CV dei candidati per compiere indagini sulle referenze	Valutazione dei candidati	Dati personali	Nome, Cognome, Email, Indirizzo, Numero telefono fisso, Numero telefono mobile, Immagine	Candidati
7								
8								
9								
10								
11								
12								
13								
14								
15								
16								
17								
18								
19								
20								

Registro dei Trattamenti | Registro dei Rischi | Registro Impatti Privacy

Il 3° step parte 1: Valutazione del Rischio

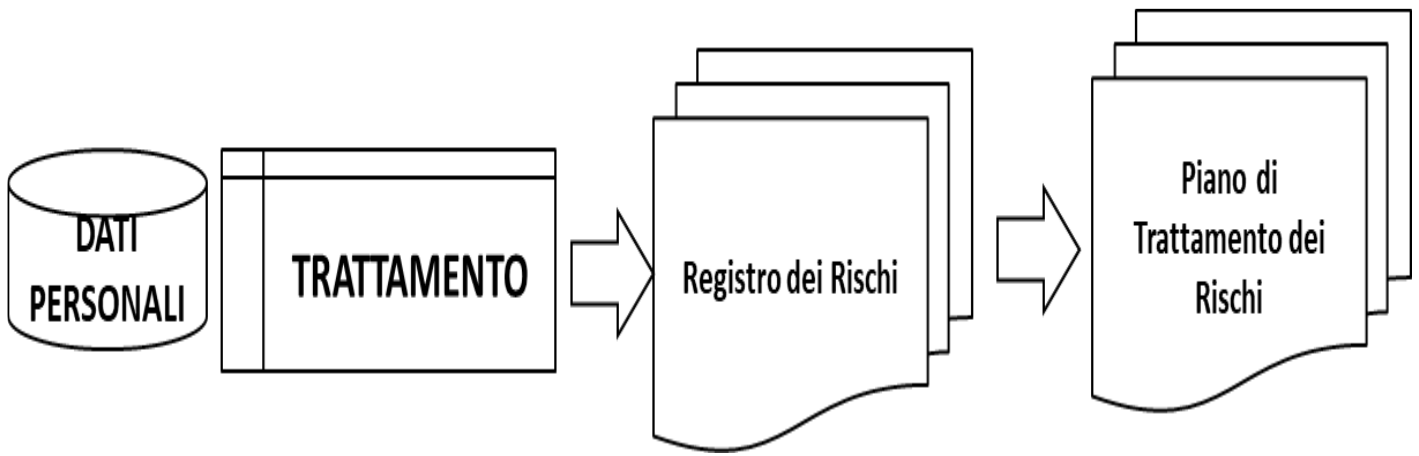
Valutazione del Rischio



Il 3° step parte 2: Redazione del Registro Rischi

A4 1

	A	B	C	D	E	F	G	H	
3	ID Rischio	Contesto	Tipologia del Contesto	Fonte di rischio	Valutazione sulla protezione dei dati personali	TITOLARE DEL RISCHIO	OBIETTIVO	OBIETTIVO	O
4	1	Esterno	Contesto Normativo	Normative generali	Tutti i trattamenti esaminati nel registro, in contrasto con il GDPR, non sono allo stato supportati da misure organizzative adeguate quali: - un aggiornamento delle informative (a dipendenti, candidati, visitatori, fornitori, videosorvegliati) - un aggiornamento delle nomine a responsabile interno, esterno, amministratore di sistema, incaricato e responsabile della videosorveglianza - un aggiornamento del Regolamento per la videosorveglianza e delle misure tecniche costituite da doppia password di accesso ai sistemi - un aggiornamento delle istruzioni agli incaricati - l'erogazione della formazione - l'adozione di policy di data breach, data retention, diritti dell'interessato, privacy by design e Privacy Impact Assessment - l'adozione di tempi di conservazionedei dati adeguati -l'adozione di un Piano Organizzativo per la Gestione dei dati personali - la archiviazione in armadi o uffici chiusi a chiave Per maggiore dettagli si vedano i report di Documental e Verbal Legal Assessment	Titolare trattamento	Confidenzialità	Integrità	Di à
		Esterno	Contesto	Normative settoriali	Non vi sono specifiche normative settoriali applicabili alla				Di



Il 4° step: Piano di trattamento del rischio

Il piano di trattamento del rischio

Misure Tecniche e Organizzative adeguate:

- Revisione/adozione/aggiornamento di tutta la documentazione privacy (informative, nomine, consensi)
- Aggiornamento/Implementazione **misure organizzative adeguate** come:
  - Certificazioni e codici di condotta
  - Politiche:
    - Policy Privacy by Design e by Default
    - Policy Data Retention, Deletion e Destruction
    - Policy Data Breach
    - Policy Privacy Impact Assessment
    - Policy Diritti interessato
    - Policy IT
    - Manuale della Protezione dei Dati Personali e relativo approccio metodologico
    - Registri del Trattamento
    - Piano Organizzativo Protezione dei dati
  - Formazione
  - Data Protection Officer

- Aggiornamento/Implementazione **misure tecniche adeguate**:
  - Misure IT
  - Privacy by design
  - Privacy by default

- Aggiornamento/Implementazione **registri**, **controlli periodici, tools di self assessment** e polizze assicurative

Quando

25 maggio 2018 ….

Contatti

Avv. Nadia Martini

Associate Partner e Head of Data Protection Italy

@. Nadia.martini@roedl.it – Tel. 02.6328841

LE FONTI AWARDS WINNER 2017

IP & TMT 2017 Awards by legalcommunity – Giovedì 11 maggio 2017 – Studio dell'anno Privacy RÖDL & PARTNER

Formazione

- Laurea in Giurisprudenza conseguita presso l'Università di Milano
- Iscritta all'Albo degli avvocati di Milano
- Master in IP; Master in IT; Master in Data protection

Esperienze professionali

- Privacy Officer Certificato secondo lo standard ISO/IEC 17024:2008
- Membro del Gruppo di Lavoro per il Regolamento Privacy Europeo istituito dal Garante della Privacy
- Dal 2016 Associate Partner di Rödl & Partner Milano e responsabile del dipartimento di Data Protection e Privacy

Skills

- Data Protection e Privacy
- Proprietà Intellettuale
- Information Technologies
- Compliance

Lingue

- Italiano
- Inglese

Attività principali

- Assistenza giudiziale e stragiudiziale a clienti italiani e stranieri in tutte le problematiche di Data Protection (es. Marketing, Profiling, E-Commerce, Targeting, CRM, social media, verifiche preliminari, Cookies, trattamento dei dati personali, Apps, E-Health e Smart Devices, attività come DPO, valutazione dei rischi, implementation del GDPR), Diritto d'autore (validità, uso e contraffazione dei diritti d'autore, redazione e negoziazione di contratti commerciali), Diritto Industriale (validità, uso e contraffazione di marchi, brevetti, disegni, modelli, know how, internet, IGP, DOP, DOC; concorrenza sleale, pubblicità)
- Implementation del GDPR in società di primaria importanza

Contatti

Rödl & Partner

Avvocati, Dottori Commercialisti, Revisori Legali e Consulenti del Lavoro
Attorneys-at-Law, Tax Consultants, Certified Public Accountants and Labour Consultancy
Rechtsanwälte, Steuerberater, Wirtschaftsprüfer, Arbeitsrechtsberater

Milano
Largo Donegani, 2
20121 (MI)
Tel.: +39-02-6328841
Fax: +39-02-63288420
info@roedl.it

Padova
Via F. Rismondo, 2/E
35131 (PD)
Tel.: +39-049-804 6911
Fax: +39-049-8046920
padua@roedl.it

Roma
P.zza S.Anastasia, 7
00186 (RM)
Tel.: +39-06-96701270
Fax: +39-06-3223394
roma@roedl.it

Bolzano
P.zza Walther- von- der-Vogelweide 8
39100 (BZ)
Tel.: +39-0471-1943200
Fax: +39-0471-1943220
bozen@roedl.it

Ogni singola persona conta“, per i Castellers e per noi.

Le “torri umane” simboleggiano in modo straordinario la cultura di Rödl & Partner. Incarnano la nostra filosofia di coesione, equilibrio, coraggio e spirito di squadra. Mostrano la crescita che scaturisce dalle proprie forze, elemento che ha fatto di Rödl & Partner quello che è oggi. „Força, Equilibri, Valor i Seny“ (Forza, equilibrio, coraggio e intelligenza) sono i valori dei Castellers, così vicini ai nostri. Per questo, nel maggio 2011, Rödl & Partner ha stretto una cooperazione con i Castellers di Barcellona, ambasciatori nel mondo dell’antica tradizione delle “torri umane”. L’associazione catalana incarna, insieme a molte altre, questa preziosa eredità culturale.