



*La tranquillità di
cui la tua azienda
ha bisogno.*





CHI SIAMO

Siamo dati! E un gruppo di più di 10 consulenti di privacy, cyber security e avvocati specializzati nel mondo del web e delle aziende italiane. Come la nostra piattaforma in Cloud con la quale rendiamo più semplice la gestione dei dati dei nostri clienti.

Saprai sempre cosa hai fatto per proteggere i tuoi dati e averli sempre a portata di mano in caso di necessità.



MISSION

Cerchiamo di semplificare la vita dei nostri clienti, aiutandoli nella gestione dei propri dati, facendogli guadagnare l'unica cosa al mondo che non ha prezzo. **TEMPO**



VISION

I Dati non sono semplici numeri, ogni cosa che facciamo quotidianamente è un dato e quindi potremmo dire che noi stessi siamo dati e come tali vanno protetti. Dobbiamo porci l'obiettivo di conoscerci meglio attraverso i numeri e grazie ad essi ridurre la nostra impronta digitale per noi e il pianeta.

FOLLOW US





TEAM EASYGDPR



Francesca Biello
Marketing e
comunicazione



Caterina Acampora
Strategist &
Content Creator



Fabrizio Ronca
Innovation
Manager



Gianluca Muggittu
Project
Manager



Francesco Bazzoni
Direttore
Commerciale

DPO



Martina Lonardi



Francesco Tola



Luigi Rendina

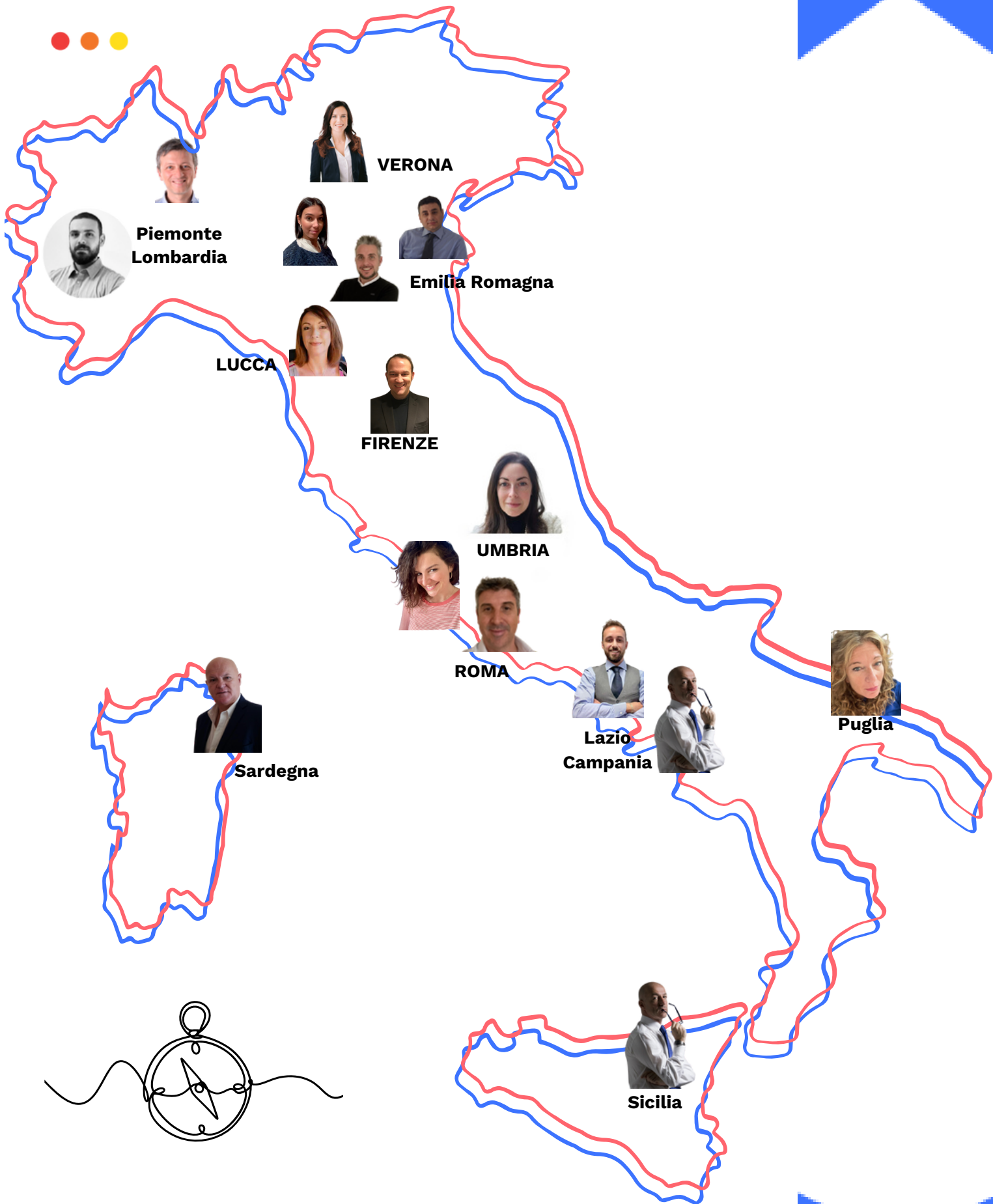


Barbara Fortunato



Miriam Carmassi





I NOSTRI CONTATTI



LA NOSTRA SUITE



EASYGDPR[®]



EASYDPO[®]



EASYTECH



EASYSECURITY

TECHNOLOGIES & CYBERSECURITY

I PUNTI DI FORZA

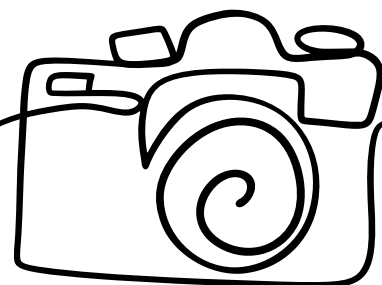
- Servizio Gestito
- Assistenza dedicata
- Servizio a valore aggiunto
- Identità digitale

COSE CHE DEVI SAPERE

Non ti spaventeremo dicendoti che se non adegui la tua azienda alla normativa GDPR rischi il 4% di multa del tuo fatturato annuo. Questo lo sai già.

Quello che non sai forse è quanto vale la perdita dei tuoi dati, dei tuoi clienti, il fermo attività della tua azienda.

Quanto vale in termini di reputazione? Perché potenziali clienti dovrebbero scegliere la tua azienda se non proteggi i loro dati?



EASYGDPR

WWW.EASYGDPR.IT

CONTATTA@EASYGDPR.IT



PERCHÈ DPO?

La data protection non è un'attività da svolgere in una sola volta per poi accantonarla. Al contrario, richiede un costante lavoro di monitoraggio nel tempo, aggiornando le informative e i dati sul registro dei trattamenti, tenendo informato personale e vertici aziendali sui nuovi rischi.

La figura del DPO, deve sempre essere coinvolta in tutto ciò che riguarda la "privacy". Per venire incontro ai clienti che hanno questo tipo di esigenza EasyGDPR ha creato il servizio EASY DPO, la figura del DPO erogata in modalità As A Service.

Il DPO, o responsabile per la protezione dei dati personali (RPD) è una figura introdotta dal Regolamento Europeo GDPR (Reg. UE 679/2016). Si tratta di un soggetto designato dall'azienda affinché possa supportarla nella gestione degli adempimenti in materia di trattamento e protezione dei dati personali .

La sua funzione è fondamentale per garantire, ed essere in grado di dimostrare, la piena conformità alla normativa, e nello specifico al principio di "accountability" (responsabilità) come descritto nell'articolo 24 del GDPR.

A CHI SERVE?

A tutte le aziende che vogliono usufruire di un supporto nella gestione degli adempimenti in materia di trattamento e protezione dei dati personali e nella comunicazione con il Garante della Privacy in qualsiasi momento.

La sua funzione è fondamentale per garantire, ed essere in grado di dimostrare, la piena conformità alla normativa, e nello specifico al principio di "accountability" (responsabilità) come descritto nell'articolo 24 del GDPR.

CHI È OBBLIGATO?

A titolo esemplificativo e non esaustivo:

- concessionari di servizi pubblici (trasporto pubblico locale, raccolta dei rifiuti, gestione dei servizi idrici ecc.),
- istituti di credito;
- imprese assicurative;
- sistemi di informazione creditizia;
- società finanziarie;
- società di informazioni commerciali;
- società di revisione contabile;
- società di recupero crediti;
- istituti di vigilanza;
- partiti e movimenti politici;
- sindacati; caf e patronati;
- società operanti nel settore delle utilities (telecomunicazioni, distribuzione di energia elettrica o gas, ecc.);
- imprese di somministrazione di lavoro e ricerca del personale;
- società operanti nel settore della cura della salute, della prevenzione/diagnostica sanitaria quali ospedali privati, terme, laboratori di analisi mediche e centri di riabilitazione;
- società di call center;
- società che forniscono servizi informatici;
- società che erogano servizi televisivi a pagamento.





QUALI SONO I REQUISITI DELLA FIGURA?

Il Responsabile della protezione dei dati RDP o DPO Data Protection Officer, nominato dal titolare del trattamento o dal responsabile del trattamento, dovrà:

1. possedere un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali, anche in termini di misure tecniche e organizzative o di misure atte a garantire la sicurezza dei dati. Non sono richieste attestazioni formali o l'iscrizione ad appositi albi professionali, anche se la partecipazione a master e corsi di studio/professionali può rappresentare un utile strumento per valutare il possesso di un livello adeguato di conoscenze;

2. adempiere alle sue funzioni in piena indipendenza e in assenza di conflitti di interesse . In linea di principio, ciò significa che il RPD non può essere un soggetto che decide sulle finalità o sugli strumenti del trattamento di dati personali;

3. operare alle dipendenze del titolare o del responsabile oppure sulla base di un contratto di servizio (RPD/DPO esterno).

Il titolare o il responsabile del trattamento dovranno mettere a disposizione del Responsabile della protezione dei dati le risorse umane e finanziarie necessarie all'adempimento dei suoi compiti.





COMPITI E INCARICHI DEL DPO

Il Data Protection Officer nasce per svolgere funzioni diverse, alcune di natura ispettiva e altre di natura consulenziale:

- **Consulenza** – informare e sensibilizzare il titolare o il responsabile del trattamento, nonché i dipendenti di questi ultimi, riguardo agli obblighi derivanti dal regolamento e da altre disposizioni in materia di protezione dei dati;
- **Vigilanza** – Sorvegliare l'osservanza del GDPR e delle policy per la protezione dati adottate dal Titolare o dal Responsabile, inclusi l'attribuzione della responsabilità, la sensibilizzazione e la formazione del personale coinvolto nei trattamenti, valutando i rischi di ogni trattamento alla luce della natura, dell'ambito di applicazione, del contesto e delle finalità;
- **Fornire Pareri** – Fornire un parere in merito alla DPIA (Data Protection Impact Assessment, Valutazione d'impatto sulla protezione dei dati), valutando se sia opportuno condurla e sorvegliandone lo svolgimento dopo aver definito le modalità di esecuzione.
- **Collaborazioni** – Collaborare con l'Autorità di controllo e gli interessati, fungendo da punto di contatto per facilitare l'accesso delle Autorità ai documenti e alle informazioni necessarie per lo svolgimento delle loro attività di indagine, correzione, autorizzazione e consulenza attribuite dal GDPR

LA NOSTRA SQUADRA È COMPOSTA DA PROFESSIONISTI QUALIFICATI E CERTIFICATI PER L'ASSUNZIONE DI QUESTO IMPORTANTE RUOLO

LA NOSTRA ASSICURAZIONE

Nasce in Italia il professionista della Privacy, il D.P.O. (Data Protection Officer) o Responsabile protezione dati (R.D.P.), una nuova figura professionale normata dal Regolamento U.E. n. 2016/679 (GDPR), pubblicato sulla Gazzetta Ufficiale Europea il 4/5/2016.

Moltissime Aziende ed Enti pubblici, dal 26.05.2018 devono adeguare il proprio regolamento Privacy, i propri processi di trattamento dati e individuare il DPO/Responsabile Protezione Dati che può essere un dipendente/dirigente dell'azienda oppure un professionista esterno.

Ad oggi il DPO non deve essere iscritto in un apposito albo, ma è necessaria una comprovata competenza in materie giuridiche e informatiche; Il DPO assiste in tutto ciò che è Privacy il Responsabile del Trattamento dell'azienda / ente pubblico ed è la persona di riferimento e di contatto per gli utenti / clienti, alla quale possono rivolgersi per tutte le questioni inerenti il trattamento dei loro dati personali.

La copertura R.C. professionali del DPO tutelano il Responsabile Protezione Dati, sia esso un professionista o un dipendente, per i danni involontariamente cagionati all'azienda e/o a terzi nello svolgimento di tutte le mansioni e funzioni svolte sulla base del regolamento europeo 2016/679 sulla protezione dei dati personali e le norme vigenti in materia.

Le coperture assicurative che abbiamo prevedono l'abbinamento di una polizza RC Patrimoniale ad una polizza rimborso delle spese di tutela legale e peritale.





LA NOSTRA OFFERTA

EASYDPO AS A SERVICE

Le skills richieste dal ruolo del DPO sono molteplici e variegate, e difficilmente una singola persona fisica è in grado di possederle tutte quante. Per questo motivo il nostro servizio Easy DPO viene erogato come persona giuridica. Solo in questa maniera è possibile garantire realmente la piena conformità normativa ai compiti richiesti dal ruolo stesso, e nel contempo offrire al cliente un team di esperti che possano coprire la totalità delle esigenze generate dalla complessa tematica della Privacy e Data Protection.

Il nostro Team è composto da Avvocati, Cybersecurity Manager, Specialisti IT, Specialisti dei processi Aziendali, Formatori, Problem Solver ed Auditor, con esperienza più che ventennale nel campo Privacy e Sicurezza delle informazioni

Il servizio Easy DPO per l'azienda nasce da un progetto costruito in modalità completamente custom per il cliente :

- Identificazione esigenza
- Videocall di screening
- Creazione progetto ad-hoc
- Welcome Call
- Gestione del processo e roadmap di lavoro
- Audit periodico
- Canone annuale certo





LA NOSTRA OFFERTA

VALUTAZIONE DI IMPATTO (DPIA) E RISCHIO DEL TRATTAMENTO

La Valutazione d'impatto (DPIA), è un processo di analisi dei rischi specifico molto importante, che deve essere effettuato nei casi dove i diritti e le libertà delle persone fisiche sono particolarmente a rischio. Gli ambiti di applicazione dove una DPIA è obbligatoria sono molteplici, come ad esempio la video sorveglianza su larga scala, la profilazione continua delle persone, la conformità degli applicativi gestionali aziendali (CMR), la gestione dei dati particolari (sensibili) come quelli sanitari, solo per citarne alcuni.

La valutazione di impatto deve contenere:

- **la descrizione sistematica dei trattamenti previsti**, la finalità del trattamento, compreso la base giuridica (quindi l'eventuale interesse legittimo) utilizzata dal titolare);
- **la valutazione della necessità e proporzionalità** del trattamento in relazione alla finalità;
- **la valutazione dei rischi** per i diritti e le libertà degli interessati;
- **le misure previste per affrontare i rischi**, incluse le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati e dimostrare la conformità al regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Il titolare e il responsabile del trattamento provvedono a sviluppare la valutazione di impatto. E' preferibile che sia una squadra a portare avanti la valutazione, in modo che più componenti possano dare un contributo. La valutazione implica l'analisi e la descrizione delle aree critiche da esaminare, del profilo di tutti i soggetti coinvolti, gli effetti e le conseguenze del trattamento dei dati, una valutazione dei rischi collegati, e quindi la stesura di un piano di mitigazione dei rischi. Il DPO analizzerà il rapporto e proporrà eventuali migliorie. Se il rapporto è approvato si passa all'attuazione delle misure di sicurezza proposte.





LA NOSTRA OFFERTA

ISO 27001

Qualunque sia il settore, il vostro sistema informativo è il cuore del vostro business. La certificazione ISO 27001 ne garantisce la protezione, il miglioramento e le prestazioni.

Cybersecurity, protezione dei dati personali, controllo dei dati, gestione dei sistemi informativi: assicurate i vostri sistemi informativi con ISO 27001.

La certificazione ISO/IEC 27001 di AFAQ dimostra che avete implementato un efficace sistema di gestione della sicurezza delle informazioni (ISMS) basato sullo standard internazionale di riferimento, ISO 27001. Definisce una metodologia per identificare le minacce informatiche, controllare i rischi associati alle informazioni critiche della vostra organizzazione e mettere in atto misure di protezione appropriate per garantire la riservatezza, la disponibilità e l'integrità delle informazioni.

La certificazione ISO 27001 di AFAQ non è solo per host di dati, start-up, multinazionali o aziende IT.

Tutte le organizzazioni, aziende e autorità locali, di tutte le dimensioni e in tutti i settori che detengono dati, fisici o dematerializzati, sono interessate.

I VANTAGGI DI QUESTA CERTIFICAZIONE

- Identificare le minacce e i pericoli per il tuo sistema informatico
- Mobilitare i vostri team intorno a un progetto comune
- Migliorare le vostre pratiche per rendere sicuro il vostro sistema informativo
- Controllare i costi legati alla sicurezza informatica
- Sostenere il tuo business
- Aumentare la fiducia dei vostri clienti e soddisfare i loro requisiti di sicurezza





I NOSTRI CONTATTI

contatta@easygdpr.it

www.easygdpr.it

SEGUICI ANCHE SUI NOSTRI
SOCIAL & BLOG





● ● ●
E A S Y D P O[®]

*Ogni linea, punto
o dato ha la sua
complessità e
caratteristica.
Scegli quella fa
per te.*

