

GDPR – come adeguarsi al Regolamento Europeo

CRISTINA COLUCCI
Comitato Privacy & Gdpr
Fondazione Torino Wireless

Fondazione Torino Wireless

La nostra mission:

contribuire alla
competitività del territorio,
accelerando la
crescita delle imprese
che usano le tecnologie
come fattore strategico di
sviluppo e affiancando le
istituzioni nella
progettazione e gestione dei
processi di innovazione



Torino Wireless per il GDPR

Esperienza e competenza nella gestione di processi di **supporto a cluster di imprese e a soggetti pubblici**

Un team di auditor e sistemi di **assessment e valutazione certificati e assicurati**

Facilità di approccio grazie agli strumenti online e alla piattaforma in cloud



Conformità al GDPR: come fare

Tutte le imprese dal 25 Maggio dovranno garantire una protezione ottimale dei dati personali che trattano ed essere in grado di dimostrare in ogni momento la loro conformità documentandola.



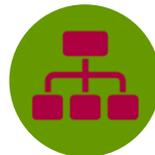
1. Designare un esperto



4. Gestire i rischi



2. Mappare



5. Organizzare



3. Individuare le priorità



6. Documentare

Nominare un DPO: sono obbligato?

La nomina di un responsabile della protezione dei dati è obbligatoria se:

- Sei un ente pubblico
- Sei una società la cui attività di base ti porta a svolgere un regolare e sistematico monitoraggio delle persone su larga scala, o a trattare su larga scala i cosiddetti dati "sensibili" o relativi a condanne penali e reati

Il DPO è una risorsa importante per comprendere e rispettare gli obblighi del regolamento, per dialogare con le autorità per la protezione dei dati e per ridurre i rischi di contenzioso.



Designare un DPO

*Prima di **nominare** il tuo rappresentante per la protezione dei dati, assicurati che queste tre condizioni siano soddisfatte:*

- Possiede le competenze richieste
- Dispone di mezzi sufficienti per svolgere i suoi compiti
- Ha la capacità di agire in modo indipendente



Mappare i trattamenti sui dati personali

Per ogni trattamento dei dati personali, porsi le seguenti domande:

- CHI?
- COSA?
- PERCHÉ?
- DOVE?
- FINO A QUANDO?
- COME?



Quali azioni per ciascun trattamento

- **Assicurati** che **solo i dati strettamente necessari** per il perseguimento dei tuoi obiettivi siano raccolti ed elaborati.
- **Identifica la base giuridica** su cui si basa il trattamento (ad esempio: consenso della persona, interesse legittimo, contratto, obbligo legale)
- **Verifica** che i tuoi **fornitori** conoscano i loro nuovi obblighi e le loro responsabilità, assicurati che ci siano clausole contrattuali che ricordino gli obblighi del fornitore per quanto riguarda la sicurezza, la riservatezza e la protezione dei dati personali trattati .
- **Pianifica** come esercitare i **diritti degli interessati** (diritto di accesso, rettifica, diritto alla portabilità, ritiro del consenso ...)
- **Controlla** le **misure di sicurezza** in atto



Trattamenti che richiedono una vigilanza speciale



- Stai elaborando dati particolari
- Il tuo trattamento ha lo scopo o l'effetto di un monitoraggio sistematico su vasta scala o di un'area accessibile al pubblico
- Stai trasferendo dati al di fuori dell'unione europea



Gestisci i rischi



Se hai identificato un trattamento di dati personali che può comportare un **alto rischio** per i diritti e le libertà degli interessati, dovrai condurre una **valutazione** del suo **impatto** sulla **protezione dei dati**



Che cos'è una DPIA

È uno studio che contribuisce a creare un'elaborazione dei dati che rispetti la privacy e che dimostri la conformità del trattamento con GDPR. Una DPIA è uno strumento di valutazione dell'impatto sulla privacy.

Una DPIA contiene:

- Una descrizione del trattamento e delle sue finalità
- Una valutazione della necessità e proporzionalità delle operazioni di trattamento
- una valutazione del rischio per i diritti e le libertà delle persone interessate
- le misure previste per far fronte ai rischi



Quando la DPIA è obbligatoria

Si deve condurre una DPIA per qualsiasi trattamento che possa comportare rischi elevati per i diritti e le libertà delle persone interessate (articolo 35 del GDPR).

Nelle linee guida del G29 sono definiti 9 criteri per aiutarti a determinare se il tuo trattamento può causare rischi elevati :

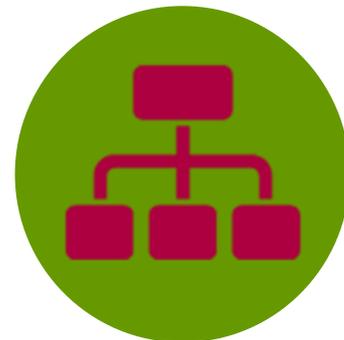
- Valutazione basata sulla profilazione personale
- Decision making automatizzato con effetti legali sulle persone
- Monitoraggio (video sorveglianza) su vasta scala
- Dati sensibili o dati di natura altamente personale
- Dati personali trattati su larga scala
- Matching e combinazione di dataset diversi
- Dati riguardanti persone vulnerabili
- Uso innovativo di dati o applicazione di nuove soluzioni tecnologiche o organizzative
- Esclusione dal beneficio di un diritto, servizio o contratto



Organizzare i processi interni

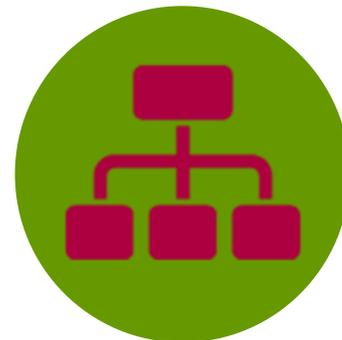
Per garantire un **livello elevato di protezione dei dati personali** in ogni momento, occorre:

- implementare procedure interne che garantiscano la protezione dei dati
- tenere conto di tutti gli eventi che possono verificarsi durante la vita di un trattamento



Cosa implica organizzare i processi interni

- **prendere in considerazione la protezione dei dati personali nella progettazione** di un'applicazione o di un trattamento
- **aumentare la consapevolezza e organizzare il feedback delle informazioni** creando un piano di formazione e comunicazione tra i dipendenti
- **gestire i reclami e le richieste degli interessati per l'esercizio dei loro diritti**
- **anticipare le violazioni dei dati** fornendo, in alcuni casi, la notifica all'autorità di protezione dei dati entro 72 ore e alle persone interessate quanto prima.



Conformità del documento

Per dimostrare la tua conformità alle regole, devi creare e consolidare la documentazione necessaria. Le azioni e i documenti completati in ogni fase devono essere rivisti e aggiornati regolarmente per garantire la protezione continua dei dati.



Quali documenti devo predisporre

DOCUMENTAZIONE SUL TRATTAMENTO DEI DATI PERSONALI

- **Registro dei trattamenti**
- **Valutazioni di impatto sulla protezione dei dati (DPIA)** per i trattamenti che possono rappresentare un rischio elevato per i diritti e le libertà delle persone
- **Inquadramento dei trasferimenti di dati** al di fuori dell'Unione Europea (incluse clausole contrattuali standard, BCR e norme vincolanti d'impresa)

INFORMAZIONI ALLE PERSONE

- **Informative**
- Modelli di **raccolta del consenso delle persone interessate**
- Procedure messe in atto per **l'esercizio dei diritti**

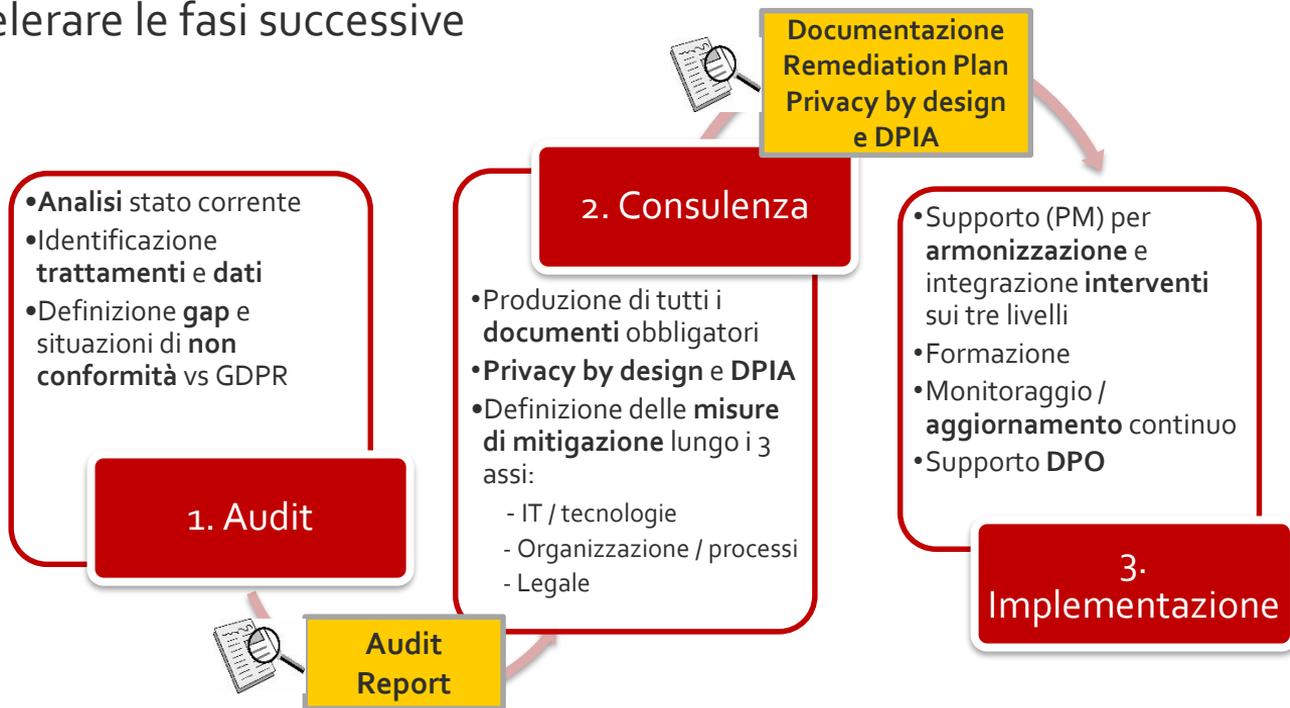
CONTRATTI CHE DEFINISCONO I RUOLI E LE RESPONSABILITÀ

- **Contratti con fornitori**
- Procedure interne **per violazioni dei dati**
- Certezza del **consenso al trattamento dei dati** da parte delle persone interessate



Il processo per il servizio GDPR

Un intervento suddiviso in fasi, ciascuna definita (tempi, costi) con **risultati certi** e in grado di accelerare le fasi successive



Metodologia, competenze, documenti sono certificati e assicurati

1. Audit di conformità GDPR

Verifica della conformità rispetto al GDPR:

1. **Censimento dei dati e dei relativi trattamenti:** analisi dei dati trattati in azienda e verifica di quelli interessati al trattamento GDPR
2. **Addetti Privacy:** definizione dei ruoli ricoperti da chiunque operi sui dati personali, sia direttamente (ad es. elaborandoli, modificandoli), sia indirettamente (ad esempio chi effettua i back-up)
3. **Misure adottate:** analisi delle misure adottate dall'azienda per garantire la sicurezza ed il corretto trattamento dei dati, evidenziando le misure minime di sicurezza previste.

Il servizio richiede il coinvolgimento del management aziendale nelle giornate di avvio dell'Audit e in quella di restituzione dei report finali e delle raccomandazioni

Questa fase produce un report di conformità

2. Consulenza: la documentazione GDPR

Fornitura della **documentazione** obbligatoria **GDPR** basata sulle analisi di dettaglio eseguite nella verifica di conformità GDPR ed è quindi **specificatamente definita per il Cliente**. Tutta la documentazione è **garantita GDPR** compliant e **assicurata** in caso di errori e rimane sempre **memorizzata e tracciata sul sistema PrivacyLab**.

La documentazione comprende:

- Registro del trattamento dei dati
- Informativa per ogni trattamento
- Consensi
- Nomine (addetti e responsabili)

Questa fase produce i documenti richiesti dal GDPR

3. Privacy by design

La **valutazione di impatto** (DPIA) rappresenta uno degli elementi di maggiore rilevanza nel nuovo quadro normativo del GDPR, una **buona prassi** al di là dei casi di obbligatorietà di legge e permette di realizzare concretamente un principio fondamentale del GDPR, ossia la **protezione dei dati fin dalla fase di progettazione** (Privacy by design).

Il servizio descrive un trattamento di dati per valutarne la necessità e la proporzionalità nonché i relativi rischi, allo scopo di approntare misure idonee ad affrontarli. Il servizio analizza le informazioni relative a:

- Analisi dei rischi
- Piano di compliance
- Piano di formazione

Questa fase produce il report di analisi dei rischi e la DPIA

Privacy Lab: il valore della Piattaforma



Sviluppata in cloud da **MetisLab Srl**, è un SW che garantisce:

- ✓ **Certificazione** di conformità al Regolamento 
- ✓ **Assicurazione** contro ogni errore tecnico da CBL Insurance Europe 
- ✓ **Aggiornamento** costante rispetto al Regolamento GDPR (RU 16/679)

Che cosa fa:

- 1 Guida il processo di **Valutazione dei Rischi**, supportando la **determinazione delle misure** necessarie per la **mitigazione** degli stessi
- 2 Supporta il **Monitoraggio dell'intero processo di trattamento** dei dati e di tenere sempre sotto controllo la struttura organizzativa
- 3 Genera tutta la **documentazione** necessaria (Registro dei Trattamenti, DPIA, atti di nomina, contratti, informative, cookie policy, ...)

Compresa nel servizio di Audit / Consulenza erogato da Torino Wireless

QUESTA È LA TUA DASHBOARD

Se vuoi accedere alla versione precedente, puoi ancora farlo da qui: [Accedi](#)

I TUOI DOCUMENTI



INFORMATIVE

● Visualizza documenti



NOMINE

● Visualizza documenti



PRIVACY BY DESIGN

● Visualizza documenti



REGISTRO DEI TRATTAMENTI

● Visualizza documenti



VALUTAZIONE DI IMPATTO

● Visualizza documenti



ARCHIVIO STORICO

● Visualizza documenti

GESTIONE DEL PORTALE



LICENZE

● Inserisci rinnovi e nuovi codici



AZIENDE

● Gestione dati azienda



UTENTI

● Gestione utenti licenza



IMPORTA DATI

A breve disponibile



Censimento dei Trattamenti

Per poter generare la documentazione e verificare Liceità, Modalità dei trattamenti, compliance al GDPR ecco la prima sezione da affrontare.

[VAI AL CENSIMENTO](#)



Addetti Privacy

Vengono definiti i ruoli ricoperti da chiunque operi sui dati personali, sia direttamente (elaborandoli, modificandoli, ecc.) sia indirettamente.

[VAI AGLI OPERATORI](#)



Privacy by Design

Vengono inserite le misure adottate dall'azienda per garantire la sicurezza ed il corretto trattamento dei dati. Il sistema vi guiderà per riuscire a verificare la privacy by Design dei vostri trattamenti.

[VAI ALLE MISURE](#)



Valutazione di impatto

Vengono inserite le informazioni relative all'analisi dei rischi, al piano di compliance ed al piano di formazione. Il completamento di questa sezione è facoltativo.

[VAI ALLA VALUTAZIONE DI IMPATTO](#)



ELENCO DEI TRATTAMENTI EFFETTUATI DALL'AZIENDA

Nascondi



Un trattamento comprende tutte le operazioni che vengono effettuate sui dati personali di cui l'azienda ha titolarità.

Ogni azienda effettuerà diversi tipi di trattamento, ad esempio: trattamenti relativi al "personale dipendente".

Questa tipologia di trattamento comprenderà tutte le operazioni necessarie relative al personale dipendente, ad esempio la gestione degli orari di lavoro, la gestione delle trattenute sindacali, la gestione delle malattie.

Un'altra tipologia di trattamento potrebbe essere generata dall'apertura di un sito internet o di una pagina facebook, nel caso in cui l'azienda decida di recuperare informazioni sui visitatori per sfruttarle per attività di marketing o pubblicitarie.

PRIVACYLAB GDPR propone come aiuto alcune tipologie standard di trattamenti.

Scegliendo la tipologia appropriata, il sistema vi proporrà negli step successivi le impostazioni solitamente associate a questi trattamenti.

RICORDATEVI, dovete inserire tutti i trattamenti sui dati di persone fisiche quindi: Posta elettronica, Sito WEB, Pagine Social, Gestionale (se avete come clienti persone fisiche), CRM, Videosorveglianza, Dipendenti, Curricula, etc.

TRATTAMENTO	TIPOLOGIA	DESCRIZIONE	CONTO TERZI	
Acquisti	Acquisti		No	Modifica Elimina
Facebook	Social Network	Promozione aziendale tramite social	No	Modifica Elimina
Gestione Personale	Gestione Personale		No	Modifica Elimina

NUOVO TRATTAMENTO

PASSA ALLA FASE SUCCESSIVA

Gli interessati

- 1 Interessati al trattamento 8
 - agenti e rappresentanti
 - clienti
 - consulenti e liberi professionisti, anche in forma associata
 - fornitori
 - Navigatori Sito Internet
 - personale dipendente e personale parasubordinato**
 - A **dati trattati**
 - B finalità del trattamento
 - C modalità del trattamento
 - D categorie di addetti
 - E comunicazione dei dati
 - F diffusione dei dati
 - G periodo di conservazione
 - H trasferimento dei dati
 - potenziali clienti
 - Referenti presso Aziende Fornitrici

Dati degli interessati Nascondi

È ora necessario raccogliere i dati necessari per realizzare le informative ai soggetti interessati al trattamento. Scegliere, tra i dati presenti nelle banche dati, i dati che fanno riferimento nello specifico a 'dati degli interessati'. Se volete aggiungere un tipo di dato non presente, tornate indietro ed inseritelo nel trattamento a cui va associato, sotto la voce 'Tipi di Dati'.
Ricordiamo che:

1. L'informativa deve essere data all'atto di acquisizione dei dati presso l'interessato, o prima dell'acquisizione.
2. Se i dati personali non sono raccolti presso l'interessato, il comma 4 dell'art. 13 prevede che l'informativa sia resa agli interessati all'atto della registrazione dei dati o, quando è prevista la loro comunicazione, non oltre la prima comunicazione.
3. Se i dati non sono stati raccolti presso l'interessato, ma comunicati da terzi,

<input type="checkbox"/>	QUALI DATI TRATTI PER QUESTA CATEGORIA DI INTERESSATI?	
<input type="checkbox"/>	Adesione a sindacati	Dato Particolare
<input type="checkbox"/>	Attività economiche, commerciali, finanziarie e assicurative	Dato Comune
<input type="checkbox"/>	Codice fiscale ed altri numeri di identificazione personale	Dato Comune
<input type="checkbox"/>	Convinzioni religiose	Dato Particolare
<input type="checkbox"/>	dati relativi al tipo di lavoro ed alla retribuzione	Dato Comune
<input type="checkbox"/>	Dati relativi alla famiglia e a situazioni personali	Dato Comune
<input type="checkbox"/>	Dati relativi allo svolgimento delle attività economiche dell'interessato.	Dato Comune
<input type="checkbox"/>	Informazioni concernenti i provvedimenti giudiziari.	Dato Giudiziario
<input type="checkbox"/>	Informazioni concernenti la qualità di imputato od indagato.	Dato Giudiziario
<input type="checkbox"/>	Istruzione e cultura	Dato Comune
<input type="checkbox"/>	Lavoro	Dato Comune
<input type="checkbox"/>	Log File di Navigazione Internet	Dato Particolare
<input type="checkbox"/>	Nominativo, indirizzo o altri elementi di identificazione personale	Dato Comune

DATI TRATTATI

FINALITÀ DEL TRATTAMENTO

MODALITÀ DEL TRATTAMENTO

CATEGORIE DI ADDETTI

COMUNICAZIONE DEI DATI

DIFFUSIONE DEI DATI

PERIODO DI CONSERVAZIONE

TRASFERIMENTO DEI DATI

Informative e consensi

INFORMATIVA GDPR (0)

INFORMATIVE 196/2003 (0)



Informativa GDPR

Nascondi



È possibile scegliere se rendere pubblica un'informativa. In questo modo sarà inserita nell'informativa il link all'indirizzo web in cui gli interessati potranno visionare l'informativa sempre aggiornata. Dopo aver selezionato le informative che si desidera pubblicare salvare le impostazioni facendo clic sul bottone sottostante

STATO	INFORMATIVA PER	ULTIMA GENERAZIONE	PUBBLICA	
—	agenti e rappresentanti	16/05/2018	<input type="checkbox"/>	Modifica Anteprima PDF
—	clienti	20/04/2018	<input type="checkbox"/>	Modifica Anteprima PDF
—	consulenti e liberi professionisti, anche in forma associata	non generato	<input type="checkbox"/>	Modifica Anteprima PDF
—	fornitori	non generato	<input type="checkbox"/>	Modifica Anteprima PDF
—	Navigatori Sito Internet	non generato	<input type="checkbox"/>	Modifica Anteprima PDF
—	personale dipendente e personale parasubordinato	non generato	<input type="checkbox"/>	Modifica Anteprima PDF
—	potenziali clienti	non generato	<input type="checkbox"/>	Modifica Anteprima PDF
—	Referenti presso Aziende Fornitrici	non generato	<input type="checkbox"/>	Modifica Anteprima PDF

SALVA IMPOSTAZIONI PER IL WEB



Accadimenti per la sede : Sede Principale azienda

Nascondi



Selezionare i rischi, assegnando la frequenza e la gravità ipotizzate. Vedi anche la tabella di riferimento:

Frequenza		Gravità	
molto bassa	1 volta ogni 10 anni circa	molto bassa	il danno risulta accettabile
bassa	1 volta ogni 2 anni circa	bassa	il danno non comporta importanti problemi
alte	1 volta ogni 10 mesi circa	alta	il danno comporta molti problemi
molto alta	1 volta ogni 2 mesi circa	molto alta	il danno comporta conseguenze molto serie

Rischio totale iniziale per:

CASSETTO BUSTE PAGA (52/100)

PC AMMINISTRAZIONE (24/100)

ARMADIO AMMINISTRAZIONE (1/100)

Tipi di dati presenti:

- DATI COMUNI
- DATI PARTICOLARI
- DATI PARTICOLARI GIUDIZIARI

Tipi di archivio presenti:

- ARCHIVIO CARTACEO
- ARCHIVIO DIGITALE
- IN RETE PUBBLICA



ACCADIMENTI PER:

FREQUENZA

GRAVITÀ



Allagamento

molto bassa

molto alta



Indisponibilità erogazione energia elettrica

bassa

bassa



Fenomeni climatici (Uragani, Nevicate, Fulmini)

molto bassa

bassa

INSERISCI UN NUOVO ACCADIMENTO

SALVA

SALVA E PASSA ALLA FASE SUCCESSIVA

Misure adottate



Misure Adottate

Nascondi



Il presente documento è ad uso interno dell'azienda, per avere un riferimento chiaro su quali siano le misure minime da adottare in funzione dei dati trattati e delle unità di archiviazione utilizzate. Nel documento è anche riportato se tali misure sono già state implementate o meno in azienda, a seconda che siano state inserite o no nelle Misure Adottate.

STATO	DOCUMENTO	DESCRIZIONE	ULTIMA GENERAZIONE	SCARICA
-	Privacy by Design	Privacy by Design	non generato	Modifica Anteprima PDF
-	Elenco misure di sicurezza	Descrizione generale delle misure di sicurezza tecniche ed organizzative di cui art 32, paragrafo 1 del Regolamento Europeo, per trattamenti ed archivi	non generato	Modifica Anteprima PDF
-	Misure consigliate	Descrizione delle misure consigliate in riferimento alle misure minime dell'Allegato B D.Lgs 196/2003. Nonostante tale misure non siano più obbligatorie, rimangono una linea guida delle misure minime di sicurezza da adottare.	10/04/2018	Modifica Anteprima PDF
-	Ripristino dei dati	Piano di Ripristino dei dati	non generato	Modifica Anteprima PDF
-	Accesso controllato agli archivi	Obsoleto. Elenco Soggetti autorizzati ad accedere agli archivi cartacei con dati particolari o giudiziari dopo l'orario di chiusura, come per D.lgs 196/2003	non generato	Modifica Anteprima PDF
-	Piano di Formazione	Piano di Formazione Addetti	10/04/2018	Modifica Anteprima PDF

Grazie!

crisrina.colucci@torinowireless.it
gdpr@torinowireless.it