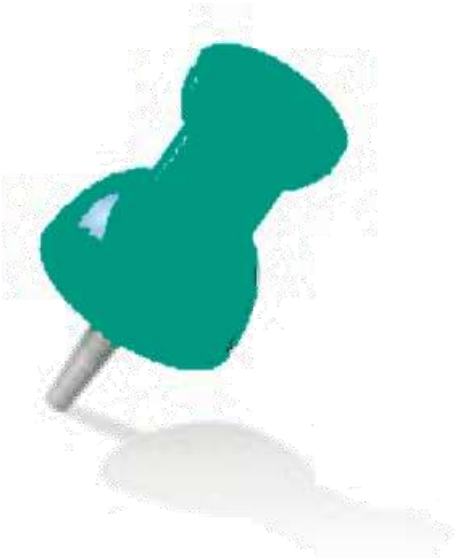
8 Linee guida GDPR per i Club

(General Data Protection Regulation)

Rotary
Distretto 2060



Indice

GDPR - Regolamento UE 2016/679

Il nuovo Regolamento (UE) 2016/679 per la Protezione dei Dati o GDPR (General Data Protection Regulation) determina le "linee guida" da adottare in materia di Protezione delle Persone Fisiche con riguardo al Trattamento dei Dati nonché alla libera circolazione di tali dati.

È importante sottolineare il fatto che, bensì l'obbligo sia per tutte le organizzazioni, i "Dati" a cui si riferisce il Regolamento sono quelli che riconducono o che si possono in qualche modo ricondurre a Persone Fisiche e non giuridiche.

Scarica Regolamento GDPR Regolamento Generale Protezione Dati UE 2016/679 nel formato pdf (circa 88 pagine) – link.

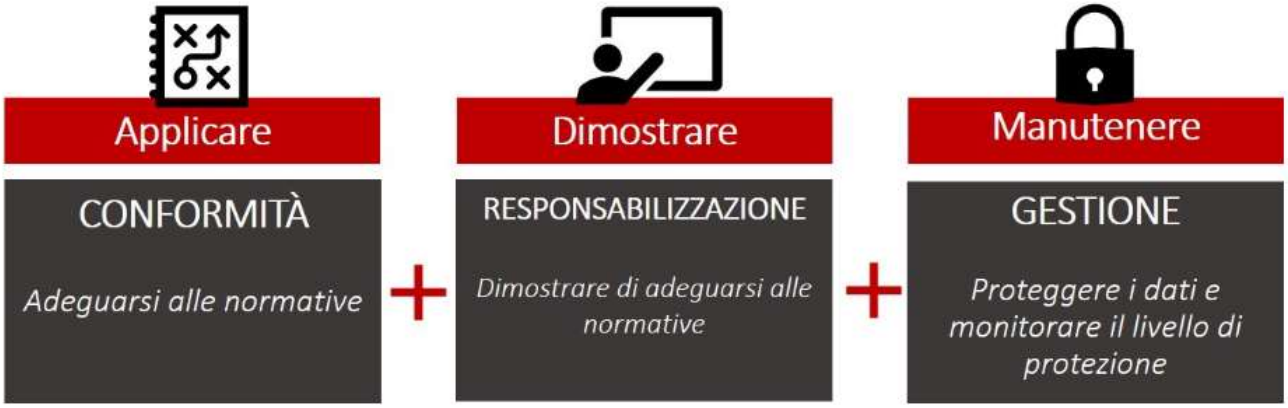
Differenze tra GDPR e attuale "Legge Privacy" D.lgs 196/2003

La novità principale del nuovo regolamento è che sparisce il concetto di "MISURE MINIME", alla base dell'attuale normativa D.Lgs 196, per lasciare il posto a quello di "MISURE ADEGUATE".

Ma, la vera rivoluzione, è l'introduzione del nuovo principio di "ACCOUNTABILITY" (Responsabilizzazione).

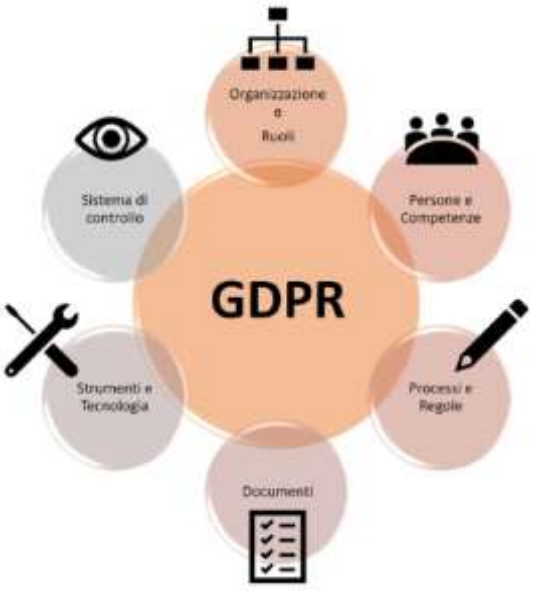
Tale principio di fatto attribuisce più discrezionalità ma, al tempo stesso, maggiore responsabilità al "Titolare del Trattamento" su tutto quello che concerne la protezione dati con un inasprimento consistente delle sanzioni previste in caso di inadempienza.

Se è vero che viene lasciato più spazio alla discrezionalità è anche vero che, il Titolare ed il Responsabile del Trattamento hanno il preciso dovere di dimostrare le ragioni che hanno determinato le scelte fatte.



Soggetti del trattamento nel nuovo GDPR

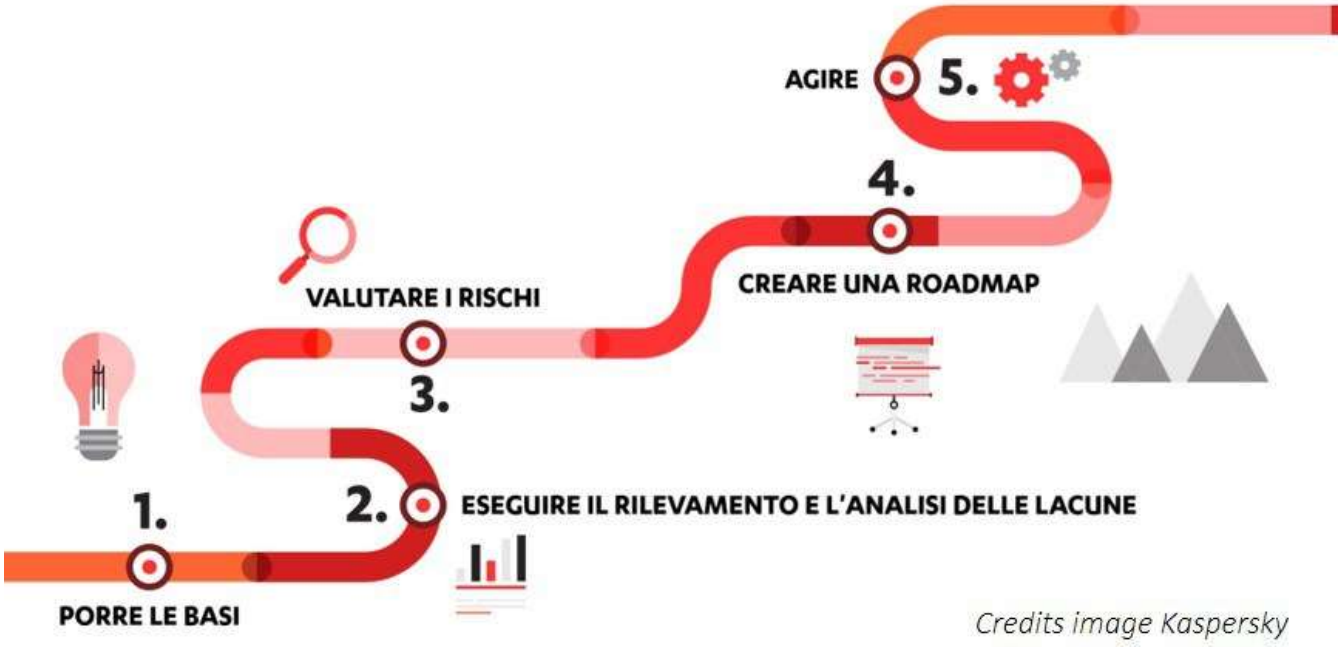
- **INTERESSATO** al Trattamento: la persona fisica oggetto del trattamento dati.
- **TITOLARE** del Trattamento: la persona fisica o giuridica (Governatore, Presidente di Club) titolare del trattamento.
- **RESPONSABILE** del Trattamento: la persona fisica o giuridica responsabile di un determinato trattamento. Può essere anche esterno mediante nomina (es. dati in Hosting, provider di posta, servizio archiviazione, ecc.) o interno (es. Dirigenti di Distretto, Dirigenti di Club, Presidente Commissione Informatica).
- **INCARICATI** del trattamento: la persona fisica autorizzata dal Titolare o dal Responsabile a compiere operazioni di trattamento dei dati (es. Dirigenti Distretto e Club, segretarie Distretto, e Club, Componenti Commissione Informatica).
- **DPO** (Data Protection Officer) o Privacy Officer: è una nuova figura opzionale introdotta nel 2016 dal GDPR che viene nominata solo in particolari situazioni.
  La sua responsabilità è osservare, valutare, organizzare il trattamento, vigilare nel rispetto delle normative privacy europee e nazionali.



- Entrambi, Titolare e Responsabile, rispondono legalmente.
- Possono essere nominati anche più Responsabili del trattamento.
- Gli Incaricati del trattamento sono nominati dal Titolare o dai Responsabili.

Piano della Privacy del Distretto 2060

Il progetto 'GDPR strumenti digitali Distretto 2060' è stato avviato a fine gennaio 2018 dalla Commissione Informatica con l'intento di adeguare i informatici digitali distrettuali ai requisiti richiesti dal GDPR.
L'approccio metodologico adottato è stato il seguente.



Credits image Kaspersky

1. Porre le basi - Coinvolgimento Governatori - febbraio-marzo 2018.
2. Rilevare - Analisi dei servizi digitali distrettuali - marzo-aprile 2018.
3. Valutare i rischi – Sviluppo matrice dei rischi - aprile-maggio 2018.
4. Creare una RoadMap – da sviluppare nel periodo maggio-giugno 2018.
5. Agire – da avviare a giugno 2018 per poi proseguire.

Risultato finale della Fase 3.: GDPR dei servizi digitali del Distretto 2060.

Piano di azione per prevenire la violazione dei dati – RoadMap

Stabiliti gli obiettivi e le priorità, definito lo scenario e deciso come agire in base all'analisi dei rischi del trattamento dei dati, si definisce un piano di azione che è composto da specifici progetti, ognuno con un suo responsabile, risorse assegnate, competenze e scadenze.

Il piano di azione di riduzione dei rischi è composto da:

- Quick actions – azioni di breve/brevissimo periodo.
- Medium actions – azioni di medio periodo, della durata di circa un anno.
- Long actions – azioni di lungo periodo, che richiedono decisioni organizzative e tecnologiche, importanti impegni di risorse umane e finanziarie.
- Preventive actions – azioni preventive che prevengano l'insorgere di un potenziale rischio medio/alto.
- Formazione - formazione per le risorse coinvolte e per il monitoraggio.

Una vera e propria ROADMAP con le azioni da eseguire: da chi ha la responsabilità (definizione ruoli e competenze), in che modo ed in che tempi, la documentazione da produrre, le comunicazioni interne ed esterne, gli interventi infrastrutturali (IT), la consulenza ed infine la formazione ai Responsabili ed al personale.

Raccolta consenso e adeguamento informativa

Il trattamento dei dati personali è lecito se si fonda su un'idonea base giuridica.

Per quanto concerne il **consenso**, questo deve essere libero, specifico, informato e inequivocabile.

Non è ammesso tacito o presunto. Nel modulo di raccolta del consenso non è ammessa la presenza di eventuali caselle precompilate. La richiesta del consenso deve essere chiaramente distinguibile da altre richieste rivolte all'interessato.

Occorre prestare molta attenzione alla modulistica utilizzata.

Se il consenso è già stato raccolto e rispetta i requisiti del Regolamento (deve essere manifestato attraverso "dichiarazione o azione positiva inequivocabile") non occorre procedere con una ulteriore richiesta.

Per quanto concerne l'**informativa**, il Regolamento specifica le caratteristiche: deve avere forma concisa, trasparente, intelligibile per l'interessato e facilmente accessibile; deve utilizzare un linguaggio chiaro e semplice.

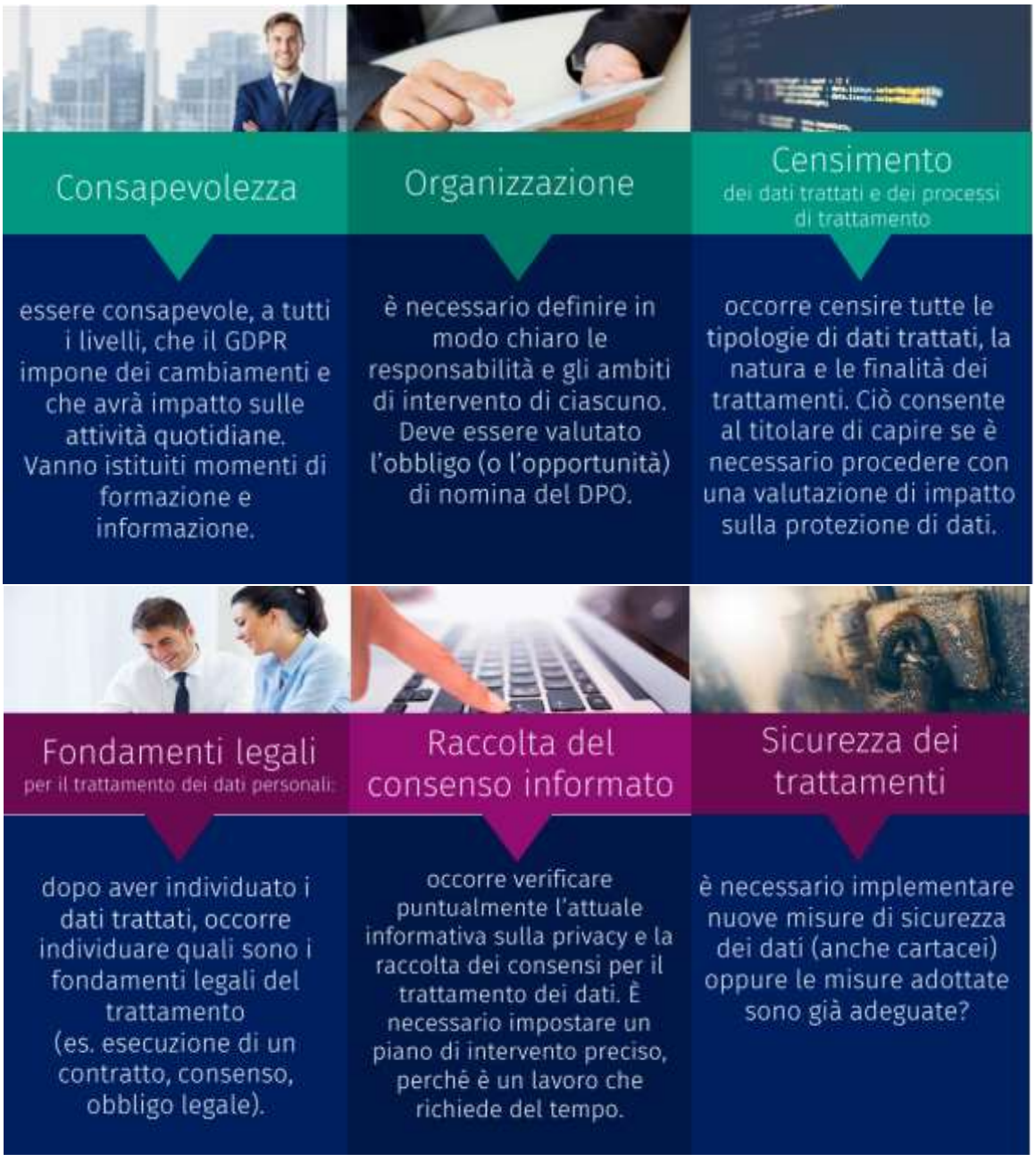
L'informativa è data, in linea generale, per iscritto e "preferibilmente in formato elettronico [..] attraverso un sito Web".

In caso di raccolta presso l'interessato dei dati che lo riguardano, il Titolare è tenuto a fornire all'interessato determinate informazioni.

Traccia modulistica da utilizzare – da richiedere alla segreteria o assistenza:

- Consenso informativo per il Socio.
- Consenso informativo per i fornitori.
- Consenso informativo potenziali Soci e per curricula.
- Informazione ai Soci comunicazione tramite eMail e pubblicazioni.
- Nomina responsabile trattamento interno ed esterno.
- Nomina del custode delle copie credenziali.
- Lettera ai prestatori di servizi.

Cosa fare per essere pronti al GDPR



GDPR e strumenti digitali

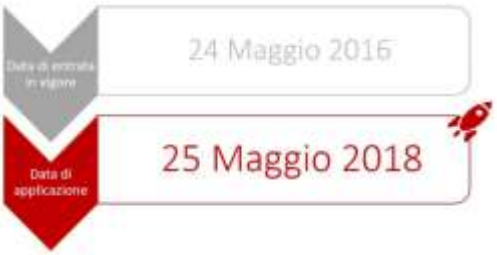
I servizi digitali del Distretto 2060 sono stati progettati e rilasciati per soddisfare il più possibile i requisiti del GDPR. Allo stato attuale sono da ritenersi affidabili, stabili, sicuri e conformi (GDPR compliance).

Come si devono organizzare i Club: per verificare la conformità al GDPR servizi digitali adottato del Distretto 2060 consultare la seguente check list.

Strumento Digitale D2060	In uso presso il Club	GDPR
Anagrafe ClubRunner	Si	GDPR D2060
	No	(*1)
Archiviazione ownCloud	Si	GDPR D2060
	No	(*1)
Posta di segreteria D2060	Si	GDPR D2060
	No	(*1)
Portali Club D2060 (Joomla)	Si	GDPR D2060
	No	(*1)

Con tutte risposte 'Si' i Club possono adottare il GDPR sviluppato dal Distretto.

Con risposta/e 'No' (*1) i Club sono costretti a sviluppare un GDPR autonomo, integrandolo con il GDPR del Distretto 2060 per i soli servizi digitali utilizzati.



Conclusioni

Il GDPR sta procedendo a grandi passi anche nella nostra organizzazione, che ha deciso di affrontarlo in un solo modo:

- Adottando un approccio maturo e moderno che parte dalla consapevolezza che, nel mondo digitale, tutti le attività sono ormai diventate Data Driven e il GDPR può essere quello stimolo in più ed una guida utile per mettere finalmente in atto quelle misure che servono al nostro Distretto per valorizzare e proteggere il patrimonio dei dati e tutte le esperienze maturate, e quindi non solo quella relativa ai dati personali oggetto del Regolamento.

Per adeguarsi al GDPR distrettuale i Club devono:

- Adottare i moderni servizi digitali forniti dal Distretto 2060 (ClubRunner, archiviazione ownCloud, posta, portali di Club D2060, ecc.).
- Allinearsi al regolamento interno diretto ad evitare comportamenti inconsapevoli che possano innescare problemi o minacce alla sicurezza dei dati ed al Brand Rotary.
- Eliminare supporti cartacei utilizzando il più possibile supporti digitali.
- Evitare l'archiviazione di dati e informazioni su supporti magnetici/ottici locali, utilizzando i servizi Cloud erogati dal Distretto (ownCloud).

Se si interpreta il GDPR come un'opportunità per crescere e rafforzarsi, e non come una mera formalità, si potranno ottenere sicuramente maggiori benefici nei prossimi anni e si potranno affrontare con più serenità progetti di servizio particolarmente complessi senza commettere "passi falsi" nella comunicazione digitale.