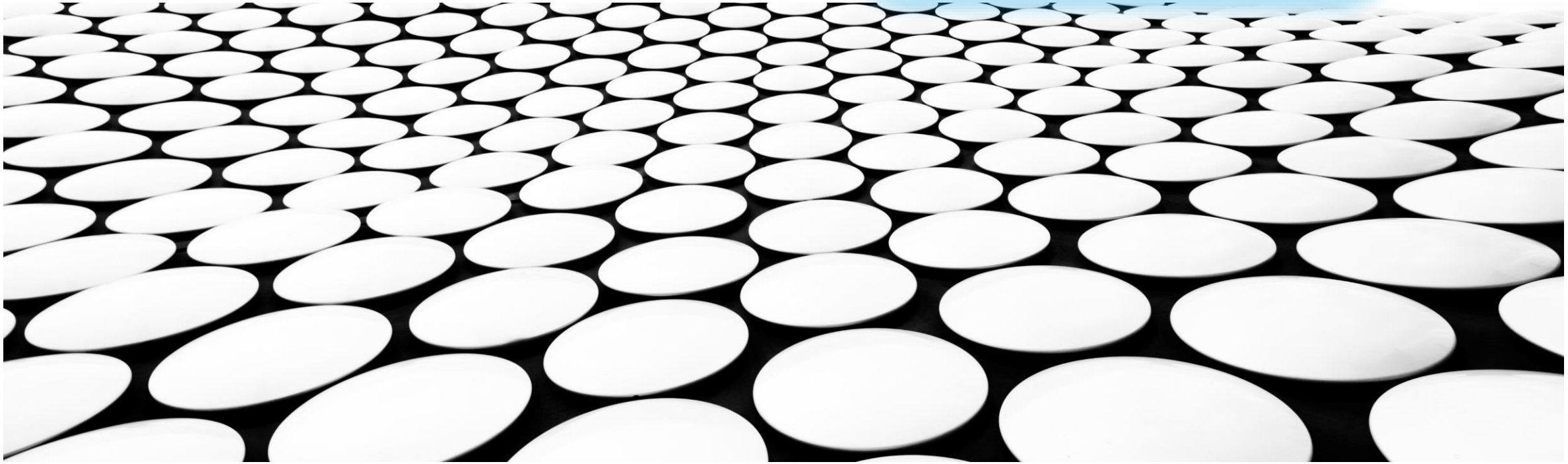
RGPD E SOCIAL MEDIA



Scopo della presentazione è valutare l'interdipendenza tra il **Regolamento Generale sulla Protezione dei Dati - RGPD UE 2016/679 -** ed **i social media** ed in tale ottica cercheremo di capire quali sono le cose importanti da tenere a mente, quando usiamo i social per motivi propri e per motivi di lavoro.

I ***social network*** sono sistemi software rappresentati da gruppi di individui connessi socialmente in rete tra loro; mentre, con ***social media*** si definiscono i servizi che offrono la possibilità di condividere contenuti digitali come Twitter, Facebook, sistemi di divulgazione come WikiPedia, Youtube, e mondi virtuali ludici come Meta, ecc.)

Attenzione, però, che per social media non intendiamo solo i ***social network*** (ad esempio Facebook, Instagram, Twitter e così via) ma anche tutti quegli strumenti che si usano per **trattare dati personali in un'organizzazione aziendale**; quindi, anche gli strumenti per gestire le newsletter, per organizzare i gruppi di lavoro, quelli per fare ***profilazione***, quelli per gestire una attività di e-commerce e così via.

L'Articolo 4 del Regolamento dice che la profilazione è **qualsiasi forma di trattamento automatizzato**, che ha per oggetto **dati personali** e che ha come **scopo una valutazione su determinati aspetti personali**, per analizzarli o farne delle previsioni. Sono aspetti che possono riguardare il rendimento professionale di una persona fisica, la sua situazione economica, la sua salute, i suoi gusti, interessi e i comportamenti, la sua affidabilità, la sua ubicazione e i suoi spostamenti.

I Diritti dell'Interessato

All'*Interessato*, ovvero *la persona fisica a cui si riferiscono i dati personali*, il RGPD UE 2016/679 riconosce i seguenti importanti diritti elencati nel Capo III – *Diritti dell'Interessato* - :

il diritto ad essere informato (*Articoli 12-13-14*);

il diritto di accesso ai dati (*Articolo 15*);

il diritto di rettifica (*Articolo 16*);

il diritto alla cancellazione dei dati, o «*diritto all'oblio*» (*Articolo 17*);

il diritto alla limitazione del trattamento (*Articolo 18*);

il diritto alla portabilità dei dati (*Articolo 20*);

il diritto ad opporsi a determinate forme di trattamento (*Articolo 21*);

Il diritto a non essere sottoposto a decisioni basate unicamente sul trattamento automatizzato dei dati che lo riguardano (*Articolo 22*).

Il Regolamento Generale sulla Protezione dei Dati Personali – RGPD UE 2016/679 -

1) Il Regolamento si applica quando c'è un **Titolare del Trattamento -** o un **Responsabile del Trattamento - che ha uno stabilimento all'interno dell'Unione Europea** (27 Stati compresa l'Italia);

cioè si applica a qualsiasi attività che è effettiva e reale e che avviene all'interno del territorio dell'Unione Europea, indipendentemente dal fatto che il trattamento poi avvenga fuori dall'UE.

Lo stabilimento (azienda, attività produttiva, ecc.) ha una sede all'interno dell'Unione Europea?
Si applica il Regolamento, anche se poi i dati vengono trattati a Singapore.

2) Il RGPD si applica anche quando il **Titolare -** o il **Responsabile -** non ha una Sede Legale o Amministrativa o Produttiva all'interno dell'Unione Europea, ma **tratta dati personali di Interessati che sono all'interno dell'Unione Europea.**

Ovvero, il Regolamento si applica a chi eroga servizi o beni, anche gratuitamente, e per farlo tratta, salva, legge o sposta dati personali ed anche a chi monitora utenti, ovvero fa attività di profilazione, geo-localizzazione, attività di marketing, tracciamento anche attraverso i cookie (Siti WEB).

Lo stabilimento è in Kazakistan e vende beni anche in Europa ad Interessati Europei?
Si applica il Regolamento.

Nei ***social media*** ci sono 4 cose importanti da tenere bene in considerazione rispetto al trattamento dei dati personali:

1 – **La maggior parte dei social media vengono dagli Stati Uniti** e quindi:
a) usano un linguaggio molto semplice e lontano dal nostro (perché sono anglosassoni);
b) hanno una **concezione della riservatezza (*privacy*) completamente diversa dalla nostra** e così, quando andiamo a leggere i termini e le condizioni del servizio o l'informativa sul trattamento dei dati personali di questi strumenti, è facile perdersi.

2 – **Bisogna capire quando si applica il Regolamento** e se vengono fatti dei trattamenti di dati personali di cittadini europei, al di fuori dell'Unione Europea;

Ad esempio, alcuni social, come ***MailUp***, che si usa per inviare le newsletter, sono in UE; mentre ***Mailchimp***, invece, no. Ovvero, sono due social che svolgono la tessa funzione, certo uno strumento simile, ma il paese d'origine è diverso.

3 – **Quali sono i soggetti che nella pratica utilizzano i social all'interno dell'azienda.**

Chi utilizza i social non sono tanto i soggetti previsti dal Regolamento (Titolare, Responsabile, Interessato) ma, per esempio, sono le Persone Autorizzate, che inviano le newsletter ovvero le altre Persone Autorizzate che gestiscono la sezione «*lavora con noi*» del sito WEB aziendale.

E quindi è importante capire chi fa cosa all'interno dell'organizzazione.

4 - **La Contitolarità**.

Nel caso dei social media può succedere che si presenti una situazione in cui un gruppo di imprese raccoglie i dati delle stesse persone e invia le newsletter, fa selezione del personale, fa delle promozioni dedicate, ecc. e visto che le aziende comunicano tra loro possono passarsi i dati personali raccolti.

Il Regolamento prescrive che sia regolamentato il loro rapporto definendo se sono Contitolari o Responsabili Esterni.

Quindi, i Titolari del Trattamento, anche nella scelta dello strumento, ovvero il social media, devono capire se questo è adeguato o meno e come vengono trattati i dati personali degli interessati.

La *missione aziendale* (*mission*) chiarisce già che relazione ha il social con i dati personale degli Interessati.

La missione che il social dichiara è un buon indicatore del suo **approccio al trattamento dei dati**; perché i social hanno uno scopo e su questa base modellano anche la loro organizzazione (*governance)* dal punto di vista del trattamento dei dati personali.

Quale esempio si consideri Google e vediamo la missione di Google

La mission di Google è quella di organizzare le informazioni a livello mondiale e renderle **universalmente accessibili**.

Ovvero, ci fa capire che, se andiamo a chiedere la rimozione di qualche nostro dato a Google, Google propenderà sempre per lasciare le informazioni in rete (*on line*) in violazione e spregio dei ***Diritti dell'Interessato*** sanciti dal Regolamento (Articoli dal 15 al 22 ed in particolare Articolo 17).

Inoltre, i social media non sono solo americani.

Non esiste solo ***Facebook*** o ***Istagram*** o ***Twitter***; infatti ci sono dei paesi che non li utilizzano proprio e che hanno i loro social network e ad oggi i social cinesi e quelli russi non sono per adesso tanto conosciuti per cui è importante capire quali social aprire e soprattutto **dove hanno i server e qual è la loro provenienza** perché, dal punto di vista della riservatezza e del trattamento dei dati personali, funzionano in modo diverso da quanto previsto nei paesi che fanno parte dell'Unione Europea.

Quindi, prima di usare tali media, bisogna verificare chi sono le aziende proprietarie e dove si trovano (fuori o dentro all'Unione Europea) per capire qual è l'impatto sul trattamento dei nostri dati personali.

Skype e ***LinkedIn*** sono proprietà di Microsoft. ***WhatsApp*** e ***Instagram*** sono di proprietà Facebook (Metaverse o semplicemente Meta). ***YouTube*** è di Google. ***Tik Tok*** è della azienda cinese ByteDance.

Gli strumenti di alcuni social sono rivolti alle persone, per uso personale, mentre altri sono studiati e prodotti per uso aziende (*business*).

Social network (gruppi di individui connessi socialmente in rete tra loro) e social media (servizi che offrono la possibilità di condividere contenuti digitali come Twitter, Facebook, WikiPedia, Youtube, Meta, ecc.) danno due tipi di strumenti; ma lo stesso strumento, ad esempio Facebook, molte volte però offre sia l'***uso personale***

ad esempio si può usare un profilo Facebook e usarlo per seguire la squadra di calcio, pubblicare le catene di Sant'Antonio e farsi i selfie al bar o al ristorante, ecc.

che l'**uso aziendale**

ad esempio si può aprire una pagina Facebook aziendale per la propria attività commerciale e fare le sponsorizzazioni per avere più clienti.

Nei due casi sembra che si usi lo stesso strumento mentre in realtà si dovrebbero usare **due strumenti diversi.**

Per il business i social mettono a disposizione sistemi appositamente studiati e, ad esempio, Facebook mette a disposizione ***Pixel***, ***Workplace*** e ***WhatsApp Business***.

I Dati Personali resi pubblici

I dati personali possono essere resi pubblici direttamente dall'Interessato e tale circostanza ne autorizza di per sé il trattamento, anche in caso di dato personale cosiddetto ***particolare*** (che, ai sensi dell'Articolo 9 del Regolamento, rivela l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, dati genetici, biometrici, dati relativi alla salute, alla vita oppure orientamento sessuale).

Il trattamento dei dati personali resi accessibili acquista, quindi, particolare rilievo rispetto al tema delle pubblicazioni su *social network* quali piattaforme telematiche sulle quali il dato non solo circola ma può essere anche estratto, diffuso, raffrontato per altro trattamento con finalità diverse ed ulteriori, quale il marketing.

Il dato personale si considera ***reso pubblico*** quando esso è conoscibile da chiunque perché contenuto in registri, elenchi, atti o documenti pubblici o, altrimenti, perché reso noto direttamente dall'Interessato, anche attraverso il proprio comportamento in pubblico.

Ne consegue che **condividere dati su un social network costituisce indubbio consenso a rendere pubblicamente accessibili quelle informazioni**, ovviamente nei limiti delle finalità cui il trattamento è teso.

Il limite della Finalità del Trattamento

Il trattamento dei dati personali resi manifestamente pubblici è strettamente connesso al ***principio di limitazione delle finalità del loro trattamento***, di cui all'Articolo 5 del Regolamento, poiché soprattutto il *Consenso* (dichiarato o attuato) al trattamento del dato personale accessibile può riferirsi solo agli scopi determinati, espliciti, legittimi e compatibili la sua pubblicizzazione (per esempio per la finalità di interazione e contatto fra diversi utenti di social network).

Ovvero, **il Consenso al trattamento di propri dati personali tramite inserimento ed interazione su piattaforme telematiche di contatto deve intendersi inerente alle funzioni tipiche del social network** e non anche a finalità ulteriori, quali ad esempio per spam e marketing.

Un caso di riferimento è, infatti, quello deciso dal **Garante per la Protezione dei Dati Personali** (2017) in tema di ***email promozionali*** con il quale veniva dichiarato illecito il trattamento di dati personali (quali gli indirizzi di posta elettronica) acquisiti tramite Linkedin e Facebook e, in assenza di specifico Consenso, utilizzati per l'invio di numerose comunicazioni promozionali.

A seguito dell'entrata in vigore del Regolamento (considerando anche il *D.Lgs. 196/2003 e D.Lgs. 101/2018)* è **previsto che il trattamento di dati accessibili per finalità di promozione commerciale deve presupporre il Consenso specifico dell'Interessato.**

I Diritti dell'Interessato

All'*Interessato*, ovvero *la persona fisica a cui si riferiscono i dati personali*, il RGPD UE 2016/679 riconosce i seguenti importanti diritti elencati nel Capo III – *Diritti dell'Interessato* - :

il diritto ad essere informato (*Articoli 12-13-14*);

il diritto di accesso ai dati (*Articolo 15*);

il diritto di rettifica (*Articolo 16*);

il diritto alla cancellazione dei dati, o «*diritto all'oblio*» (*Articolo 17*);

il diritto alla limitazione del trattamento (*Articolo 18*);

il diritto alla portabilità dei dati (*Articolo 20*);

il diritto ad opporsi a determinate forme di trattamento (*Articolo 21*);

Il diritto a non essere sottoposto a decisioni basate unicamente sul trattamento automatizzato dei dati che lo riguardano (*Articolo 22*).

I Diritti degli Utenti nei Social Network

L'utilizzo improprio di un social network può arrivare a ledere i diritti di alcune persone ed espone a rischi non solo chi li utilizza in modo diretto ma anche le persone che inconsapevolmente appaiono nei contenuti diffusi.

Il social network è il ***Titolare*** dei dati personali degli Interessati, in questo caso gli utenti utilizzatori, e in quanto tale determina le finalità e i mezzi di trattamento dei dati personali.

L'azienda che gestisce il social network e che utilizza i dati personali di un soggetto è tenuta a rilasciare una Informativa per illustrare le finalità e le modalità del trattamento dei dati ai sensi dell'Articolo 13 del Regolamento UE 2016/679 - RGPD.

L'utilizzo gratuito di un social network non giustifica in nessun modo il fatto che i dati personali dell'utente possano essere trattati per finalità non contemplate nell'Informativa.

D'altra parte in spregio al Regolamento UE, le aziende che gestiscono i social network possono analizzare i profili degli utenti, le loro preferenze e le loro reti di contatti per cedere successivamente (dietro lauti compensi) queste informazioni ad altre aziende che utilizzeranno tali dati per promuovere offerte commerciali mirate o per sostenere campagne di vario genere.

Riservatezza e inserimento Dati Personali nei Social Network

Inserendo dati personali su un social network ***se ne perde il controllo*** e spesso si concede al fornitore del servizio la licenza di utilizzare il materiale che si inserisce senza limiti di tempo.

Installando sul proprio telefono, tablet o altro dispositivo elettronico, le applicazioni dei social network si concede l'accesso alla propria lista dei contatti, al microfono o a contenuti multimediali personali (immagini, fotografie e video) non indispensabili al funzionamento dell'app stessa.

Dietro l'offerta di un servizio gratuito molto spesso si verifica l'utilizzo per molteplici fini dei dati degli utenti.

Benché la diminuzione della propria riservatezza sia un evento logicamente conseguente alla condivisione volontaria di dati personali sui social network, **l'utilizzo in modo improprio dei social network espone a gravi rischi legati ad un uso improprio o fraudolento dei dati personali** come ad esempio trattamento illecito di dati, atti persecutori, danni alla reputazione, furto d'identità, truffe, phishing, diffusione illecita di immagini personali.

(*Il phishing è un tipo di truffa effettuata su Internet (via email o messaggio) attraverso la quale un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso, fingendosi un ente affidabile in una comunicazione digitale*)

Come proteggere la propria ed altrui Riservatezza

L'utente deve diventare parte attiva nel processo di prevenzione e protezione della propria riservatezza.

La miglior difesa per proteggere la riservatezza delle persone durante l'utilizzo di social network consiste nell'**utilizzare il buon senso e nell'attuare alcune elementari misure di sicurezza:**

•prima dell'iscrizione, leggere l'informativa sul trattamento dei dati personali fornita dal social network;

•prima dell'iscrizione leggere il contratto e le condizioni d'uso del social network;

•accertare di poter recedere facilmente l'iscrizione al social network e di poter cancellare tutte le informazioni pubblicate;

•controllare le modifiche periodiche del contratto che vengono introdotte unilateralmente dai social network;

•disattivare le funzioni di geolocalizzazione presenti sulle applicazioni dei social network, così come sullo smartphone e sugli altri strumenti utilizzati per il collegamento a Internet;

•controllare le impostazioni dei livelli di sicurezza del proprio profilo social, modificarle e renderle più restrittive, soprattutto se si interagisce con persone non conosciute realmente;

•limitare al massimo la disponibilità di informazioni personali;

•controllare i diritti di accesso concessi alle applicazioni dei social network installate sul proprio smartphone affinché non possano accedere ai propri dati personali e utilizzarli senza consenso;

•rifiutare il consenso all'utilizzo dei propri dati per attività di marketing (compresi i *cookie*) se non si desidera ricevere pubblicità;

•non pubblicare fotografie altrui senza il Consenso dell'Interessato o dei genitori in caso si vogliano pubblicare foto di minori;

•Non pubblicare immagini, fotografie e video scaricate da Internet in violazione del Diritto d'Autore senza aver verificato l'assenza di marchi e copyright;

•non pubblicare dati personali quali numeri di telefono, indirizzi di residenza o foto che potrebbero adattarsi ed essere utilizzate per la falsificazione di un documento d'identità;

•creare password di accesso al social network complesse e difficilmente riconducibili alla propria identità/vita privata;

• cambiare spesso la password di accesso ai social network e non utilizzare la stessa password per diversi account;

•utilizzare password diverse da quelle utilizzate su altri siti web (ad esempio per la posta elettronica o per la gestione del conto corrente bancario online);

•non comunicare a terzi la propria password e conservarla in un luogo sicuro;

•non accedere al social network utilizzando wi-fi pubblici e aperti;

•se si accede al proprio profilo social da un PC pubblico o utilizzato da altri non salvare mai la password ed effettuare sempre la disconnessione (*logout*) al temine della propria sessione;

•installare e configurare firewall e antivirus tenendoli costantemente aggiornati;

•verificare le impostazioni dei cookie;

•attivare tutti gli strumenti disponibili per controllare le attività dei minori sui social network;

•segnalare ogni abuso e violazione sui canali predisposti dai social network e dalle Autorità competenti.

Pubblicazione sui Social Media di Immagini, Fotografie e Video di Minori

Oltre alle attività commerciali ed educative anche le parrocchie devono interrogarsi circa la legittimità della pubblicazione sui propri siti o social media parrocchiali delle immagini, fotografie e dei video dei minorenni (o anche dei maggiorenni laddove possano essere considerati dati personali inquadrati dagli Articoli 9 e 10 del Regolamento UE e relative alle comuni attività oratoriane (catechesi, grest, vacanze, esperienze caritative, ecc.).

Considerata la delicatezza dell'argomento e l'ampia tutela che l'ordinamento giuridico riconosce ai minori, occorre prestare la massima prudenza.

Le regole della prudenza sono semplici;

1 - conoscere le normative cogenti, quali il Regolamento UE 2016/679 - RGPD, il Decreto Generale CEI del 24 maggio 2018 e la Legge 633/1941 (Diritto d'Autore);

2 - non adottare comportamenti superficiali.

Condizione per la Pubblicabilità

Le immagini, fotografie ed i video che riprendono minorenni e/o maggiorenni impegnati in attività di oratorio (catechesi, gioco, feste, attività sportiva, gite vacanze marine e montane, ecc.) sono **dati personali** la cui pubblicazione è disciplinata dalla normativa vigente.

In alcuni casi le immagini, fotografie e video potrebbero anche essere qualificati come dati personali ***particolari*** in quanto idonei, ai sensi dell'Articolo 9 del Regolamento UE 2016/679, "*a rivelare le convinzioni religiose*» dell'Interessato.

Condizione necessaria e base giuridica per il trattamento è la consegna della ***Informativa sul Trattamento dei Dati*** e la conseguente acquisizione del ***Consenso*** scritto degli Interessati prima di procedere alla pubblicazione e alla divulgazione delle immagini, fotografie e dei video.

Naturalmente, quando si tratta di Interessati minori, il Consenso deve essere espresso congiuntamente dagli esercenti la responsabilità genitoriale o tutoria (per i genitori è richiesta la firma congiunta).

Regole Generali

Per la pubblicazione occorre osservare puntualmente tutti gli impegni assunti nella Informativa e:

- verificare che le foto pubblicate riprendano solo persone che hanno espresso il consenso alla pubblicazione;

- eliminare definitivamente le foto (oppure rendere irriconoscibile il volto delle persone nelle riprese di gruppo) quando l'Interessato revoca il Consenso alla pubblicazione;

- rendere irriconoscibili i volti delle persone che non hanno espresso il Consenso alla pubblicazione ma che appaiono nelle foto di gruppo che saranno pubblicate.

Indicazioni Operative

1. Senza aver acquisito il Consenso scritto di cui sopra (per ciascuna persona ripresa) astenersi dal pubblicare le foto e i video di minori e/o dal trasmetterli a terzi;
2. in caso di riprese video e foto di gruppo, è necessario il Consenso per ciascuna persona ripresa;
3. quando le foto ed i video riguardano i minori, il Consenso deve essere concesso da entrambi i genitori. A tal proposito si segnala che il Garante della Protezione dei Dati Personali (GPDP) stigmatizza l'uso di alcuni genitori di pubblicare (o far pubblicare) in modo indiscriminato le foto dei propri figli minori … e, dunque, anche la decisione di acconsentire alla pubblicazione delle foto dei propri figli minorenni … e, dunque, anche la prassi delle parrocchie (e dei loro collaboratori) di pubblicare in modo scriteriato ed esagerato le foto ed i video sui social parrocchiali;
4. con riferimento ai social intestati alla parrocchia o all'oratorio o ai gruppi parrocchiali, considerato che le foto e i video possono essere condivisi da terzi, e quindi *propagarsi* sul WEB (con tutti gli evidenti rischi che ne conseguono), per saggia prudenza si deve procedere alla loro pubblicazione con estrema cautela e prudenza (per non mettere in pericolo il minore);
5. i social intestati alle persone fisiche (anche se sacerdoti, educatori, formatori e collaboratori) non sono coperti dalle autorizzazioni acquisite dalla parrocchia; di contro si espone a pericolo la parrocchia che decide di rilanciare sui propri social foto ricevute o condivise dai social di terzi.