VADEMECUM
IN MATERIA DI PRIVACY
E RELATIVI ADEMPIMENTI

NOTA INTRODUTTIVA

La gestione del progetto richiede la raccolta di alcune informazioni relative sia ai beneficiari diretti che alle risorse umane coinvolte nelle attività.
Ogni Partner incluso nel Progetto è pertanto tenuto a raccogliere – nel pieno rispetto della normativa sulla privacy – sia informazioni riguardanti tutte le risorse umane impegnate nelle attività, delle quali va rendicontato il costo del lavoro, sia informazioni riguardanti una parte dei beneficiari diretti degli interventi (da concordare con l'ente finanziatore), dei quali vanno rilevati i principali dati socio anagrafici e di esito.
Prima di essere inclusi nelle attività, le risorse umane coinvolte e i beneficiari diretti del progetto (ovvero, i genitori o i loro tutori legali nel caso di minorenni o altri soggetti non autonomi) devono ricevere le specifiche informative e prestare espressamente i correlati consensi al trattamento dei dati, in ossequio a quanto previsto dal Regolamento Europeo n. 679 del 2016 (di seguito, il "**GDPR**") e dal D.Lgs. n. 196 del 2003, come modificato dal D.Lgs. n. 101 del 2018 (di seguito, il "**Codice privacy**").
Fondazione Con Il Sud e Con i Bambini hanno predisposto un Kit Documentale contenente i modelli 'FORM' da utilizzare per la raccolta delle informative e la gestione delle responsabilità interne al partenariato.
E' opportuno precisare che le persone che non riceveranno l'informativa e non sottoscriveranno il correlato consenso non potranno né svolgere attività nell'ambito del Progetto né beneficiare dei programmi e delle iniziative finanziate
I dati saranno raccolti, anche in più momenti dello svolgimento del Progetto (e in alcuni casi anche dopo la fine dello svolgimento dello stesso per le valutazioni d'impatto), da ciascun Partner, mediante l'utilizzo dei formulari standard che vi saranno trasmessi dall'ufficio di monitoraggio e saranno caricati sulla piattaforma Chàiros a cura del Soggetto Responsabile.
Ogni Partner del Progetto, nell'ambito dello svolgimento della propria attività di raccolta dei dati personali, è tenuto al rispetto della disciplina prevista dal GDPR e dal 'Codice privacy' vigenti, nonché di tutti gli adempimenti ivi previsti.
A tal proposito si precisa che:

- possono anche essere raccolti dati appartenenti a categorie particolari previste all'art. 9, comma 1 del GDPR, quali, a titolo esemplificativo e non esaustivo, i dati relativi alla salute, alla vulnerabilità sociale, alla disabilità, ecc.;
- il Soggetto Responsabile del Progetto è autonomo "Titolare del trattamento" dei dati (ai sensi dell'art. 4, n. 7 del GDPR) per finalità legate alla realizzazione del Progetto;
- le risorse umane coinvolte nelle attività progettuali e i beneficiari del Progetto devono ricevere, rispettivamente, le specifiche informative e prestare il connesso consenso al trattamento dei loro dati, con modulistica conforme allo standard trasmesso in allegato alla presente. In tali informative, Titolare del trattamento è sempre il Soggetto responsabile, il quale può avvalersi o meno di Partner per raccogliere, in prima battuta, i dati delle risorse umane coinvolte nel Progetto e dei beneficiari del medesimo;
- ogni Partner, nella misura in cui raccoglie e trasmette i dati al Soggetto responsabile, è nominato per iscritto da quest'ultimo (Allegato n. 5) "Responsabile del trattamento dei dati" (ai sensi dell'art. 28 del GDPR)[1];
- ogni Partner, in qualità di Responsabile del trattamento dei dati, deve, tra gli altri adempimenti privacy: a) istituire e aggiornare un Registro del trattamento (ai sensi dell'art. 30 del GDPR); b) avere adeguate misure tecniche ed organizzative (ai sensi degli artt. 32 e segg. del GDPR); c) in caso di trattamento su "larga scala" di categorie particolari di dati *ex* art. 9 del GDPR, nominare un Responsabile della protezione dei dati (ai sensi dell'art. 37 del GDPR);
- infine Con i Bambini, in qualità di ente finanziatore del Progetto, è anch'essa autonomo "Titolare del trattamento dei dati" (ai sensi dell'art. 4, n. 7 del GDPR) che gli vengono comunicati dal Soggetto

[1] La qualità di Responsabile del trattamento dei dati nell'ambito del Progetto non esclude che il Partner stesso sia autonomo Titolare dei dati nell'ambito delle proprie attività ordinarie.

Responsabile, mediante inserimento nella piattaforma Chàiros, per finalità legate alla realizzazione del Progetto stesso; a tal riguardo, la Fondazione Con il Sud e l'Impresa sociale Con i Bambini s.r.l. , quali titolari della piattaforma Chàiros, nomineranno per iscritto il Soggetto responsabile "Responsabile del trattamento" dei dati (ai sensi dell'art. 28 del GDPR).

I FORM contenuti nel kit documentale andranno compilati e personalizzati a cura del Soggetto responsabile, si invita a fare attenzione alle informazioni da inserire ed alle possibili alternative previste dai documenti (testi evidenziati)

Kit Documentale

Nome FORM	**Descrizione**	**Compilazione**	**Sottoscrizione**
FORM 1) Informativa e consenso beneficiari (dati raccolti dai Partner);	Consente al partner di raccogliere i dati sui beneficiari del progetto (compresi recapiti e nominativi) e trasmetterli al Soggetto responsabile che si occuperà di caricarli in piattaforma Chàiros ed inviarli all'ente finanziatore. Consente all'ente finanziatore o ad eventuali altri partner (purché designati come titolari del trattamento) di ricontattare i beneficiari per finalità di valutazione degli esiti derivanti dalla partecipazione al progetto.	A cura del partner nel momento dell'iscrizione del beneficiario ad un'attività o servizio realizzato nell'ambito del progetto.	Destinatari diretti che partecipano ad attività intensive e durature realizzate nell'ambito del progetto.
FORM 2) Informativa e consenso risorse umane (Partner);	Consente al partner di raccogliere i dati sulle risorse umane (compresi recapiti e nominativi) coinvolte nella realizzazione delle attività di progetto e trasmetterli al Soggetto responsabile che si occuperà di caricarli in piattaforma Chàiros ed inviarli all'ente finanziatore. Consente all'ente finanziatore o ad eventuali altri partner (purché designati come titolari del trattamento) di ricontattare i beneficiari per finalità di valutazione del progetto realizzato.	A cura del partner contestualmente alla contrattualizzazione della risorsa da coinvolgere nel progetto.	Risorse umane coinvolte nella realizzazione del progetto.
FORM 3) Informativa e consenso beneficiari (dati raccolti dal Soggetto responsabile);	Consente al Soggetto responsabile di raccogliere i dati sui beneficiari del progetto (compresi recapiti e nominativi) e trasmetterli, tramite inserimento nella piattaforma Chàiros, all'ente finanziatore. Consente all'ente finanziatore o ad eventuali altri partner (purché designati come titolari del trattamento) di ricontattare i beneficiari per finalità di valutazione degli esiti derivanti dalla partecipazione al progetto.	A cura del Soggetto responsabile nel momento dell'iscrizione del beneficiario ad un'attività o servizio realizzato nell'ambito del progetto.	Destinatari diretti che partecipano ad attività intensive e durature realizzate nell'ambito del progetto.
FORM 4) Informativa e consenso risorse umane (Soggetto responsabile);	Consente al Soggetto responsabile di raccogliere i dati sulle risorse umane (compresi recapiti e nominativi) coinvolte nella realizzazione delle attività di progetto e trasmetterli e trasmetterli, tramite inserimento nella piattaforma Chàiros, all'ente finanziatore. Consente all'ente finanziatore o ad eventuali altri partner (purché designati come titolari del trattamento) di ricontattare i beneficiari per finalità di valutazione del progetto realizzato	A cura del Soggetto responsabile contestualmente alla contrattualizzazione della risorsa da coinvolgere nel progetto.	Risorse umane coinvolte nella realizzazione del progetto.
FORM 5) Designazione a Responsabile del trattamento del Partner (da parte del Soggetto responsabile);	Consente al Soggetto responsabile di trattare le informazioni fornite dai partner rispetto ai beneficiari ed alle risorse umane coinvolte nel progetto.	A cura del Soggetto responsabile contestualmente alla definizione degli accordi di partenariato.	Partner che hanno in carico la gestione di quote di budget o la presa in carico di destinatari diretti

PRINCIPI GENERALI

INTRODUZIONE

Il 25 maggio 2018 è entrato in vigore in tutti i Paesi della UE il Regolamento UE n. 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (di seguito, il "**GDPR**"), adottato dal Parlamento Europeo e dal Consiglio il 27 aprile 2016. Tutti coloro che trattano dati personali nell'ambito delle proprie finalità istituzionali o commerciali (ovvero non per scopi meramente personali), vale a dire i c.d. "Titolari del trattamento", i quali agiscono direttamente o per il tramite dei c.d. "Responsabili del trattamento" o dei propri c.d. "Designati al trattamento", hanno l'obbligo di uniformarsi alla nuova normativa, pena l'applicazione di pesanti ed inasprite sanzioni, soprattutto pecuniarie.

Infatti, il GDPR ha una portata generale e si applica a qualunque trattamento di dati personali di persone fisiche (i c.d. "Interessati") che si trovano nel territorio della UE, anche se effettuato da soggetti (Titolare del trattamento o Responsabile del trattamento) non stabiliti nella UE, quando le attività di trattamento riguardano l'offerta di beni o la prestazione di servizi ai suddetti Interessati nella UE oppure il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo nella UE (art. 3 del GDPR). Il GDPR ha sicuramente cambiato la prospettiva con la quale il tema della *privacy* deve essere affrontato, per le numerose disposizioni introdotte e gli altrettanti numerosi specifici adempimenti previsti. Ad esempio, il GDPR non indica più le c.d. "misure minime" da attuare, ma impone la responsabilità del Titolare del trattamento (c.d. "*accountability*") di definire le misure più adeguate tra tutte quelle possibili, e di garantire poi la conformità (c.d. "*compliance*") dei trattamenti eseguiti.

Ciò implica la libertà del Titolare del trattamento nell'approntare le misure adeguate alla protezione dei dati personali, senza basarsi solamente su modelli precompilati o documentazione *standard*: oltre a prevedere delle misure di base (in applicazione del principio della c.d. "*privacy by default*"), ciascun Titolare del trattamento dovrà adottare delle procedure modellate sulle necessità e caratteristiche specifiche del trattamento svolto all'interno della propria realtà (c.d. "*privacy by design*"). Tutto ciò con lo scopo di assicurare la protezione delle persone fisiche (i soggetti Interessati) nel trattamento dei propri dati personali, specialmente di quelli un tempo definiti come "sensibili" ed ora "appartenenti a categorie particolari di cui all'art. 9 del GDPR".

Una volta entrato in vigore il GDPR, è stato necessario rendere conforme la normativa italiana in materia di privacy, ossia il D.Lgs. 30 giugno 2003, n. 196 (di seguito, il "**Codice**") a quella europea; a tal riguardo, il D.Lgs. 10 agosto 2018, n. 101, pubblicato in Gazzetta Ufficiale il 4 settembre 2018 ed entrato in vigore il 19 settembre dello stesso anno, ha attualizzato le disposizioni del Codice alla realtà sovranazionale. Necessario, dunque, interpretare le modifiche apportate al Codice già esistente e comprendere come lo stesso è stato integrato per adattarlo alle disposizioni introdotte dal GDPR e, soprattutto, per prendere piena cognizione e dare completa attuazione al nuovo quadro normativo e regolamentare (che verrà ulteriormente integrato e dovrà essere interpretato anche alla luce delle indicazioni che verranno fornite dal Garante e anche dalle linee guida del Gruppo di Lavoro dei Garanti *privacy* europei).

Tanto premesso, si è ritenuto opportuno predisporre il presente *vademecum*, per consentire a tutte quelle realtà che trattano dati personali nell'ambito della propria attività istituzionale, di familiarizzare e rafforzare la propria cognizione della materia e adeguarsi prontamente, ponendo in essere una serie di adempimenti da essa previsti, prima che – cessato il c.d. "periodo di moratoria" di 8 mesi – aumenti l'attività ispettiva e di controllo demandata al Garante.

Risulta, dunque, quanto mai opportuno leggere con attenzione il presente *vademecum* che, senza pretese di esaustività e completezza, data la complessità e ampiezza della materia, vuole essere di primo aiuto e di supporto pratico, al fine di acquisire consapevolezza della tutela da garantire agli aventi diritto ma anche delle sanzioni, inasprite dal GDPR, al fine di effettuare una consapevole valutazione del rischio e attuare gli adempimenti applicabili e necessari per conformarvisi.

DEFINIZIONI

Dato personale	Qualsiasi informazione riguardante una persona fisica identificata o identificabile (c.d. "Interessato").
Interessato	Persona fisica identificata o identificabile. E' identificabile la persona fisica che può essere identificata, direttamente o indirettamente, mediante il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
Larga scala	Il numero degli interessati coinvolti, il volume dei dati trattati, la durata delle attività di trattamento o l'estensione geografica del trattamento rende impossibile precisare la quantità di dati oggetto di trattamento o il numero di interessati in modo da coprire tutte le eventualità (ad esempio, il trattamento di dati relativi a pazienti svolto da un ospedale nell'ambito delle ordinarie attività; trattamento di dati relativi agli spostamenti di utenti di un servizio di trasporto pubblico; trattamento di dati di geolocalizzazione raccolti in tempo reale per finalità statistiche da un responsabile specializzato nella prestazione di servizi di questo tipo a clienti di una catena internazionale; trattamento di dati relativi alla clientela da parte di una compagnia assicurativa o una banca nell'ambito delle ordinarie attività; trattamento di dati personali da parte di un motore di ricerca per finalità di pubblicità comportamentale; trattamento di dati (metadati, contenuti, ubicazione) da parte di fornitori di servizi telefonici o telematici).
Particolari categorie di dati di cui all'art. 9 del GDPR	Dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose, politiche o filosofiche, o l'appartenenza sindacale, nonché il trattamento di dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona. Si tratta dei vecchi dati c.d. "sensibili".
Trattamento	Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, la diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

PRINCIPI GENERALI

Liceità e correttezza
Ogni trattamento di dati personali deve essere svolto in maniera lecita e corretta, **informando** l'Interessato circa la raccolta, l'utilizzo ed altri eventuali successivi trattamenti dei dati forniti. Per essere lecito, il trattamento di dati personali deve fondarsi sul **consenso** dell'Interessato o su **altra base giuridica** prevista dal GDPR (artt. 6 e 9) o dal Codice.

Finalità e pertinenza
Tale principio prevede che vi sia una corrispondenza tra quanto dichiarato dal Titolare del trattamento e quanto effettivamente accade nel trattamento dei dati. Pertanto, i dati personali raccolti e trattati devono essere adeguati, pertinenti e, soprattutto, limitati a quanto necessario per le finalità del trattamento dichiarato. L'esplicitazione delle finalità di trattamento deve essere antecedente all'acquisizione del consenso e all'inizio delle attività di trattamento poiché solo in tal modo è possibile garantire che il consenso dell'Interessato sia effettivamente informato.

Trasparenza
Per essere trasparente, il trattamento dovrà essere effettuato secondo modalità predefinite e previamente rese note all'Interessato, che sarà quindi pienamente consapevole non solo della tipologia di dati raccolti, ma anche delle modalità con cui tali dati sono stati raccolti e verranno trattati. La trasparenza non riguarda solo il contenuto delle informazioni, ma anche le modalità con cui tali informazioni sono fornite all'Interessato.

Necessità e minimizzazione
Tale principio prevede che non vi sia alcuna eccedenza nei trattamenti di dati. Pertanto, il trattamento deve essere necessariamente vincolato alle finalità dichiarate dal Titolare nell'informativa. Nell'effettuare il trattamento con strumenti informativi, il Titolare dovrà preferire l'utilizzo di dati anonimi rispetto a quello di dati personali. In applicazione di tale principio, i programmi informatici dovranno essere configurati per preferire l'utilizzo di dati anonimi laddove possibile.

Accuratezza
Il Titolare del Trattamento deve verificare che i dati raccolti siano corretti, veritieri e completi; deve trattare dati esatti e deve organizzare la propria struttura al fine di garantire il controllo sulla veridicità.
Il Titolare ha quindi l'obbligo di garantire un elevato *standard* di qualità nel trattamento dei dati, dal momento che il Trattamento di dati personali inesatti o incompleti potrebbe determinare una falsa rappresentazione dell'Interessato e comportare conseguenze indesiderate.

Integrità e confidenzialità
Il Titolare del trattamento deve adottare tutte le misure ragionevoli affinché dati personali inesatti siano rettificati o cancellati. I dati personali devono essere trattati in modo da garantirne un'adeguata sicurezza e riservatezza, e impedirne l'accesso o l'utilizzo non autorizzato, ad esempio mediante l'adozione di adeguate misure di sicurezza (protezione con password di accesso, pseudonimizzazione e cifratura).

Limitazione all'archiviazione
La conservazione dei dati, che costituisce una modalità di trattamento, deve essere effettuata solo per il tempo strettamente necessario agli scopi stabiliti nelle finalità del trattamento stesso. Tuttavia, occorre contemperare tale diritto con l'esigenza del Titolare di adempiere ad obblighi di legge che impongono determinati obbligo di conservazione dei dati (ad esempio obbligo di conservazione delle scritture contabili).

LE FIGURE RILEVANTI

Il Titolare del trattamento
È la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali (art. 4, punto 7, del GDPR). Il Titolare del trattamento ha la responsabilità in merito alla valutazione del rischio e all'organizzazione degli strumenti e delle procedure idonei a tutelare i diritti degli Interessati; ha l'onere di provare di aver adottato misure organizzative e tecniche coerenti con le prescrizioni del GDPR, anche con riferimento alla periodica verifica dell'effettivo funzionamento delle misure di sicurezza adottate.

Il Responsabile del trattamento
È la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento (art. 4, punto 8, del GDPR).

È la persona incaricata (con atto di nomina a Responsabile del trattamento *ex* art. 28 del GDPR) dal Titolare del trattamento a:
- trattare i dati personali;
- supervisionare il trattamento dei dati da parte dei soggetti Designati *ex* art. 29 del GDPR e 2-*quaterdecies* del Codice;
- implementare le proprie misure di sicurezza;
- tenere il Registro delle attività di trattamento svolte, laddove obbligatorio o istituito su base volontaria (si veda il seguente paragrafo 4.7);
- eventualmente (se non fatto dal Titolare) designare il Responsabile della Protezione dei Dati *ex* art. 37 del GDPR (di seguito, l'"**RPD**"), laddove obbligatorio o nominato su base volontaria (si veda il seguente paragrafo 3.3).

Il Responsabile della Protezione dei Dati ("RPD")
È una nuova figura introdotta dal GDPR. La relativa nomina è obbligatoria solo nei seguenti casi:
- il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccetto le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;
- le attività principali del Titolare del trattamento o del Responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli Interessati su larga scala;
- le attività principali del Titolare del trattamento o del Responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali *ex* art. 9 del GDPR o di dati relativi a condanne penali e a reati *ex* art. 10 del GDPR.

Anche laddove non obbligatorio per legge, il Titolare del trattamento e il Responsabile del trattamento possono comunque nominare l'RPD su base volontaria, per ragioni di opportunità.

L'incarico di RPD può essere ricoperto alternativamente da:
a. un dipendente/collaboratore del Titolare o del Responsabile, che non sia in conflitto di interessi con i medesimi (circostanza molto difficile da realizzarsi);
b. un soggetto giuridicamente esterno al Titolare o Responsabile del trattamento;
c. a condizione che possieda un'approfondita conoscenza della normativa e delle prassi in materia di *privacy* (secondo il Considerando 81 del GDPR, deve trattarsi di una persona che presenti "*garanzie sufficienti, in particolare in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto misure tecniche e organizzative che soddisfino i requisiti del GDPR, anche per la sicurezza del trattamento*").

L'assunzione dell'incarico non determina l'assunzione di responsabilità personali in caso di inosservanza del GDPR, spettando al Titolare del trattamento o al Responsabile del trattamento garantire ed essere in grado di dimostrare che le operazioni di trattamento sono conformi alle disposizioni del GDPR (art. 24, paragrafo 1, del GDPR). Qualora non sia nominato l'RPD, tali compiti dovranno essere assolti dal Titolare o dal Responsabile del trattamento. I compiti dell'RPD sono:

a. informare e fornire consulenza al Titolare del trattamento o al Responsabile del trattamento nonché ai collaboratori (Designati) che eseguono il trattamento in merito agli obblighi introdotti dalla normativa;
b. sorvegliare l'osservanza della normativa in materia;
c. curare la sensibilizzazione e la formazione del personale (Designati) che partecipa ai trattamenti e alle connesse attività di controllo;
d. fornire, se richiesto e laddove previsto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
e. cooperare con l'Autorità di controllo locale (di seguito, il "**Garante privacy**").

NB: le nomine devono essere effettuate per iscritto e si consiglia sempre di raccogliere la firma per accettazione da parte del RPD (per il principio della *accountability*).

Il Designato al trattamento dei dati
Secondo l'art. 2-*quaterdecies* del Codice e l'art. 29 del GDPR, il Titolare del trattamento o il Responsabile del trattamento dei dati – con l'eventuale supporto dell'RPD – dovrà procedere a:
- nominare e autorizzare per iscritto i Designati al Trattamento (dipendenti e/o collaboratori che trattano i dati e accedono a determinate banche dati), fornendo specifiche istruzioni sulle finalità e modalità del trattamento delle specifiche categorie di dati trattati dal Designato;
- verificare che i Designati al trattamento dei dati si siano impegnati alla riservatezza o abbiano un adeguato obbligo legale alla riservatezza (art. 29 del GDPR);
- sensibilizzare e formare i Designati al Trattamento al tema della *privacy*, sia con riferimento ai vincoli normativi che con riferimento alle procedure e/o strumenti adottati internamente per garantire il rispetto del GDPR.

GLI ADEMPIMENTI

Quali sono gli adempimenti privacy introdotti dal GDPR e quelli già esistenti?
Il GDPR da un lato ha introdotto alcuni nuovi adempimenti privacy in capo a Titolari e Responsabili del trattamento, dall'altro ha integrato e rafforzato obblighi già esistenti. Nello specifico, attualmente ciascun Titolare e Responsabile deve verificare se ha l'obbligo di porre in essere i seguenti adempimenti:
- valutazione del rischio e analisi organizzativa caso per caso (novità);
- adozione di misure di sicurezza idonee (già previsto, da integrare eventualmente);
- informativa (già prevista, da integrare);
- acquisizione del consenso (già prevista);
- conferimento degli incarichi (già previsto, da integrare eventualmente con la nomina dell'RPD);
- istituzione e aggiornamento del Registro del Trattamento dei dati (novità);
- formazione degli operatori (già previsto ma rafforzato);
- notifica delle violazioni privacy – c.d. "*data breach*" (novità).

Valutazione del rischio e analisi organizzativa caso per caso
Si tratta della Valutazione d'impatto sulla protezione dei dati personali, la c.d. "*Data Protection Impact Assessment*" (di seguito, la "**DPIA**"). L'art. 35 del GDPR prescrive l'onere, in capo al Titolare del trattamento, di compiere in via preliminare al trattamento una valutazione d'impatto sulla protezione dei dati "*quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche*". La DPIA è richiesta in modo particolare se il Titolare del trattamento effettua:
- una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
- un trattamento, su larga scala, di categorie particolari di dati personali *ex* art. 9 del GDPR o di dati relativi a condanne penali o a determinati reati *ex* art. 10 del GDPR;
- la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Secondo il Considerando 76 del GDPR, "*La probabilità e la gravità del rischio per i diritti e le libertà dell'Interessato dovrebbero essere determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio dovrebbe essere considerato in base a una valutazione oggettiva*

mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato". La DPIA serve per determinare, in particolare, "*l'origine, la natura, la particolarità e la gravità di tale rischio. L'esito della valutazione dovrebbe essere preso in considerazione nella determinazione delle opportune misure da adottare per dimostrare che il trattamento dei dati personali rispetta*" il GDPR (Considerando 84 del GDPR).

La DPIA contiene almeno:

- una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal Titolare del trattamento;
- una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
- una valutazione dei rischi per i diritti e le libertà degli Interessati;
- le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al GDPR, tenuto conto dei diritti e degli interessi legittimi degli Interessati e delle altre persone in questione.

Ad ogni modo si segnala che, anche laddove non obbligatoria, la DPIA può essere effettuata su base volontaria, ed anzi, è considerata buona prassi e consente al Titolare del trattamento di identificare e gestire al meglio potenziali rischi che non sarebbero stati altrimenti rilevati e prevenire possibili violazioni che altrimenti si sarebbero verificate. Essa costituisce, quindi, uno strumento utile per dimostrare, in caso di ispezione del Garante privacy, il rispetto del GDPR, in ossequio al principio di *accountability* (responsabilizzazione).

Adozione di misure di sicurezza idonee

Il GDPR non prevede misure di sicurezza standard valide in ogni caso. In base al principio di responsabilizzazione, il Titolare e il Responsabile del trattamento, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio, devono effettuare una valutazione caso per caso e adottare le misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio concretamente esistente (art. 32 del GDPR).
Tali misure di sicurezza possono consistere, a titolo di esempio, in:

- ridurre al minimo il trattamento dei dati personali;
- garantire trasparenza per quanto riguarda le funzioni ed il trattamento dei dati personali;
- ripartire in modo chiaro le responsabilità nel trattamento;
- adottare le misure tecnologiche adeguate ad assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento (ad esempio, la pseudonimizzazione e la cifratura dei dati personali);
- redigere un regolamento per l'utilizzo dei sistemi informatici e delle banche dati cartacee, assicurandone l'adozione e il rispetto da parte di tutti i responsabili e i designati.

Secondo il Garante privacy, le misure minime di sicurezza previste dal Codice possono costituire "*un nucleo centrale minimo per garantire la sicurezza dei dati*", ma il Titolare e il Responsabile del trattamento dovranno effettuare, caso per caso, una valutazione delle misure tecniche e organizzative più idonee a garantire un livello di sicurezza adeguato al rischio. Non è nemmeno possibile ritenere sufficiente o necessaria l'adozione delle misure di sicurezza riportate all'interno dell'art. 32 del GDPR, perché occorrerà sempre una valutazione caso per caso.

Informativa
L'obbligo di rendere all'Interessato l'informativa *privacy* prima di effettuare un trattamento di dati personali raccolti presso l'Interessato stesso[2] - salvo casi particolari[3] - era già previsto dal Codice (art. 13 del Codice, oggi abrogato a seguito dell'avvento del D.Lgs. n. 101 del 2018). Il GDPR ha rafforzato e ampliato i diritti degli Interessati e, dunque, si rende necessario aggiornare le informative già a suo tempo fornite agli Interessati, nella vigenza della vecchia normativa. Sebbene non sia espressamente previsto l'obbligo di fornire un'informativa scritta, è assolutamente raccomandabile fornire per iscritto l'informativa per documentare l'assolvimento di tale adempimento (sempre per il principio della *accountability*). Si consiglia anche di raccogliere la firma dell'Interessato per presa visione[4].

L'informativa deve avere forma concisa, trasparente, intelligibile per l'Interessato e facilmente accessibile; occorre utilizzare un linguaggio chiaro e semplice, ma la stessa deve comunque contenere tutti gli elementi richiesti dall'art. 13 del GDPR. È consigliabile elaborare informative specifiche per ciascuna tipologia di Interessato (ad esempio, l'informativa per i dipendenti e collaboratori, l'informativa per i fornitori, l'informativa per i clienti, la *privacy policy* per gli utenti del sito *internet*, ecc.).

NB: ogni volta che le finalità del trattamento cambiano, il GDPR impone di informarne nuovamente l'Interessato prima di procedere al trattamento ulteriore.

Gli elementi da inserire nell'informativa conforme al nuovo art. 13 del GDPR sono i seguenti.

○ Le finalità e le modalità del trattamento cui sono destinati i dati	Già previsto dal Codice
○ La natura obbligatoria o facoltativa del conferimento dei dati	Già previsto dal Codice
○ La base giuridica del trattamento (ad esempio, il consenso espresso dall'Interessato o l'esecuzione di un contratto di cui l'Interessato è parte)	Novità del GDPR
○ Le conseguenze di un eventuale rifiuto di rispondere	Già previsto dal Codice
○ 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 Designati, se nominati in tal senso in quanto trattano dati per conto del Titolare o in qualità di autonomi titolari del Trattamento, se estranei all'originario trattamento eseguito dal Titolare) e l'ambito di diffusione dei dati medesimi	Già previsto dal Codice
○ Ove applicabile, l'intenzione del Titolare del trattamento di trasferire dati personali a un Paese terzo o a un'organizzazione internazionale e, se del caso, attraverso quali strumenti (attenzione alle *newsletter* inviate attraverso programmi di invio massivo a *mailing lists*, spesso gestite da soggetti *extra* UE)	Novità del GDPR
○ I diritti dell'Interessato	Già previsto dal Codice, ma da aggiornare con i nuovi diritti previsti dal GDPR (artt. 15 e segg.)
○ Gli estremi identificativi del Titolare del trattamento e, ove presente, del Responsabile del trattamento	Già previsto dal Codice
○ I dati del Responsabile della Protezione dei Dati personali (RPD), se nominato	Novità del GDPR

[2] Nel caso di dati personali non raccolti direttamente presso l'Interessato (art. 14 del GDPR), l´informativa deve essere fornita entro un termine ragionevole che non può superare un mese dalla raccolta, oppure al momento della comunicazione (non della registrazione) dei dati (a terzi o all´Interessato).
[3] Ai sensi dell'art. 13, paragrafo 4, dell'art. 14, paragrafo 5 e dell'art. 23, paragrafo 1 del GDPR, spetta al Titolare, in caso di dati personali raccolti da fonti diverse dall'Interessato, valutare se la prestazione dell'informativa agli Interessati comporti uno sforzo sproporzionato.
[4] È preferibile il formato elettronico (soprattutto nel contesto di servizi online: art. 12, paragrafo 1 e Considerando 58 del GDPR), anche se sono ammessi "altri mezzi", quindi può essere fornita anche in modalità cartacea. Il GDPR ammette l'utilizzo di icone per presentare i contenuti dell'informativa in forma sintetica, ma solo "in combinazione" con l'informativa estesa (art. 12, paragrafo 7, del GDPR); tali icone dovranno essere identiche in tutta la UE e saranno definite prossimamente dalla Commissione Europea stessa.

○ L'esistenza di un processo decisionale automatizzato, compresa la profilazione, indicando anche la logica di tali processi decisionali e le conseguenze previste per l'Interessato	Novità del GDPR
○ Il periodo di conservazione dei dati o i criteri utilizzati per determinare tale periodo	Novità del GDPR

Per quanto riguarda **i diritti dell'Interessato**, l'informativa può elencarli analiticamente[5] o fare un rinvio agli artt. 15 e segg. del GDPR. In ogni caso, è importante indicare che l'Interessato ha diritto di presentare reclamo al Garante privacy qualora il Titolare non fornisca riscontro alle richieste dell'Interessato nei tempi previsti (un mese dalla richiesta – estendibile fino a tre mesi in casi di particolare complessità – entro il quale il Titolare deve comunque dare un riscontro all'Interessato anche in caso di diniego) o la risposta fornita dal Titolare non fosse soddisfacente. Per quanto riguarda le finalità del trattamento, occorre tenere sempre a mente il **principio di pertinenza** del trattamento stesso alle finalità per le quali i dati sono stati raccolti (come dichiarato nell'informativa).

Acquisizione del consenso

Al di fuori dei casi nei quali esiste una differente base giuridica che legittima il trattamento dei dati[6], cosicché si può procedere al trattamento senza previamente raccogliere il consenso dell'Interessato, si rende necessario raccogliere e documentare l'acquisizione del consenso.

[5] Gli artt. 15 e segg. del GDPR conferiscono all'Interessato il diritto di ottenere:
la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile;
l'indicazione dell'origine dei dati personali, delle finalità e modalità del trattamento, della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici, degli estremi identificativi del Titolare;
l'aggiornamento, rettifica, integrazione, cancellazione, trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge (compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono raccolti o successivamente trattati);
l'attestazione che tali operazioni sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si riveli impossibile o comporti un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.
L'Interessato ha inoltre il diritto:
- di revocare in qualsiasi momento il consenso prestato al trattamento dei dati personali (senza pregiudizio della liceità del trattamento basata sul consenso prestato prima della revoca);
- di opporsi, in tutto o in parte, per motivi legittimi, al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
- di opporsi, in tutto o in parte 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;
- di proporre reclamo al Garante privacy nei casi previsti dal GDPR;
- alla portabilità dei dati personali (diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un Titolare del trattamento e diritto di trasmettere tali dati a un altro Titolare del trattamento senza impedimenti da parte del Titolare del trattamento cui li ha forniti) nei limiti di cui all'art. 20 del GDPR.

[6] Art. 6 del GDPR:
- esecuzione di un contratto di cui l'Interessato è parte;
- adempimento di un obbligo di legge;
- salvaguardia degli interessi vitali dell'Interessato o di un'altra persona fisica;
- esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento;
- perseguimento del legittimo interesse del Titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'Interessato.

Art. 9 del GDPR:
- assolvimento degli obblighi ed esercizio dei diritti specifici del Titolare del trattamento o dell'Interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale;
- tutela di un interesse vitale dell'Interessato o di un'altra persona fisica qualora l'Interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
- il trattamento è effettuato da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'Interessato;
- dati personali resi manifestamente pubblici dall'Interessato;
- accertamento, esercizio o difesa di un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
- motivi di interesse pubblico;
- finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali;
- motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici;
- archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.

Il consenso può essere espresso verbalmente per i dati personali c.d. "comuni" (non appartenenti a categorie particolari per i quali è invece obbligatoria l'acquisizione per iscritto, come quelli di cui all'art. 9 e 10 del GDPR), ma è sempre e comunque preferibile che sia manifestato e acquisito per iscritto (sempre in virtù del principio di *accountabiliy*). Deve essere un consenso espresso (non vale il principio del silenzio-assenso) e va prestato con specifico riferimento alle varie tipologie di trattamento che il Titolare intende effettuare e che richiedono la prestazione del consenso. È possibile acquisirlo attraverso moduli, ivi inclusi quelli *online*, ma non possono essere proposte caselle pre-spuntate (deve essere assicura la libertà di scelta e la facoltà di negare il consenso anche solo con riferimento a certi trattamenti). Nel caso in cui il trattamento dei dati assolva a più finalità, è necessario che il consenso sia espresso in maniera specifica per ogni singola finalità di trattamento che richiede la prestazione del consenso.

Per i minori di età, il Decreto Attuativo ha fissato in 14 anni il limite di età al di sopra della quale la prestazione del consenso da parte dell'Interessato sarà ritenuta valida ed efficace (al di sotto della quale è necessario che il consenso sia prestato dai genitori o chi ne fa le veci).

Conferimento degli incarichi
Già nella vigenza del solo Codice, era prevista la facoltà per il Titolare del trattamento di designare uno o più **Responsabili del Trattamento** (individuati tra soggetti che per esperienza, capacità ed affidabilità fornivano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di Trattamento, ivi compreso il profilo relativo alla sicurezza), con indicazione specifica per iscritto dei compiti affidati. Attualmente, questa facoltà è divenuto un vero e proprio obbligo.

Quindi, i soggetti terzi a cui vengono affidati trattamenti (o parti di trattamento) del Titolare debbono essere nominati per iscritto **Responsabili del Trattamento esterni**. Costoro trattano i dati personali per conto del Titolare, attenendosi alle indicazioni ricevute dal medesimo. In ogni caso, il Titolare ha la responsabilità sulla scelta della figura del Responsabile (c.d. "*culpa in eligendo*") e deve vigilare sul rispetto delle istruzioni impartite (c.d. "*culpa in vigilando*"). Inoltre, l'art. 2-*quaterdecies* del Codice prevede anche che le operazioni di trattamento possono essere effettuate solo da soggetti **Designati**, i quali operano sotto la diretta autorità del Titolare o del Responsabile, attenendosi alle istruzioni impartite. La nomina è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito.

Tali principi si ritrovano anche nel GDPR. Secondo l'art. 28 del GDPR, qualora un trattamento debba essere effettuato per conto del Titolare del trattamento, quest'ultimo ricorre unicamente a Responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'Interessato; invece, secondo l'art. 29 del GDPR, il Responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del Titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal Titolare del trattamento. Sempre secondo l'art. 28 del GDPR, sotteso alla nomina di Responsabile del trattamento vi deve essere un contratto (o altro atto giuridico) che vincoli il Responsabile del trattamento al Titolare del trattamento e che disciplini i compiti, la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di Interessati, gli obblighi e i diritti del Titolare del trattamento.

Istituzione e aggiornamento del Registro del trattamento dei dati
È un nuovo adempimento previsto dall'art. 30 del GDPR, il quale – in base alle "Istruzioni del Garante privacy sul registro dei trattamenti" dell'8 ottobre 2018 – è praticamente obbligatorio per tutti i soggetti che trattano dati personali in forma non occasionale. Tra i contenuti del Registro del trattamento dei dati si segnalano le seguenti informazioni:

- chi è e come si può contattare il Titolare del trattamento e l'RPD (se nominato);
- finalità del trattamento dei dati personali;
- tipologie di dati trattati e di trattamenti effettuati;
- basi giuridiche su cui si fonda il trattamento e casi in cui è previsto il consenso degli Interessati (da dove risulta la prestazione del consenso);
- diverse categorie di Interessati;
- a chi possono essere comunicati i dati e se possono essere comunicati anche ad organizzazioni internazionali o ad organizzazioni con sede fuori dalla UE e relative garanzie assicurate;
- denominazione dei Responsabili esterni del trattamento (se nominati);

- modalità di conservazione dei dati;
- dopo quanto tempo (c.d. "*data retention*") o in che casi si procedere alla cancellazione dei dati;
- quali sono i rischi nel trattamento dei dati e quali sono le misure di sicurezza tecniche e organizzative adottate.

Il Registro del trattamento, dopo essere stato istituito e predisposto, deve essere aggiornato periodicamente, qualora vi sia un nuovo trattamento o i trattamenti già in essere subiscano delle modifiche sostanziali.

Formazione degli operatori
Come detto, l'art. 2-*quaterdecies* del Codice e l'art. 29 del GDPR prevedono che il Titolare o il Responsabile del trattamento istruiscano coloro che hanno accesso ai dati personali, attraverso un apposito atto scritto, mediante il quale dette persone vengono nominate Designati del trattamento. La centralità della formazione è confermata anche dall'art. 32, par. 4 del GDPR che impone al Titolare del trattamento ed al Responsabile del trattamento di far sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali, non tratti tali dati se non sia stato istruito in tal senso.

Occorre pertanto che il Titolare effettui un'adeguata formazione ed istruzione del personale (Designati del trattamento) in materia di protezione dei dati. La formazione costituisce una misura di sicurezza, un onere a carico del Titolare del trattamento, un diritto e dovere per dipendenti e collaboratori che trattano dati personali. Il Titolare del trattamento dovrà quindi pianificare un piano di formazione e aggiornamento (dando priorità ai nuovi assunti e alle figure di maggior rilievo nel trattamento dei dati), stanziare apposite risorse nei propri *budget*, pianificare *test* per verificare il livello di apprendimento e soluzioni alternative in caso di risultati negativi.

La formazione dovrebbe, alla luce dell'impianto del GDPR, presentare un taglio interdisciplinare (con sessioni sia informatiche che giuridiche) e pragmatico e riguardare tutti i soggetti. La stessa dovrebbe essere finalizzata ad illustrare i rischi generali e specifici dei trattamenti di dati, le misure organizzative, tecniche ed informatiche adottate, nonché le responsabilità e le sanzioni. Nel caso di mancata erogazione della formazione sono infatti applicabili le sanzioni elencate al paragrafo seguente.

L'adempimento degli obblighi formativi è inoltre spesso oggetto anche di accertamenti ispettivi da parte del Garante privacy (che effettua tali ispezioni avvalendosi della Guardia di Finanza). Già in vigenza del Codice, infatti, il Garante privacy richiedeva, in sede di ispezioni, di acquisire il programma ed il piano di formazione in materia di *privacy*, i materiali erogati al personale, il *test* finale di valutazione e le istruzioni agli Incaricati al trattamento (ora Designati).

Notifica delle violazioni privacy – c.d. "*data breach*"
In caso di violazione dei dati personali – a meno che sia improbabile che tale violazione presenti un rischio per i diritti e le libertà degli interessati – il Titolare del trattamento è tenuto a notificare la violazione al Garante entro 72 ore dal momento in cui ne viene a conoscenza. In caso di ritardo nella notifica, deve specificare i motivi del ritardo.
N.B. Per violazione dei dati personali non si intende solo il furto o la manomissione dei medesimi, ma anche situazioni molto più comuni quali, ad esempio, lo smarrimento di un pc portatile o di un *device*, o la clonazione delle credenziali di accesso a piattaforme in *cloud* o simili.

La notifica deve almeno:
a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di Interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
b) comunicare il nome e i dati di contatto dell'RPD (ove nominato) o di altro punto di contatto presso cui ottenere più informazioni;
c) descrivere le probabili conseguenze della violazione dei dati personali;
d) descrivere le misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi (art. 33 del GDPR).

Il Titolare del trattamento deve documentare ogni violazione, le relative circostanze, conseguenze, i provvedimenti adottati (in virtù del principio della *accountability*). Tale documentazione consente al Garante privacy di verificare il rispetto del GDPR.

LE SANZIONI

Il profilo sanzionatorio è uno degli aspetti di maggior innovazione introdotti dal GDPR. In particolare, al fine di rendere più efficace e cogente detta normativa, specialmente nei confronti dei grandi gruppi di imprese internazionali, sono state sensibilmente inasprite le sanzioni in caso di commissione di violazioni. Il GDPR prevede le seguenti sanzioni amministrative pecuniarie:

A. fino a 10 milioni di euro, o per le imprese fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente (se superiore), ad esempio nei casi di:
   - violazione delle misure di sicurezza o non individuazione di tali misure;
   - mancata nomina dell'RPD nei casi in cui la nomina è obbligatoria per legge;
   - mancata istituzione e tenuta del Registro del trattamento dei dati nei casi obbligatori per legge;
B. fino a 20 milioni di euro, o per le imprese fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente (se superiore), ad esempio nei casi di:
   - violazione dei principi base del trattamento, compresa la mancata acquisizione del consenso;
   - mancata informativa all'Interessato sulle modalità di trattamento dei suoi dati e sui suoi diritti;
   - violazione delle norme sul trasferimento dei dati a un paese terzo od organizzazione internazionale fuori della UE.

Il Garante privacy dovrà provvedere affinché le sanzioni amministrative pecuniarie inflitte ai sensi del GDPR siano in ogni singolo caso effettive, proporzionate e dissuasive. Infine, i singoli Stati della UE potranno introdurre norme relative ad altre sanzioni per le violazioni del GDPR, in particolare per le violazioni non soggette alle sanzioni amministrative pecuniarie sopra indicate; anche tali sanzioni dovranno essere effettive, proporzionate e dissuasive.

I PROGETTI FINANZIATI DA CON I BAMBINI E FONDAZIONE CON IL SUD

Nell'ambito della propria attività istituzionale di erogazione dei contributi, l'Impresa sociale Con i Bambini (di seguito "**CON I BAMBINI**") e la Fondazione Con il Sud (di seguito "**Fondazione**") utilizzano una piattaforma informatica denominata "Chàiros" (di seguito, la "**Piattaforma**"), con titolarità comune, la quale consente la raccolta delle richieste di contributi e la gestione dei progetti finanziati.

Le organizzazioni che richiedono detti contributi sono organizzate in partenariati composti: a) da un soggetto responsabile del Progetto finanziato (di seguito, il "**Soggetto responsabile**"), che rappresenta l'ente cui formalmente viene assegnato il contributo e che accede alla Piattaforma per l'inserimento di circa il 90% delle informazioni richieste; b) più soggetti della partnership (di seguito, i "**Partner**"), che collaborano con il Soggetto Responsabile per la realizzazione delle attività progettuali e possono accedere alla Piattaforma per caricarvi la residua quota di informazioni.

Con riferimento alla gestione dei Progetti finanziati, la Piattaforma consente di svolgere, tra le altre, due funzioni rilevanti ai fini della privacy:

- la raccolta dei dati delle persone fisiche che partecipano alle attività realizzate dal partenariato, ossia i reali beneficiari dei Progetti finanziati (di seguito, i "**Beneficiari**");
- la rendicontazione dei contributi erogati, ovvero la raccolta e la catalogazione della documentazione delle spese sostenute da tutti i Partner, quali, ad esempio, il pagamento delle risorse umane, l'acquisto di beni e/o servizi, i rimborsi per le trasferte, il vitto e/o l'alloggio, ecc.

Raccolta dei dati personali dei Beneficiari

I Soggetti responsabili sono tenuti, per alcuni dei Beneficiari delle attività incluse nel Progetto finanziato (comprese le attività svolte dagli altri soggetti della partnership), a compilare un form elettronico sulla Piattaforma Chàiros, in cui sono inserite le caratteristiche anagrafiche e socio-culturali dei Beneficiari, incluse le particolari categorie di dati di cui all'art. 9 del GDPR.
L'insieme delle informazioni inserite nella Piattaforma può essere visualizzato ed estrapolato dalla medesima:

- dal Soggetto Responsabile, per quanto riguarda il proprio Progetto finanziato e con riferimento a tutte le attività svolte dai Partner che vi partecipano;
- dalla Fondazione Con il Sud e dall'Impresa sociale Con i Bambini, per quanto riguarda tutti i Progetti da loro finanziati.

L'estrapolazione dei dati consente di effettuare analisi a diversi livelli di aggregazione (ad esempio, età media dei Beneficiari, distribuzione per genere, per territorio, per tipologia di attività svolta, ecc.). Inoltre, l'estrapolazione dei dati consente alla Fondazione e a CON I BAMBINI di sapere con esattezza il numero e la tipologia di Beneficiari delle diverse attività progettuali, nonché di effettuare verifiche in loco (mediante interviste orali e/o questionari) in merito alla loro effettiva partecipazione. Ovviamente, i Soggetti Responsabili, quali autonomi Titolari del trattamento, possono utilizzare i dati dei Beneficiari relativi al proprio Progetto finanziato afferenti le attività svolte dai Partner, per finalità proprie.

Rendicontazione delle spese sostenute

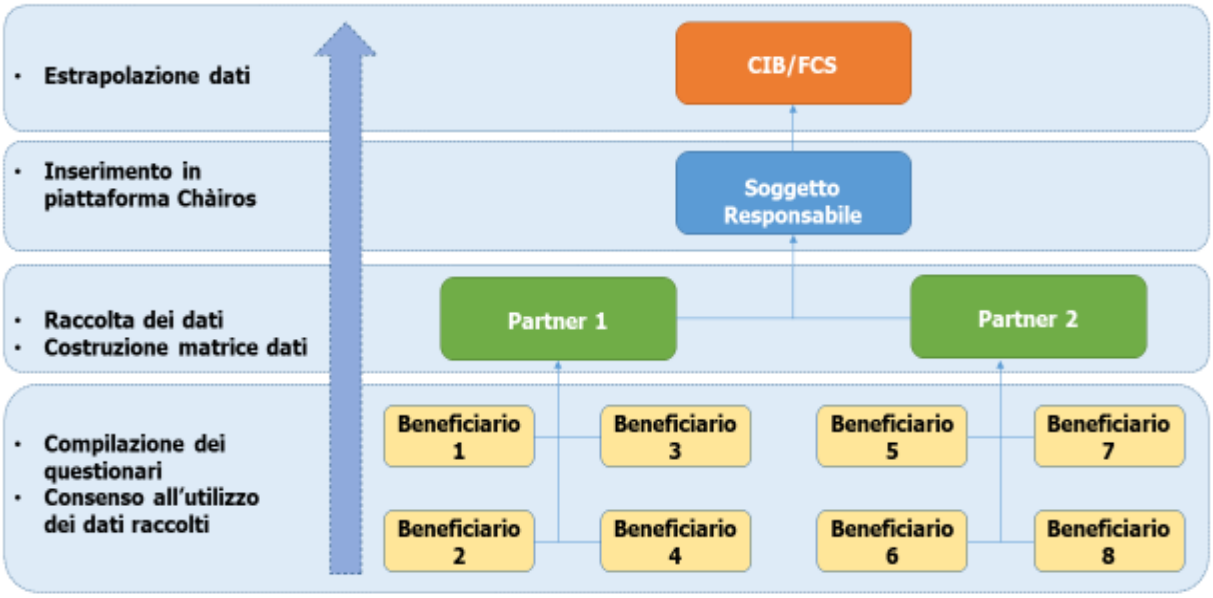
I Soggetti Responsabili sono tenuti a raccogliere copia della documentazione giustificativa delle spese sostenute da tutti i Partner e caricarla su un'apposita sezione della Piattaforma. L'insieme delle informazioni inserite nella Piattaforma può essere visualizzato ed estrapolato dalla medesima:

- dal Soggetto Responsabile, per quanto riguarda le spese sostenute per il proprio Progetto finanziato, con riferimento a tutte le attività svolte dai Partner che vi partecipano;
- dalla Fondazione e da CON I BAMBINI, per quanto riguarda le spese sostenute da tutti i Soggetti Responsabili e da tutti i Partner di tutti i Progetti finanziati.

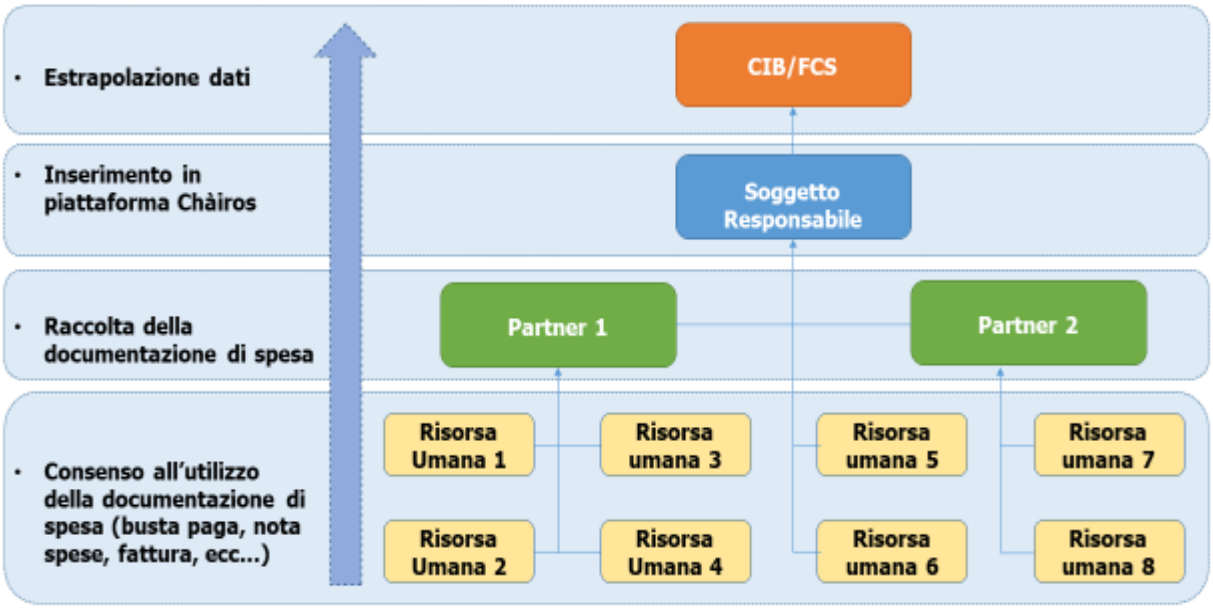
L'estrapolazione di siffatti dati consente di effettuare analisi sulle tipologie di spese presentate e determina la liquidazione delle diverse tranche di contributo. La liquidazione del contributo avviene dalla Fondazione o da CON I BAMBINI ai singoli Soggetti Responsabili dei Progetti finanziati, i quali – a loro volta – provvedono poi a riversare le quote spettanti agli altri Partner delle singole attività progettuali, sulla base delle spese inserite nella Piattaforma.

Schema dei flussi di dati personali
Al fine di comprendere meglio il complesso trattamento di dati illustrato al paragrafo precedente, di seguito si riporta schematicamente il flusso di dati afferente, rispettivamente, i Beneficiari e le spese sostenute.

***I.* Flusso dei dati personali dei beneficiari**



***II.* Flusso dei dati personali delle risorse umane rendicontate**



Adempimenti privacy
Una volta che è stato delineato il flusso dei dati personali ed il novero dei soggetti coinvolti, a diverso titolo, nel trattamento, occorre illustrare gli adempimenti privacy in campo, rispettivamente, al Partner, al Soggetto Responsabile, alla Fondazione e a CON I BAMBINI.

Partner
I Beneficiari (minori di età), in quanto Interessati al trattamento (nonché proprietari delle particolari categorie di dati di cui all'art. 9 del GDPR), devono ricevere un'informativa privacy ove il Soggetto Responsabile del Progetto finanziato è Titolare del trattamento ed è altresì prevista la prestazione di un espresso consenso alla comunicazione dei loro dati alla Fondazione o a CON I BAMBINI.

Infatti, I dati personali dell'Interessato vengono raccolti, in nome e per conto del Soggetto Responsabile (Titolare del trattamento per finalità legate alla realizzazione del Progetto finanziato), presso il Partner, il quale – a sua volta – risulterà autonomo Titolare del trattamento dei predetti dati, laddove li tratti per finalità proprie e diverse dalla realizzazione delle attività progettuali sovvenzionate.

Come detto, nell'informativa occorrerà prevedere un espresso consenso a che i dati del Beneficiario vengano comunicati alla Fondazione o a CON I BAMBINI, quali autonomi Titolari del trattamento, e si dovrà spiegare che detta comunicazione avverrà mediante l'inserimento nella piattaforma Chàiros, di cui entrambi risultano titolari; ovviamente, nell'informativa i Beneficiari verranno rassicurati sull'adeguatezza delle misure informatiche adottate per trattare (quindi anche trasferire) i loro dati, nonché sul periodo di c.d. "*data retention*" del trattamento.

In qualità di autonomi Titolari del trattamento, i Partner dovranno ottemperare ai seguenti adempimenti privacy:
- nominare, all'interno del proprio personale, i Designati del trattamento *ex* art. 2-*quaterdecies* del Codice ed *ex* art. 29 del GDPR, i quali tratteranno i dati dei Beneficiari inserendoli in data base cartacei e/o informatici, per poi inviarli al Soggetto Responsabile;
- rilasciare al proprio personale (ad esempio, ai docenti) adeguate informative privacy *ex* art. 13 del GDPR;
- adottare adeguate misure di sicurezza, fisiche e informatiche, per proteggere le proprie banche dati, specialmente perché contengono i dati dei Beneficiari e dei docenti appartenenti a particolari categorie di cui all'art. 9 del GDPR;
- prevedere e istituzionalizzare un'apposita procedura in caso di violazione dei dati (c.d. "*data breach*");
- istituire e successivamente tenere aggiornato un Registro del trattamento *ex* art. 30 del GDPR;
- effettuare una Valutazione d'impatto sulla protezione dei dati personali (di seguito, la "**DPIA**") *ex* art. 35 del GDPR (posto che i Partner svolgono, con i dati dei Beneficiari e dei docenti, un trattamento, su larga scala, di categorie particolari di dati personali *ex* art. 9 del GDPR);
- nominare un proprio RDP *ex* art. 37 del GDPR (posto che le attività principali dei Partner consistono nel trattamento, su larga scala, di categorie particolari di dati personali *ex* art. 9 del GDPR);
- provvedere ad una adeguata formazione privacy del proprio personale.

Dal momento che il Partner rilascia le informative e raccoglie i successivi consensi dei Beneficiari in nome e per conto del Soggetto Responsabile, quest'ultimo – limitatamente a tale trattamento – dovrà nominare per iscritto il primo Responsabile *ex* art. 28 del GDPR.

Le stesse considerazioni finora svolte per il trattamento di dati personali dei Beneficiari valgono anche per quelli dei docenti che partecipano al Progetto finanziato, i cui dati vengono comunicati al Soggetto Responsabile (prima) e alla Fondazione o a CON I BAMBINI (poi), ai fini della corretta rendicontazione delle spese e dell'erogazione dei fondi necessari alla realizzazione delle attività progettuali proposte; anche a costoro dovrà essere fornita idonea informativa privacy e richiesti i necessari consensi.

Soggetti Responsabili
Il Soggetto Responsabile del Progetto finanziato è il Titolare del trattamento nell'informativa da sottoporre ai Beneficiari; poiché i dati personali di quest'ultimi vengono raccolti e inizialmente trattati presso un soggetto

terzo, ossia il Partner, lo stesso dovrà essere designato per iscritto Responsabile del trattamento *ex* art. 28 del GDPR.

Una volta che il Soggetto Responsabile avrà ricevuto dal Partner la banca dati cartacea o informatica con le informazioni dei Beneficiari, sarà sua cura caricarla sulla piattaforma informatica "Chairos", di titolarità comune della Fondazione e di CON I BAMBINI.
In questo ambiente informatico protetto, il Soggetto Responsabile potrà vedere (e dunque trattare) i dati personali dei Beneficiari e dei docenti solo afferenti il proprio Progetto finanziato, mentre la Fondazione e CON I BAMBINI avranno accesso all'intero database di tutti i Progetti da loro sovvenzionati.

In particolare, il Soggetto Responsabile che inserirà i dati dei Beneficiari e dei docenti (buste paga, eventuali note spese, fatture, fogli presenze, ecc.) dovrà assicurare (magari mediante un apposito pop-up e successivo flag) che tali dati siano stati legittimamente raccolti, sia in termini di rilascio delle informative che di acquisizione dei correlati consensi; la presente procedura sarà a tutela della Fondazione e di CON I BAMBINI, mallevandole da eventuali doglianze promosse dai Beneficiari e dai docenti stessi.

Dal momento che anche i Soggetti Responsabili rivestono il ruolo di autonomi Titolari del trattamento, anch'essi dovranno ottemperare ai seguenti adempimenti privacy:

- nominare, all'interno del proprio personale, i Designati del trattamento *ex* art. 2-*quaterdecies* del Codice ed *ex* art. 29 del GDPR, i quali riceveranno i dati dei Beneficiari e dei docenti dai Partner e, successivamente, li caricheranno sulla Piattaforma;
- rilasciare al proprio personale (ad esempio, ai docenti) adeguate informative privacy *ex* art. 13 del GDPR;
- adottare adeguate misure di sicurezza, fisiche e informatiche, per proteggere le proprie banche dati, specialmente perché contengono i dati dei Beneficiari e dei docenti appartenenti a particolari categorie di cui all'art. 9 del GDPR;
- prevedere e istituzionalizzare un'apposita procedura in caso di violazione dei dati (c.d. "*data breach*");
- istituire e successivamente tenere aggiornato un Registro del trattamento *ex* art. 30 del GDPR;
- effettuare una DPIA *ex* art. 35 del GDPR (posto che i Soggetti Responsabili svolgono, con i dati dei Beneficiari e dei docenti, un trattamento, su larga scala, di categorie particolari di dati personali *ex* art. 9 del GDPR);
- nominare un proprio RDP *ex* art. 37 del GDPR (posto che le attività principali dei Soggetti Responsabili consistono nel trattamento, su larga scala, di categorie particolari di dati personali *ex* art. 9 del GDPR);
- provvedere ad una adeguata formazione privacy del proprio personale.

Dal momento che il Soggetto Responsabile carica i flussi dei dati personali dei Beneficiari e dei docenti sulla Piattaforma, di titolarità comune della Fondazione e di CON I BAMBINI, quest'ultimi – limitatamente a tale trattamento ossia, il mero accesso alla Piattaforma e il successivo caricamento dei dati
– dovranno nominare per iscritto il primo Responsabile ex art. 28 del GDPR.

Fondazione e CON I BAMBINI
La Fondazione e CON I BAMBINI sono a loro volta, rispettivamente, autonomi Titolari del trattamento dei singoli Progetti che finanziano, a fronte dei quali ricevono dai Soggetti Responsabili degli stessi i flussi dei dati dei Beneficiari e dei docenti, tutti caricati sulla piattaforma Chàiros (di seguito, la "**Piattaforma**"); per tale ragione, la Fondazione e CON I BAMBINI dovranno nominare per iscritto Responsabili del trattamento *ex* art. 28 del GDPR tutti i Soggetti Responsabili.

Siffatta comunicazione dei dati giuridicamente è resa possibile dal fatto che, nelle specifiche informative privacy rilasciate ai Beneficiari e ai docenti dei Progetti finanziati, è stato espresso apposito e specifico consenso alla comunicazione dei dati alla Fondazione o a CON I BAMBINI, i quali, successivamente, potranno poi anche ricontattare gli Interessati, rilasciando loro adeguata informativa, al fine di realizzare interviste sulla soddisfazione dei partecipanti in merito alle attività progettuali realizzate e/o proporre questionari finalizzati al medesimo scopo, nonché al fine di coinvolgerli in ulteriori altri loro progetti e/o iniziative istituzionali.

Il fatto di gestire tutti i flussi dei dati personali dei Beneficiari e dei docenti sulla Piattaforma, ossia su un ambiente informatico, impone alla Fondazione e a CON I BAMBINI la previsione e la concreta attuazione di

misure di sicurezza (in questo caso informatiche) assolutamente adeguate alla rilevanza (particolari categorie di dati di cui all'art. 9 del GDPR) e alla quantità (larga scala) dei dati trattati.

Infatti, se da un lato la Fondazione e CON I BAMBINI possono tutelarsi con un'adeguata malleva in merito alla circostanza che i dati inseriti dai Soggetti Responsabili nella Piattaforma siano stati acquisiti dagli stessi legittimamente (ossia, informando Beneficiari e docenti di tutto il processo ed acquisendo i necessari consensi), dall'altro devono – tra gli altri adempimenti – effettuare una specifica DPIA che possa minimizzare il rischio di c.d. "*data breach*" e di altre violazioni di dati personali.
Inoltre, poiché sicuramente la Fondazione e CON I BAMBINI avranno affidato la gestione tecnico-informatica della Piattaforma ad un *software house* specializzata, quest'ultima dovrà essere nominata per iscritto Responsabile del trattamento ex art. 28 del GDPR (da verificare se anche con obbligo di nomina dell'Amministratore di Sistema oppure no).

Pertanto, la Fondazione e CON I BAMBINI, quali autonomi Titolari del trattamento, dovranno anch'essi ottemperare ai seguenti adempimenti privacy:

- nominare, all'interno del proprio personale, i Designati del trattamento *ex* art. 2-*quaterdecies* del Codice ed *ex* art. 29 del GDPR, i quali tratteranno i dati dei Beneficiari e dei docenti inseriti dai Soggetti Responsabili nella Piattaforma;
- rilasciare al proprio personale (ad esempio, ai docenti) adeguate informative privacy *ex* art. 13 del GDPR;
- adottare adeguate misure di sicurezza, fisiche e informatiche, per proteggere la Piattaforma, specialmente perché contiene i dati dei Beneficiari e dei docenti appartenenti a particolari categorie di cui all'art. 9 del GDPR;
- prevedere e istituzionalizzare un'apposita procedura in caso di violazione dei dati (c.d. "*data breach*");
- istituire e successivamente tenere aggiornato un Registro del trattamento *ex* art. 30 del GDPR;
- effettuare una DPIA *ex* art. 35 del GDPR (posto che la Fondazione e CON I BAMBINI svolgono rispettivamente, con i dati dei Beneficiari e dei docenti, un trattamento, su larga scala, di categorie particolari di dati personali *ex* art. 9 del GDPR);
- nominare un proprio RDP *ex* art. 37 del GDPR (posto che le attività principali della Fondazione e di CON I BAMBINI consistono rispettivamente nel trattamento, su larga scala, di categorie particolari di dati personali *ex* art. 9 del GDPR);
- provvedere ad una adeguata formazione privacy del proprio personale.

In particolare, anche al fine di monitorare costantemente la conformità della Piattaforma e di tutta la struttura e procedura – informatica e non – ad essa connessa, la Fondazione e CON I BAMBINI hanno nominato l'Avv. Alessio Briganti dello Studio Legalitax quale proprio RPD, i cui recapiti mail sono, rispettivamente, **rpd@fondazioneconilsud.it** e **rpd@conibambini.org**.

Kit documentale

Al fine di consentire ai diversi enti coinvolti a vario titolo nei Progetti finanziati (la Fondazione, CON I BAMBINI, i Soggetti Responsabili e i Partner) di ottemperare alle previsioni del GDPR, gli uffici hanno messo a disposizione i seguenti *form* (predisposti specificatamente per il caso in oggetto), da fornire e/o far sottoscrivere ai diversi soggetti ivi indicati, come richiesto dalla normativa vigente:

FORM. 1) informativa e consenso beneficiari (per il Partner);
FORM. 2) informativa e consenso risorse umane (per il Partner);
FORM 3) informativa e consenso beneficiari (per il Soggetto Responsabile);
FORM. 4) informativa e consenso risorse umane (per il Soggetto Responsabile);
FORM. 5) atto di designazione come responsabile del trattamento dei dati (per il Partner);