Memo privacy

Dal 25 maggio si applica la nuova normativa in materia di protezione dei dati personali.

Con il presente "Memo", destinato in particolare alle ***micro*** *e* ***piccole*** *imprese, si intende fornire un quadro generale e meramente indicativo degli adempimenti da porre in essere per l'adeguamento alle disposizioni contenute nel Regolamento.*

Per un'impresa commerciale la cui attività non implica il trattamento di dati particolari (cioè i "vecchi" dati sensibili: salute, opinioni politiche, sindacali, religiose, ecc.), il Regolamento ha un impatto piuttosto contenuto, anche se non trascurabile che lo pone sostanzialmente in linea con le regole vigenti da oltre 20 anni in materia di privacy.

Va comunque subito evidenziato che la nozione di micro o piccola impresa non è meramente correlata alla quantità di dati e di informazioni che può essere trattata: infatti anche un'entità con uno o due dipendenti può essere in grado di processare, con strumenti automatizzati e software ad hoc, milioni di dati e informazioni ogni giorno, e di farli circolare in tutto il mondo.

Pertanto, anche per le piccole realtà, è ***fondamentale*** *procedere ad una* ***ricognizione dell'attività*** *che viene svolta.*

Dovrà quindi anzitutto essere effettuata una mappatura dei dati che vengono raccolti e trattati all'interno dell' azienda.

Le imprese dovranno effettuare ***un'analisi dei trattamenti****, ossia verificare quali trattamenti vengono fatti e a quali fini (ad esempio: trattamenti per gestione dei clienti, per gestione dei dati del personale, a fini di marketing e così via).*

Inoltre, è ***molto importante*** *che le imprese individuino* ***la tipologia dei dati*** *che vengono trattati con riferimento ai soggetti che ci forniscono le informazioni. In particolare, se si trattano dati comuni o dati particolari (i "vecchi" dati sensibili) nella propria attività.*

Infine, è necessario procedere ad un'analisi dell'organizzazione interna dell'impresa che dovrebbe riguardare chi, dentro l'azienda, tratta i dati, ossia individuare il titolare, gli eventuali responsabili esterni, i soggetti autorizzati, i destinatari, ecc.

Quest'ultima ricognizione permette di mappare l'eventuale organico, individuando anche i flussi dei dati.

Nel caso in cui, oltre alla classica attività di vendita, si dovessero vendere beni anche online o si utilizzasse un programma fedeltà, gli adempimenti saranno ovviamente più gravosi.

1. Integrare l'informativa

L'informativa costituisce il presupposto per la raccolta dei dati. Nel momento in cui si raccolgono dati deve essere fornita un'informativa.

Il regolamento introduce ulteriori elementi rispetto a quelli previsti dall'art. 13 del d.lgs 196/2003, che oggi contiene 7 elementi fondamentali (Finalità del trattamento; Modalità del trattamento; Natura obbligatoria o facoltativa del conferimento dei dati; Conseguenze del rifiuto di fornire i dati; Soggetti o categorie di soggetti cui i dati possono essere comunicati o che possono venirne a conoscenza; I diritti che spettano all'interessato; Gli estremi identificativi del titolare).

Le novità riguardano la forma ed il contenuto.

FORMA: l'informativa dovrà essere "*concisa, trasparente, inteleggibile e facilmente accessibile, con un linguaggio chiaro e semplice soprattutto per quelle destinate ai minore*",

CONTENUTO: dovrà invece essere aggiornato con i seguenti elementi:

- la base giuridica del trattamento (ad esempio: i dati sono utilizzati per l'esecuzione del contratto)
- i legittimi interessi perseguiti dal titolare nel caso il trattamento sia necessario per il loro perseguimento (esempio: l'imprenditore che vuole tutelare la sua attività attraverso un sistema di videosorveglianza);
- periodo di conservazione dei dati o nel caso in cui non fosse possibile individuarlo dei criteri per determinarlo. (es.: la durata può essere legata al periodo di validità del contratto o all'erogazione del servizio)
- L'intenzione di trasferire i dati in un Paese terzo (cioè extra UE);
- Il diritto di proporre reclamo all'autorità di controllo;
- L'esistenza di un processo decisionale automatizzato compresa la profilazione ove ricorra;
- Dati di contatto del Dpo ove ricorra.

Pertanto, alla luce delle novità indicate**, le informative attualmente in uso dovranno essere aggiornate quanto meno con il periodo di conservazione dei dati, che non potrà essere illimitato; ciò determina un cambiamento della politica di conservazione di dati.**

2. *Verificare la necessità del consenso al trattamento dei dati*

Dopo aver fornito un'informativa completa di tutti gli elementi previsti dal regolamento comunitario, affinché il trattamento dei dati raccolti sia effettuato in conformità alle disposizioni di legge, sarà necessario acquisire, ove richiesto, uno specifico consenso da parte degli interessati; detto consenso, per essere validamente manifestato, dovrà essere:
Informato, libero, specifico ed inequivocabile.

Esso rappresenta una condizione legittimante il trattamento dei dati, salvo che non rientri nelle deroghe espressamente previste.

In alcuni casi, infatti, non è richiesto il consenso delle persone interessate, ad esempio:

•nei casi in cui il trattamento sia necessario per l'esecuzione di un contratto di cui l'interessato è parte (ad esempio il trattamento dei dati per la concessione di un mutuo bancario, trattamento dei dati necessari per l'esecuzione di un contratto già in essere, come quelli per la fatturazione di un prodotto o servizio);
•quando il trattamento è previsto da un obbligo di legge (come ad esempio quello che impone agli alberghi di comunicare le generalità delle persone alloggiate alle autorità di pubblica sicurezza);
•per la salvaguardia di interessi vitali dell'interessato o di un'altra persona (ad esempio l'interessato è impossibilitato a prestare il consenso);
•per l'esecuzione di un compito di interesse pubblico;
per il perseguimento del legittimo interesse subordinandolo al fatto che non prevalgono gli interessi o i diritti e le libertà fondamentali (ad esempio divieto di riprendere i lavoratori nella loro attività lavorativa).

Ricorrendo una delle precedenti ipotesi, il consenso non è necessario ed è sufficiente la consegna dell'informativa (con ricevuta che attesti la presa visione da parte dell'interessato), che conferma così la centralità della propria funzione nell'ambito del trattamento dei dati personali.

Nel caso in cui il trattamento abbia più finalità il consenso dovrà essere prestato per ciascuna di esse.

Si evidenzia che non si possono trattare categorie particolari di dati (i "vecchi" dati sensibili) se non si riceve il consenso da parte dell'interessato, che in questo caso deve essere esplicito. L'acquisizione del consenso scritto soddisfa la condizione del consenso esplicito.

In particolare, affinché il consenso sia "*inequivocabile*" è necessario che la relativa richiesta sia chiaramente distinguibile dalle altre richieste; ad esempio all'interno della modulistica è necessario prestare attenzione alla formula utilizzata per prestare il consenso.

Non viene, pertanto, soddisfatto il requisito di "inequivocabilità", e si verifica una situazione a rischio, nel caso di: silenzio dell'interessato o l'inattività di questo o nel caso in cui il consenso non è chiaramente distinguibile in una clausola specifica separata dalle altre clausole del contratto o non è chiara la formula del consenso o non c'è scritto che il consenso può essere revocato.

Per le carte fedeltà si rileva che con la sottoscrizione del contratto di fidelizzazione è possibile utilizzare i dati del cliente solo al fine di ricevere sconti, premi bonus; è invece richiesto un **consenso specifico** per usare gli stessi dati per altri fini come ad esempio: per la profilazione, lo studio di comportamenti e delle scelte di acquisto o il marketing in generale. Si rileva che i clienti consumatori possono non dare il consenso all'uso dei dati per tali scopi, senza però rinunciare alla tessera di fidelizzazione.

In particolare, si rileva che il Garante con Provv. del 2010, ha chiarito che non è necessario richiedere il consenso per inviare comunicazioni promozionali che riguardino prodotti e servizi alla persona che ha già acquistato, dallo stesso titolare, beni analoghi (**cosiddetto "soft spam**").

Naturalmente il cliente deve essere adeguatamente informato anche riguardo alla possibilità di opporsi in qualunque momento all'uso dei propri dati, in maniera agevole e gratuita, anche a voce o con l'invio di una e-mail, ottenendo un tempestivo riscontro dall'impresa che confermi l'interruzione delle comunicazioni commerciali.

A tal proposito, è bene ricordare che l'utilizzo dei dati personali per finalità di **marketing diretto** non può essere reso di fatto obbligatorio, condizionando ad esempio l'accesso ai contenuti informativi di un sito web al rilascio del consenso a trattare i dati per finalità diverse, quali la profilazione e il marketing.

Infine, quando si acquisiscono liste di dati personali da soggetti terzi e non direttamente dagli interessati, prima di utilizzarli è, necessario verificare se gli interessati abbiano dato il proprio consenso (magari con verifiche a campione sui dati acquistati) al tipo di trattamento dati che si vuole svolgere, come quello per l'invio di offerte commerciali.

Il consenso che è stato raccolto precedentemente al 25 maggio p.v. resta valido se acquisito secondo le modalità sopra riportate.

Profilazione

Un'altra innovazione che inciderà in maniera trasversale sulle scelte delle imprese sarà la disciplina dettata in materia di profilazione. Marketing, sicurezza, monitoraggio dei clienti, analisi, controllo: presuppongono spesso

un'attività di profilazione. Le imprese che se ne occupano, come core business o per processi aziendali, avranno l'obbligo di fornire comunicazioni particolarmente precise e chiare agli interessati.

Se si profila la clientela va integrata l'informativa ed acquisito il consenso.

Infine, posto che il trattamento che comporta la profilazione del dato determina un rischio elevato, sarà necessario effettuare, prima del trattamento, una valutazione di impatto sulla protezione dei dati**.**

Altri istituti ed adempimenti

1- Revisione la Nomina del responsabile esterno

Tra gli ulteriori adempimenti richiesti dalla normativa sul trattamento dei dati, non va dimenticata l'analisi dei contratti o comunque dei rapporti con i fornitori esterni.

Accade, infatti, di frequente che l'azienda usufruisca di servizi da parte di soggetti esterni (ad esempio servizi informatici in outsourcing, oppure servizi offerti da un call center o da un altro tipo di fornitore sito web, mail, gestione dipendenti) che richiedono, per l'adempimento delle obbligazioni contrattuali, l'accesso a dati personali comuni, o rientranti in categorie particolari, raccolti dal titolare.

In tali casi, le imprese che forniscono detti servizi, al fine di poter legittimamente trattare i dati, devono nominare tali soggetti responsabili esterni del trattamento.

A tal proposito si segnala che il paragrafo 3 dell'art 28 del Regolamento, impone requisiti minimi ai contratti o alle lettere di nomina a responsabile esterno in cui viene disciplinata la durata del trattamento, la natura e le finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento.

Pertanto, nel caso in cui il responsabile esterno ricorra ad un altro soggetto (cd. sub-Responsabile), per adempiere a specifiche attività di trattamento per conto del titolare, è necessario che tale soggetto sia preventivamente autorizzato dal titolare del trattamento.

La Commissione e le autorità nazionali di controllo (fra cui il Garante) stanno valutando la definizione di clausole contrattuali tipo da utilizzare a questo scopo.

Tale nomina, secondo quanto previsto dall'art.28 del Regolamento, deve contenere:

a) Durata, natura e finalità del Trattamento, il tipo di dati oggetto di trasferimento e le categorie di interessati:

L'impegno del Responsabile a:

b) Trattare i dati, esclusivamente per le finalità connesse all'esecuzione del contratto, e su istruzioni documentate del Titolare;

c) Garantire che i soggetti autorizzati dal Responsabile stesso a compiere operazioni di trattamento sui dati, siano vincolati alla riservatezza;

d) Adottare all'interno della propria struttura, le misure di sicurezza di cui all'art.32 del Regolamento UE 2016/679;

e) Non nominare sub responsabili se non su espressa autorizzazione scritta del Titolare;

f) Predisporre misure tecniche ed organizzative adeguate per consentire al Titolare di assolvere il proprio obbligo di dare seguito nei tempi previsti ad eventuali richieste per l'esercizio dei diritti degli interessati;

g) Assistere il Titolare nel garantire il rispetto degli obblighi in materia di sicurezza del trattamento e di eventuale consultazione preventiva ai sensi dell'art. 36 del Regolamento;

h) Cancellare o fornire copia del dati al Titolare, alla conclusione del rapporto;

i) Mettere a disposizione del Titolare tutte le informazioni necessarie per dimostrare l'adempimento degli obblighi di cui alla presente nomina ed a consentire, se del caso collaborandovi, le atti

2- *Rivedere la Nomina delle persone autorizzate al trattamento*

Il titolare del trattamento dovrà verificare se ha **autorizzato i suoi collaboratori al trattamento dei dati raccolti** e, se lo ha già fatto (ci si riferisce alle nomine ad *incaricati* come erano individuati questi soggetti dalla disciplina vigente fino al 24 maggio 2018), è necessario che verifichi se l'atto di nomina che ha utilizzato è conforme alle indicazioni previste dal regolamento.

Nell'azienda è, infatti, molto frequente che il titolare del trattamento si avvale di collaboratori che svolgono compiti e funzioni connesse al trattamento dei dati.

Il titolare e il responsabile devono, pertanto, provvedere ad autorizzare tali persone, che agiscono sotto l'autorità del titolare o del responsabile, con un atto di nomina o altre modalità.

3-Registro dei trattamenti

L'art. 30 del regolamento comunitario prevede anche l'obbligo, per il titolare o il responsabile del trattamento, di tenere i registri delle attività di trattamento effettuate.

Anche in questo caso, la redazione di un registro dei trattamenti, per le piccole imprese per quanto semplificato, appare consigliabile.

L'obbligo di tenuta non si applica alle imprese ed alle organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati ovvero di dati sensibili e biometrici o dati personali relativi a condanne penali o a reati.

L'obbligo, pertanto, di tenere il registro dei trattamenti prescinde dal requisito dimensionale; infatti la previsione del registro dei trattamenti c'è ad esempio nel caso in cui i dati oggetto del trattamento fanno rifermento a dati particolari; ad es. il dato relativo allo stato di salute di un dipendente.

Il registro dei trattamenti consente al titolare/responsabile di disporre di un quadro aggiornato dei trattamenti in essere che può essere molto utile, se non quasi indispensabile, soprattutto nelle aziende più strutturate, per la valutazione del rischio.

Il registro dovrà essere messo a disposizione dell'Autorità di controllo in caso di ispezioni e controlli.

L'Autorità sta valutando di rilasciare un modello di registro dei trattamenti sul proprio sito, che i singoli titolari del trattamento potranno integrare.

Il registro del trattamento del titolare deve contenere le seguenti informazioni:

- nome e dati di contatto del titolare, contitolare, rappresentante del titolare e del DPO;
- finalità del trattamento;
- descrizione delle categorie di interessati e delle categorie di dati personali;
- categorie di destinatari cui i dati sono stati o saranno comunicati, anche all'estero;
- i trasferimenti di dati personali verso un paese terzo;
- i termini ultimi previsti per la cancellazione delle diverse categorie di dati (le politiche di conservazione dei dati);
- descrizione delle misure di sicurezza adottate

Le informazioni contenute nei registri tenuti dal responsabile sono invece relative al trattamento svolto per conto del titolare del trattamento. I contenuti del registro sono fissati, come detto, nell'art. 30; tuttavia, niente vieta a un titolare o responsabile di inserire ulteriori informazioni se lo si riterrà opportuno proprio nell'ottica della complessiva valutazione di impatto dei trattamenti svolti.

Il Garante ha specificato che la tenuta del registro dei trattamenti non costituisce un mero adempimento formale bensì costituisce parte integrante di un sistema di corretta gestione dei dati personali.

Per tale motivo, il Garante ha invitato tutti i titolari di trattamento e i responsabili, a prescindere dalle dimensioni dell'organizzazione, a compiere i passi necessari per dotarsi di tale registro e, in ogni caso, a compiere un'accurata ricognizione dei trattamenti svolti.

4-La violazione dei dati cd. Data Breach

L'art. 4 del regolamento comunitario definisce la violazione dei dati o *data breach* come la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso a dati personali trasmessi conservati o comunque trattati.

Il rischio che si verifichi la perdita dei dati aumenta sicuramente se si fa e-commerce; tuttavia il medesimo rischio potrebbe verificarsi anche in una piccola realtà.

Il regolamento comunitario precisa che, quando si configura una violazione dei dati, il titolare del trattamento deve notificare la violazione all'Autorità di controllo senza ingiustificato ritardo, se possibile entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati presenti un rischio per i diritti e le libertà delle persone fisiche (valutazione che spetta al titolare).

E' ammessa la notifica oltre il suddetto termine purché questa sia giustificata dai motivi del ritardo.

La notifica al Garante è obbligatoria in caso di rischio probabile; la comunicazione all'interessato è, invece, obbligatoria in caso di rischio elevato.

Ogni volta in cui si dovesse verificare una violazione dei dati personali, il titolare del trattamento e tutti coloro che trattano i dati dovrebbero essere in grado di reagire con prontezza.

E' opportuno quindi, a seconda dei dati trattati, valutare la necessità di dotarsi di una procedura, da seguire in caso di necessità, che dettagli come contenere, gestire e rimediare alle violazioni; valutare i rischi; effettuare la notifica.

E', inoltre, consigliabile verificare che il titolare sia in grado di dimostrare che i dipendenti sono stati istruiti alla gestione delle violazioni dei dati.

5-Nomina il Responsabile della protezione dei dati o DPO

Il Dpo è una figura designata dal titolare o dal responsabile del trattamento per assolvere a funzioni di supporto e controllo, consulenza, formazione e informazione in merito all'applicazione del Regolamento medesimo

E' importante capire quando la designazione del DPO è obbligatoria posto che, in molti casi, le PMI possono essere esentate.

A cercare di risolvere i dubbi sull'esatto perimetro applicativo di questa norma erano intervenute le "*Linee guida sui responsabili della protezione dei dati*" del 5 aprile 2017, emesse dal Gruppo dei Garanti Europei WP 243. A chiarire, però, ulteriormente i casi in cui la nomina del DPO è obbligatoria sono intervenute le risposte dell'Autorità Garante italiana pubblicate sulla pagina istituzionale della stessa http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/8036793uto alla nomina del DPO.

Il punto 4, del documento del Garante precisa che laddove si rileva che "*Nei casi diversi da quelli previsti dall'art. 37, par. 1, lett. b) e c), del Regolamento (UE) 2016/679, la designazione del responsabile del trattamento non è obbligatoria (ad esempio, in relazione a trattamenti effettuati da liberi professionisti operanti in forma individuale; agenti, rappresentanti e mediatori operanti non su larga scala; imprese individuali o familiari; piccole e medie imprese, con riferimento ai trattamenti dei dati personali connessi alla gestione corrente dei rapporti con fornitori e dipendenti*)."

In particolare il Garante precisa che le piccole e medie imprese con riferimento ai trattamenti dei dati personali connessi al gestione dei dati personali afferenti alla gestione corrente dei rapporti con i fornitori ed i dipendenti, non sono tenute a nominare il Dpo.

6. Il principio di responsabilizzazione (accountability) in cosa consiste?

Il regolamento pone con forza l'accento sulla "responsabilizzazione" (*accountability* nell'accezione inglese) di titolari e responsabili, ossia, sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento.

Con il principio della responsabilizzazione, previsto dal regolamento comunitario, si chiede al titolare del trattamento di mettere in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al regolamento.

L’adeguatezza delle misure deve essere valutata in base alla natura, all’ambito, al contesto o alle finalità o probabilità e gravità dei rischi, deve essere dimostrata dal titolare del trattamento e questo implica oneri formali e sostanziali.

Questo cambio di prospettiva del Regolamento, determina pertanto una accentuata responsabilizzazione di chi tratta i dati, che comporta la necessità di documentare le scelte fatte.

Il primo fra gli adempimenti richiesti è la "data protection by default and by design", ossia la necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili "al fine di soddisfare i requisiti" del regolamento e tutelare i diritti degli interessati. E’ poi prevista la gestione del rischio inerente al trattamento. Quest'ultimo è da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati tali impatti dovranno essere analizzati attraverso un apposito processo di valutazione tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative che il titolare ritiene di dover adottare per mitigare tali rischi.

7. Misure di sicurezza

Le misure di sicurezza devono "garantire un livello di sicurezza adeguato al rischio" del trattamento (art. 32, paragrafo 1); in questo senso, la lista di cui al paragrafo 1 dell'art. 32 è una lista aperta e non esaustiva ("tra le altre, se del caso"). Per lo stesso motivo non potranno sussistere dopo il 25 maggio 2018 obblighi generalizzati di adozione di misure "minime" di sicurezza (ex art. 33 Codice) poiché tale valutazione sarà rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificamente individuati come da art. 32 del regolamento. Si richiama l'attenzione anche sulla possibilità di utilizzare l'adesione a specifici codici di condotta o a schemi di certificazione per attestare l'adeguatezza delle misure di sicurezza adottate.

Tuttavia, l'Autorità potrà valutare la definizione di linee-guida o buone prassi sulla base dei risultati positivi conseguiti in questi anni; inoltre, per alcune tipologie di trattamenti (quelli di cui all'art. 6, paragrafo 1), lettere c) ed e) del regolamento) potranno restare in vigore (in base all'art. 6, paragrafo 2, del regolamento) le misure di sicurezza attualmente previste attraverso le disposizioni di legge volta per volta applicabili: è il caso, in particolare, dei trattamenti di dati sensibili svolti dai soggetti pubblici per finalità di rilevante interesse pubblico nel rispetto degli specifici regolamenti attuativi (ex artt. 20 e 22 Codice), ove questi ultimi contengano disposizioni in materia di sicurezza dei trattamenti.

Sarà necessario, infine, garantire la sicurezza del trattamento ad esempio la crittografia può, infatti, rivelarsi essenziale, ed estremamente potente, in casi

concreti di violazione dei dati anche accidentale (si pensi al dipendente che smarrisce lo smartphone o il computer aziendale) e, nella pratica, si applica cifrando le informazioni sui server, negli archivi e sui dispositivi.

Applicazione della nuova normativa

Il regolamento è entrato in vigore il 24 maggio del 2016, esso si applica a partire dal 25 maggio, quando dovrebbe essere garantito l'allineamento tra la normativa nazionale e le disposizioni del provvedimento comunitario.

Il Governo italiano ha predisposto uno schema di decreto legislativo finalizzato ad adeguare il quadro normativo nazionale che però, al momento, non ha completato l'iter di approvazione.

Lo schema di decreto non abroga completamente il Codice privacy, ma soltanto le disposizioni in contrasto con la normativa comunitaria.

Avremo pertanto un mini-Codice novellato cui si sommerà anche il nuovo decreto legislativo che, oltre a contenere le novelle al Codice vigente, contiene altresì nuove norme di coordinamento destinate a non confluire nel Codice novellato.

TIPOLOGIA DI DATI O TRATTAMENTI	ADEMPIMENTI PRIVACY
Trattamento dei dati	**E' obbligatorio procedere al trattamento dei dati secondo i principi di liceità, correttezza, trasparenza. I dati personali possono essere utilizzati solo per gli scopi per i quali sono stati originariamente raccolti.**
Conservazione dei dati	**Il titolare del trattamento deve mettere in atto procedure di conservazione del dato in modo da garantire che lo stesso sia conservato per un periodo non**

	superiore a quello necessario per lo scopo per cui era stato raccolto. E' infine necessario che vengano attuate procedure per garantire che i dati alla scadenza del termine indicato vengano distrutti in modo sicuro in conformità con le politiche di conservazione.
Dati dipendenti	**E' necessario fornire un'informativa all'atto dell'assunzione.** **I dipendenti che per motivi di servizio vengono a contatto con i dati devono essere nominati autorizzati al trattamento.**
Dati dei soci	**E' necessario fornire un'informativa all'atto dell'adesione**
Consenso	**E' obbligatorio acquisire il consenso salvo deroghe.** **(ad es. trattamento dati necessario alla stipula di un contratto di rapporti di lavoro)**
Formazione buste paga dipendenti/consulenti	**Individuare come persone autorizzate al trattamento dei collaboratori che per ragioni di servizio accedono ai dati anche di categorie particolari dei dipendenti e nomina del Responsabile Esterno (facoltativo) del Trattamento in caso di affidamento del servizio a collaboratori esterni.**

Rapporti con consulenti	**Nomina a Responsabili Esterni del Trattamento a favore di tutti i fornitori che per lo svolgimento dell'incarico affidato abbiano accesso a dati anche di categorie particolari raccolti dal Titolare del Trattamento.**
Rapporti contrattuali	**In caso di trasmissione, da parte di terzi, di dati personali da questi raccolti, accertarsi che il consenso sia stato preventivamente richiesto ed ottenuto. Per semplicità si consiglia l'inserimento di apposita clausola nei relativi contratti.**
Registro delle attività di trattamento	**E' obbligatorio per realtà aziendali con più di 250 addetti. Tuttavia, l'obbligo prescinde dal requisito dimensionale nel caso in cui i dati oggetto del trattamento possano presentare un rischio per i diritti e le libertà degli interessati, il trattamento non sia occasionale o includano dati sensibili, genetici, biometrici, giudiziari.**
Data breach (violazione dei dati personali)	**L'adempimento nel rispetto dei termini previsti dal regolamento è un obbligo che incombe su tutti i titolari del trattamento dati.** **Il titolare deve predisporre piani e procedure per affrontare la situazione ed eventualmente fornire all'Autorità la documentazione di tutte le violazioni subite. Per far fronte alle violazioni dei dati deve predisporre procedure di cooperazione tra il titolare ed i fornitori.**

Verifica del sistema di adeguatezza delle misure adottate	**Il titolare deve valutare i rischi del trattamento dei dati personali che tratta e deve predisporre un programma di sicurezza documentato che specifichi le misure tecniche e organizzative e logiche per un trattamento dei dati conforme al GDPR.** **Ad esempio per trasferire, archiviare e ricevere informazioni dovrebbe impiegare tecnologie specifiche per rendere il dato anonimo e quando non è più necessaria la conservazione dei dati personali, gli stessi dovrebbero essere distrutti, cancellati o resi anonimi.**
Formazione	**Dal momento che la formazione del personale assume un ruolo fondamentale, il Titolare dovrà predisporre un piano di formazione annuale che coinvolga tutti i soggetti che a vario titolo vengono coinvolti nel trattamento.**
DPO (Data protection Officer) o Responsabile della protezione dei dati	**Nel caso in cui si dovesse decidere che un DPO non è obbligatorio per l'attività che viene svolta è necessario documentare i motivi che hanno determinato la scelta.**