ITALIA
F.I.M.A.A.

PRIVACY
REGOLAMENTO UE
n. 2016/679

Avv. Daniele Mammani – mammani@tin.it

ITALIA
F.I.M.A.A.

COSA può intendersi per PRIVACY

- Diritto alla riservatezza delle informazioni personali e della propria vita privata
- Dominio sui propri dati personali
- Diritto di decidere l'uso dei propri dati personali (da parte di chi, dove, come, quando, e per quali scopi) ed esercitare un pieno controllo sugli stessi

PRIVACY: NASCITA DEL DIRITTO

- 15.12.1890 USA – Warren e Brandeis: «Right to privacy» Rapporto tra diritto ad informare, diritto dell'opinione pubblica ad essere informata e rispetto della riservatezza. (The right to be let alone)
- 1950 CEDU Convenzione europea dei diritti dell'uomo – art. 8 Diritto al rispetto della vita privata e familiare
- Cass. 20.4.1963 n. 990: riconosce una «Tutela della riservatezza della vita privata»
- 1981 CEDU Convenzione 108 – consenso per trattamento automatizzato dei dati dei cittadini
- 1995: **Direttiva CE 95/46**
- 1996: **L. 675/1996** (recepisce la Dir. CE 95/46) -> prima legge italiana in materia di privacy

NORMATIVA ATTUALMENTE IN VIGORE IN ITALIA

- **D. Lgs. 196/2003** c.d. Codice della Privacy **->** (a seguito dell'entrata in vigore del Reg. UE 2016/679) applicabile **solo** alle **persone giuridiche** e all'**e-commerce**
- **Regolamento UE 2016/679** (abroga la direttiva CE 95/46) -> applicabile **solo** per le **persone fisiche**
- **Provvedimenti Garante europeo**
- **Provvedimenti Garante italiano**

REGOLAMENTO UE 2016/679

- Diversamente dalle Direttive è immediatamente applicabile negli Stati membri
- È stato pubblicato nella Gazzetta Ufficiale dell'Unione Europea il 4 maggio 2016 e quindi è entrato in vigore il 24 maggio 2016
- **deve essere applicato dal 25 maggio 2018**

REGOLAMENTO UE 2016/679

Struttura del Regolamento:

- 173 considerando
- 99 articoli

ITALIA
F.I.M.A.A.

SCOPO DEL REGOLAMENTO UE 2016/679

Il Regolamento Ue n. 2016/679 si pone l'obiettivo di stabilire un complesso normativo volto alla **protezione del trattamento dei dati personali** delle persone fisiche, nonché di disciplinare le regole sulla **libera circolazione dei dati personali**.

Il Regolamento dell'Unione Europea produce effetti immediatamente vincolanti all'interno dell'ordinamento giuridico degli Stati membri e le norme in esso contenute prevalgono sulle normative in materia di privacy già addottate dai singoli Stati membri dell'UE (in Italia il D. Lgs. 30 giugno 2003, n. 196).

Categorie di imprese
PMI

CONSIDERANDO N. 13

«Le istituzioni e gli organi dell'Unione e gli Stati membri e le loro autorità di controllo sono invitati a considerare le esigenze specifiche delle micro, piccole e medie imprese nell'applicare il presente Regolamento»

ITALIA F.I.M.A.A.

segue: **Categorie di imprese**

Raccomandazione Commissione n. 361 del 6 maggio 2003 (2003/362/CE) (richiamato dal cons. n. 13)

Art. 2:

- Microimprese: < 10 persone e fatturato annuale o totale bilancio ≤ 2 milioni €
- Piccole Imprese: < 50 persone e fatturato annuale o totale bilancio ≤ 10 milioni €
- Medie Imprese:
  - < 250 persone e fatturato annuale ≤ 50 milioni €

  o
  - totale bilancio annuo ≤ 43 milioni €

PRINCIPI GENERALI DEL REGOLAMENTO (art. 5)

I **dati personali** sono:

- **Trattati** in modo -> **lecito** / **corretto** / **trasparente**
- **Raccolti** per finalità -> **determinate** / **esplicite** / **legittime**
- **Adeguati**, **pertinenti** e **limitati** a quanto necessario rispetto alle finalità -> Minimizzazione dei dati
- **Esatti** / **aggiornati**
- **Limitazione della conservazione** -> per il tempo adeguato alle finalità
- **Integrità** / **sicurezza** -> misure tecniche organizzative adeguate

PRINCIPALI MODIFICHE ALLA PRECEDENTE NORMATIVA

- Liceità del trattamento (art. 6)
- Consenso (art. 7)
- Dati particolari (art. 9) ex dati sensibili
- Informativa (art. 12 e ss.)
- Diritto alla cancellazione (diritto all'oblio, art. 17)
- Responsabilità titolare – accountability (art. 24)
- Sicurezza del trattamento (art. 32)
- Trasferimento dei dati verso paesi terzi (art. 44 e ss.)
- Autorità di controllo (art. 51 e ss.)
- Sanzioni (art. 83)

ITALIA
F.I.M.A.A.

PRINCIPALI NOVITA'

- Diritto alla portabilità dei dati (art. 20)
- Privacy by design e by default (art. 25)
- Registro delle attività di trattamento (art. 30)
- Notifica di una violazione - Data breaches (art. 33)
- Valutazione di impatto (art. 35)
- Data Protection Officer (D.P.O.) (art. 37)
- Codici di condotta (art. 40)
- Certificazione / marchi (art. 42)
- Cooperazione tra autorità di controllo (art. 60 e ss.)

DATI PERSONALI
DEFINIZIONE (art. 4)

- **Qualsiasi informazione** riguardante una **persona fisica** identificata o identificabile (**interessato**)
- Si considera **identificabile** la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un dato identificativo come:
  - Nome
  - Numero di identificazione (cod. fisc. ...)
  - Dati relativi all'ubicazione
  - Identificativo online
  - Altri elementi caratteristici della identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale

CATEGORIE PARTICOLARI DI DATI

- **DATI PARTICOLARI** (ex dati sensibili) (art. 9) : quelli che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici, i dati biometrici intesi ad individuare in modo univoco una persona, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
- **Dati relativi a CONDANNE PENALI E REATI** (art. 10): possono essere trattati soltanto sotto il controllo dell'autorità pubblica

TRATTAMENTO DEI DATI PARTICOLARI (art. 9)

- **E' vietato trattare i dati particolari .**

Deroghe al divieto (alcuni casi):

- esplicito consenso dell'interessato per uno o più finalità specifiche;
- il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale;
- il trattamento è necessario per la tutela di un interesse vitale dell'interessato o di un'altra persona fisica se l'interessato si trovi nell'incapacità di prestare il proprio consenso.

A QUALI DATI PERSONALI NON SI APPLICA IL REGOLAMENTO UE 2016/679

Il Regolamento UE **non si applica** ai **dati personali** delle **persone decedute**.

Gli Stati membri possono prevedere norme riguardanti il trattamento dei dati personali delle persone decedute.

TRATTAMENTO DEI DATI (art. 4 n. 2)

- Qualsiasi operazione o insieme di operazioni relativi ai dati personali e concernenti la:
  - Raccolta
  - Registrazione
  - Organizzazione
  - Strutturazione
  - Conservazione
  - Adattamento o modifica
  - Estrazione
  - Consultazione
  - Uso
  - Comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione
  - Raffronto o interconnessione
  - Limitazione
  - Cancellazione o distruzione

PROFILAZIONE DEI DATI (art. 4 n. 4)

- Qualsiasi forma di **trattamento automatizzato** di dati personali consistenti nell'**utilizzo dei dati personali per valutare** determinati aspetti personali relativi a una persona fisica, in particolare per **analizzare o prevedere** aspetti riguardanti:
  - il rendimento professionale
  - la situazione economica
  - la salute
  - le preferenze personali
  - gli interessi
  - l'affidabilità
  - il comportamento
  - l'ubicazione o gli spostamenti

ITALIA
F.I.M.A.A.

SOGGETTI PREVISTI

- **TITOLARE** DEL TRATTAMENTO
- **RESPONSABILE** DEL TRATTAMENTO
- **INCARICATI**
- **D.P.O.** (Data Protection Officer)

- **INTERESSATI**

IL TITOLARE DEL TRATTAMENTO (art. 4 n. 7 e art. 24)

- 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**

- Il Titolare è quindi l'IMPRESA, non è una persona fisica, tranne che si tratti di ditta individuale.

IL RESPONSABILE DEL TRATTAMENTO (art. 4 n. 8)

- La **persona fisica** o **giuridica**, **l'autorità pubblica**, il **servizio** o **altro organismo** che **tratta dati personali** per conto del titolare del trattamento

Segue IL RESPONSABILE art. 28

- Figura opzionale (può essere nominato quando la struttura aziendale è complessa)
- Supporto del Titolare in relazione agli obblighi privacy
- Deve possedere garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate (requisito di competenza)
- Compiti stabiliti per contratto (disciplina del trattamento, durata, natura, finalità del trattamento, ecc.)

ITALIA F.I.M.A.A.

Segue: RESPONSABILE DEL TRATTAMENTO (art. 28)

Il **contratto** deve prevedere, tra le diverse condizioni:

- che il Responsabile tratti i dati su istruzione documentata del Titolare del trattamento;
- garantisca che le persone autorizzate al trattamento si siano impegnate alla riservatezza;
- siano rispettati tutti gli obblighi necessari a garantire la sicurezza del trattamento;
- cancelli o restituisca al Titolare tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento;
- avvisi il Titolare che un'istruzione violi il Regolamento.

GLI INCARICATI (art. 29)

- I soggetti che hanno accesso ai dati personali
- Agiscono con l'autorizzazione del Titolare o del Responsabile
- Ricevono istruzioni dal Titolare

ITALIA
F.I.M.A.A.

IL D.P.O.
DATA PROTECTION OFFICER (art. 37)

- **Designazione** del **D.P.O.** da parte del **Titolare del trattamento** e del **Responsabile del trattamento** quando:
  - il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate 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 di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10.

ITALIA
F.I.M.A.A.

SEGUE: IL D.P.O. (art. 37)

Provvedimento del **Garante** (faq n. 4):

- la **designazione del DPO non è obbligatoria** in relazione ai trattamenti effettuati da **mediatori** operanti non su larga scala

LICEITA' DEL TRATTAMENTO (art. 6)

Il Trattamento è lecito quando:

- l'interessato **ha espresso il proprio consenso al trattamento dei propri dati** per una o più specifiche finalità;
- è necessario all' **esecuzione di un contratto** di cui l'interessato è parte o all'esecuzione di **misure precontrattuali** adottate su richiesta dello stesso;
- è necessario per **adempiere ad un obbligo legale** a cui è soggetto il titolare del trattamento;
- è necessario per **la salvaguardia degli interessi vitali** dell'interessato o di un'altra persona fisica ovvero quando è necessario per l'esecuzione di un compito di interesse pubblico o per il perseguimento del legittimo interesse del titolare del trattamento.

IL CONSENSO (art. 7)

Le **caratteristiche del consenso**, affinché sia **valido** e **correttamente acquisito**, sono:

- **informato** (quindi preceduto sempre da una idonea informativa);
- **libero** (privo da condizionamenti) e **revocabile** (in qualsiasi momento);
- **specifico** (per ciascuna finalità perseguita);
- **espresso** (ciò significa che non ci si può avvalere banalmente di un silenzio-assenso);
- **esplicito** (non è ammesso infatti un comportamento concludente);
- **inequivocabile** (deve essere certo al di là di ogni ragionevole dubbio, in termini di formulazione e contesto di riferimento).

E' esclusa ogni forma di consenso tacito

REVOCA DEL CONSENSO (art. 7)

- L'interessato ha il **diritto di revocare** il proprio **consenso** in **qualsiasi momento**

- La revoca del consenso non pregiudica mai la liceità del trattamento basata sul consenso prima della revoca

INFORMATIVA (artt. 13 – 14)

- Quel **nucleo di informazioni** che il titolare del trattamento è tenuto a fornire ai soggetti di cui si appresta a trattare i dati
- È **sempre necessaria**

INFORMATIVA: INFORMAZIONI DA FORNIRE QUALORA I DATI PERSONALI SIANO RACCOLTI PRESSO L'INTERESSATO (art. 13)

- l'**identità** e i **dati di contatto del titolare** e, ove applicabile del suo rappresentante;
- i **dati di contatto** del **Responsabile della Protezione dei Dati**;
- le **finalità del trattamento**;
- i **legittimi interessi perseguiti** dal titolare o da terzi;
- eventuali destinatari dei dati;
- l'eventuale intenzione del titolare di trasferimento dei dati ad un paese terzo;

ITALIA F.I.M.A.A.

Segue: INFORMATIVA: INFORMAZIONI DA FORNIRE QUALORA I DATI PERSONALI SIANO RACCOLTI PRESSO L'INTERESSATO (art. 13)

- il **periodo di conservazione** dei dati o, se non è possibile, i criteri utilizzati per determinare tale periodo;
- il **diritto di accesso** ai dati da parte dell'interessato, il **diritto di rettifica** e di **cancellazione**, la limitazione del trattamento o l'opposizione allo stesso e il **diritto alla portabilità**;
- il **diritto di revoca** del consenso;
- il **diritto di reclamo** all' autorità di controllo;
- l'**obbligatorietà** o la **non obbligatorietà** di **comunicare dati**, nonché le possibili conseguenze di un eventuale rifiuto;
- **l'esistenza di un processo automatizzato** come la profilazione e l'indicazione delle logiche utilizzate, dell'importanza e delle conseguenze del trattamento;
- nel caso in cui i dati raccolti vengano utilizzati per una finalità diversa da quella per cui gli stessi sono stati ottenuti obbligo di nuova informativa.

INFORMAZIONI DA FORNIRE QUALORA I DATI PERSONALI NON SIANO STATI OTTENUTI PRESSO L'INTERESSATO (art. 14)

Il **Titolare del trattamento** fornisce all'interessato un'**informativa**:

- **entro un termine ragionevole** dall'ottenimento dei dati, al più tardi **entro un mese** in considerazione delle specifiche circostanze in cui i dati sono trattati;
- in caso di prevista comunicazione con altro destinatario al più tardi al momento della prima divulgazione dei dati;
- nel caso in cui i dati siano destinati alla comunicazione con l'interessato al più tardi al momento della prima comunicazione all'interessato.

In tutti questi casi, ad ogni modo, **l'informativa deve contenere**:

- **tutto quanto indicato** per l'ipotesi in cui i dati siano raccolti presso l'interessato (**art. 13 Reg. n. 2016/679**);
- le **categorie dei dati** personali in questione;
- la **fonte di provenienza dei dati** e se questa ha carattere pubblico.

Anche in questo caso il titolare del trattamento, prima di procedere con qualsivoglia ulteriore trattamento non previsto inizialmente, deve fornire all'interessato le informazioni in merito alla diversa finalità dell'utilizzo dei suoi dati personali.

ITALIA F.I.M.A.A.

SEGUE: **INFORMAZIONI DA FORNIRE QUALORA I DATI PERSONALI NON SIANO STATI OTTENUTI PRESSO L'INTERESSATO (art. 14)**

Casi in cui **può essere omessa l'informativa**:

- se si **dispone già delle informazioni** o sono informazioni note;
- se comunicare tali informazioni comporta uno **sforzo sproporzionato** o è impossibile (valutazione che spetta al titolare del trattamento);
- se **l'ottenimento dei dati** o la loro comunicazione, sono **previsti dal diritto dell'Unione**;
- se i dati devono restare riservati per un obbligo di **segreto professionale**.

IL DIRITTO DI ACCESSO DELL'INTERESSATO (art. 15)

- Il diritto di ottenere dal titolare la **conferma che sia o meno in corso un trattamento** dei dati personali e in tal caso di ottenere l'accesso ai dati

- Il titolare deve indicare il **periodo di conservazione** previsto o, se non è possibile, i criteri utilizzati per definire tale periodo, nonché le **garanzie** applicate in caso di **trasferimento** dei dati verso Paesi terzi.

- I titolari, inoltre, possono consentire agli interessati di **consultare direttamente, da remoto** e in modo sicuro, i propri dati personali.

TEMPI DI ATTUAZIONE DEI DIRITTI DELL'INTERESSATO

- Il titolare è tenuto a **rispondere alle richieste dell'interessato** senza ingiustificato ritardo e al più tardi **entro un mese**

- Il **termine** di un mese **può essere prorogato** di **due mesi**, se necessario, tenuto conto della complessità e del numero di richieste

- Titolare **informa l'interessato** di tale proroga e dei motivi del ritardo **entro un mese** dal ricevimento della richiesta

- Se **non ottempera** alla richiesta dell'interessato, il titolare **informa** l'interessato senza ritardo e al più tardi **entro un mese dal ricevimento della richiesta, del motivi dell'inottemperanza** e della possibilità di proporre reclamo ad un'autorità di controllo e di proporre ricorso giurisdizionale

ITALIA
F.I.M.A.A.

IL DIRITTO DI RETTIFICA (art. 16)

- diritto di ottenere dal titolare del trattamento la **rettifica dei dati personali inesatti** senza ingiustificato ritardo

- diritto di ottenere **l'integrazione dei dati personali incompleti**

IL DIRITTO ALLA CANCELLAZIONE
DIRITTO ALL'OBLIO (art. 17)

- Il diritto "all'oblio" si configura come un **diritto alla cancellazione dei propri dati personali** in forma rafforzata.

- E' previsto l'obbligo per i titolari (se hanno "reso pubblici" i dati personali dell'interessato: ad esempio, pubblicandoli su un sito web) di informare della richiesta di cancellazione altri titolari che trattano i dati personali cancellati, compresi 'qualsiasi link, copia o riproduzione'.

IL DIRITTO DI LIMITAZIONE DEL TRATTAMENTO (art. 18)

- diritto di **ottenere dal titolare del trattamento la limitazione del trattamento** quando:
  - l'interessato **contesta l'esattezza dei dati personali**, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali
  - il **trattamento è illecito** e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo
  - benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria
  - l'interessato si è **opposto al trattamento ai sensi dell'articolo 21**, paragrafo 1, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

IL DIRITTO ALLA PORTABILITA' DEI DATI (art. 20)

Si tratta di uno dei **nuovi diritti** previsti dal Regolamento.

- Diritto dell'interessato a **ricevere**, **in un formato strutturato**, di uso comune e leggibile da dispositivo automatico**, i dati personali che lo riguardano** forniti ad un titolare del trattamento

- **Diritto di trasmettere** i suddetti dati ad un altro titolare del trattamento

- Si applica se il trattamento dei dati è effettuato con mezzi automatizzati

ITALIA F.I.M.A.A.

IL DIRITTO DI OPPOSIZIONE (art. 21)

- Consente all'interessato di **opporsi in qualsiasi momento**, per **motivi connessi alla sua situazione particolare**, al **trattamento dei dati** personali che lo riguardano.

- Il **titolare potrà continuare a trattare** i dati in suo possesso solo ove dimostri "l'esistenza di **motivi legittimi cogenti** per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria".

- Per i trattamenti che comportano attività di profilazione o di marketing diretto, il regolamento prevede che: "**qualora l'interessato si opponga al trattamento per finalità di marketing diretto, i dati personali non potranno più essere oggetto di trattamento per tali finalità**".

PRINCIPIO DI ACCOUNTABILITY (artt. 5 e 24)

- Al **titolare del trattamento** è affidato l'incarico di **decidere autonomamente le modalità**, le garanzie e i limiti del trattamento dei dati.

- Il titolare deve essere quindi in grado di **dimostrare di avere adottato misure giuridiche adeguate ed efficaci**, organizzative e tecniche, per la protezione dei dati personali, elaborando specifici modelli organizzativi.

RESPONSABILITA' DEL TITOLARE accountability (art. 24)

- Il **titolare del trattamento**, oltre a mettere in atto misure tecniche ed organizzative adeguate per garantire che il trattamento compiuto sia conforme al Regolamento, deve anche **dimostrare che tali misure siano effettive**.

- L'**inadempimento** è costituito dall'**incapacità** del titolare di dimostrare di **aver adottato idonee misure di sicurezza** per garantire un trattamento legittimo.

- **L'adesione ai codici di condotta** o ricorrendo al **rilascio di certificazioni** da parte di appositi organismi riconosciuti con provvedimenti dell'Autorità Garante, può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento.

ITALIA F.I.M.A.A.

PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE E PROTEZIONE PER IMPOSTAZIONE PREDEFINITA (privacy by design e by default - art. 25)

- Il **titolare prima di compiere una qualsiasi operazione di trattamento, deve verificare se le misure tecniche ed organizzative che intende attuare siano adeguate** avendo riguardo:

- al tipo di dati trattati, al contesto in cui avviene il trattamento e alla finalità dello stesso, alla probabilità e gravità di eventuali attentati ai diritti e libertà degli interessati.

- Ogni operazione che ha ad oggetto dati personali deve essere preceduta da **un'attenta progettazione delle singole fasi di trattamento** nelle quali il titolare predispone i presidi e le procedure per minimizzare i rischi di perdita, alterazione o accesso non autorizzato ai dati personali.

FASI DI PROGETTO

Il processo per ottenere l'adeguamento alle normative in tema di sicurezza delle informazioni e di trattamento dei dati personali può essere strutturato come segue :

- **ANALISI DEL CONTESTO AZIENDALE**
- **FINALITA' DEL TRATTAMENTO**
- **DEFINIZIONE DEL PERIMETRO DI SICUREZZA E AMBITO DI APPLICAZIONE**
- **DEFINIZIONE DEGLI ASSET E CENSIMENTO DEGLI ARCHIVI CON DATI PERSONALI**
- **ANALISI, VALUTAZIONE E GESTIONE DEL RISCHIO DATI**
- **ACQUISIZIONE DI PROCEDURE DOCUMENTATE, AZIONI, ATTIVITA' E CONTROMISURE**
- **DEFINIZIONE DELLO STATO DI RISCHIO: AZIONI E POSSIBILI CONTROMISURE**

REGISTRO DELLE ATTIVITA' DI TRATTAMENTO (art. 30)

Ogni **Titolare** di trattamento tiene **un Registro delle attività di trattamento**.

Il Registro deve contenere:

- il nome ed i dati di contatto del titolare del trattamento;
- le finalità del trattamento;
- una descrizione delle categorie di interessati e delle categorie di dati personali;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
- i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- una descrizione generale delle misure di sicurezza tecniche ed organizzative.

ITALIA F.I.M.A.A.

SEGUE: REGISTRO DELLE ATTIVITA' DI TRATTAMENTO (art. 30)

REGISTRO DEI TRATTAMENTI

EX ART. 30 REGOLAMENTO UE 2016/679

		Registro emesso in data:	Revisione:
A	**ANALISI DEL CONTESTO**		
A.01	Attività svolta:		
A.02	Forma sociale:		
A.03	Sede dell'attività:		
A.04	Struttura dei luoghi di svolgimento dell'attività:		
A.05	Numero dei titolari dell'attività:		
A.06	Numero dei dipendenti:		
A.07	Numero dei collaboratori:		
A.08	Raccolta e gestione dei dati:	□ elettronica □ cartacea	
A.09	Descrizione sistemi informatici presenti:		
A.10	Titolare del trattamento: (nominativo e dati di contatto)	_____ _____ _____	
A.11	Contitolare del trattamento: (se presente) (nominativo e dati di contatto)	_____ _____ _____	
A.12	Rappresentante del titolare del trattamento: (se presente) (nominativo e dati di contatto)	_____ _____ _____	
A.13	Responsabile della protezione dei dati: (se presente) (nominativo e dati di contatto)	_____ _____ _____	
A.14[1]	Il titolare ha aderito ad un codice di condotta (art. Reg.):	□ si: _____ □ no	
A.15[2]	Il titolare ha aderito ad un sistema di certificazione (art. 42 Reg.):	□ si: _____ □ no	
B	**FINALITA' DEL TRATTAMENTO DEI DATI**		
B.01	Finalità del trattamento dei dati personali degli interessati raccolti dal titolare:	□ anagrafica □ svolgimento attività principali e accessorie □ promozione servizi del titolare □ promozione servizi terzi □ rilevazione abitudini di consumo □ profilazione dei dati ex art. 4 n. 4 Reg. Eu 679/2016 □ rapporto di lavoro / collaborazione	

[1] Campo da compilare quando i codici di condotta saranno approvati
[2] Campo da compilare quando i sistemi di certificazione saranno approvati

1

ITALIA F.I.M.A.A.

SEGUE: REGISTRO DELLE ATTIVITA' DI TRATTAMENTO (art. 30)

- Anche il **Responsabile del trattamento**, laddove nominato, tiene un Registro di tutte le categorie di attività relative al trattamento svolte per conto del Titolare
- I **Registri** sono tenuti in forma scritta, o in formato elettronico, e sono messi, a richiesta, a disposizione dell'autorità di controllo
- **non si applica alle imprese o organizzazioni con meno di 250 dipendenti**, a meno che:
  - il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato
  - il trattamento non sia occasionale
  - o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10

SICUREZZA DEL TRATTAMENTO (art. 32)

- Considerando:
  - **lo stato dell'arte**
  - **dei costi di attuazione**
  - **della natura**
  - **dell'oggetto**
  - **del contesto**
  - **delle finalità del trattamento**
  - **del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche**
- Il titolare del trattamento e il responsabile del trattamento adottano le **misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio**

ITALIA F.I.M.A.A.

SEGUE: SICUREZZA DEL TRATTAMENTO

- Le misure tecniche e organizzative comprendono, tra le altre, se del caso:
  - la **pseudonimizzazione e la cifratura dei dati personali**
  - la capacità di **assicurare** su base permanente la **riservatezza, l'integrità, la disponibilità e la resilienza** dei sistemi e dei servizi di trattamento
  - la capacità di **ripristinare tempestivamente la disponibilità e l'accesso** dei dati personali in caso di incidente fisico o tecnico
  - una procedura per **testare, verificare e valutare regolarmente l'efficacia** delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento

ITALIA
F.I.M.A.A.

SEGUE: SICUREZZA DEL TRATTAMENTO

- Nel **valutare l'adeguato livello di sicurezza**, si tiene conto in special modo dei **rischi presentati dal trattamento** che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati
- L'adesione a un **codice di condotta** approvato o a un meccanismo di **certificazione** approvato può essere utilizzata come elemento per dimostrare la conformità ai requisiti
- Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali **non tratti tali dati se non è istruito** in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri

NOTIFICA DI UNA VIOLAZIONE DEI DATI PERSONALI ALL'AUTORITA' DI CONTROLLO (Data breaches art. 33)

- In caso di **violazione dei dati personali**: il titolare, senza ritardo, **deve darne comunicazione all'Autorità Garante** a meno che non sia in grado di dimostrare che la violazione non costituisca un rischio per i diritti e le libertà delle persone fisiche.

- La **notifica dovrà avvenire entro 72 ore** e comunque senza ingiustificato ritardo.

COMUNICAZIONE DI UNA VIOLAZIONE DEI DATI ALL' INTERESSATO (art. 34)

- Quando la **violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento deve comunicare la violazione all'interessato** senza ingiustificato ritardo

- **Non è richiesta la comunicazione** all'interessato quando:
- il **titolare del trattamento ha messo in atto le misure tecniche ed organizzative adeguate di protezione** e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura.

- il **titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio** elevato per i diritti e le libertà degli interessati.

- La comunicazione richiederebbe **sforzi spropositati**. In tal caso si procede invece ad una comunicazione pubblica.

VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI (art. 35)

- **Quando un trattamento può comportare un rischio elevato per i diritti e le libertà delle persone interessate** (a causa del monitoraggio sistematico dei loro comportamenti, o per il gran numero dei soggetti interessati di cui sono trattati dati sensibili, o anche per una combinazione di questi e altri fattori)
- In particolare quando si utilizzano **nuove tecnologie**
- Obbligo a carico dei titolari di svolgere una **valutazione di impatto in via preliminare**
- I titolari devono:
  - garantire l'osservanza delle disposizioni del Regolamento
  - dimostrare adeguatamente in che modo garantiscono tale osservanza

CODICI DI CONDOTTA
(art. 40)

Possono essere **redatti dalle associazioni** e **dalle organizzazioni** che rappresentano categorie di titolari del trattamento o di responsabili del trattamento e devono tenere conto delle caratteristiche specifiche dei settori di riferimento e delle diverse esigenze connesse alle dimensioni aziendali.

- Il **progetto di codice** dovrà essere **sottoposto all'Autorità Garante nazionale** e se il parere è positivo e l'applicazione del Codice riguarda solamente lo Stato membro in cui è presentato, **l'Autorità registrerà e pubblicherà il Codice realizzato.**
- Quando invece il progetto di codice di condotta si riferisca a trattamenti realizzati in vari Stati membri, prima che vi sia approvazione definitiva, occorre un secondo esame a livello europeo, con il coinvolgimento del Comitato europeo per la protezione dei dati. Se il progetto ottiene un parere favorevole, sarà registrato e pubblicato.

ITALIA
F.I.M.A.A.

CERTIFICAZIONE (art. 42)

- Istituzione di **meccanismi di certificazione** della protezione dei **dati** / **sigilli** / **marchi di protezione** dei dati allo scopo di dimostrare la conformità al regolamento dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento. Sono tenute in considerazione le esigenze specifiche delle micro, piccole e medie imprese
- La **certificazione è volontaria e accessibile** tramite una procedura trasparente
- La **certificazione non riduce la responsabilità** del titolare del trattamento o del responsabile del trattamento riguardo alla conformità al presente regolamento e lascia impregiudicati i compiti e i poteri delle autorità di controllo competenti
- Rilasciata dagli organismi di certificazione di cui all'articolo 43 o dall'autorità di controllo competente
- Rilasciata per un **periodo massimo di tre anni,** può essere rinnovata

ITALIA
F.I.M.A.A.

TRASFERIMENTO DEI DATI (art. 44)

- **Qualunque trasferimento di dati personali** oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento verso un paese terzo o un'organizzazione internazionale ha luogo soltanto se il titolare del trattamento e il responsabile del trattamento **rispettano le condizioni del Regolamento**
- Assicurare che il livello di protezione delle persone fisiche garantito dal Regolamento non sia pregiudicato

DIRITTO DI PROPORRE RECLAMO ALL'AUTORITA' DI CONTROLLO (art. 77)

L'interessato che ritenga che il trattamento che lo riguarda violi il Regolamento ha il **diritto di proporre reclamo ad un'autorità di controllo**, nello Stato membro in cui risiede abitualmente, lavora oppure del luogo ove si è verificata la presunta violazione.

L'autorità di controllo informa il reclamante dello stato o dell'esito del reclamo, compresa la possibilità di un ricorso giurisdizionale.

GARANTE DELLA PRIVACY NAZIONALE (art. 4 n. 21 e artt. 51 e ss.)

- **Autorità pubblica indipendente**
- Principali compiti da svolgere nel proprio territorio nazionale:
  - Sorveglia e assicura l'applicazione del Regolamento
  - Promuove la consapevolezza e favorisce la comprensione del pubblico rispetto ai rischi, alle norme, alle garanzie e ai diritti in relazione al trattamento
  - Consulenza al Parlamento, al Governo e ad altre istituzioni nazionali
  - Fornisce all'interessato informazioni in merito ai propri diritti
  - Tratta i reclami proposti dagli interessati
  - Svolge indagini sull'applicazione del regolamento
  - Rilascia le certificazioni
  - Approva i codici di condotta
  - Infligge le sanzioni amministrative

DIRITTO AL RISARCIMENTO E RESPONSABILITA' (art. 82)

L' articolo 82 prevede:

- il **diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento** per chiunque subisca un danno materiale o immateriale causato da una violazione del Regolamento.

- **Le azioni legali** per l'esercizio del diritto di ottenere il risarcimento del danno **sono promosse dinanzi alle autorità giurisdizionali competenti** a norma del diritto dello Stato membro in cui il titolare del trattamento o il responsabile del trattamento ha uno stabilimento.

SANZIONI AMMINISTRATIVE PECUNIARIE (art. 83)

Gli Stati membri prevedono **sanzioni amministrative fino a dieci milioni di euro o il 2% del fatturato mondiale annuo** conseguito nell'esercizio precedente

Le sanzioni devono essere determinate considerando gli elementi previsti dal regolamento, tra i quali:

- la **natura**, la **gravità** e la **durata della violazione** tenendo in considerazione la **natura, l'oggetto o la finalità del trattamento in questione,** nonché il numero di interessati lesi dal danno e il livello del danno da essi subito;
- il **carattere doloso** o **colposo** della violazione;
- le **misure adottate** dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati;
- il **grado di responsabilità** del titolare del trattamento o del responsabile del trattamento;
- **eventuali precedenti violazioni** pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento.

ITALIA F.I.M.A.A.

SEGUE: SANZIONI AMMINISTRATIVE PECUNIARIE

Gli importi delle sanzioni raddoppiano (**venti milioni o il 4% del fatturato mondiale**)nei casi di:

- **violazione delle condizioni** per il rilascio del **consenso** informato;
- **riguardino il trattamento di dati giudiziari o sensibili**;
- mancato riscontro al legittimo esercizio dei diritti dell'interessato;
- **trasferimento dei dati verso Paesi** che non garantiscono livelli adeguati di tutela;
- **violazione di un ordine dell'Autorità Garante**

SANZIONI PENALI
(art. 84)

- **Stabilite dai singoli Stati membri**
- Le sanzioni devono essere: **effettive** / **proporzionate** / **dissuasive**
- Le eventuali sanzioni devono essere notificate dallo Stato membro alla Commissione entro il 25 maggio 2018 e devono essere comunicate le modifiche