CONSENSO AL TRATTAMENTO DEI DATI PERSONALI SECONDO IL REGOLAMENTO (UE) 2016/679 (GENERAL DATA PROTECTION REGULATION)

Spettabile Cliente,

1. Si premette che la società C.R.M. Informatica s.r.l., sita in Via Achille Papa 18, 36071 Arzignano (VI), P.I. 04123950240 svolge, quali attività sociali, anche da remoto:
   - *help desk*, ovvero un servizio professionale aziendale volto a fornire assistenza e supporto tecnico e informatico all'utente;
   - assistenza tecnica informatica "in loco", ovvero presso la residenza/domicilio del cliente o presso la sede dell'azienda che la richiede;
   - assistenza tecnica informatica nella propria sede sociale;
   - il controllo di software aziendali e dell'attività dei servizi di sistema.

2. In aggiunta alle predette attività, la società offre – a richiesta del cliente – anche un pacchetto di servizi di *monitoring* (c.d. CRMM) consistenti, nello specifico, nel:
   - monitoraggio della CPU e della RAM;
   - controllo di software aziendali e dell'attività dei servizi di sistema;
   - monitoraggio dei dischi rigidi;
   - monitoraggio dell'antivirus;
   - monitoraggio del backup;
   - attività di reportistica mensile o trimestrale riguardante le strutture informatiche aziendali.

3. La CRM Informatica s.r.l. ha altresì ideato, sviluppato e brevettato – a beneficio dell'utenza interessata – un proprio software ERP, **WinflyONE**, funzionale alla gestione dei diversi processi aziendali. Tale programma informatico, in grado di adattarsi a diversi settori produttivi, offre quindi alle aziende un supporto operativo, direzionale e strategico. Per i clienti che fruiscono di tale software la società effettua, da remoto, due tipologie di assistenza:

   - quella con preventiva comunicazione all'operatore interessato, il quale accetta l'intervento del tecnico informatico incaricato;
   - quella senza preavviso esplicito, comunque strettamente correlata alle necessità operative, tecniche, logistiche del beneficiario.

   A prescindere dal tipo di supporto prestato, la società garantisce che le eventuali operazioni sui dati del cliente sono comunque strettamente proporzionali[1] e imprescindibilmente legate alla stessa attività di assistenza.

[1] Sul concetto di proporzionalità nell'ordinamento europeo si rimanda, in particolare, alle seguenti pronunce: CGUE, 22.12.2008, in C-336/07, *Kabel Deutschland*; CGUE., 5.3.2009, in C-88/07, Commissione c. Regno di Spagna; CGUE, 28.4.2009, in C-518/06, Commissione c. Repubblica italiana; CGUE., 17.9.2009, in C-182/08, *Glaxo Wellcome*; 12.1.2010, in C-229/08.

4. In virtù dei predetti servizi offerti, la CRM Informatica s.r.l. si trova invero a contatto con un numero consistente e rilevante di dati personali relativi ai fruitori di tali servizi. Con dato personale si deve quindi intendere qualsiasi informazione riguardante una persona fisica identificata o identificabile (ovvero, l'interessato)[2].

5. La società assicura dunque i propri clienti sul fatto che le eventuali operazioni "sensibili" sono sempre realizzate nell'interesse e a beneficio dei clienti, in modo coerente e connesso alla natura e alla tipologia delle prestazioni offerte. Ciò a presidio della stessa funzionalità ed efficienza degli stessi servizi effettuati.

6. Proprio in relazione alla disponibilità di informazioni personali dei clienti, la società intende acquisire il consenso degli interessati, garantendo che questo sia espresso in maniera libera, specifica, informata e inequivocabile[3]. In tal modo, la CRM Informatica s.r.l. vuole conformarsi pienamente a quanto previsto dalla più recente normativa europea sulla privacy e trattamento dei dati (Regolamento 679/2016, c.d. GDPR), attualmente vigente.

7. Volendo quindi perseguire tale finalità informa che è stato individuato, all'interno dell'azienda, quale responsabile del trattamento dei dati personali, Maurizio Colombara, nato a Valdagno, il 19/01/1961, CF: CLMMRZ61A19L551R. Egli, infatti, dotato di competenza professionale specifica in materia ed in ambito informatico, opera concretamente e direttamente sul complesso dei dati personali a disposizione della società.

8. Inoltre, la C.R.M. Informatica s.r.l. nomina altresì quale responsabile della protezione dati (c.d. *data protection officer*[4]), il Dott. Andrea Colombara, nato ad Arzignano, il 10/04/1992, CF. CLMNDR92D10A459I, quale figura professionale con particolari competenze in campo informatico, di valutazione del rischio e di analisi dei processi. Il suo compito è quello di assicurare una gestione corretta dei dati personali degli interessati e di porsi come referente principale dell'azienda in tale ambito[5].

9. La stessa società assicura inoltre che le informazioni dei clienti di cui dispone saranno conservati con modalità e per un arco di tempo limitato a quanto strettamente necessario rispetto alla/e finalità del trattamento, ed in maniera assolutamente riservata.

10. La invitiamo quindi - onde garantire la massima trasparenza possibile - a prendere visione della disciplina normativa sotto riportata (pagina 3 e ss.) cui la CRM Informatica s.r.l. si atterrà in materia di *privacy*, al fine di tutelare i Suoi diritti sotto ogni aspetto. Si chiede, infine, di apporre la propria firma (leggibile) volta all'acquisizione di un consenso informato quanto al trattamento dei dati resi accessibili.

[2] Definizione tratta dall'art. 4 comma 1, n. 1 del Regolamento 679/2016.
[3] Requisiti del consenso richiesti dall'art. 4, comma 1, n. 11 del Regolamento 679/2016.
[4] Previsto dall'art. 38 del Regolamento 679/2016.
[5] Per una più approfondita disamina dei compiti del responsabile dei dati personali vedasi l'art. 39 del Regolamento 679/2016.

Principi generali del trattamento di dati personali

Ogni trattamento di dati personali deve avvenire nel rispetto dei principi fissati all'articolo 5 del Regolamento (UE) 2016/679, ovvero:

- liceità, correttezza e trasparenza del trattamento, nei confronti dell'interessato;
- limitazione della finalità del trattamento, compreso l'obbligo di assicurare che eventuali trattamenti successivi non siano incompatibili con le finalità della raccolta dei dati;
- minimizzazione dei dati: ossia, i dati devono essere adeguati pertinenti e limitati a quanto necessario rispetto alle finalità del trattamento;
- esattezza e aggiornamento dei dati, compresa la tempestiva cancellazione dei dati che risultino inesatti rispetto alle finalità del trattamento;
- limitazione della conservazione: ossia, è necessario provvedere alla conservazione dei dati per un tempo non superiore a quello necessario rispetto agli scopi per i quali è stato effettuato il trattamento;
- integrità e riservatezza: occorre garantire la sicurezza adeguata dei dati personali oggetto del trattamento.

Il Regolamento (articolo 5, paragrafo 2) richiede al titolare di rispettare tutti questi principi e di essere "in grado di comprovarlo". Questo è il principio detto di "responsabilizzazione" (c.d. *accountability*) che viene poi esplicitato ulteriormente dall'articolo 24, paragrafo 1, dove si afferma che "il titolare mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al GDPR".

Assicurare la liceità del trattamento di dati personali

Il GDPR, come già previsto dal Codice in materia di protezione dei dati personali, prevede che ogni trattamento deve trovare fondamento in un'idonea base giuridica. I fondamenti di liceità del trattamento di dati personali sono indicati all'articolo 6 e consistono nel:

- consenso, adempimento obblighi contrattuali, interessi vitali della persona interessata o di terzi, obblighi di legge cui è soggetto il titolare, interesse pubblico o esercizio di pubblici poteri, interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati.

Consenso

Quando il trattamento si fonda sul consenso dell'interessato, il titolare deve sempre essere in grado di dimostrare (articolo 7.1 GDPR) che l'interessato ha prestato il proprio consenso, che è valido se:

- all'interessato è stata resa l'informazione sul trattamento dei dati personali (articoli 13 o 14 del Regolamento);
- è stato espresso dall'interessato liberamente, in modo inequivocabile e, se il trattamento persegue più finalità, specificamente con riguardo a ciascuna di esse. Il consenso deve essere sempre revocabile.

Occorre verificare che la richiesta di consenso sia chiaramente distinguibile da altre richieste o dichiarazioni rivolte all'interessato (articolo 7.2), per esempio all'interno della modulistica.

Non è ammesso il consenso tacito o presunto (per esempio, presentando caselle già spuntate su un modulo).

Quando il trattamento riguarda le "categorie particolari di dati personali" (articolo 9 Regolamento) il consenso deve essere "esplicito"; lo stesso vale per il consenso a decisioni basate su trattamenti automatizzati (compresa la profilazione – articolo 22).

Trasparenza del trattamento: l'informativa agli interessati

Fatte salve alcune eccezioni, chi intende effettuare un trattamento di dati personali deve fornire all'interessato alcune informazioni anche per metterlo nelle condizioni di esercitare i propri diritti (articoli 15-22 GDPR).

QUANDO

L'informativa (disciplinata nello specifico dagli artt. 13 e 14 del Regolamento) deve essere fornita all'interessato prima di effettuare il trattamento, quindi prima della raccolta dei dati (se raccolti direttamente presso l'interessato: articolo 13).

Nel caso di dati personali non raccolti direttamente presso l'interessato (articolo 14), l'informativa deve essere fornita entro un termine ragionevole che non può superare 1 mese dalla raccolta, oppure al momento della comunicazione (non della registrazione) dei dati (a terzi o all'interessato)

COSA

I contenuti dell'informativa sono elencati in modo tassativo negli articoli 13, paragrafo 1, e 14, paragrafo 1 GDPR. In particolare, il titolare deve sempre specificare i dati di contatto del RPD-DPO (**Responsabile della protezione dei dati - *Data Protection Officer***), ove esistente, la base giuridica del trattamento, qual è il suo interesse legittimo se quest'ultimo costituisce la base giuridica del trattamento, nonché se trasferisce i dati personali in Paesi terzi e, in caso affermativo, attraverso quali strumenti (esempio: si tratta di un Paese terzo giudicato adeguato dalla Commissione europea; si utilizzano BCR di gruppo; sono state inserite specifiche clausole contrattuali modello, ecc.).

In tutti i casi, il titolare deve specificare la propria identità e quella dell'eventuale rappresentante nel territorio italiano, le finalità del trattamento, i diritti degli interessati (compreso il diritto alla portabilità dei dati), se esiste un responsabile del trattamento e la sua identità, e quali sono i destinatari dei dati.

Il GDPR prevede anche ulteriori informazioni in quanto "necessarie per garantire un trattamento corretto e trasparente": in particolare, il titolare deve specificare il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione, e il diritto di presentare un reclamo all'autorità di controllo.

Se il trattamento comporta processi decisionali automatizzati (anche la profilazione), l'informativa deve specificarlo e deve indicare anche la logica di tali processi decisionali e le conseguenze previste per l'interessato.

COME

L'informativa è data, in linea di principio, per iscritto e preferibilmente in formato elettronico (soprattutto nel contesto di servizi online: articolo 12, paragrafo 1, e considerando 58). Sono comunque ammessi "altri mezzi", quindi può essere fornita anche in forma orale, ma nel rispetto delle caratteristiche di cui sopra (articolo 12, paragrafo 1).

Il GDPR ammette l'utilizzo di icone per presentare i contenuti dell'informativa in forma sintetica, ma solo "in combinazione" con l'informativa estesa (articolo 12, paragrafo 7); queste icone in futuro dovranno essere uniformate in tutta l'UE attraverso l'intervento dalla Commissione europea.

In base al GDPR, si deve porre particolare attenzione alla formulazione dell'**informativa**, che deve essere soprattutto **comprensibile e trasparente per l'interessato**, attraverso l'uso di un **linguaggio chiaro e semplice**. In particolare, bisogna ricordare che per i minori si devono prevedere informative idonee.

Principio di "responsabilizzazione" dei responsabili del trattamento: principali elementi

Il GDPR prevede obblighi specifici in capo ai responsabili del trattamento. Secondo l'art. 28 del Regolamento 679/2016: **"**i responsabili del trattamento presentano garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate in modo che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato".

Il GDPR (articolo 28) prevede dettagliatamente gli specifici compiti attribuiti al responsabile del trattamento. I trattamenti, da parte di tale responsabile, sono disciplinati da un contratto o da un altro atto giuridico a norma del diritto dell'Unione o degli altri Stati membri. Questo atto deve disciplinare tassativamente almeno le materie riportate al paragrafo 3 dell'articolo 28 al fine di dimostrare che il responsabile fornisce "garanzie sufficienti", quali, in particolare:

- la natura, durata e finalità del trattamento o dei trattamenti assegnati
- le categorie di dati oggetto di trattamento
- le categorie degli interessati

Una novità del GDPR è la possibilità di designare sub-responsabili del trattamento da parte di un responsabile (articolo 28, paragrafo 4), per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano titolare e responsabile primario; quest'ultimo risponde dinanzi al titolare dell'inadempimento dell'eventuale sub-responsabile, anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso "non gli è in alcun modo imputabile" (articolo 82, paragrafo 1 e paragrafo 3).

Registro dei trattamenti

Tutti i responsabili di trattamento, **eccettuati gli organismi con meno di 250 dipendenti** - ma solo se non effettuano trattamenti a rischio (articolo 30, paragrafo 5) - devono tenere un registro delle operazioni di trattamento, i cui contenuti sono indicati all'articolo 30. Si tratta di uno strumento fondamentale allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda o di un soggetto pubblico, indispensabile per ogni valutazione e analisi del rischio. Il registro deve avere **forma scritta**, anche elettronica, e deve essere esibito su richiesta al Garante.

Misure di sicurezza

Il responsabile del trattamento è obbligato ad adottare misure tecniche e organizzative **idonee a garantire un livello di sicurezza adeguato al rischio del trattamento**. L'obiettivo è invero evitare la distruzione accidentale o illecita, la perdita, modifica, rivelazione, o l'accesso non autorizzato.

Fra tali misure, il GDPR menziona, in particolare, la pseudonimizzazione e la cifratura dei dati; misure per garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; misure atte a garantire il tempestivo ripristino della disponibilità dei dati; procedure per verificare e valutare regolarmente l'efficacia delle misure di sicurezza adottate.

La lista di cui al paragrafo 1 dell'articolo 32 GDPR è una lista aperta e non esaustiva ("tra le altre, se del caso").

Per questi motivi, **non possono sussistere dopo il 25 maggio 2018 obblighi generalizzati di adozione di misure "minime" di sicurezza poiché tale valutazione è rimessa**, caso per caso, **al responsabile in rapporto ai rischi specificamente individuati** come da articolo 32 del Regolamento.

Vi è, inoltre, la possibilità di utilizzare l'adesione a specifici codici di condotta o a schemi di certificazione per attestare l'adeguatezza delle misure di sicurezza adottate (articolo 32, paragrafo 3).

Responsabile della protezione dei dati

La designazione di un responsabile della protezione dati (RPD-DPO) è finalizzata a facilitare l'attuazione della normativa da parte del responsabile (articolo 39). Non è un caso, infatti, che fra i compiti del RPD rientrino "la sensibilizzazione e la formazione del personale" e la sorveglianza sullo svolgimento della valutazione di impatto di cui all'articolo 35, oltre alla funzione di punto di contatto per gli interessati e per il Garante rispetto a ogni questione attinente l'applicazione del Regolamento.

La sua designazione è obbligatoria in alcuni casi (articolo 37 del Regolamento 679/2016) In particolare, per quanto di interesse, il responsabile della protezione dei dati deve essere nominato quando (lettera b) del summenzionato articolo): "**le attività principali 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**".

I diritti degli interessati

I titolari del trattamento devono rispettare le modalità previste per l'esercizio di tutti i diritti da parte degli interessati, stabilite, in via generale, negli artt. 11 e 12 del Regolamento. Più nel dettaglio, tali diritti sono meglio specificati negli artt. da 15 a 20 del GDPR e consistono, in sintesi, nel:

- diritto di accesso dell'interessato;

- diritto alla cancellazione (diritto all'oblio);

- diritto di limitazione di trattamento;

- obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento;

- diritto alla portabilità dei dati.

In fede,

Arzignano, il _____

Il sottoscritto_____