




29 MARZO 2018

**DPIA DATA PROTECTION IMPACT ASSESSMENT**  
REGOLAMENTO UE 2016/679 – CD. "GDPR"

LORIS MODENA  
ARTE E INFORMATICA DI LORIS MODENA E C. SAS  
Via Santa Croce sull'Arno, 9 00148 Roma (RM)



## Sommario

Necessità di una DPIA e di un DPO .....	2
Tipologia dei dati raccolti .....	2
Base giuridica del trattamento .....	2
Flusso di dati/acquisizione .....	3
Flusso di dati / trattamento.....	3
Dati relativi alla navigazione.....	3
Consensi richiesti.....	3
Consensi moduli di contatto.....	4
Consenso di accesso remoto .....	4
Potenziale impatto sulla Privacy.....	4
Misure di mitigazione del rischio.....	4
Responsabile della protezione dei Dati (RPD / DPO) .....	6
Modifiche delle disposizioni .....	6
Conclusioni .....	6

## Necessità di una DPIA e di un DPO

I servizi erogati e i software forniti da Arte e Informatica non sono indirizzati alle persone fisiche e sono rivolti esclusivamente a finalità professionali e alle imprese. Di conseguenza i dati trattati in prevalenza non riguardano le persone fisiche se non in casi eccezionali e sporadici. Anche nel caso di gestione occasionale di dati personali essi non rientrano nelle tipologie sensibili che obbligano l'azienda a dotarsi una DPIA (Data Protection Impact Assessment) come riportato dalle linee guida del gruppo Art 29. Esaminando il regolamento GDPR si è ritenuto che non vi è necessità avvalersi di un DPO (Data protection officer), si è deciso comunque di nominare un RPD e comunicarlo al garante.

Il Titolare del Trattamento ha comunque deciso di dotarsi di una DPIA per garantire la corretta gestione dei dati forniti dai propri clienti e i dati di proprietà dei clienti stessi, residenti sui server e sistemi di backup gestiti direttamente da Arte e Informatica.

## Tipologia dei dati raccolti

Arte e Informatica non rivolgendosi alle persone fisiche non registra nessun dato personale che non sia inerente all'attività professionale del cliente. I dati da noi raccolti sono i seguenti:

- Nome e cognome del titolare e/o responsabili dell'impresa o attività professionale.
- Recapiti postali, email e telefoni inerenti alle imprese e attività professionali.
- Accessi e login ai sistemi informatici forniti del cliente.
- Backup forniti dal cliente o effettuati per conto dello stesso.

## Base giuridica del trattamento

Il trattamento di questi dati è necessario per adempire al mandato implicito contenuto nelle richieste di informazioni e erogazione dei servizi. I dati raccolti sono dati aziendali nella maggioranza reperibili pubblicamente in quanto riportati dagli stessi clienti sui propri Siti Web e nella propria comunicazione aziendale e/o tramite semplice visura camerale. Il rischio inerente alla privacy per questa tipologia di dati è nullo.

Differente il caso dei backup e accessi e login ai sistemi informatici del cliente, se questi dati sono reperiti in modo occasionale al fine di fornire assistenza o erogare un servizio saranno distrutti in modalità sicura immediatamente dopo lo svolgimento della mansione richiesta, invitando il cliente a revocare gli accessi e i login assegnati ad Arte e Informatica. Nel caso che accessi, login e backup sono legati all'erogazione di un servizio quale un contratto di assistenza sistemistica, la fornitura di housing e hosting per i Siti Web, le stesse modalità di trattamento saranno oggetto di un contratto specifico in quanto le misure di sicurezza e le modalità cambiano a seconda della tipologia del servizio stesso. Il rischio inerente alla privacy è legato alla natura stessa dei dati e accessi forniti dal cliente che sarà informato dei rischi annessi e immediatamente se viene rilevato un accesso non autorizzato o di un eventuale perdita degli stessi. Qualsiasi sia la natura dei dati e accessi forniti saranno prese le misure di sicurezza quali la crittografia e la protezione tramite password, riservando per gli stessi la massima riservatezza.

## Flusso di dati/acquisizione

I dati sono raccolti tramite i moduli presenti sui siti web di Arte e Informatica dedicati ai servizi erogati o attraverso le informazioni rilasciate telefonicamente o di persona dai nostri clienti. Alcuni clienti si rivolgono a noi tramite email o tramite servizi di chat quali Zendesk, WhatsApp o assistenza integrata nei Marketplace tramite i quali Arte e Informatica vende i propri software e servizi. La tipologia dei dati, come già menzionato, non riguarda persone fisiche, se non nel caso occasionale che gli stessi non siano inerenti con l'attività professionale. I dati inerenti alle persone fisiche anche e trattati in modo occasionale saranno utilizzati solo ai fini dell'erogazione delle mansioni richieste.

## Flusso di dati / trattamento

I dati presenti nei nostri database non riguardano persone fisiche, né minori. Sono archiviati sui sistemi informatici nella sede di Arte e Informatica o nei Server Web e NAS ubicati nel territorio europeo in prevalenza in Germania e Francia. Nel caso di spedizione di prodotti e/o documenti tramite corriere o posta alcuni dati quali (ragione sociale, nome e cognome, indirizzo e recapito telefonico) possono essere condivisi temporaneamente con il corriere incaricato della consegna.

## Dati relativi alla navigazione

I cookie installati sui nostri siti aziendali sono principalmente di tipologia tecnica e sono cancellati al termine della sessione. Quelli rimanenti servono solo a identificare l'utente, ogni nostro sito è dotato di una specifica informativa riguardo ai cookies utilizzati sullo stesso. I siti aziendali di Arte e Informatica registrano inoltre i log di accesso al server e ai suoi servizi, questi log registrano alcune informazioni che riguardano i dispositivi quali: IP pubblico, versione del browser e sistema operativo. Necessari sia per identificare errori lato server o di comunicazione, nonché tentativi di intrusione e accesso non autorizzato al server o alle applicazioni web su esso ospitate, anche ai fini della tutela dell'utente stesso. Arte e Informatica si avvale di sistemi di statistica atti a valutare l'impatto dei propri siti (numero di pagine scaricate, siti di provenienza, zone geografiche, lingue dei browser, ecc. ...) ogni sito riporta nella Privacy Policy la tipologia e finalità dei sistemi di rilevamento adottati, che variano a seconda delle tipologie e finalità dei siti stessi.

## Consensi richiesti

Nel caso di registrazione alla newsletter è richiesta in forma esplicita il consenso e l'accettazione dell'informativa sulla privacy, inoltre è richiesta una conferma tramite email per la quale è stata richiesta l'iscrizione alla newsletter stessa. Nel caso di ordine/acquisto di prodotti e servizi sono richiesti esclusivamente i dati necessari alla fornitura del bene acquistato e/o servizio unitamente ai dati necessari alla fatturazione, nella fase di ordine è richiesta oltre all'accettazione dei termini e condizioni d'uso anche dell'informativa della privacy al fine della ricezione di informazioni commerciali. Questo anche se non è obbligatorio in quanto i prodotti e servizi forniti da Arte e Informatica non sono destinati a persone fisiche, ma il Titolare del Trattamento ha deciso di estendere la richiesta di consenso anche alle società e liberi professionisti.

## Consensi moduli di contatto

I moduli di richiesta informazioni sui prodotti e servizi, sono finalizzati alla soddisfazione di richieste degli utenti, non prevedono dunque per il GDPR nessuna tipologia di consenso. La richiesta di consenso non solo non è obbligatoria, ma creerebbe confusione e difficoltà al cliente stesso, di conseguenza la richiesta diretta tramite WhatsApp, Zendesk Chat e similari sono esclusi da tale richiesta.

## Consenso di accesso remoto

Durante le assistenze fornite ai clienti si rende spesso necessario un accesso remoto ai loro sistemi, per il quale si richiede sempre il consenso all'utente e avviene tramite software (Arte e Informatica utilizza nello specifico TeamViewer) che rispettano tutte le disposizioni.

Nel caso di contratti di assistenza sistemistica su server, client e apparati di rete di proprietà del cliente, le modalità e finalità degli accessi sono regolamentati dai singoli contratti in essere.

## Potenziale impatto sulla Privacy

Non gestendo dati relativi alle persone fisiche la loro alterazione o cancellazione non sortirebbe nessun danno alle persone interessate. Anche nel caso che i dati presenti nel nostro database fossero copiati da terzi e/o resi pubblici, non ne deriverebbe un danno in quanto per la maggioranza sono dati già disponibili con semplici visure camerali o riportati sulla documentazione aziendale dei clienti.

Un eventuale furto o copia di backup e dati di accesso potrebbe configurare un rischio per la sicurezza del cliente per questo applichiamo agli stessi un livello di protezione che adottiamo anche per proteggere i sorgenti e i documenti riservati di Arte e Informatica. Nello specifico i backup e i database contenenti gli accessi ai sistemi informatici sono crittografati (AES, Rijndael) con una password robusta cambiata ogni sei mesi, l'accesso agli stessi è effettuato esclusivamente da personale altamente qualificato.

Un eventuale perdita/furto degli stessi archivi non presenta dunque un rischio elevato e nel caso avvenga, il cliente sarà subito avvisato in modo da consentire allo stesso di cambiare per esempio gli accessi e le password di accesso ai propri sistemi.

## Misure di mitigazione del rischio

Arte e Informatica pone la massima priorità alla protezione dei dati implementando più livelli di sicurezza per la protezione dei dati e aggiornando i sistemi e le procedure per ridurre al minimo il rischio di furto di dati e/o la perdita degli stessi. Le procedure e i sistemi adottati sono rafforzati dalla necessità da parte di Arte e Informatica di proteggere i sorgenti dei propri software e la propria proprietà intellettuale oltre alla necessità di garantire ai propri clienti una gestione attenta dei dati di loro proprietà ubicati sui nostri sistemi informatici.

- **Durata del trattamento:** ogni tre anni vengono cancellati dalle newsletter i nominativi che non hanno più contattato Arte e Informatica e/o non hanno acquistato software e servizi. La cancellazione riguarda i database e le liste dell'invio delle informative commerciali anche relativi alle aziende, ad eccezioni dei dati necessari ai fini fiscali. La cancellazione da questi archivi avviene anche in caso di richiesta da parte degli interessati.

- **Formazione del personale:** attualmente nessun dipendente ha accesso ai dati, se in futuro sarà necessario i dipendenti saranno formati nella gestione dei dati stessi.
- **Password e crittografia:** tutti i database presenti nel nostro ufficio sono protetti da password, i dischi fissi delle postazioni e dei server sono a loro volta protetti da crittografia. I backup remoti sia verso il cloud che verso memorie di massa esterne sono crittografati in modo da prevenire i rischi dovuti a smarrimenti o furti.
- **Protezione della connessione:** tutti i Siti Web aziendali sono protetti da certificato SSL e viene usata una VPN professionale al fine di mitigare al massimo il rischio derivante dall'intercettazione del traffico soprattutto quando si opera in chiaro tramite i protocolli HTTP e FTP.
- **Accessi dall'esterno, backup remoti e cloud:** ove possibile utilizziamo l'autenticazione a due fattori (2FA), utilizzando tecnologie Secure Sockets Layer (SSL)/Transport Layer Security (TLS) e prediligiamo i servizi che offrono crittografia AES (Advanced Encryption Standard) a 256 bit. Inoltre, applichiamo numerose misure di sicurezza fisiche e logiche per proteggere le informazioni degli utenti dagli accessi non autorizzati. Tutti i server accessibili da remoto sono dotati di firewall e protezione AntiDDoS e registrano gli accessi tramite log di sistema al fine di rilevare eventuali accessi non autorizzati e/o errori del software.
- **Software:** Arte e Informatica utilizza solo software professionale e corredato da licenza d'uso originale e/o programmi open source, effettuando aggiornamenti periodici e seguendo ogni avviso di sicurezza che riguardi le soluzioni adottate sia in ambito server che client. Questo per ridurre al minimo i rischi relativi alla sicurezza informatica: l'uso di programmi piratati ad avviso del Titolare del Trattamento sono considerati un rischio non accettabile, a tal fine promuoviamo anche verso i nostri clienti l'adozione di software e sistemi operativi originali.
- **Protezione antivirus, malware, exploit e ransomware:** Arte e Informatica adotta sistemi antivirus e di protezione evoluti e professionali.
- **Documenti cartacei:** Arte e Informatica riduce al minimo la documentazione cartacea limitandola a quanto previsto ai fini fiscali. é fatto divieto al personale e collaboratori di riciclare la carta, onde evitare che per una svista vengano diffusi dati sensibili o che possano costituire un rischio per la sicurezza informatica sia interna che quella riguardante i clienti. Ogni documento cartaceo anche momentaneo è distrutto prima di essere conferito al riciclo: onde evitare il rischio che sia possibile reperire password o informazioni scritte momentaneamente a mano durante un'assistenza remota o telefonica.
- **HDD e memorie di massa dismessi:** ogni supporto di massa dismesso è archiviato nella sede di Arte e Informatica. Se avviato allo smaltimento il supporto è cancellato in modo sicuro e definitivo attraverso l'uso di appositi software.

## Responsabile della protezione dei Dati (RPD / DPO)

Il responsabile della protezione dati **Per. Ind. Loris Modena** titolare di Arte e Informatica e c. sas - Via Santa Croce sull'Arno 9 - 00148 Roma (RM) P.IVA e CF: 13213161006 - REA: RM – 1430113. Eventuali comunicazioni riguardanti il GDPR possono essere inoltrate a [admin@arteinformatica.eu](mailto:admin@arteinformatica.eu).

## Modifiche delle disposizioni

Il presente documento può essere aggiornato a seguito della necessità di adottare nuove misure e procedure, a seguito di comunicazioni da parte del Garante della Privacy e/o a seguito di elementi che emergono durante il trattamento dei dati.

## Conclusioni

La valutazione del rischio relativo alla protezione dei dati in linea generale quella adottata come base generale e minima a tutti i contratti in essere che possono integrare disposizioni aggiuntive necessarie ai casi specifici. Il documento è messo a conoscenza a tutti i collaboratori e partner che operano con Arte e Informatica al fine che adottino le condizioni minime da noi rilevate, necessarie alla protezione e trattamento dei dati.