Allegato 2 - Misure tecniche e organizzative adottate dal Responsabile del trattamento

1. Controllo dell'accesso

Le sedi dell'Officina sono suddivise in zone con livelli di sicurezza diversi, in cui i locali ove vengono custoditi computer e server rientrano nella classificazione più elevata. L'accesso a tali locali è consentito solo a personale autorizzato.
Gli accessi all'Officina sono monitorati attraverso sistemi di allarme e di videosorveglianza

2. Controllo dell'accesso ai sistemi

L'accesso ai sistemi e alle applicazioni è integrato mediante numerose direttive che consentono l'identificazione e l'autenticazione degli individui e dei singoli utenti, il controllo dell'accesso.
Le password vengono verificate automaticamente per controllare che abbiano idonee caratteristiche di sicurezza e talune devono essere cambiate periodicamente. Gli ID e le password utente vengono bloccati automaticamente dopo un numero predefinito di tentativi errati e dopo un periodo di inattività prestabilito l'attività dei client viene disattivata.
I client portatili sono basati su crittografia come standard. Client, server e array di dischi non portatili sono crittografati a seconda della necessità.

3. Controllo dell'accesso ai dati

Il sistema impedisce lo svolgimento delle attività non previste dai diritti di accesso assegnati. Il sistema di controllo delle autorizzazioni e dell'accesso ai dati si basa su un sistema interno personalizzato in cui gli utenti possono richiedere l'accesso e che garantisce un controllo degli accessi differenziato. Talvolta i dettagli dell'autorità di accesso (ad esempio l'autorizzazione di creare, modificare o eliminare i record) sono definiti all'interno dell'applicazione. In questi casi, il proprietario del sistema ottiene l'applicazione ma gestisce la distribuzione direttamente o mediante un amministratore di sistema.

4. Controllo della divulgazione dei dati

L'Officina impone il rispetto della legislazione nazionale e internazionale, a prescindere dal luogo dove sono svolte le operazioni. Le norme riguardanti l'integrità personale si basano sul GDPR e sulle altre norme vigenti in materia, eventualmente integrate dalla legislazione nazionale. A seconda della classificazione delle informazioni, il Cliente può richiedere per le informazioni un livello di protezione maggiore, ad esempio la crittografia. L'accesso remoto alla rete aziendale dell'Officina è sempre protetto e la crittografia all'interno della rete dipende dai requisiti del Cliente. La crittografia dei dati archiviati non è offerta come servizio standard, con l'eccezione dei client mobile soggetti a crittografia locale. La crittografia viene fornita come servizio aggiuntivo a pagamento su richiesta del Cliente. Il prezzo del servizio di crittografia è definito sulla base dei prezzi praticati dai fornitori dei servizi IT.

5. Controllo dei dati immessi

L'Officina, tramiti i propri fornitori di servizi IT, ha la possibilità di registrare tutte le azioni svolte nei sistemi e nelle applicazioni. L'utilizzo o meno di tale funzionalità dipende dal contratto stipulato con il Cliente, che deve essere a conoscenza della classificazione delle informazioni in relazione all'integrità (personale). Non è disponibile alcuna funzione automatica che, in sé, possa valutare l'utilizzo, la modifica, lo spostamento o l'eliminazione eventuali di dati di integrità personale.

6. Controllo della disponibilità

L'Officina, direttamente o tramite i propri fornitori di servizi IT, esegue periodici controlli della disponibilità dei dati e dell'integrità dei back-up, al fine di assicurare la gestione della continuità aziendale in caso di evento dannoso. Procedure di disaster recovery sono stabilite dall'Officina e/o dai fornitori di servizi IT.
L'officina, tramite i propri fornitori di servizi IT, ha implementato in modo avanzato misure di contrasto ai software dannosi, o malware. Le azioni fisiche di implementazione che ne derivano consistono nell'utilizzo di software di protezione dal malware su diversi livelli, con prodotti di diversi fornitori, al fine di evitare i possibili punti deboli presentati dai singoli prodotti. Tali misure si applicano a server e a client e sono integrate da firewall personali e da IPS/IDS su tutti i client e sul layer di rete.
L'Officina esegue inoltre periodica formazione al personale dipendente sui rischi derivanti da malware e sulle misure di protezione e prevenzione da attuare.