Allegato 1
Misure tecniche e organizzative di sicurezza adottate da NetRelay

NetRelay applica le seguenti misure di sicurezza organizzative e tecniche ai servizi di cui al contratto stipulato con il cliente, e si impegna a garantire un livello di sicurezza non inferiore a quanto di seguito descritto.

Misure di sicurezza organizzative

Policy interne
Il Responsabile applica dettagliate policy, alle quali tutta l'utenza con accesso ai sistemi informativi ha l'obbligo di conformarsi e che sono finalizzate a garantire comportamenti idonei ad assicurare il rispetto dei principi di riservatezza, disponibilità ed integrità dei dati nell'utilizzo delle risorse informatiche.
Periodicamente si procede alla revisione e aggiornamento delle nomine per i Responsabili del trattamento, nonché delle informative destinate agli interessati e ad altri soggetti terzi.
Adozione di un Registro delle attività di trattamento, indispensabile per dimostrare la conformità di tutti i trattamenti a quanto previsto nella nuova regolamentazione europea e assicurare un sano ciclo di gestione dei dati personali.
Adozione di una specifica procedura per regolamentare eventuali episodi di violazione di dati personali (c.d. "data breach"), mediante comunicazioni all'Autorità Garante o agli interessati al trattamento.

Autorizzazione accessi logici
Sono stati definiti i profili di accesso ai sistemi informativi necessari all'esecuzione delle operazioni di trattamento e il loro utilizzo nel rispetto del least privilege (minimo privilegio): ogni programma ed ogni utente operano utilizzando il minimo insieme di privilegi necessari a portare a termine il proprio compito.
I profili di autorizzazione sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.
Tali profili sono oggetto di controlli periodici finalizzati alla verifica della sussistenza delle condizioni per la conservazione dei profili attribuiti.

Gestione interventi di assistenza
Gli interventi di assistenza sono regolamentati allo scopo di garantire l'esecuzione delle sole attività previste contrattualmente e impedire il trattamento eccessivo di dati personali la cui titolarità è in capo al Cliente.

Analisi dei rischi
NetRelay ha predisposto una propria metodologia per l'analisi e la valutazione dei trattamenti che, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, presentino un rischio elevato per i diritti e le libertà delle persone fisiche allo scopo di procedere con la valutazione dell'impatto sulla protezione dei dati personali prima di iniziare il trattamento.

Gestione degli incidenti
NetRelay ha realizzato una specifica procedura di Incident Management allo scopo di garantire il ripristino delle normali operazioni di servizio nel più breve tempo possibile, qualora sia previsto contrattualmente, garantendo il mantenimento dei livelli migliori di servizio.

Data Breach
Il Responsabile ha implementato un'apposita procedura finalizzata alla gestione degli eventi e degli incidenti con un potenziale impatto sui dati personali che definisce ruoli e responsabilità, il processo di rilevazione (presunto o accertato), l'applicazione delle azioni di contrasto, la risposta e il contenimento

dell'incidente / violazione nonché le modalità attraverso le quali effettuare le comunicazioni delle violazioni di dati personali al Cliente.

Formazione
Il Responsabile è costantemente coinvolto in attività di aggiornamento e formazione sulla corretta gestione dei dati personali.

Misure di sicurezza tecniche

Firewall
I dati personali sono protetti contro il rischio d'intrusione di cui all'art. 615-quinquies del codice penale mediante sistemi mantenuti aggiornati in relazione alle migliori tecnologie disponibili.

Sicurezza linee di comunicazione
Tutti i protocolli di comunicazione sia in entrata sia in uscita sono sicuri, quindi la trasmissione di e-mail ed allegati avviene sempre in maniera crittografata, in modo da evitare la divulgazione non autorizzata o l'accesso ai dati personali trasmessi.

AntiVirus e AntiSpam
I sistemi sono protetti contro il rischio di intrusione e l'azione di programmi mediante l'adozione di idonei strumenti elettronici aggiornati con cadenza periodica.
Sono in uso strumenti antivirus mantenuti costantemente aggiornati.

Credenziali di autenticazione
I sistemi hw e sw sono configurati con modalità idonee a consentirne l'accesso unicamente a soggetti dotati di credenziali di autenticazione che ne consentono la loro univoca identificazione. Fra questi, codice associato a una parola chiave, riservata e conosciuta unicamente dallo stesso.

Parola chiave
Relativamente alle caratteristiche di base ovvero lunghezza minima, assenza di elementi riconducibili agevolmente al soggetto, regole di complessità e robustezza, visualizzazione e archiviazione, la parola chiave è gestita conformemente alle best practice. Ai soggetti ai quali sono attribuite le credenziali sono fornite puntuali istruzioni in relazione alle modalità da adottare per assicurarne la segretezza.

Logging
I sistemi hw e sw sono configurabili con modalità che consentono il tracciamento degli accessi e, ove appropriato, delle attività svolte in capo alle diverse tipologie di utenze protette da adeguate misure di sicurezza che ne garantiscono l'integrità.

Backup e Restore
Sono eseguiti backup periodici, ad esclusione dei servizi per i quali è responsabilità del cliente effettuare e gestire i backup. Per il Servizio Web Hosting e il Servizio Mail sono previsti backup periodici in conformità ad esigenze di Disaster Recovery. Dove contrattualmente previsto, e limitatamente al Servizio Web Hosting, possono aggiungersi ulteriori pianificazioni dei processi di backup, per le quali i clienti hanno facoltà di chiedere le relative operazioni di ripristino.

Amministratori di Sistema
Relativamente a tutti gli utenti che operano in qualità di Amministratori di Sistema, il cui elenco è mantenuto aggiornato e le cui funzioni attribuite sono opportunamente definite in appositi atti di nomina, è gestito un sistema di log management finalizzato al puntuale tracciamento delle attività svolte ed alla conservazione di tali dati con modalità inalterabili idonee a consentirne ex post il monitoraggio.

Data Center

I servizi di data center sono erogati da soggetti individuati come Responsabili (ulteriori) del trattamento. Il data center è situato in Francia e l'interconnessione ridondata con altro data center distante pochi chilometri garantisce soluzioni di disaster recovery e business continuity ottimizzate. Di seguito una breve sintesi delle misure di sicurezza adottate con riferimento ai servizi di data center:

Sicurezza fisica:

Soltanto i dipendenti accreditati possono accedere fisicamente ai server ospitati.

Accesso ai datacenter consentito esclusivamente tramite badge, sorveglianza video e umana 24/7.

Sale dotate di sistemi di rilevamento di particelle di fumo.

Personale tecnico presente 24 ore su 24, 7 giorni su 7.

Infrastrutture high availability:

Doppio collegamento per le linee elettriche.

Gruppi elettrogeni con autonomia di ben 48 ore.

Almeno 2 collegamenti rete al datacenter, all'interno 2 sale di rete gemelle che garantiscono la continuità di servizio.

Capacità di rete avanzate: connettività 10Gb+ e 40Gb+ sulla rete principale.

Certificazioni:

ISO 27001:2005 per la fornitura e l'utilizzo di infrastrutture dedicate di Cloud Computing.

ISO 27002 e ISO 27005 per la gestione della sicurezza e la valutazione dei rischi e degli interventi associati.

Certificazioni SOC 1 e 2 tipo II che attestano il livello di sicurezza.

Performance ecologiche:

98% delle sale server senza impianti di climatizzazione.

Il watercooling permette di disperdere il 70% del calore emesso dal processore.

L'aircooling smaltisce il restante 30%.

Consumi energetici dimezzati.