SISMIC SISTEMI

DICHIARAZIONE DI CONFORMITA' DEI "SOFTWARE PER LA GESTIONE DELLE CENTRALI OPERATIVE DELLE FORZE DI POLIZIA E PER LA GESTIONE DEL CONTROLLO DEGLI ACCESSI NEI CENTRI STORICI E ZTL" ALLE MISURE MINIME DI SICUREZZA ADOTTATE PER GARANTIRE LA CONFORMITA' SECONDO LE DIRETTIVE AgID

DESCRIZIONE DELL'AZIENDA E DELLE SUE ATTIVITÀ

SISMIC SISTEMI Srl nasce nel 1983 con la missione di progettare e produrre apparati e sistemi nel settore dell'elettronica e dell'automazione industriale unendo la tecnologia della comunicazione radio con quella informatica.
La società sviluppa nel tempo progetti e tecnologie proprietarie di radiocomunicazione nei seguenti settori:

- Controllo traffico aereo
- Radio Taxi
- Pubblica Sicurezza
- Protezione Civile
- Società che gestiscono la raccolta e lo smaltimento dei rifiuti solidi urbani

Nel 2000 la Società progetta e realizza le Centrali Operative per le Questure di Firenze e Savona affacciandosi così al settore inerente i sistemi operativi dedicati alle Forze dell'Ordine, con particolare riferimento all'integrazione della comunicazione radio con la rete telematica.
Nel 2001 SISMIC SISTEMI Srl sviluppa una linea di Centrali Operative, la prima delle quali sarà installata presso il Comando della Polizia Municipale di Firenze, progettate e realizzate in funzione delle esigenze specifiche dei corpi di Polizia Locale, Municipale e Provinciale.
Queste Centrali Operative integrano in una rete informatica le funzioni di:

- Controllo accessi ZTL
- Video-sorveglianza
- Comunicazioni radio e telefoniche
- Registrazione delle conversazioni radio e telefoniche
- Radiolocalizzazione dei mezzi mobili tramite tecnologia GPS
- Gestione dei turno del personale
- Memorizzazione degli eventi
- Elaborazione di statistiche

Le Centrali Operative realizzate su piattaforma WEB permettono la remotizzazione dei posti operatore in sedi decentrate e su mezzi mobili opportunamente attrezzati. L'architettura e la tecnologia utilizzate permettono il collegamento a reti informatiche di terze parti per l'integrazione di sistemi e banche dati.
La Società, mediante l'utilizzo di risorse umane altamente qualificate, progetta e realizza autonomamente gli elementi sia hardware che software costituenti il sistema.
Nel 2004 SISMIC SISTEMI srl ha conseguito la certificazione ISO 9001, rinnovandola ed estendendola nel corso degli anni fino alla versione attuale che copre tutti i processi relativi settori di competenza delle proprie attività (ea 19, 28 e 33).
Nel 2007 SISMIC SISTEMI srl ha conseguito l'omologazione ai sensi del DPR 250/99 di un sistema proprietario per la rilevazione degli accessi di veicoli ai centri storici e alle Zone a Traffico Limitato, rinnovandola ed estendendola fino alla versione attuale che risulta essere conforme alle normative vigenti in materia.

Regolamento Europeo (UE) 679/2016
Regolamento Generale Protezione Dati (RGPD)
General Data Protection Regulation (GDPR)

SISMIC SISTEMI rispetta i principi e criteri dettati dal nuovo Regolamento (UE) 2016/679 della Commissione Europea, di seguito abbreviato in GDPR, in tutti i trattamenti di dati personali che l'azienda ha in essere, sia quelli dei dipendenti, che quelli dei clienti o collaboratori. L'azienda presta molta attenzione alla protezione dei dati personali in un qualunque trattamento che venga eseguito.

Poiché nelle applicazioni per la gestione delle centrali operative delle Forze di Polizia e per la rilevazione degli accessi di veicoli ai centri storici e alle Zone a Traffico Limitato, si trattano dati personali sia dei soggetti gestori, quali gli operatori delle amministrazioni, sia dei soggetti individui singoli che vengono eventualmente intercettati o registrati al loro passaggio, SISMIC SISTEMI per essere in pieno conforme ai principi del Regolamento (UE) 679/2016, è in grado di implementare anche la 'privacy by design' nei programmi software rilasciati al Cliente.

L'Art. 25 del GDPR 'Protezione dati: Privacy by Design e Privacy by default' introduce un nuovo concetto che distingue tra i compiti del titolare (by default) e i compiti di chi sviluppa l'applicazione informatica (by design), SISMIC SISTEMI in questo caso, mettendo a disposizione degli strumenti volti a facilitare il titolare, e i futuri operatori, a rispettare riservatezza e sicurezza.
In questa breve relazione cerchiamo di evidenziare quali funzionalità contengono gli applicativi sviluppati da SISMIC SISTEMI per soddisfare il GDPR in questo senso.

Gli applicativi sviluppati da SISMIC SISTEMI aderiscono sia alle indicazioni della circolare AgID n.2/2017 del 18 aprile 2017 in relazione alle "Misure minime di sicurezza ICT per le pubbliche amministrazioni (Direttiva del Presidente del Consiglio dei Ministri 1 agosto 2015)", sia al Reg. UE 2016/679 in termini di protezione delle persone fisiche e dei loro dati personali.

—> Misure minime di sicurezza ICT per le pubbliche amministrazioni - Circolare AgID n.2/2017
—> General Data Protection Regulation (GDPR) - Regolamento (UE) 2016/679

Le due normative sono in qualche modo complementari: la prima si concentra su aspetti di sicurezza informatica del sistema; la seconda sancisce i principi fondamentali di protezione delle persone fisiche coinvolte dalla applicazione e la tutela dei loro dati personali.
La Circolare AgID punta soprattutto alla sicurezza informatica del sistema con gestione login, password, architettura ed infrastruttura applicativa, integrità e resilienza dei dati, back-up e recupero dati, sistemi di controllo anti-intrusione e anti-virus.
Gli applicativi sviluppati da SISMIC SISTEMI offrono agli utenti molte potenziali funzionalità di sicurezza, che l'utente decide se attivare o meno. Tra queste citiamo, login per accesso con funzioni differenziate a seconda del profilo utente, tracciamento dell'operato delle varie login, monitoraggio e sistema di allarmistica per notifica di anomalie o tentativi di operazioni fallite, regole per il cambio password forzato, VPN dedicati, crittografia di canale trasmissivo, crittografia di alcuni dati, procedure di back-up e di disaster recovery.

GDPR opera in uno scenario specifico per la protezione dei dati personali, in cui possiamo articolare almeno 3 attori:

- il personale di polizia o di altra PA, che utilizza l'applicativo software per svolgere il proprio lavoro, tramite un palmare in remoto o all'interno della centrale operativa, con login di utente semplice o amministratore, che opera come 'titolare del trattamento';
- l'addetto SISMIC che interviene da remoto per gestione, controllo, eventuale assistenza e riparazione guasto, che opera come 'responsabile di trattamento' dietro quindi nomina scritta del titolare;
- i cittadini che vengono individuati dal sistema, spesso inconsapevolmente, e che devono essere controllati ai termini di legge, questi operano come 'interessati'.

Formazione del personale

La prima strategia decisa da SISMIC SISTEMI è stata quella di investire sul proprio personale, provvedendo alla loro formazione sul GDPR, principi ed obblighi, per la protezione delle persone fisiche e sul trattamento dei relativi dati personali.
Un esperto esterno ha svolto una formazione di 4 ore, con test finali di valutazione tutti superati, al personale dell'azienda che sviluppa gli applicativi potenzialmente relativi al GDPR, oppure al personale che può venire a contatto con dati personali di altri interessati.

Diritti degli interessati (Artt. 15-22 GDPR)

In relazione alla tipologia del servizio offerto dal modulo software installato, in accordo con la Committente, SISMIC SISTEMI provvede a fornire il supporto necessario al titolare, qualora si presentassero casi di richiesta o reclamo da parte di alcuni utenti interessati, che vogliono far valere i propri diritti secondo il regolamento GDPR.
Da notare comunque che molti degli applicativi sviluppati da SISMIC SISTEMI srl non creano un trattamento basato sul consenso degli interessati, ma trova la sua base giuridica in motivi di ordine pubblico e di polizia, quindi anche i diritti Artt. 15-22 sono fortemente ridimensionati pur restando sempre validi.

Sicurezza dei dati (Art. 32 del GDPR)

Gli applicativi sviluppati e forniti da SISMIC SISTEMI rispettano le richieste di sicurezza del GDPR in quanto offrono potenzialmente alcune funzionalità che il titolare decide se implementare o meno:

- back up dati sia locali che remote;
- profili di accesso diverse a seconda del profilo utente;
- regole per la creazione e per il cambio password;
- password a 2 livelli o password 'one time';
- controlli (tipo checksum) per integrità file;
- crittografia di canale nella trasmissione;
- crittografia dei dati integrale o parziale;
- pseudonimizzazione;
- firewall e antivirus;
- monitoraggio dei flussi e accessi anche tramite analisi dei log file.

Violazione dei dati (Artt. 33 e 34 del GDPR)

Monitoraggio costante e tracciamento di eventuali tentativi di violazione del sistema, supporto al titolare per individuare eventuali 'data breach' con accesso non autorizzato, distruzione o alterazione di dati personali. Le violazioni al sistema vengono documentate nel Registro delle violazioni.
In ottemperanza con quanto previsto agli Art. 33 e 34 SISMIC SISTEMI srl si impegna a rispettare i tempi di comunicazione previsti dal GDPR, supportando il titolare nel preparare la notifica al Garante per la privacy entro 72 ore; se necessario, anche la comunicazione agli interessati coinvolti nella violazione.

Riservatezza dei dati personali

SISMIC SISTEMI srl fornisce il supporto agli utenti dei propri applicativi, per rispettare quanto previsto dal GDPR in termini di riservatezza delle persone fisiche. Gli operatori SISMIC sono formati e competenti in materia di protezione e riservatezza dei dati personali secondo il nuovo Regolamento (UE) 2016/679. In tal senso il sistema limita la visibilità dei dati personali, in particolare degli interessati, ma anche degli operatori della Committente, allo stretto necessario. L'operatore SISMIC non può visualizzare i dati personali di interessati o di agenti/funzionari se non ha in tal senso una autorizzazione specifica dal titolare, infatti il sistema usa dei codici di riferimento neutrali degli utenti, che quindi non consentono l'identificazione della reale persona fisica interessata.