Documento	GESTIONE DEGLI INCIDENTI INFORMATICI
Classe / tipologia	Procedura gestionale / Politiche della Sicurezza privacy e PD
Adempimenti	PROVV. "**DATA BREACH**" 2/7/2015 - Artt. **32, 33 e 34 REG.679/16**
Documenti relati	INDEX679, SOP3_3, DT679, PolPP, **IO-DB01**, DVR/IP, **RV-DB01**
Basi giuridiche	Piano di adeguamento 2018-19 con migrazione dal Codice Privacy

CONTENUTI

1 - Dichiarazione del Titolare del Trattamento (TDT)

I Sistemi Informativi della nostra organizzazione sono strutturati e configurati per attendere tutti i requisiti di *compliance* del Reg.679/16 (**Artt.24, 25**). A tale scopo è stato intrapreso un Piano di Adeguamento (**PDA**) con il quale sono state disegnate e realizzate adeguate misure fisiche, logiche ed organizzative in grado di realizzare un sistema di Gestione, Controllo e Mantenimento dei livelli di sicurezza informatica.

La presente procedura viene riferita anche nelle politiche, nelle informative e nel disciplinare interno privacy (**DIP679**) ai sensi del Regolamento Privacy e Protezione dei Dati.

2 - Istituzione del Gruppo di Risposta aziendale (Accountability Artt. 5 e 24)

La Sicurezza Informatica aziendale è condotta a diversi livelli di implementazione e per ciò che riguarda la cosidetta "data breach" è stato istituito un gruppo di lavoro responsabilizzato e impegnato a soddisfare per conto del titolare questi obblighi normativi.

Il gruppo di risposta è composto da:

- ***Responsabile del trattamento o Supervisore Sistema Privacy aziendale (SSP)***
- ***Amministratore di Sistema – LAN/WAN, network ICT (ADS secondo nomina)***
- ***Amministratore delle Banche Dati e Archivi digitali (secondo nomina)***
- ***Responsabile del Trattamento o Sub responsabile esterno (secondo nomina)***

Tutti i soggetti privacy coinvolti sono stati nominati e/o designati e/o delegati in ragione delle rispettive competenze di ruoli e funzioni, siano essi interni o esterni al sito operativo/stabilimento ai sensi del Regolamento.

NOTA: La gestione degli Incidenti Informatici è comune a tutti i Trattamenti gestiti internamente (vedi Registro dei Trattamenti, RDTA). Le infrastrutture ICT sono intese solo come apparati HW e SW locali alla sede cui questo manuale fa riferimento.

☐	TITOLARE	.....
☐	RESPONSABILE	.....
☐	TEAM DI LAVORO	.....
☐	ADS / DBA	.....

3 - Procedura operativa di risposta agli incidenti informatici

Sinossi: **SA** (Soggetto Autorizzato), **SSAA** (Soggetti Autorizzati), **GDR-IT** (Gruppo di Risposta IT), **DTIA** (Disciplinare Tecnico Infomatico Aziendale)

3.1 - Per il Titolare la sicurezza fisica del dato è un presupposto indispensabile affinché la *data protection* possa realizzarsi. Per questo adotta adeguate contromisure e sistemi pratici in ambito *cybersecurity* in grado di tenere i dati al riparo da "*data breach*"**.**

3.2 - Questa Procedure Gestionale indica come il Titolare ha scelto di dimostrare le pratiche adeguate e proporzionate per assicurare il dato ed escludere forme gravi di proprie responsabilità (Artt. 5, 24). Tali misure organizzative, fisiche e logiche sono proattive così che, nel caso un *data breach* dovesse verificarsi, il Titolare possa rimanere *compliant* con il regolamento che esige esplicitamente una notifica al Garante e se del caso ai diretti Interessati.

3.3 - La **Figura 1** nella tavola I rappresenta il flusso logico di riferimento per lo standard operativo. Tale prassi è stata oggetto di formazione e istruzione sia per il Gruppo di Risposta (**GDR-II**) che per tutti i Soggetti Autorizzati (vedi fogli di nomina e designazioni)

3.4 - La procedura gestionale consta di una Procedura Operativa **PROII** (in questo contesto), ma anche della Istruzione Operativa correlata di cui al documento **IO-DB01** nella quale si trovano le specifiche, le check-list e le istruzioni oggetto di formazione per tutti i ruoli legati all'adempimento c.d. del "*Data Breach*"

NOTA: Eventuali omissioni, ritardi e inadeguatezza della notificazione sono circostanza che verranno comunque poste a carico del TdT, senza che si possa opporre all'Autorità di controllo l'avvenuto conferimento di delega al RDT

La presente procedura gestionale e i documenti **IO-DB01 e RVDB01** sono parte integrante del Manuale del Sistema Privacy e Protezione dei Dati Personali (**MSPPD**)