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

- Dichiarazione del Titolare del Trattamento
- Istituzione del Gruppo di Risposta IT (GDR-IT)
- Procedura Operativa della Risposta all'Incidente Informatico
- Tabella misure ICT e Modulistica della Autorità di controllo (**PROII**)
- Procedura di Istruzione e affiancamento ai Soggetti Autorizzati (**SSAA**)
- TAVOLA I – figure e grafiche del Flusso Procedurale
- TAVOLA II – Fac-simile modulistica per notifica "*Data Breach*"

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**)

4 - Tabella contromisure ICT di monitoraggio e controllo

Per conformarsi agli adempimenti informatici per il "*Data Breach*" il Titolare ha incaricato il personale informatico di adottare le contromisure proattive secondo i principi di progettazione By Design e By Default.

La **Tabella 1** riassume le maggiori contromisure ICT per ambito infrastrutturale rimandando alle singole istruzioni operative dei Soggetti nominati e autorizzati secondo competenze e funzioni assegnate e firmate.

Ambito	ISTRUZIONE / PROCEDURA OPERATIVA	STATUS
Misure fisiche	• Continuità di alimentazione e stabilità elettrica apparati critici	A
	• Accesso controllato dei serramenti dei luoghi del Data Center	A
	• Accesso controllato e/o sorvegliato ai locali con armadi tecnici e dei Punti di Accesso WI-FI	A
	• Accesso controllato e/o sorvegliato ai locali in cui si svolgono trattamenti cartacei	A
Misure logiche	• Gestione licenze e automatismi per Aggiornamenti e Patch management SysOP	A
	• Configurazioni apparati di Network: Modem, Firewall, Switch, NAS – Su tutti i dispositivi sono configurate politiche di NAT/PAT secondo segmentazione di flusso dati e categorie di SSAA; static DHCP su tutti IP-device	A
	• Prassi di Archiviazione e stoccaggio digitale con cifratura di sicurezza alter sito	A
	• Configurazione ACL: paternità di accesso funzionale per tutte le risorse condivise (Tutte le credenziali di Sistema sono protette a mezzo "VAULT")	A
	• Sorveglianza Data Loss Prevention su base Appliance automatica	A
Misure organizzative	• Formazione a tutto il personale anche transitorio o in periodo di stage	A
	• Formazione e responsabilizzazione scritta per personale esterno in appalto a servizi ICT (Ecs. Agenzie di manutenzione toner, Assistenza remota IT da terzi)	A
	• Affisione di vetrofanie e divulgazione di ordini del giorno per SSAA	A

***A** – Applicato, **NA** – Non applicabile*

NOTA: completa elencazione delle misure operative sui Sistemi Informativi (HW e SW) sono raccolte le check-list e le registrazioni delle attività approntate dagli addetti informatici nel dossier "Data Breach".

4.1 - Il sistema di controllo e monitoraggio sulle infrastrutture ICT per la pronta segnalazione di eventuali violazioni della sicurezza informatica rileva a mezzo di Alert di messaggistica uno o tutti i componenti del Gruppo di Risposta. In tale circostanza si innesca un raccordo organizzativo per la immediata analisi dell'incidente informatico.

4.2 – Il primo dei componentti del **GDR-IT** (o eventualmente il un SA) riporta immediatamente Il confronto dei componenti del **TDT**

4.3 – I Componenti del GRD-IT concordano telefonicamente la ripartizioni delle diligenze previste dal **DTIA**

4.4 – Si formalizza una registrazione delle fasi di analisi e conclusioni dell' Incidente

4.5 – Si formalizzano le decisioni informando il TDT in merito alle eventuali comunicazioni alla Autorità di Controllo e se del caso agli Interessati

Dettagli delle Istruzioni Operative della versione corrente del MPPD nel documento: **IO-DB01**.

5. Modulistica della Autorità di controllo (Art.55)

5.1 - Nei casi di cui al Paragrafo 4.5 della procedura PROII, il coordinamento del **GDR-IT** ricorre alla modulistica approntata dalla Autorità di Controllo

5.2 - I fac-simile cartacei sono scaricati dal sito Istituzionale del Garante, vengono copilati e quindi trasmessi secondo applicazione dell' Art. 32 e 33 secondo istruzioni associate ai documenti tratti dal sito istituzionale del Garante. A titolo di dimostrazione si riportano in TAVOLA II una immagine del frontespizio del fac-simile secondo versione corrispondente all'anno di validità della versione corrente del MSPPD.

Il coordinamento del GDR-IT utilizza il link della Autorità:

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1915835

Tuttavia una copia già stampata del facsimile è detenuto dal coordinatore del GDR-IT per una pronta reazione nella fase operativa di emergenza dovuta a violazioni dei dati.

La codifica della copia informativa del documento del FacSimile è: **FS-DB679NAG.PDF**

Nel caso si ricada in una situazione di conclamata e verificata ipotesi di compromissione di Dati Personali tale per cui si dovrà effettuare una notifica anche agli Interessati, non esiste un fac simile standard cartaceo e si priviligeranno mezzi comunicativi elettronici diretti (sms, email, chat; vedi doc. **IO-DB01**).

NOTA: i moduli di cui al punto 5.2 sono supervisionati dal DPO (se nominato) dopo la compilazione prima della loro trasmissione all'ufficio deputato della Autorità. Tutte le configurazioni SW del Sistema IT sono oggetto di copie di sicurezza periodiche e le prassi di automatismo (batch, bash, script) sono accessibili tramite credenziali specifiche del personale nominato.

6. Procedure di istruzione e affiancamento

Il Sistema di Gestione degli Incidenti Informatici richiede che non solo il personale informatico ma anche tutti i Soggetti Autorizzati (SSAA) siano formati e istruiti in merito all'adempimento della Sicurezza dei Dati per la prevenzione della Perdita e la Compromissione dei Dati (Data Breach)

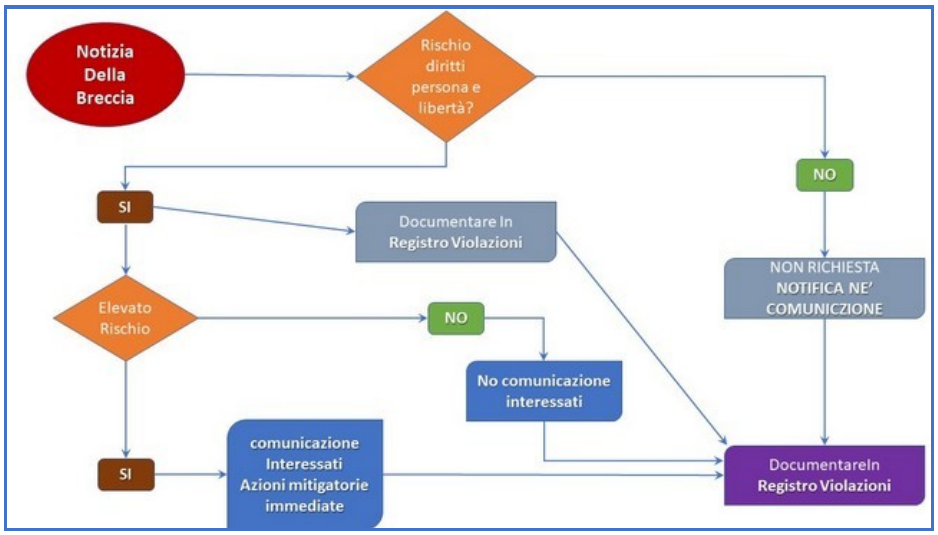
A questo scopo il Titolare ha incluso nel Piano di Adeguamento (PDA) anche in Piano di Informazione e Formazione. In merito alla Gestione degli incidenti informatici tutti i SSAA sono messi a parte delle prassi di cui alla Procedura Operativa di Risposta agli Incidenti Informatici (PROII)

Questo garantisce un alto grado di consapevolezza grazie alla quale tutta l'azienda è in grado di comportarsi correttamente e fattivamente anche quando un evento avverso informatico si verifichi al di fuori della protezione degli apparati e dei SW nella dotazione IT.

L'importanza di un affiancamento e delle istruzioni presso i **SSAA** è essenziale proprio perché le minacce cyber in informatica puntano solitamente agli operatori EndPoint, in quanto più suscettibili.

TAVOLA 1

Figura 1 – Flusso logico operativo del gruppo di risposta per il "*Data Breach*"



Tratto dalle seguenti fonti e basi giuridiche di riferimento:

NOTIFICA/COMUNICAZIONE VIOLAZIONE SICUREZZA - *Artt «33 e 34 e Linee Guida WP 29 sulla notificazione della violazione del trattamento ai sensi del Regolamento 2016/679 — n. 250/rev. 01 del 3 ottobre 2917, adottata il 6 febbraio 2018.*

TAVOLA II

FS-DB679NAG

Allegato 1 al Provvedimento del 2 luglio 2015

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

VIOLAZIONE DI DATI PERSONALI

MODELLO DI COMUNICAZIONE AL GARANTE

Secondo quanto prescritto dal Provvedimento del 2 luglio 2015, le amministrazioni pubbliche sono tenute a comunicare al Garante all'indirizzo: databreach.pa@pec.gpdp.it le violazioni dei dati personali (*data breach*) che si verificano nell'ambito delle banche dati (qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti, art. 4, comma 1, lett. *p* del Codice) di cui sono titolari.

La comunicazione deve essere effettuata entro 48 ore dalla conoscenza del fatto, compilando il modulo che segue.

Amministrazione titolare del trattamento

Denominazione o ragione sociale _____

Provincia _____ **Comune** _____

Cap _____ **Indirizzo** _____

Nome persona fisica addetta alla comunicazione _____

Cognome persona fisica addetta alla comunicazione _____

Funzione rivestita _____

Indirizzo PEC e/o EMAIL per eventuali comunicazioni _____

Recapito telefonico per eventuali comunicazioni _____

Eventuali Contatti (altre informazioni) _____

1