DOCUMENTAZIONE DI SISTEMA PRIVACY E PROTEZIONE DATI PERSONALI

EDIZIONE n. (Anno 2018-19)

Istruzione operativa : **NM-LCAADS679**

Versione : **Rif. : VAAS679, DISI679**

Ultima revisione : **MIGRAZIONE INCARICHI GDPR-EU/REG.2016/679**

Oggetto: REGISTRAZIONE DEGLI ACCESSI – GESTIONE LOG (Prec. G.U. N. 45 del 24 02 2009)

ADOZIONE DI MISURE DI CONTROLLO PER GLI AMMINISTRATORI DI SISTEMA

Documenti di Due Diligence

Su raccomandazione della autorità e in merito alle misure semplificative di cui in oggetto la Società ha adottato un disciplinare interno redatto in modo congiunto secondo attribuzioni segregate di responsabilità. Il Titolare ha disposto che il sistema informativo sia sempre monitorato in modo duplicato da parte dei due sistemisti delegati ADS e DBA (dove presente). Questa misura permette di tracciare in modo terzo gli accessi e l'operato di tutti gli interventi tecnici svolti nell'interesse della Società.

Sono quidi ammessi interventi concorrenti comunque distinti e separati affinchè la società terza possa controllare tutti i soggetti dei Sistemi Informativi. Le attività monitorate ai sensi di quanto in oggetto sono riscontrate via log digitali e registrazioni di verbali (vedi Disciplinare Interno Sicurezza Informatica, **DISI**).

I Logs digitali sono files residenti in copie speculari e storicizzate dalla Società che pertengono :

A). Logs di Accessi a oggetti INTRANET,
B). Protocolli di trasmissione/ricezione dati FTP e http, Impianto antiintrusione perimetrale dell'area di ufficio,
C). LOGON e uso delle stazioni di lavoro,
D). cambiamenti di configurazioni delle stazioni Server,
E) esiti di procedure di conservazioni dati di sicurezza

Tulle le istruzioni operative e le specifiche tecniche in carico al FHS saranno fornite dall' ADS con separate scritture o direttive verbalizzate in sede di incontri presso sede della committente. Dove necessario il Garante raccomanda stipula di contratti SLA

Amministratore di Sistema

Timbro e firma
Rappresentante legale fornitore

.....

.....

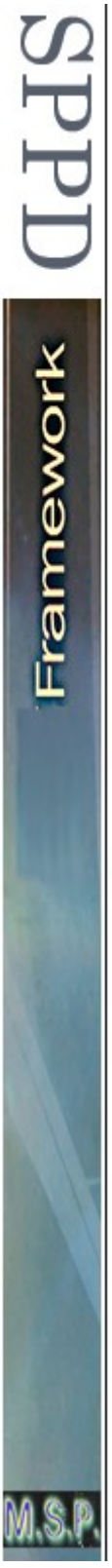
Titolare del Trattamento

.....

Per le deleghe agli amministratori di sistema si consultino i documenti DEL1/4. Per le attribuzioni segretgate di mansioni come da disciplinare interno si consulti VAAS196. Copie conformi del presente documeto sono conservate dalla società presso locazione custodita insieme alle credenziali delle persone delegate.

DOCUMENTAZIONE DI SISTEMA PRIVACY E PROTEZIONE DATI PERSONALI

EDIZIONE n. (Anno 2018-19)



Istruzione operativa : RMOADS679

Versione : Rif. : VAAS679, DISI679

Ultima revisione : MIGRAZIONE INCARICHI GDPR-EU/REG.2016/679

Oggetto: Registro interventi di manutenzione ordinaria del Sistema Informativo

Data	Ora	Operatore / Incaricato	Dati Funzione aziendale	POSTAZIONE (sito o funzione)	Firma

COMPILAZIONE : *ALL'ESAURIMENTO DELLE CASELLE DISPONIBILI RISTAMPARE COPIE CONFORMI (O FOTOCOPIE DEL MODELLO)*

L'inventario si riferisce al campo di applicazione del Punti 3, 3.1, 3.2, e 4.0 del Manuale del Sistema Informativo (vedi MSI/196) che riporta le modalità di Autorizzazioni per Amm. SI e il Disciplinare Interno (DI196).

Amministratore di Sistema

Timbro e firma

Rappresentante legale fornitore

……

……

Titolare del Trattamento

……

Per le deleghe agli amministratori di sistema si consultino i documenti DEL1/4. Per le attribuzioni segretgate di mansioni come da disciplinare interno si consulti VAAS196. Copie conformi del presente documeto sono conservate dalla società presso locazione custodita insieme alle credenziali delle persone delegate.

Documento	ISTRUZIONE OPERATIVA SUL "DATA BREACH"
Classe / tipologia	RAPPORTO OPERATIVO/ Politiche della Sicurezza privacy e PD
Adempimenti	PROVV. "**DATA BREACH**" 2/7/2015 - Artt. **32 e 33 REG.679/16**
Documenti relati	INDEX679, SOP3_3, DT679, PolPP, **RV-DB01**, DVR/IP, **DP-PG679**
Basi giuridiche	Piano di adeguamento 2018-19 con migrazione dal Codice Privacy

CONTENUTI

- Rapporto Operativo delle Misure ICT Data Breach
- ANNESSO A – copia del *journalling* delle attività associate al Rapporto Operativo

Il presente Rapporto spiega tipologicamente quali misure ICT sono state adottate a fronte dei rischi informatici legati ai trattamenti individuati nei trattamenti per garantire la "massima" protezione e prevenzione agli incidenti informatici previsti dal provvedimento "Data Breach". Tutti gli elementi del *Report* sono associati al verbale dell' **Annesso A**

Continuità elettrica apparati critici

Una unità UPS è stata installata e configurata tramite connessione USB al Server principale dell'armadio tecnico della Azienda. Il dimensionamento dell' UPS è stato calcolato in modo da garantire il dopiio dell'assorbimento richiesto rispetto alle specifiche tecniche elettriche del Server principale di LAN (vedi censimento HW)

Anti-intrusione e videosorveglianza in sede

Un impianto di antifurto IR è installato in tutti i punti di controllo delle aree di lavoro della sede. L'impianto anti-intrusione non è collegato o interattivo con gli apparati ICT. Nessuna Video Sorveglianza è installata alla data di rilascio di questo rapporto.

Controllo di accesso fisico

Tutti gli ambienti fisici dei locali di trattamenti cartacei sono controllati e dotati di serramenti meccanici in dotazione ai Soggetti Autorizzati secondo mansionamento e istruzioni di formazione da loro sottoscritte in sede di nomina/designazione/delega.

Controllo degli apparati WI-FI

Gli apparati Access Point come ripetitori (APs) della connessione wi-fi aziendale sono posti ad altezza e/o inseriti in mobili con serramento. Durante le ore di ufficio gli APs sono posti in aree normalmente presidiate e/o sorvegliate.

Tutti gli APs sono stati configurati in modo proprietario rispetto alla dotazione di fabbrica. Le chiavi crittografiche sono conservate in un sistema Vault Digitale la cui Master Pass-phrase è nelle disponibilità dei soli ADS e del TDT

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

Licenze SW e aggiornamenti di sicurezza

Tutto il SW aziendale, sia esso di Sistema o applicativo, è acquistato con licenze di utilizzo proprietarie e con contratto automatico di rinnovo e aggiornamento di sicurezza.

Il c.d. "Patches Management", è comunque oggetto di revisione / supervizione su base annuale e/o in occasione delle scadenze di rinnovo delle Licenze. Sia ADS/DBA informano il TDT su base almeno annuale circa indicenti e/o malfunzionamenti e/o anomalie di fornitura

Sicurezza ICT perimetrale

Tutto il flusso del traffico di connettività (entrata/uscita e WAN/LAN) è sottoposto ad un controllo di *appliance* continuo su un dispositivo Firewall. Oltre alle *appliance* del produttore per Data Loss Prevention (DLP) e monitoraggio IDS/IDP/IPS sono state opportunamente applicate politiche di:

- ***DHCP statico (associazione IP / MAC-address)***
- ***Instradamenti NAT (Network Address Translation) di segmentazione di rete secondo toponomastica aderente ai vari operatori/funzioni aziendali***
- ***Instradamenti PAT (Port Address Translation) secondo protocolli di servizi critici quali RDP/TV/DBserver***
- ***Black e White lists per le URL di navigazione***
- ***Community Registry: WOT, GHOSTERY, uBLOCK su tutte le stazioni di lavoro***

NOTA: La classe di Firewall adottata è di tipo UTM con *Pattern Recognition*, quindi anche tutto il traffico legato alla posta elettronica corporativa, è posto sotto misure di sicurezza adeguate (anti-virus, antispam, signature malware ecc.)

Copie di Sicurezza e storicizzazioni di Dati e Sistemi

Ai fini delle procedure adeguate di sicurezza informatica relative a copie/repliche digitali dei repertori aziendali legati al trattamento dei dati personali, l'Azienda ha centralizzato prassi automatiche e semi-manuali su un apparato NAS. Questo dispositivo dotato di sistema embedded Linix con IDE proprietario centralizza la gestione dello stoccaggio di LOG, alberature di cartelle di rete, di repliche di Database oltre che di immagini di backup dei sistemi operativi di Servers critici.

Ai fini delle misure di sicurezza di livello "adeguato" ad uno standard di disaster recovery, tutto il patrimonio delle copie INTRALAN sono replicate in storicizzazioni CLOUD.

La replica viene svolta con protocolli di trasmissione HTTPS e SFTP/FTPS di contenuti che sono anche cifrati prima (o durante) il trasferimento di stoccaggio *alter sito*.

Documento	REGISTRO RECLAMI PRIVACY
Classe / tipologia	Registro / Politiche della Sicurezza privacy e PD
Adempimenti	PROVV. "**DATA BREACH**" 2/7/2015 - Artt. **32 e 33 REG.679/16**
Documenti relati	INDEX679, SOP3_3, DT679, RDTA, DVR/IP, **DP-PG679**
Basi giuridiche	Piano di adeguamento 2018-19 con migrazione dal Codice Privacy

CONTENUTI

La politica gestionale del documento RP-PG01 e la relativa Istruzione Operativa prevedono che in merito alla gestione dei *Reclami Privacy* e più in particolare per ciò che attiene le segnalazioni tutelate dalla espressione e l'esercizio dei Diritti dell'Interessato ai sensi del Reg.679/16, venga detenuto un REGISTRO DEI RECLAMI

Questo documento R-RP01 compendia i due riferimenti di cui sopra e viene preso in carica dal GDR-IT sotto controfirmato

ISTRUZIONE D'USO E COMPILAZIONE

La registrazione di un reclamo viene registrata nel modulo annesso al presente documento. Ogni modulo identifica un sintetico rapporto descrittivo associato alle seguenti informazioni base:

- *Nome operatore del GDR-IT*
  Data e ora della segnalazione
  Descrizione reclamo
  Valutazione descrittiva danno/gravità
  Descrizione delle reazione e gestione contromisure
  Estremi documentazione e/o fascicolo
  Comunicazione ufficiale esito del reclamo a TDT/RDT e DPO se nominato

Il modulo R-RP01 opportunamente compilato viene firmato stampato e acquisito in copia digitale per essere pubblicato sul MSPPD del sito INTRALAN aziendale (se presente).

☐	TITOLARE	……
☐	RESPONSABILE	……
☐	GRUPPO RISPOSTA	……
☐	ADS / DBA	……

REGISTRO DEI RECLAMI PRIVACY

REGISTRO RECLAMI PRIVACY
REG.679/16 Artt- 5-20 diritti degli interessati
INDEX679, SOP3_3, DT679, RDTA, DVR/IP,
Piano di adeguamento 2018-19 con migrazione dal Codice Privacy

MODULO DI RILEVAMENTO

Data:.....	Operatore:	Ore: .....

DESCRIZIONE INIZIALE RECLAMO : .....

.....

.....

VALUTAZIONE DANNO / GRAVITA' PRESUNTA : ..... / .....

DESCRIZIONE ATTIVITA' DI RISPOSTA: .....

.....

.....

ESTREMI DOCUMENTAZIONE / FASCICOLI ATTIVITA' DI RISPOSTA :.....

.....

.....

ESITI UFFICIALI DEL RECLAMO :.....

.....

.....

☐	TITOLARE	.....
☐	RESPONSABILE	.....
☐	GRUPPO RISPOSTA	.....
☐	ADS / DBA	.....

Documento	REGISTRO VIOLAZIONI INFORMATICHE
Classe / tipologia	Registro / Politiche della Sicurezza privacy e PD
Adempimenti	PROVV. "**DATA BREACH**" 2/7/2015 - Artt. **32 e 33 REG.679/16**
Documenti relati	INDEX679, SOP3_3, DT679, **IO-DB01**, DVR/IP, **DP-PG679**
Basi giuridiche	Piano di adeguamento 2018-19 con migrazione dal Codice Privacy

CONTENUTI

La politica gestionale del documento DB-PG679 e la relativa Istruzione Operativa IO-DB01 prevedono che in merito alla gestione degli incidenti informatici aziendali e più in particolare per ciò che attiene le violazioni di cui al provvedimento c.d. "Data Breach" venga detenuto un REGISTRO DELLE VIOLAZIONI (RV-DB01)

Questo documento compendia i due riferimenti di cui sopra e viene preso in carica dal GDR-IT sotto controfirmato

ISTRUZIONE D'USO E COMPILAZIONE

La registrazione di un evento di violazione viene registrata nel modulo annesso al presente documento. Ogni modulo identifica un sintetico rapporto descrittivo associato alle seguenti informazioni base:

- *Nome operatore del GDR-IT*
  Data e ora dell' evento avverso
  Descrizione evento
  Valutazione danno/gravità presunta
  Valutazione danno/gravità definitiva
  Descrizione delle attività di risposta
  Estremi documentazione e/o fascicolo attività di risposta
  Conclusioni ufficiali del TDT

Il modulo RV-DB01 opportunamente compilato viene firmato stampato e acquisito in copia digitale per essere pubblicato sul MSPPD del sito INTRALAN aziendale (se presente).

☐	TITOLARE	.....
☐	RESPONSABILE	.....
☐	GRUPPO RISPOSTA	.....
☐	ADS / DBA	.....

REGISTRO DELLE VIOLAZIONI INFORMATICHE

REGISTRO VIOLAZIONI INFORMATICHE
PROVV. "**DATA BREACH**" 2/7/2015 - Artt. **32 e 33 REG.679/16**
INDEX679, SOP3_3, DT679, **IO-DB01**, DVR/IP, **DP-PG679**
Piano di adeguamento 2018-19 con migrazione dal Codice Privacy

MODULO DI RILEVAMENTO

Data:.....	Operatore:	Ore: .....

DESCRIZIONE INIZIALE EVENTO: .....

.....

.....

VALUTAZIONE DANNO / GRAVITA' PRESUNTA : ..... / .....

VALUTAZIONE DANNO / GRAVITA' RILEVATA : ..... / .....

DESCRIZIONE ATTIVITA' DI RISPOSTA: .....

.....

.....

ESTREMI DOCUMENTAZIONE / FASCICOLI ATTIVITA' DI RISPOSTA :.....

.....

.....

CONCLUSIONI UFFICIALI DEL TDT:.....

.....

.....

☐	TITOLARE	.....
☐	RESPONSABILE	.....
☐	GRUPPO RISPOSTA	.....
☐	ADS / DBA	.....

Documento	ISTRUZIONE OPERATIVA SUL "DATA BREACH"
Classe / tipologia	Istruzione operativa / Politiche della Sicurezza privacy e PD
Adempimenti	PROVV. "**DATA BREACH**" 2/7/2015 - Artt. **32 e 33 REG.679/16**
Documenti relati	INDEX679, SOP3_3, DT679, PolPP, **RV-DB01**, DVR/IP, **DP-PG679**
Basi giuridiche	Piano di adeguamento 2018-19 con migrazione dal Codice Privacy

CONTENUTI

- Istruzione operativa del Sistema di Controllo e monitoraggio Data Breach
- **ISTRUZIONE E FORMAZIONE PER "LA DATA BREACH" IN AZIENDA**

Questo documento fa compendio con la procedura di gestione **DB-PD679** e la Procedura Operativa in essa contenuta **PROII**. Taki riferimenti, congiuntamente considerati, rappresentano la struttura e le prassi funzionali del sistema aziendale approntato per adempiere agli obblighi del c.d. provvedimento di "Notifica della violazione dei dati" o la c.d. "*Data Breach*".

Il contenuto seguente riporta la politica delle pratiche adottate sulle quali è stata svolta adeguata formazione e affiancamento (Vedi Piano di Formazione, **PDFA**).

SOMMARIO PROCEDURE PASSO PASSO

1. AVVISARE SENZA INDUGIO LE PERSONE COMPETENTI
2. QUALIFICARE E QUANTIFICARE LA VIOLAZIONE
3. ADOTTARE LE MISURE NECESSARIE PER MINIMIZZARE LE CONSEGUENZE
4. EFFETTUARE LE NOTIFICAZIONI ALL'AUTORITÀ GARANTE, A MENO CHE NON SIA IMPROBABILE CHE SUSSISTA UN RISCHIO PER I DIRITTI E LE LIBERTA' DELLE PERSONE FISICHE
5. SE IL RISCHIO È ELEVATO EFFETTUARE LE COMUNICAZIONI ANCHE AGLI INTERESSATI
6. IN OGNI CASO ANNOTARE TUTTE LE VIOLAZIONI (ANCHE SE NON NOTIFICATE) NEL REGISTRO DELLE VIOLAZIONI (**RV-DB01**)

A compendio dello schema procedurale si veda la videografica della Autorità di Controllo in allegato al MSPPD "**RG-DB Garante.PDF"**

☐ TITOLARE .....

☐ RESPONSABILE .....

☐ TEAM DI LAVORO .....

☐ ADS / DBA .....

ISTRUZIONE E FORMAZIONE PER LA "DATA BREACH" IN AZIENDA

In virtù degli **Artt. 33 e 34 del GDPR** il Titolare del Trattamento (TDT) deve notificare tutte le violazioni dei dati personali al Garante e comunicare con le Persone Interessate in caso di alto rischio per i diritti e la libertà personali.

La violazione dei dati personali, il c.d. ***data breach***, è una violazione della sicurezza che comporta accidentalmente o illecitamente, distruzione, perdita, alterazione, divulgazione o accesso non autorizzati di dati di natura personale trasmessi, conservati o altrimenti elaborati.

Il titolare del trattamento ha l'obbligo di documentare - e di esibire ad eventuale richiesta del Garante - qualsiasi violazione dei dati personali, le circostanze che l'hanno causata, le sue conseguenze e i provvedimenti adottati per porvi rimedio.

Se il Titolare si è avvale di un Responsabile del Trattamento (o Referente Privacy), quest'ultimo ha l'obbligo di notificare al Titolare, senza ingiustificato ritardo dal momento in cui ne viene a conoscenza, qualsiasi violazione dei dati personali. È raccomandabile che tale obbligo sia oggetto di una specifica clausola contrattuale con il RDT e questo deve avvalersi del supporto di un Gruppo di Risposta agli Incidenti Informatici (**GDR-II** come da nomine e designazioni).

In caso di alta probabilità di rischio dei diritti e delle libertà personali, il TDT deve notificare al Garante e comunicare agli interessati tutte le violazioni dei dati personali di cui viene a conoscenza.

In applicazione del principio generale di *Accountability* (**Art. 29**), è rimessa al Titolare del Trattamento la valutazione di probabilità o meno che lo specifico *data breach* possa presentare un rischio per i diritti e le libertà degli assistiti e degli interessati. Laddove la valutazione abbia esito affermativo, non oltre le **72 ore** dalla presa di coscienza (**GDPR, Art. 33**) il TDT deve notificare la violazione al Garante della protezione dei dati personali (in qualità di autorità competente), specificando, tra l'altro:

- ***la natura della violazione dei dati personali (categorie e numero approssimativo di persone e record di dati in questione);***
- ***Il nome e le informazioni di contatto del DPO (se applicabile) o, comunque, di un punto di contatto da cui è possibile ottenere ulteriori informazioni;***
- ***le implicazioni di rischio e conseguenze della violazione;***
- ***le misure adottate o da adottare per mitigare qualsiasi conseguenze negative.***

Il modulo per la notifica – solo online – della violazione dei dati personali è a disposizione del Titolare sul sito del Garante (vedi **PG-DB01**).