Documento	DISCIPLINARE INTERNO SIUREZZA INFORMATICA
Classe / tipologia	Politiche della Sicurezza privacy e PD
Adempimenti	Artt. **32 REG.679/16**
Documenti relati	INDEX679, DT679, PolPP, RDTA, DVR/IP
Basi giuridiche	Piano di adeguamento Edizione 2018-19 migrazione dal Codice

DISCIPLINARE INTERNO DEL TRATTAMENTO DEI DATI PERSONALI CON STRUMENTI INFORMATICI

Questo documento è parte integrante della documentazione delle istruzioni e delle procedure operative per la tutela delle informazioni e della sicurezza del dato ai sensi del Regolamento Privacy europeo Reg. 679/2016

INTEGRAZIONE ALLA INFORMATIVA E FORMAZIONE DI AGGIORNAMENTO DEGLI ADDETTI DELLA AZIENDA.

La Società ha adempiuto agli obblighi e alle prescrizioni di legge del Dlg 196/03. In particolare ed in riferimento al punto di cui in oggetto, la Società ha recepito i pronunciamenti della Autorità concernenti le norme interne di informativa e disciplinare tecnico per tutti i soggetti che nella Società, ognuno per competenza, abbia una responsabilità nel trattamento delle informazioni con gli strumenti informatici e non, comunque eseguiti secondo le finalità circostanziate previste dal proprio DPS.

Richiamo di nozioni dal Piano di Formazione e affiancamento (PFA)
Ognuno degli addetti e delle figure del Sistema Privacy ha assunto propria responsabilità con lettera di delega e relativo foglio di nomina ai sensi del Regolamento. Con l'impegno sottoscritto l'operatore si è conformato alla Policy della Società descritta dal presente Disciplinare Interno, conosce i documenti di propria pertinenza e recepisce le istruzioni impartite anche a mezzo di aggiornamento e formazione continua (anche solo verbale). Questo documento pubblicamente consultabile da chiunque, descrive in modo schematico le misure tecniche e le regole interne cui conformarsi all'interno della infrastruttura informativa. Tutti gli operatori (interni ed esterni) hanno comunque ricevuto formazione diretta da parte degli Amministratori di Sistema (ADS) su mandato della Società.

Le politiche del Disciplinare Interno riguardano sia i trattamenti automatizzati che quelli cartacei e/o semplicemente le trasmissioni verbali di informazioni.

Il presente documento, professionalmente competenza degli Amministratori di Sistema, è stato approvato dal Titolare del Trattamento prima di essere divulgato e viene sottoscritto per accettazione informata da operatori, soggetti privacy e soggetti incaricati secondo nomina e/o norme contrattuali vincolanti se esterni alla azienda.

☐	TITOLARE	……
☐	RDP / REFP	……
☐	TEAM DI LAVORO	……
☐	ADS / DBA	……

Documento	TABELLA DEGLI ADEMPIMENTI DEL TITOLARE
Classe / tipologia	Istruzione operativa / Politiche della Sicurezza privacy e PD
Adempimenti	Accountability ART. 24 REG.679/16
Documenti relati	INDEX679, SOP3_3, DT679, PolPP, RDTA, DVR/IP
Basi giuridiche	Piano di adeguamento 2018-19 con migrazione dal Codice Privacy

Il Titolare del Trattamento (TDT) viene istruito sui propri obblighi in materia di Privacy e Protezione dei Dati dal proprio Consulente Privacy e/o dal proprio DPO (quando nominato).
Il TDT controfirma per presa visione e accettazione tutti gli obblighi derivanti dall'Artt.5 e 24 del Reg.679/2016 ottemperando anche a tutti i riferimenti di legge dell'intero Sistema di Privacy e Protezione dei Dati secondo principio di responsabilizzazione.
In fondo alla tabelle viene riportata una legenda della cromatura degli adempimenti classificata per rilevanza, gravità ed ordine di priorità delle attività correlate all'obbligo individuato nella sinossi del Regolamento (colonna di destra)

Adempimento	Capo, articolo
I principi applicabili al trattamento dei dati personali I dati debbono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato. Le finalità devono essere determinate, esplicite e legittime; i dati: adeguati, pertinenti, esatti ed aggiornati, oltre che limitati a quanto necessario rispetto alle finalità, e comunque da trattare in modo da garantirne un'adeguata sicurezza.	II - 5
Acquisizione del consenso da parte dell'interessato e casistica di esonero dal relativo obbligo Ciascun titolare deve distinguere i casi in cui per eseguire un trattamento è richiesto il (previo) consenso dell'interessato, da quelli in cui non è necessario acquisirlo. La richiesta del consenso deve essere presentata in modo distinto da altre richieste, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Quando per un trattamento è necessario il consenso, il titolare deve essere in grado di dimostrare che il consenso è stato effettivamente prestato.	II - 6, 7
Il consenso dei minori a fronte di servizi ICT Nei casi in cui è richiesto il consenso, il trattamento di dati relativo all'offerta diretta di servizi della società dell'informazione ai minori è lecito se il minore che ha prestato il consenso ha compiuto 16 anni. In caso di minori di 16 anni, deve essere acquisito il consenso di colui/coloro che ha/hanno la responsabilità genitoriale del minore e il titolare deve adoperarsi in ogni modo ragionevole, in considerazione delle tecnologie disponibili, per verificare la detta circostanza.	II - 8

☐ TITOLARE .....

☐ RESPONSABILE .....

☐ TEAM DI LAVORO .....

☐ ADS / DBA .....

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	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*"**.**

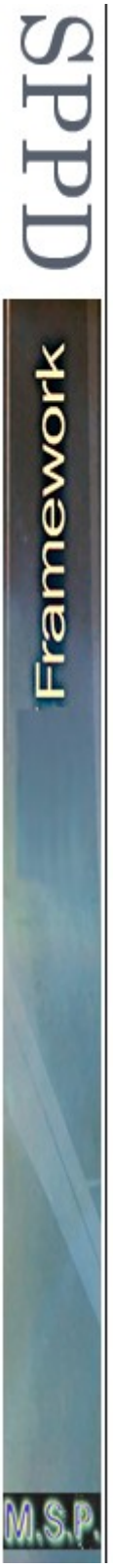
3.2 - Questa Procedure Gestionale indica come il Titolare ha scelto di dimostrare le pratiche adeguate e proporzionate per assicurare il dato ed escludere forme gravi di proprie responsabilità (Artt. 5, 24). Tali misure organizzative, fisiche e logiche sono proattive così che, nel caso un *data breach* 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**)



Documento	INFORMATIVA RESA A INTERESSATI - CLIENTI
Classe / tipologia	Informativa – Modulistica del MSPPD
Adempimenti	Art. **13 - REG.679/16 – MOD. CONSENSO** Art. 7 **- REG.679/16**
Documenti relati	INDEX679, SOP3_3, DT679, PolPP, DVR/IP, **DP-PG679**
Basi giuridiche	Piano di adeguamento 2018-19 con migrazione dal Codice Privacy

Principali informazioni sul trattamento dei Vostri dati personali come persone fisiche rese ai sensi dell'Art. 13 Regolamento EU 679/2016.

Titolare: ……..
Sede Legale: ……..
Cod.Fisc / P.IVA : ……..
Legale Rappr. :……..

Il Titolare del trattamento (di seguito Titolare o TDT) informa che tutti i suoi dipendenti, collaboratori e le altre persone fisiche che, in base ai consensi da lei espressi, abbiano accesso ai Vostri dati, operano sotto la diretta autorità dello stesso; costoro, sono nominati Soggetti Autorizzati (SSAA) al trattamento dei dati personali secondo le prescrizioni normative vigenti ed hanno ricevuto, al riguardo, adeguate istruzioni operative.

Qualunque informazione correlata al trattamento dei suoi personali può essere chiesta:

- Invio email : ……
- Servizio Clienti : ……
- Contatto sito web : ……
- Posta ordinaria all' indirizzo della sede legale sopra indicata.

Le nostre finalita'

Raccogliamo ed elaboriamo i Vostri dati solo se necessari e pertinenti con la finalità del trattamento conforme alle prescrizioni legali secondo le quali un trattamento di dati personali è legittimo in relazione, al fine del trattamento stesso.

Raccogliamo ed elaboriamo i Vostri dati con finalità determinate, esplicite e legittime e secondo modalità compatibili con tale finalità. Per questo abbiamo prestabilito gli scopi del trattamento che esplicitiamo all'Interessato perché possa comprendere che non sfruttiamo dati superflui.

I dati personali raccolti e le modalità di raccota dipendono dai prodotti e servizi che Voi acquistate o attivate, ma anche da come li utilizzate nella interazione con il Titolare. E' possibile, ed è concesso dal Regolamento Privacy che il Titolare possa aver ricevuto i Vostri dati da terze parti, ed in questo caso Voi avete dato il consenso a condividerli.

Il Titolare tratta i Suoi dati secondo basi giuridiche per:

- dare esecuzione alle clausole derivanti dal contratto sottoscritto e gestire le sue richieste, incluse – ad esempio – l'elaborazione dei dati relativi ai servizi di supporto ed assistenza nello sviluppo ed eventuale migrazione dei database, dei servizi di assistenza e garanzia resi in fase postvendita, di fatturazione dei servizi e la relativa gestione del credito;
- propri legittimi interessi, come la prevenzione delle frodi, la tutela del rischio del credito, la gestione di eventuali contenziosi, il mantenimento della sicurezza e il miglioramento della qualità dei servizi;
- adempiere ad eventuali obblighi previsti dalle leggi vigenti, da regolamenti o dalla normativa comunitaria, o soddisfare richieste provenienti dalle autorità, gli adempimenti connessi alla corretta gestione delle attività fiscali e contabili cui è tenuta l'azienda;
- fornire servizi ulteriori rispetto all'esecuzione del contratto, ad esempio per inviarle comunicazioni commerciali. In questo caso il Titolare Vi chiede un espresso consenso che sarà facoltativo e che potrà revocare in qualsiasi momento, anche dopo la cessazione del rapporto contrattuale

Come collezioniamo i Vostri dati

I Vostri dati possono essere raccolti attraverso vari mezzi/strumenti informativi e in alcune circostanze e/o situazioni che elenchiamo di seguito:

- mentre navigate sul nostro sito ufficiale (*coockies* e *beacons* vedi Tipologie di Dato sotto)
- se acquistate o utilizzate un nostro prodotto o servizio;
- se ci contattate per informazioni o supporto attraverso i nostri canali di assistenza;
- se Vi iscrivete a *newsletter* o ad altri nostri servizi e/o abbonamenti;
- se fornite il consenso informato a condividere le Vs informazioni ad altre società, come i nostri *partners* commerciali, o fornitori
- se le Vs informazioni sono state pubblicamente disponibili per le nostre finalità

Quali tipologie di dato

- Informazioni quali nome, cognome, indirizzo, numero di telefono, data di nascita, sesso ed email;
- Informazioni bancarie, qualora scelga questi metodi di pagamento per i nostri prodotti e/o servizi;
- Dati derivanti dai cookies, web beacon e altre tecnologie WEB simili.
- Cronologia di navigazione vincolata al Vs consenso tramite i cookies o altri canali.