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 riferimenti	Primo Piano di adeguamento Edizione 2023-24

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	……

Testo di politica interna per i servizi di monitoraggio e controllo dei trattamenti di dati svolti con dispositivi di elaborazione elettronica

Indicazioni generali del Disciplinare Interno (documento : DISI196)

Il Disciplinare Interno dei Sistemi Informatici (di seguito **DISI**) viene stilato dalle figure tecniche, quindi dall'Amministratore di Sistema designato (uno o più).

Per la Autorità del Garante il **DISI** è dovuto a tutti i soggetti incaricati (o Responsabili Esterni del Sistema Privacy, **RESP**) che devono conformarsi in modo informato alla Politica aziendale in materia di Privacy e Protezione dei Dati secondo i principi di responsabilizzazione, minimizzazione e e pertinenza delle finalità dei trattamenti di Dati Personali.

Prassi e misure di sicurezza per la protezione dei dati (Anti-intrusione e perimetro IT)

In accordo ai principi di Autenticazione e Autorizzazione, tutto il personale interno alla Società, si attiene alle disposizioni per il quale è stato istruito in merito alle misure ant-intrusive e di accesso delle risorse del Sistema informativo.

Tutte le stazioni di lavoro sono fornite di sistema di controllo all'accenzione (**Autenticazione**) e di utilizzo dei software applicativi dedicati (**Autorizzazione**). Il personale incaricato si attiene alle disposizioni previste in ogni momento del trattamento dei dati secondo quando previsto dal documento di Delega e di foglio di Nomina sottoscritti annualmente quale designazione.

In caso di assenza o allontanamento temporaneo dalla propria postazione, ogni operatore è tenuto a predisporre e attuare le adeguate misure di sicurezza IT assegnate. In qualunque momento, per esigenze sopraggiunte e anche solo verbalmente, l'operatore può ricevere deroghe o controindicazioni sul tipo di utilizzo della stazione di lavoro cui si adeguerà contestualmente.

Prassi e misure di sicurezza per la conservazione dei dati (PCS-PG679)

Il DPS aziendale riporta alcuni documenti e una serie di registri che provano l'essere in opera e il mantenimento di un sistema (prassi automatiche e/o procedure di persone) finalizzate alla sicurezza delle informazioni. I registri sono compilati secondo assegnazioni di delega e nomina per tutte le figure del Sistema Privacy: gli operatori sono consapevoli della stesura del DPS aziendale e hanno libero accesso alla sua consultazione secondo competenza.

Prassi e misure di sicurezza nell'utilizzo delle risorse hardware e software (Infrastruttura proprietà)

La Società è proprietaria degli strumenti di calcolo ed elaborazione utilizzati routinariamente dagli operatori e da tutto il personale pertanto ne detiene il controllo e la facoltà di verifica continua ai fini superiori di *Business Continuity* aziendale.

Le misure adottate per la salvaguardia della operatività e della funzionalità di sistemi e apparati e dispositivi sono infatti disposte perché la prevenzione di danni alla infrastruttura del Sistema Informativo, è essa stessa una misura di salvaguardia delle informazioni

Norme cautelative per servizi telematici

La Società si attiene alle disposizioni del bollettino della Autorità in materia di misure e prassi di controllo e monitoraggio degli eventuali servizi telematici quali posta elettronica, WEB e Servizi di frontiera ad accesso riservato come VPN e RD.

Gli operatori incaricati, in ragione delle proprie mansioni sono informati delle prassi di sicurezza e monitoraggio effettuate a norma di legge. Il monitoraggio del traffico di rete (se applicato ai protocolli di comunicazione) non è preventivo ed è confinato alla politica perimetrale INTRANET e WAN. In particolare per la navigazione Internet sono adottate politiche di "white & black lists".

In ogni caso i servizi sono abilitati in modo specifico a seconda delle esigenze delle diverse stazioni di lavoro con il proposito di mantenere in regime H24 la massima operatività e di schermare, ovvero limitare al minimo, le possibili esposizioni a attacchi esterni o perdite accidentali di dati. Anche gli ADS designati vengono controllati dalla Società tramite un sistema di Loggatura nelle stazioni di lavoro.

Dispositivi rimovibili di memoria di massa (Veicolazione extramurale di informazione)

Tutte le stazioni di lavoro (fisse o portatili) sono configurate dagli Amministratori di Sistema secondo indicazioni della Proprietà. Gli operatori, in nessun caso modificheranno o tenteranno di modificare le configurazioni di sistema del proprio posto di lavoro. Laddove necessario, sarà preventivamente interpellato un Amministratori di Sistema e verrà informato il Titolare del Trattamento.

Tutti gli operatori si astengono dall'utilizzo di dispositivi di storage esterni al sistema. Quando necessario o irrinuciabile, dell'uso di un dispositivo di memoria esterno viene preventivamente informato un Amministratore di Sistema; in assenza di un supervisore l'operatore effettua le procedure preventive di controllo per il quale è stato istruito o si astiene da iniziative incerte.

Alcune stazioni di lavoro in aree sensibili (Es : ingresso/accettazione) hanno bloccato l'uso dei driver USB, IE1394 e comunque le porte di comunicazioni esterne a livello di dispositivo fisico (BIOS/UEFI)

Regola generale di "pertinenza" come da prescrizione legale (Diritto societario)

In nessun caso il personale coinvolto nelle finalità del trattamento dei dati personali e delle informazioni di business, utilizza infrastruttura di sistema o dispositivi di elaborazione e memoria di massa, per trattare dati che non pertengono le ragioni di business societario. Deroghe ed eccezioni sono sempre possibili, previa richiesta al Titolare del Trattamento che eventualmente darà disposizioni per gli opportuni interventi tecnici dell'Amministratore di Sistema.

Data di affisione / pubblicazione : .....

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