INDICE

1. PREMESSA 1
2. UTILIZZO DEL COMPUTER 2
3. UTILIZZO DELLE STAMPANTI, FAX E FOTOCOPIATRICI 3
4. CREDENZIALI DI AUTENTICAZIONE 3
5. UTILIZZO DI SUPPORTI ESTERNI 4
6. UTILIZZO DI COMPUTER PORTATILI 4
7. UTILIZZO DELLA POSTA ELETTRONICA 5
8. UTILIZZO DI INTERNET 6
9. SOCIAL NETWORK 6
10. CLOUD COMPUTING (NUVOLE VIRTUALI) 6
11. WI-FI PUBBLICHE 7
12. PRIVACY BY DESIGN E BY DEFAULT 7
13. INCIDENTI SULLA SICUREZZA DELLE INFORMAZIONI 8
14. OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PRIVACY 8
15. CONTROLLI 9
16. RESPONSABILITA' 9

Proprietà Gruppo Symphonie

1. PREMESSA

La progressiva diffusione delle nuove tecnologie informatiche, con il libero accesso ad internet ed alla posta elettronica da parte dei dipendenti, espone le aziende a rischi riguardanti la sicurezza dei dati personali che possono causare la distruzione o perdita delle informazioni, accesso non autorizzato e trattamento non consentito.

Il presente documento definisce le prassi adottate per garantire il rispetto della vigente normativa in materia di trattamento dei dati personali in conformità con il Provvedimento Generale del Garante per la Protezione dei dati personali del 1 marzo 2007 e il General Data Protection Regulation 2016/679 (di seguito indicato come GDPR).

Il Personal Computer affidato al dipendente è uno strumento di lavoro. Un utilizzo non corretto può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza delle informazioni aziendali.

Al contempo, il luogo di lavoro è un'organizzazione sociale nella quale va assicurata la tutela dei diritti, delle libertà fondamentali e della dignità dei lavoratori garantendo che, in una cornice di reciproci diritti e doveri, sia assicurata l'esplicazione della personalità del lavoratore e una ragionevole protezione della sua sfera di riservatezza nelle relazioni personali e professionali (Garante della protezione dei dati personali provvedimento 1 marzo 2007).

Premesso che l'utilizzo delle risorse informatiche aziendali deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro. Il Gruppo Symphonie intende adottare questo regolamento al fine di evitare che comportamenti, anche inconsapevoli, possano innescare problemi o minacce alla sicurezza nel trattamento dei dati. L'applicabilità del presente documento è estesa a tutte le Local Company del Gruppo.

L'inosservanza delle disposizioni contenute nel presente documento può dar luogo all'applicazione di sanzioni disciplinari che possono comprendere il licenziamento in base alla gravità dell'infrazione. Il D. Lgs. del 14 settembre 2015, n. 151 (Jobs Act) permette al datore di lavoro di attivare controlli difensivi atti a verificare il corretto utilizzo delle dotazioni informatiche aziendali previste per l'erogazione della prestazione lavorativa.

2. UTILIZZO DEL COMPUTER

Si dispone che tutto il personale usi la massima cura nella gestione delle apparecchiature informatiche di cui è responsabile e si attenga rigorosamente alle seguenti disposizioni:

a) utilizzare il proprio computer, le stampanti e tutte le dotazioni di lavoro in modo da salvaguardarne l'integrità e il corretto funzionamento;

b) le risorse aziendali (fax, fotocopiatrice, computer, accesso ad internet, stampanti, ecc.) sono concesse in uso al dipendente per attività lavorative e non per fini personali;

c) non è consentito installare autonomamente programmi esterni senza l'esplicita autorizzazione dell'IT Facility in quanto sussiste il pericolo di importare Virus informatici e di alterare la stabilità delle applicazioni. Non è consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dalla società. L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'azienda a gravi responsabilità civili e penali in caso di violazione della normativa a tutela dei diritti d'autore sul software (D. Lgs. 518/92 sulla tutela giuridica del software e L. 248/2000 nuove norme di tutela del diritto d'autore) che

Proprietà Gruppo Symphonie

impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore. In merito si precisa che anche il software freeware spesso è tale solo per uso personale e non aziendale e pertanto soggetto a licenza d'acquisto;

d) non lasciare incustodita la sessione di lavoro preoccupandosi di "bloccare" il computer al termine del proprio orario di lavoro o in caso di assenza momentanea; questa regola fondamentale è particolarmente importante in caso di lavoro fuori dagli uffici della società (es. smart working, lavoro presso clienti, ecc.)

e) non è consentito all'utente di modificare le caratteristiche di sistema (nome computer, indirizzi IP, DNS, Firewall, aggiornamenti automatici SW, etc.);

f) non è consentito connettere alla rete aziendale Personal Computer personali o di terzi in maniera autonoma non autorizzata dall'IT Facility. L'inosservanza di tale norma può essere causa di gravi rischi alla sicurezza e alla funzionalità aziendale in quanto se il computer portatile è infetto da virus o non dispone di idonei strumenti di protezione informatica può diventare l'anello debole della rete aziendale ed essere quindi fonte di minacce informatiche;

g) è fortemente sconsigliata la personalizzazione del desktop del computer aziendale con immagini personali;

h) qualora fosse necessario utilizzare chiavette USB o supporti di storage esterni per la copia di informazioni riservate, il dispositivo dovrà essere protetto da pwd e/o sistemi di crittografia.

i) per il rispetto di chi lavora vicino a noi non è consentito ascoltare musica ad alto volume, né gestire call e/o meetings senza dispositivi di ascolto personali (i.e cuffie, auricolari, ecc.);

j) l'utilizzo del PC per attività personali deve essere fatto nel rispetto del presente regolamento, della normativa cogente e volontaria applicabile e nell'ambito della correttezza del rapporto da lavoro dipendente. E' al contrario tassativamente vietato l'utilizzo per attività non lecite (es. Pornografia, ecc.).

k) verificare che il proprio sistema operativo venga periodicamente aggiornato;

l) informare tempestivamente l'IT Facility su potenziali rischi o problemi inerenti la sicurezza informatica della propria postazione di lavoro.

m) Informare tempestivamente l'IT Facility in caso di smarrimento o furto del proprio PC

3. UTILIZZO DELLE STAMPANTI, FAX E FOTOCOPIATRICI

a) Assicurarsi di stampare le informazioni di natura sensibile o particolarmente riservata esclusivamente su stampanti presenti all'interno dei propri uffici o in uffici in cui gli Incaricati siano autorizzati al trattamento dei medesimi dati assicurandosi di non lasciare incustoditi i documenti sulla stampante;

b) Le stampanti, le fotocopiatrici e i fax/telefax sono beni aziendali e devono essere utilizzati dal personale esclusivamente per attività di carattere lavorativo e non per scopi di natura personale;

c) Qualora si effettuino copie di documenti che contengono dati sensibili ma non sia necessaria la conoscenza di questi dati, l'Incaricato deve renderli illeggibili (con un pennarello nero) sulle copie effettuate nel rispetto dell'art. 5 del GDPR 2016/679;

Proprietà Gruppo Symphonie

d) Qualora si effettuino copie di documenti che contengono dati sensibili verificare che non rimangano code di stampa memorizzate

4. CREDENZIALI DI AUTENTICAZIONE

a) Non comunicare a nessuno la propria password. Ricordarsi che lo scopo principale per cui si usa una password è assicurare che nessun altro possa utilizzare le proprie risorse o possa farlo a nome di un altro;

b) non scrivere la password in modo che possa essere letta facilmente, soprattutto vicino al computer;

c) quando si immette la propria password verificare che non sia visibile a terzi quello che si sta digitando;

d) non usare il proprio nome utente. È la password più semplice da indovinare;

e) non utilizzare password che possano in qualche modo essere riconducibili alla propria persona come ad esempio, il proprio nome, quello della moglie/marito, dei figli, del cane, date di nascita, numeri di telefono etc;

f) la password deve essere formata da almeno 12 caratteri alfanumerici (lettere maiuscole o minuscole), ricordando che lettere maiuscole e minuscole hanno significati diversi per il sistema.

g) la password deve essere immediatamente sostituita, dandone comunicazione all'amministratore di sistema, nel caso si sospetti che la stessa abbia perso la segretezza;

h) non potranno essere riutilizzate le password scadute;

i) non inviare assolutamente password in chiaro via email, né tantomeno via WhatsApp.

j) Non archiviare file di PWD in file se non opportunamente protetti

5. UTILIZZO DI SUPPORTI ESTERNI

a) Tutti i supporti magnetici riutilizzabili (supporti di memorizzazione USB) contenenti dati riservati aziendali devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere acquisito indebitamente da personale non autorizzato; i dati memorizzati potrebbero essere recuperati anche dopo la loro cancellazione se non correttamente effettuata;

b) i supporti magnetici contenenti informazioni riservate devono essere opportunamente protetti (es. pwd, protezione fisica, ecc.)

c) la dismissione e/o il riutilizzo di supporti elettronici di memorizzazione deve essere effettuata in accordo alle procedure applicabili

d) è necessario verificare prima dell'utilizzo di dispositivi di archiviazione provenienti da fonti non sicure (es. dispositivi di 3P, clienti, trovate casualmente, ecc.)

Proprietà Gruppo Symphonie

6. UTILIZZO DI COMPUTER PORTATILI

a) L'utilizzo di computer portatili personali per finalità aziendali deve essere preventivamente autorizzato dall'IT Facility

b) ai computer portatili si applicano le stesse regole di utilizzo previste per i computer fissi connessi in rete;

c) ciascun dipendente è responsabile del PC portatile assegnatogli e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro;

d) è vietato lasciare i computer portatili nel portabagagli della macchina. Le batterie dei computer portatili (come di tutte le apparecchiature elettroniche) emettono onde elettromagnetiche che possono essere captate da scanner in possesso di malintenzionati per realizzare furti a colpo sicuro (in particolare se si parcheggia l'auto presso centri commerciali, stazioni di servizio, ecc.);

e) nel caso di computer portatili messi a disposizione del cliente\fornitore per presentazioni o eventi, assicurarsi prima e dopo l'evento, che il computer portatile non abbia dati personali o informazioni aziendali di terzi che potrebbero, anche accidentalmente, essere acquisiti indebitamente al momento dell'utilizzo. L'eventuale inosservanza della presente disposizione potrebbe dar adito a violazione sulla normativa Privacy e al Codice della Proprietà industriale (D. Lgs 30/2005 e D. Lgs n. 131/2010) sfociando, nei casi più gravi nei reati connessi allo spionaggio industriale;

f) evitare di utilizzare il computer portatile in situazioni che permettano l'acquisizione indebita di informazioni aziendali da parte di terzi (il vicino del treno o del posto sull'aereo, ecc.);

g) proteggere il portatile contro i furti. In caso di trasferte di lavoro in macchina privilegiare porta pc a zainetto (è più comodo, sicuro ed igienico per andare nei bagni degli autogrill ad esempio). Non lasciare il portatile incustodito nelle camere di albergo se queste non dispongono di casseforti murate;

h) evitare di collegarsi con il proprio computer portatile aziendale a sistemi wi-fi pubblici o di terzi privati (hotel, ristoranti, ecc.). Alcuni protocolli wi-fi e wireless hanno debolezze note e possono essere utilizzati dagli hacker per interporsi tra l'utente e il punto di connessione. In questo modo, anziché comunicare direttamente con l'hotspot, l'utente invia le proprie informazioni all'hacker, che le indirizza poi su un altro server (relay).

7. UTILIZZO DELLA POSTA ELETTRONICA

a) La casella di posta aziendale è uno strumento di lavoro. Le persone che utilizzano la casella di posta in oggetto sono responsabili del corretto utilizzo delle stesse. Rimane responsabilità del dipendente utilizzare il proprio indirizzo di posta elettronica in modo da salvaguardarne l'integrità e il corretto funzionamento;

b) non aprire messaggi di provenienza dubbia ed informare tempestivamente l'IT FAcility.

c) non inviare o memorizzare file di natura oltraggiosa o discriminatoria;

d) è vietato trasmettere all'esterno documenti di lavoro riservati in assenza dell'esplicita autorizzazione dell'RSG[1];

[1] Responsabile Sistema di Gestione

Proprietà Gruppo Symphonie

e) è obbligatorio controllare i file allegati di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti);

f) non è consentito utilizzare inoltri automatici delle mail aziendali contenenti informazioni riservate su caselle di posta personali;

g) è vietato utilizzare il proprio account di posta elettronica aziendale per registrarsi in social network (facebook, ecc.) o in domini non attinenti a finalità lavorative;

h) è assolutamente vietato aprire allegati di email di provenienza dubbia che fanno riferimento ad acquisti di e-commerce, corrieri per il ritiro di materiale, ecc.. La minaccia più grave e sempre più frequente è costituita dai ransomware che criptano i file dell'hard disk chiedono un riscatto per ottenere l'accesso agli stessi.

i) fare molta attenzione all'email false (Procura della Repubblica, Guardia di Finanza, Agenzia delle Entrate, ecc.). Spesso si tratta di attacchi informatici denominati ***Spoofing***, attraverso i quali si falsifica la propria identità digitale per penetrare all'interno della rete aziendale o per ottenere indebitamente dati e informazioni riservate;

j) informare tempestivamente IT Facility su potenziali rischi o problemi inerenti la sicurezza informatica del proprio indirizzo di posta elettronica.

In caso di assenza improvvisa o prolungata della persona assegnataria dell'indirizzo di posta, per concrete esigenze di lavoro[2], il titolare avvalendosi della collaborazione dell'IT Facility può accedere all'indirizzo email del dipendente per garantire la regolare esecuzione dei servizi e delle attività della società.

Quanto detto ha il solo fine di garantire l'operatività, la disponibilità delle informazioni e il normale svolgimento dell'attività aziendale.

In tal caso, il dipendente al suo rientro sarà debitamente informato e dovrà modificare la sua password di accesso.

8. UTILIZZO DI INTERNET

Fermo restando quanto già detto in merito all'utilizzo personale delle infrastruttura informatiche, non è permesso l'accesso a siti internet a rischio e/o con contenuti illegali; in particolare non è permesso:

a) navigare in siti che trattino in modo non corretto opinioni politiche, religiose, sindacali o sessuali;

b) partecipare per motivi non professionali, durante il proprio orario di lavoro a forum on-line, bacheche elettroniche e guest book anche utilizzando pseudonimi o nickname;

c) utilizzare chat line o social network (facebook, ecc.) non legate a fini lavorativi;

d) scaricare software gratuiti senza l'autorizzazione dell'IT Facility;

e) scaricare documenti informatici di natura oltraggiosa o discriminatoria o che trattino in modo non corretto contenuti politici, religiosi, sindacali o sessuali;

[2] Finalità legittima e rilevante per il lavoro ai sensi del regolamento 2016/679

Proprietà Gruppo Symphonie

f) nel corso dell'orario lavorativo devono essere evitati servizi in streaming audio o video (internet radio, filmati, youtube, ecc.) che potrebbero compromettere la banda disponibile e causare perdite di efficienza della rete aziendale.

9. GESTIONE E ARCHIVIAZIONE DEI DATI AZIENDALI

L'efficace gestione dei dati aziendali costituisce un elemento fondamentale per la sicurezza delle informazioni e la qualità dei servizi. Le disposizioni contenute in questo capitolo, in conformità con il Sistema Integrato di Gestione (IMS) del Gruppo, ne regolamentano le modalità operative.

La gestione di tutte le informazioni e dei database aziendali deve avvenire esclusivamente attraverso i drive condivisi autorizzati e forniti dall'azienda. È pertanto tassativamente vietato l'utilizzo di servizi di cloud storage personali o esterni, il salvataggio di dati su dispositivi locali, così come qualsiasi forma di duplicazione non autorizzata dei documenti. Questa disposizione si applica a tutte le attività correlate all'erogazione dei servizi e alla realizzazione dei progetti.

L'utilizzo esclusivo dei drive condivisi aziendali garantisce una gestione documentale centralizzata e sicura, caratterizzata da:

a) aggiornamenti in tempo reale accessibili a tutti gli utenti autorizzati

b) sistema di protezione avanzato con controlli degli accessi

c) backup automatici programmati

d) monitoraggio continuo delle attività

La gestione centralizzata dei documenti garantisce la completa tracciabilità delle operazioni, rafforzando la sicurezza dei dati e l'efficienza dei processi aziendali.

La rigorosa osservanza di queste disposizioni è pertanto essenziale per tutelare il patrimonio informativo aziendale e assicurare la conformità alle normative interne e all'IMS del Gruppo.

10. SOCIAL NETWORK

Si rimanda al Regolamento Social Media

11. CLOUD COMPUTING (NUVOLE VIRTUALI)

Ii servizi IT in cloud acquistati dal Gruppo Symphonie devono garantire:

1. la chiara identificazione del fornitore;
2. la verifica e il continuo monitoraggio dell'affidabilità del fornitore del servizio;
3. la disponibilità e la trasparenza delle clausole contrattuali;
4. l'identificazione della posizione fisica dei dati (Il trasferimento di dati in Paesi che non offrono adeguate garanzie di sicurezza potrebbe comportare un illecito trattamento dei dati personali);
5. le garanzie sulle misure di sicurezza e riservatezza sui dati;
6. le garanzie sulla disponibilità dei dati in caso di necessità;
7. le certificazioni del fornitore del servizio

Proprietà Gruppo Symphonie

12. WI-FI PUBBLICHE

L'Utilizzo delle reti WI-FI, specie se pubbliche, presenta notevoli rischi sulla sicurezza.

Deve essere evitato per quanto possibile l'utilizzo di reti WI-FI pubbliche per la trasmissione di dati riservati aziendali al fine di evitare il rischio di wi-fi phishing e devono essere seguite le seguenti regole:

a) Navigare solo in reti sicure. Verificare accuratamente il nome della rete WI-FI messa a disposizione dall'esercente prima di collegarsi;

b) Utilizzare sempre il protocollo di comunicazione HTTPS;

c) Non consentire che la connessione automaticamente alla rete più vicina; seleziona manualmente l'hotspot con cui stabilire la connessione assicurandoti che il nome dell'hotspot sia quello corretto;

d) Evitare assolutamente il collegamento a hotspot aperti ma non ufficiali;

e) Limita e-mail e messaggi istantanei alle comunicazioni informali. Se utilizzi e-mail o messaggi istantanei negli hotspot, evita di inviare dati che non dovrebbero essere divulgati in pubblico;

f) Disattiva la scheda wireless quando non viene utilizzata.

13. PRIVACY BY DESIGN E BY DEFAULT

Le disposizioni di questo capitolo sono valide per i responsabili di funzione e lo staff manageriale della società e mirano a tutelare il legale rappresentante della società da rischi sanzionatori e profili di risarcimento che possono assumere una rilevanza anche di natura penale.

L'elemento concettuale innovativo del GDPR 2016/679 impone alle aziende l'obbligo di avviare qualsiasi progetto introducendo fin dall'inizio gli strumenti a tutela dei dati personali in una fase quindi *ex ante* il trattamento del dato, ovvero dalla progettazione (privacy by design).

L'interessato, o meglio l'utente di un servizio (app, applicazione, registrazione ad un sito web, servizi on demand, ecc.) è posto al centro del progetto sin dalla sua fase iniziale seguendo un approccio risk based che valuta le attività di trattamento contestualmente ai rischi che tali attività comportano per i diritti degli utenti.

L'azienda è inoltre tenuta a progettare e dotarsi di una struttura e mezzi tali da garantire come impostazione predefinita *di default* che vengano raccolti e trattati solo i dati strettamente necessari al raggiungimento della specifica finalità definita e che questi ultimi vengano conservati solo per il tempo strettamente necessario per perseguire l'indicata finalità e resi accessibili solo al personale espressamente e preventivamente autorizzato (Privacy by default).

Alla luce delle considerazioni espresse è di fondamentale importanza che qualsiasi progetto innovativo che coinvolge il trattamento di dati personali attraverso l'attivazione di servizi e\o tecnologie, venga validato[3] prima di essere rilasciato al cliente, firmare i contratti con i fornitori eventualmente coinvolti e/o iniziare i trattamenti.

Quando il trattamento coinvolge partner esterni, gli stessi dovranno fornire idonee garanzie di compliance al GDPR il che si traduce a titolo esemplificativo e non esaustivo in:

[3] Eventualmente coinvolgendo consulenti privacy designati

Proprietà Gruppo Symphonie

1) formulare apposite dichiarazioni di impegno, clausole contrattuali, assunzione di responsabilità;
2) verificare eventuali certificazioni in possesso del fornitore;
3) attivazione di progetti pilota e test pre-contrattuali al fine di verificare funzionalmente e tecnicamente la conformità della soluzione tecnologica ai principi cardini del GDPR;
4) compilazione da parte del fornitore di questionari di self assessment;
5) collaborazione attiva da parte del fornitore all'eventuale attivazione della valutazione d'impatto nel caso in cui i criteri di trattamento dei dati personali rientrino nei casi elencati dall'istruzione operativa OPI07.4 "*Criteri di Valutazione dell'Applicabilità della DPIA*"

14. INCIDENTI SULLA SICUREZZA DELLE INFORMAZIONI

Qualsiasi incidente sulla sicurezza delle informazioni che implichi:

- la perdita (esempio perdita di supporti fisici contenenti dati personali);
- la corruzione (ad esempio virus o alterazione di dati personali);
- l'indisponibilità di accedere a dati

e più in generale qualsiasi problema legato alla sicurezza delle informazioni deve essere prontamente comunicato all'IT Facility e al RSG

La gestione degli incidenti sulla sicurezza dei dati personali dovrà avvenire nel rispetto delle disposizioni documentate nella procedura "*Gestione degli incidenti e data breach*".

15. OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PRIVACY

È obbligatorio attenersi alle disposizioni in materia di Privacy previste dal GDPR 2016/679. Il mancato rispetto delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali previste dalla legislazione vigente.

16. CONTROLLI

L'azienda adotta controlli difensivi sul suo patrimonio informativo attraverso la configurazione e l'utilizzo di firewall, antivirus e file di log come attuazione delle misure minime di sicurezza per prevenire l'attacco di hacker esterni, virus e spyware.

L'obiettivo di questi controlli è orientato esclusivamente alla sicurezza e poggia su esigenze organizzative e produttive a tutela del patrimonio hardware, software ed informativo della società.

Per tali controlli il Gruppo Symphonie si affida ad Hoverture Italia e adotta una soluzione basata su agent (ACRONIS CYBER SECURITY) che permette il monitoraggio e controllo del dispositivo relativamente a: patch management, supporto remoto, monitoraggio remoto dei workload, blocco siti, blocco delle periferiche non autorizzate, EDR, verifica software installati, backup endpoint[4]

[4] Si veda anche il Regolamento Smart Working

Proprietà Gruppo Symphonie

I controlli difensivi che potranno comprendere il monitoraggio del traffico di rete e il controllo delle postazioni informatiche di lavoro (previo preavviso), saranno adottati come misura di prevenzione per proteggere l'azienda e potranno far risalire a condotte illecite da parte del lavoratore.

Eventuali condotte illecite saranno monitorate attraverso l'intervento di personale tecnico qualificato incaricato dalla società. In tutti i casi in cui si accertino reati o frodi informatiche, la società coinvolgerà la Polizia Postale per i controlli del caso.

I file di log potranno trattare dati personali (ora di accesso ad internet, il tempo di connessione, l'indirizzo IP visitato, ecc.). Eccezionalmente, e su esplicita richiesta, i file di log potranno essere messi a disposizione dell'autorità giudiziaria secondo le prescrizioni e gli obblighi di legge.

17. RESPONSABILITA'

L'applicazione delle corrette modalità comportamentali elencate nel presente Regolamento Informatico sono da considerarsi tassative per tutti i dipendenti e/o collaboratori, pena la possibilità di incorrere in procedimenti disciplinari da parte della Società ed esporre la società alle sanzioni penali, amministrative e civili previste dalla normativa vigente (GDPR 679/2016, Legge del 18 marzo 2008, n. 48 sulla criminalità informatica).

Con questo regolamento il Gruppo Symphonie informa in modo trasparente le Local Company ed i loro collaboratori (interni ed esterni) in merito alle politiche di sicurezza sulle informazioni adottate nell'ambito del Gruppo e confida in una collaborazione attiva e responsabile da parte di tutti i destinatari del presente regolamento.

Proprietà Gruppo Symphonie