INFORMATION SECURITY MONITORING NOTICE

Effective: 15th May 2026

Language Versions

- English version (Versione Inglese)
- Italian version (Versione Italiana)

INTRODUCTION

The legal entity named on the contract of employment of the Employee, or the engagement of the Contractor (the "**Company**") has prepared this Information Security Monitoring Notice[1] (the "**Notice**") to supplement the Employee and Contractor Data Protection Notice (the "**DPN**") that you receive as an employee or contractor.

In order to achieve the purposes set out in Appendix A of this Notice, certain monitoring activities of the Company's electronic systems and devices are practiced throughout the Company.

This Notice sets out the Company's practices regarding the monitoring of data and other materials (including but not exclusively, business and personal[2] messages, communications and information) transmitted, received, processed and/or stored by the Company's electronic systems and devices. These include, but are not limited to, network, voice, computer, company issued mobile devices, instant messaging, web applications, mobile applications, social media, audio conferencing, video conferencing and fax infrastructure ("**Electronic Communications**"), printer use, the Internet, and physical access logs.

This Notice applies to all individuals or groups that have been provided with access to the Company's systems, facilities and/or information for a business purpose or supervisory function, including employees, consultants, contractors, non-executive directors and other workers in the Company (each an "**Authorized User**"). Appendix A sets out a non-exhaustive list of the communications and records which we monitor and from which we may collect any individually identifiable information on Authorized Users ("**Personal Data**") and the purposes for which we may use, transfer and disclose Personal Data.

Authorized Users who require this Notice in a language other than those provided should contact Global Information Security using the information set out in the Contact Details section. In the event this Notice is provided to an Authorized User in a language other than English, any discrepancy, conflict or inconsistency between the two language versions shall be resolved as set out in the relevant DPN.

Irrespective of location, Company approved monitoring tools and processes (which may use Artificial Intelligence) are routinely deployed by the Company to the Company's electronic systems and devices to the extent not prohibited under local laws or regulations. All monitoring activity that takes place on the Company's electronic systems and devices is conducted in accordance with this Notice.

Any Personal Data collected (directly or indirectly) in the course of the monitoring processes will be treated in accordance with the relevant DPN as issued from time to time. The processing of Personal Data is carried out with the

[1] The Information Security Monitoring Notice (ISMN), was previously titled The Cyber Security Monitoring Notice (CSMN) and may also be referred to as such in other company documentation

[2] In line with the Code of Conduct, Authorized Users are permitted limited personal use of company managed devices and applications, the internet and email for personal communications. The use of the resources may be monitored and inspected to maintain the integrity of the systems (e.g., monitoring for the introduction of malware or inappropriate data transmissions) and avoid activities that may give rise to company liability or risk.

aid of manual and electronic tools.

This Notice references key portions of relevant policies of the Company, but does not contain all of the Company's policies and requirements applicable to the use of Electronic Communications and the Internet. Authorized Users are required to comply with the requirements noted in the Company's Code of Conduct, Electronic Communications Guide and the Global Information Security Policy documents, as well as any other applicable standards issued by the Company from time to time. All capitalized terms used but not defined in this Notice shall have the meanings assigned to them in the Company's Global Information Security Policy documents.

Communications by certain regulated Company personnel are subject to additional detailed supervisory requirements and Authorized Users are reminded to consult the relevant policies and procedures for their line of business for further information.

Subject to applicable law, all Electronic Communications, including emails (encrypted[3] and unencrypted) and connections to the Internet and intranet websites using Company computing or network resources are the property of the Company and may be subject to monitoring and surveillance. This includes but is not limited to:

- **Conducting monitoring activities without giving prior notice ("covert monitoring"), in circumstances where it is permitted to do so (for example where it has suspicions of data exfiltration, criminal or other unlawful activities or breach of the Company's Compliance or Global Information Security Policies or breach of any other obligation owed to the Company) or, where required under applicable law, under a relevant warrant or authorization;**
- **Monitoring and/or blocking of inbound and outbound emails and other messaging marked to indicate that they are personal or private or otherwise of a personal nature where it has a suspicion that such emails and their contents or attachments contravene or breach applicable law or Company's Compliance or Global Information Security Policies or any other obligation owed to the Company.**

PERSONAL DATA COLLECTION AND PURPOSES OF USE

Certain monitoring activities of the Company's electronic systems and devices are practiced throughout the Company for the purposes set out in Appendix A of this Notice.

The categories of Personal Data that the Company may process whilst undertaking the monitoring outlined in this Notice and the legal grounds for such processing (including consent, where necessary) are as set out in the relevant DPN.

Authorized Users may have additional rights. Rights of Individuals, subject to applicable law, are set out in the relevant DPN. (Section VII: Access, Portability, Rectification and Suppression, Limitation and Restriction of Processing and Accuracy of Personal Data).

The Company reserves the right, subject to applicable law and without further notice, to deploy enhanced data monitoring on your bank provided computer and/or mobile device in certain circumstances (including but not limited to you having elevated privileges, elevated access, or an approaching departure date).

SENSITIVE PERSONAL DATA

The Company may collect and process certain special categories of Personal Data including Sensitive Personal Data as

3 Where the monitoring and surveillance of encrypted communications involves the breaking and re-application of encryption.

set out in the relevant DPN in the course of conducting the activities described in this Notice.

Global Information Security monitoring activities do not actively monitor for Sensitive Personal Data, however some Sensitive Personal Data may inevitably be disclosed during monitoring for other types of data.

ACCESS BY COMPANY PERSONNEL

Access to Personal Data processed pursuant to this notice is restricted to those individuals who need such access for the purposes listed in the relevant DPN including but not limited to members of the Global Information Security team and Internal Enterprise Investigations in an Authorized User's home jurisdiction and/or other jurisdictions in which the Company has operations.

DISCLOSURE

The monitoring tools and processes described in this Notice may be deployed by the Global Information Security teams of the Company and any of its affiliates and branches including those located in the U.S., the U.K., Singapore, Hong Kong and India as well as within the specific country/region of operation. Personal Data may be stored and/or processed in an Authorized Users home jurisdiction and/or other jurisdictions in which the Company has operations.

Given the global nature of the Company's activities, the Company may therefore transfer your Personal Data to countries located outside of your home country, as set out in the relevant DPN.

The Company may disclose, in accordance with applicable law, relevant Personal Data to any of its affiliates, and branches and they may process such Personal Data for the purposes set out in this Notice. In addition, the Company may disclose, in accordance with applicable law, relevant Personal Data to certain third parties as set out in relevant DPN.

SECURITY

The Company maintains appropriate technical and organisational measures to protect against unauthorised or unlawful processing of Personal Data and/or against accidental loss, alteration, disclosure or access, or accidental or unlawful destruction of or damage to Personal Data.

MODALITIES OF THE PROCESSING AND DATA RETENTION

All monitoring and surveillance activities are initially non-individualised, and only target a specific Authorized User if there are signs of abuse or irregular behaviour, for the purposes set out in this Notice. In the event personal use of bank systems results in a personal communication that requires review, any review will be undertaken in line with applicable laws, rules and regulations.

In processing Personal Data for the purposes set out in this Notice, the Company does not use automated decision making on Authorized User processes where the decision would have a legal or similarly significant effect on the Authorized User when conducting monitoring as described in this Notice. 'Automated decision making' is the process of making a decision by automated means without any human involvement.

The retention periods for each type of data and jurisdiction are outlined on the Global Records Retention Schedule found on the Global Records Management page on Flagscape. Retention requirements are available upon request for new Authorized Users who do not yet have access to the internal site. The Company will delete Personal Data after the applicable retention period.

DISCIPLINARY ACTION

Authorized Users who violate any of the policies referenced in this Notice may be subject to investigation, suspension of access and/or disciplinary proceedings (up to and including termination of employment or contract services). Authorized Users who are not employees may be subject to referral to their employer for disciplinary action. Authorized Users who violate applicable laws or regulations may be referred to law enforcement and/or regulatory officials in accordance with legal and regulatory requirements. Any material or evidence identified via the monitoring activities described in this Notice may be relied upon in any disciplinary proceedings and internal or external investigations. Authorized Users are expected to cooperate in inquiries, inspections, monitoring and recording activities if asked. Refusing to cooperate with a security investigation may result in legal or disciplinary action, including termination of employment or contract services.

CONTACT DETAILS

For questions or more information about this Notice or Global Information Security monitoring activities, Authorized Users should contact Global Information Security.

You may have the right to lodge a complaint with the Data Protection Authority for your country, for applicability and further information refer to the relevant DPN.

For questions regarding local laws and restrictions, Authorized Users should contact their local compliance officer, Data Protection Officer or legal department.

CHANGES TO THIS NOTICE

This Notice is not contractual and the Company reserves the right to modify or withdraw the Notice at any time. Should the Company make substantial changes to this Notice, it will notify Authorized Users as soon as reasonably possible by reissuing a revised Notice and/or taking other steps in accordance with applicable laws.

APPENDIX A

Refer to the matrix linked here to view the categories of data that may be collected for each purpose of use, summarized below. The matrix is available upon request for new Authorized Users who do not yet have access to the internal site.

The Company routinely deploys and uses monitoring tools and processes for the review of Electronic Communications and records transmitted, received, processed and/or stored on the Company's electronic systems and devices. The Company may collect Personal Data arising from such monitoring tools and processes. The Electronic Communications and records subject to monitoring, whether in real time or retrospectively, include, but are not limited to:

- Emails sent (outbound);
- Emails received (inbound);
- Web / internet usage, FTP, HTTP, HTTPS, Telnet;
- Print usage and content;
- Files located on desktop (outside My Documents), collaboration sites, open shares, internal Wiki's;
- Removable media, Non-Company managed devices connecting to Company system;
- Instant messaging;
- Telephone calls, VOIP calls, voicemails;
- Application access and usage logs and records;
- Network access information (including IP address and ISP);
- System access and usage logs and records (including records showing course of usage and conduct);
- Fax & Document Scanning/Imaging;
- Social media usage and content (external, non-Company);
- Open source and publicly available information;
- Security logs;
- Key strokes and screen shots (via enhanced data monitoring);
- Conferencing technologies;
- Cookies, Beacons, Sinkholes and Honeypots;
- Geolocation Data[4]
- Swipe Card entry data;
- Text Messages sent and received.

THE PURPOSES FOR WHICH WE MAY COLLECT, USE, TRANSFER AND DISCLOSE PERSONAL DATA:

The Company is committed to safeguarding the confidentiality, integrity and availability of its systems and information including customer, employee, client, corporate, proprietary, technical, personal and third-party relationship information. The Information Security - Enterprise Policy and the related Standards are designed to protect and secure the Company's information systems, networks and assets while enabling the Company to achieve its strategic objectives. Global Information Security protects the Company and its clients and third parties by instituting preparatory, preventative, detective, mitigative and responsive measures to combat cybersecurity and information security risks, as follows:

- Prepare: We protect by continually updating the Information Security Programme, which includes complying with local or foreign state and/or country specific laws to better anticipate and identify potential threats;
- Prevent: We protect by staying ahead of adversaries through the deployment of preventative controls to prevent unauthorised access to our systems and loss or misuse of confidential and proprietary information and reduce the number of incidents;

[4] Geolocation data is defined as data taken from a user's device which indicates the geographical location of that device, including GPS data or data about connection with local wifi equipment

- Detect: We protect by limiting exposure through the deployment of detective controls including firewall monitoring, anti-spam and virus protection, identity and access management and other monitoring; continuously monitoring all human and nonhuman account identities, applications, data, systems and networks;
- Mitigate: We protect by mitigating incidents through an agile and coordinated response capability;
- Respond/Recover: We protect by improving security posture through robust forensics, investigations, and lessons learned capability while addressing any compliance issues, regulatory inquiries, disciplinary actions, or legal claims.

INFORMATIVA SUL MONITORAGGIO DELLA SICUREZZA DELLE INFORMAZIONI

Data di decorrenza: 15 maggio 2026

Versioni lingue

- English version (Versione Inglese)
- Italian version (Versione Italiana)

INTRODUZIONE

La persona giuridica indicata nel contratto di lavoro del Dipendente o nell'incarico dell'Appaltatore (la "**Società**") ha redatto la presente Informativa sul monitoraggio della sicurezza delle informazioni[5] (l'"**Informativa**") per integrare l'Informativa sulla protezione dei dati di dipendenti e appaltatori (la "**DPN**") che ricevi in qualità di dipendente o appaltatore.

Al fine di realizzare gli scopi descritti nell'Appendice A della presente Informativa, alcune attività di monitoraggio dei sistemi elettronici e dei dispositivi della Società sono praticate nell'intera Società.

La presente Informativa definisce le prassi della Società in materia di monitoraggio dei dati e di altri materiali (inclusi, a titolo esemplificativo ma non esaustivo, messaggi, comunicazioni e informazioni aziendali e personali[6]) trasmessi, ricevuti, elaborati e/o archiviati sui sistemi e sui dispositivi elettronici della Società. Questi comprendono, a mero titolo esemplificativo, la rete, la voce, il computer, i dispositivi mobili rilasciati dalla Società, la messaggistica istantanea, le applicazioni web, le applicazioni mobili, i social media, le audio e videoconferenze, le infrastrutture fax (di seguito le "**Comunicazioni elettroniche**"), l'uso della stampante, Internet, nonché i registri di accesso fisico.

La presente Informativa si applica a tutti gli individui o gruppi a cui è stato fornito accesso ai sistemi, alle strutture e/o informazioni della Società per scopi aziendali o per funzione di supervisione, ivi compresi dipendenti, consulenti, contraenti, amministratori non esecutivi e altri lavoratori della Società (ciascuno di essi un "**Utente autorizzato**"). L'Appendice A stabilisce un elenco non esaustivo delle comunicazioni e dei documenti che monitoriamo e da cui possiamo raccogliere informazioni di identificazione individuale sugli Utenti autorizzati ("**Dati personali**") nonché le finalità per le quali possiamo utilizzare, trasferire e divulgare i Dati personali.

Gli Utenti autorizzati che richiedono la presente Informativa in una lingua diversa da quelle fornite devono contattare la Sicurezza globale delle informazioni utilizzando le informazioni indicate nella sezione Dettagli di contatto. Nel caso in cui la presente Informativa sia fornita a un Utente autorizzato in una lingua diversa dall'inglese, eventuali discrepanze, conflitti o difformità tra le versioni nelle due lingue saranno risolte come stabilito nella relativa DPN.

Indipendentemente dalla sede, la Società implementa regolarmente strumenti e processi di monitoraggio (che possono prevedere l'impiego dell'intelligenza artificiale e sono approvati dalla Società stessa) nei propri sistemi e dispositivi elettronici nella misura consentita dalle leggi o dalle regolamentazioni locali. Tutte le attività di monitoraggio svolte su sistemi e dispositivi elettronici della Società sono condotte in conformità alla presente

[5] L'Informativa sul monitoraggio della sicurezza delle informazioni (Information Security Monitoring Notice, ISMN), era in precedenza denominata Informativa di monitoraggio della sicurezza informatica (Cyber Security Monitoring Notice, CSMN) e potrebbe anche essere indicata come tale in altra documentazione aziendale

[6] In linea con il Codice di condotta, agli Utenti autorizzati è consentito un uso personale limitato dei dispositivi e delle applicazioni aziendali nonché di Internet e delle e-mail per le comunicazioni personali. L'uso delle risorse può essere monitorato e ispezionato per mantenere l'integrità dei sistemi (ad es., monitorare che non vengano introdotti malware o trasmessi dati inappropriati) e per evitare attività che possano dare luogo a responsabilità o rischi aziendali.

Informativa.

Tutti i Dati personali raccolti (direttamente o indirettamente) nel corso dei processi di monitoraggio saranno trattati in conformità alla relativa DPN emessa di volta in volta. Il trattamento dei Dati personali avviene con l'ausilio di strumenti manuali ed elettronici.

La presente Informativa fa riferimento a parti essenziali delle corrispondenti politiche della Società, ma non contiene tutte le politiche e i requisiti della Società applicabili all'uso delle Comunicazioni elettroniche e di Internet. Gli Utenti autorizzati sono tenuti a osservare i requisiti indicati nel Codice di condotta, nella Guida alle comunicazioni elettroniche (Electronic Communications Guide) e nei documenti relativi alla Politica globale sulla sicurezza delle informazioni (Global Information Security Policy) della Società, nonché eventuali altri standard applicabili emessi, di volta in volta, dalla Società. Tutti i termini in maiuscolo utilizzati ma non definiti nella presente Informativa saranno da intendersi nell'accezione assegnata loro nei documenti relativi alla Politica globale sulla sicurezza delle informazioni (Global Information Security Policy) della Società.

Le comunicazioni da parte di determinati membri del personale designati dalla Società sono soggette a requisiti di supervisione dettagliati aggiuntivi e gli Utenti autorizzati sono invitati a consultare le relative politiche e procedure in vigore nella propria Divisione aziendale per maggiori informazioni.

Fatta salva la legge applicabile, tutte le Comunicazioni elettroniche, ivi comprese le e-mail (crittografate[7] o meno) nonché i collegamenti ai siti Internet e Intranet per mezzo delle attrezzature informatiche e le risorse di rete della Società sono di proprietà della Società stessa possono essere soggette a monitoraggio e sorveglianza. Ciò include, a titolo esemplificativo ma non esaustivo:

- **Espletare attività di monitoraggio senza obbligo di previa notifica ("monitoraggio segreto"), in circostanze in cui è consentito farlo (ad esempio qualora si abbiano sospetti di sottrazione di dati, attività criminali, gravi attività illecite di altro genere o violazione delle Politiche globali sulla sicurezza delle informazioni o della conformità della Società o violazione di altri obblighi assunti nei confronti della Società), o, laddove richiesto ai sensi della legge applicabile, in base ad un mandato o un'autorizzazione;**
- **Monitorare e/o bloccare le e-mail in entrata e in uscita e altri messaggi contrassegnati come personali o privati, o che siano comunque di carattere personale, in cui vi sia il sospetto che il contenuto o gli allegati contravvengano o violino la legge vigente o le Politiche globali sulla sicurezza delle informazioni o sulla conformità della Società o altri obblighi assunti nei confronti della Società.**

RACCOLTA E FINALITÀ D'USO DEI DATI PERSONALI

Alcune attività di monitoraggio di sistemi e dispositivi elettronici della Società vengono espletate in tutta la Società per le finalità stabilite nell'Appendice A della presente Informativa.

Le categorie di Dati personali che la Società può trattare mentre intraprende il monitoraggio qui descritto e le basi giuridiche per tale trattamento (incluso, ove necessario, il consenso) sono quelle indicate nella relativa DPN.

Gli Utenti autorizzati possono avere diritti aggiuntivi. I diritti delle persone, fatta salva la legge applicabile, sono stabiliti nella DPN pertinente. (Sezione VII: accesso, portabilità, rettifica ed eliminazione, limitazione, restrizione del trattamento e accuratezza dei dati personali).

La Società si riserva il diritto, in base alla legge applicabile e senza ulteriore preavviso, di implementare, su computer

7 Laddove il monitoraggio e la sorveglianza delle comunicazioni crittografate comportino la disapplicazione e la riapplicazione della crittografia.

e/o dispositivo mobile, fornito dalla banca in determinate circostanze, un monitoraggio avanzato dei dati (incluso, a titolo esemplificativo ma non esaustivo, il fatto di avere privilegi elevati, accesso elevato o una data di partenza prossima).

DATI PERSONALI SENSIBILI

La Società, nel corso dello svolgimento delle attività descritte nella presente Informativa, può raccogliere e trattare determinate categorie speciali di Dati personali, inclusi i Dati personali sensibili, come stabilito nella relativa DPN.

Le attività di monitoraggio sulla sicurezza delle informazioni globali non monitorano attivamente i Dati personali sensibili, tuttavia alcuni Dati personali sensibili possono inevitabilmente essere divulgati durante il monitoraggio di altri tipi di dati.

ACCESSO DA PARTE DEL PERSONALE DELLA SOCIETÀ

L'accesso ai Dati personali trattati ai sensi della presente informativa è limitato alle persone che necessitano di tale accesso per le finalità elencate nel DPN pertinente, inclusi, a titolo esemplificativo ma non esaustivo, i membri del team Global Information Security e delle Indagini aziendali interne nella giurisdizione di origine di un Utente autorizzato e/o in altre giurisdizioni in cui la Società opera.

DIVULGAZIONE

Gli strumenti e i processi di monitoraggio descritti nella presente Informativa possono essere implementati dai Team per la sicurezza delle informazioni globali della Società e di una qualsiasi delle sue affiliate e filiali comprese quelle situate negli USA, nel Regno Unito, a Singapore, ad Hong Kong e in India, nonché nello specifico Paese/regione in cui si opera. I Dati personali possono essere conservati e/o trattati presso la giurisdizione del Paese dell'Utente autorizzato e/o in altre giurisdizioni nelle quali la Società conduce la propria attività.

Data la natura globale delle proprie attività, la Società può quindi trasferire i Dati personali degli utenti in Paesi situati al di fuori del loro Paese di origine, come stabilito nella relativa DPN.

La Società può, ai sensi della legge vigente, divulgare i Dati personali rilevanti a una qualsiasi delle sue affiliate e filiali le quali possono, a loro volta, trattarli per gli scopi stabiliti nella presente Informativa. Inoltre, la Società può divulgare, in conformità con la legge vigente, i Dati personali rilevanti a determinate terze parti come stabilito nella relativa DPN.

SICUREZZA

La Società adotta misure tecniche e organizzative adeguate volte a impedire il trattamento non autorizzato o illegale dei Dati personali e/o per proteggerli da perdite, alterazioni, divulgazione o accesso accidentali nonché da distruzione o danneggiamento accidentali o illeciti.

MODALITÀ DI TRATTAMENTO E DI CONSERVAZIONE DEI DATI

Tutte le attività di monitoraggio e sorveglianza sono inizialmente non individualizzate e si rivolgono a uno specifico Utente autorizzato solo se vi sono segni di abuso o comportamento improprio, per le finalità indicate nella presente Informativa. Nel caso in cui l'uso personale dei sistemi bancari determini una comunicazione personale che richiede una revisione, qualsiasi revisione sarà effettuata in linea con le leggi, le norme e i regolamenti applicabili.

Durante il trattamento dei Dati personali per le finalità stabilite nella presente Informativa, la Società non utilizza processi decisionali automatizzati sui processi degli Utenti autorizzati laddove tale decisione possa avere un effetto

legale o altrettanto significativo sull'Utente autorizzato durante la conduzione del monitoraggio come descritto nella presente Informativa. Per "processo decisionale automatizzato" si intende un processo decisionale eseguito con mezzi automatizzati e senza alcun coinvolgimento umano.

I periodi di conservazione per ciascun tipo di dati e ciascuna giurisdizione sono descritti nel Programma globale sulla conservazione dei documenti disponibile nella pagina Gestione globale dei documenti su Flagscape. I requisiti di conservazione sono disponibili su richiesta per i nuovi Utenti autorizzati che non hanno ancora accesso al sito interno. La Società cancellerà i Dati personali al termine del periodo di conservazione applicabile.

PROVVEDIMENTI DISCIPLINARI

Gli Utenti autorizzati che violino le politiche menzionate nella presente Informativa possono essere soggetti a indagini, sospensione dall'accesso e/o provvedimenti disciplinari (fino alla risoluzione del contratto d'impiego o di fornitura di servizi). Gli Utenti autorizzati che non siano dipendenti possono essere soggetti a segnalazione al datore di lavoro per l'adozione di eventuali provvedimenti disciplinari. Gli Utenti autorizzati che violino le leggi o le normative vigenti possono essere segnalati ai funzionari preposti alla regolamentazione e/o applicazione della legge in conformità ai requisiti legali e normativi. Eventuali materiali o prove identificati tramite le attività di monitoraggio descritte nella presente Informativa possono essere invocati in qualsiasi procedimento disciplinare e in inchieste interne o esterne. Gli Utenti autorizzati sono tenuti, qualora venga loro richiesto, a collaborare nell'ambito di indagini, di ispezioni e di attività di monitoraggio e di registrazione . Il rifiuto di collaborare nell'ambito di un'indagine di sicurezza può comportare azioni legali o provvedimenti disciplinari fino alla risoluzione del contratto di impiego o di fornitura di servizi.

RECAPITI

Per eventuali dubbi o domande in merito alla presente Informativa o alle attività di monitoraggio sulla sicurezza delle informazioni globali, gli Utenti autorizzati possono contattare la Sicurezza Globale delle Informazioni.

L'utente può avere il diritto di presentare un reclamo presso l'Autorità garante per la protezione dei dati per il suo Paese. Per l'applicabilità e per ulteriori informazioni fare riferimento alla relativa DPN.

Per questioni riguardanti le leggi e le restrizioni locali, gli Utenti autorizzati possono contattare il funzionario preposto alla conformità della propria area, il Data Protection Officer (Funzionario preposto alla protezione dei dati) oppure l'Ufficio legale.

MODIFICHE ALLA PRESENTE INFORMATIVA

La presente Informativa non ha valore contrattuale e la Società si riserva il diritto di modificarla o emendarla in qualsiasi momento. Qualora la Società apporti modifiche sostanziali alla presente Informativa, informerà gli Utenti autorizzati non appena ragionevolmente possibile rilasciando una nuova Informativa emendata e/o adottando altre misure in conformità alle leggi vigenti.

APPENDICE A

Fare riferimento alla matrice qui collegata per visualizzare le categorie di dati che possono essere raccolti per ogni finalità di utilizzo, come riassunto di seguito. La matrice è disponibile su richiesta per i nuovi Utenti autorizzati che non hanno ancora accesso al sito interno.

La Società utilizza regolarmente strumenti e processi di monitoraggio per la revisione delle Comunicazioni elettroniche e dei documenti trasmessi, ricevuti, elaborati e/o archiviati sui sistemi e dispositivi elettronici della Società stessa. La Società può raccogliere Dati personali derivanti da tali strumenti e processi di monitoraggio. Le Comunicazioni elettroniche e i registri soggetti a monitoraggio, in tempo reale o retrospettivo, includono, a titolo esemplificativo ma non esaustivo:

- E-mail inviate (in uscita);
- E-mail ricevute (in entrata);
- Utilizzo di web/internet, FTP, HTTP, HTTPS, Telnet;
- Utilizzo e contenuti della stampa;
- File posizionati su Desktop (fuori da Documenti), siti di collaborazione, condivisioni aperte, Wiki interni;
- Supporti rimovibili, dispositivi non gestiti dalla Società che si collegano al sistema della Società;
- Messaggistica istantanea;
- Chiamate telefoniche; chiamate VOIP, segreteria telefonica;
- Accesso alle applicazioni e utilizzo di registri e archivi;
- Informazioni di accesso alla rete (inclusi indirizzo IP e ISP);
- Accesso al sistema e utilizzo di registri e archivi (inclusi archivi che mostrano il corso dell'utilizzo e della condotta);
- Scansione/Acquisizione di immagini di documenti e fax;
- Utilizzo e contenuto dei social media (esterno, al di fuori della Società);
- Open source e informazioni disponibili al pubblico;
- Registri di sicurezza;
- Tasti premuti e schermate acquisite (tramite un monitoraggio dei dati migliorato);
- Tecnologie per conferenze;
- Cookie, Beacon, Sinkhole e Honeypot;
- Dati di geolocalizzazione[8]
- Dati di inserimento della carta di lettura;
- Messaggi di testo inviati e ricevuti.

FINALITÀ PER CUI POSSIAMO RACCOGLIERE, USARE, TRASFERIRE E DIVULGARE DATI PERSONALI:

La Società si impegna a salvaguardare la riservatezza, l'integrità e la disponibilità dei propri sistemi e delle proprie informazioni, tra cui informazioni relative a clienti e dipendenti, aziendali, proprietarie, tecniche, personali e di terze parti. La Sicurezza delle informazioni - Politica aziendale e i relativi Standard sono concepiti per proteggere i sistemi informativi, le reti e le risorse della Società, consentendole al contempo di raggiungere i propri obiettivi strategici. La Sicurezza globale delle informazioni protegge la Società, i suoi clienti e le sue terze parti mediante l'implementazione di misure preparatorie, preventive, investigative, attenuanti e reattive volte a combattere i rischi di sicurezza informatica e delle informazioni, come segue:

- Prepararsi: Ci proteggiamo aggiornando continuamente il Programma per la sicurezza delle informazioni, che include il rispetto di specifiche leggi locali o estere e/o nazionali il cui scopo è prevedere e identificare meglio le

[8] I dati di geolocalizzazione sono dati presi dal dispositivo di un utente che indicano la posizione geografica di tale dispositivo, inclusi i dati GPS o i dati relativi alla connessione con apparecchiature Wi-Fi locali.

potenziali minacce;

- Prevenire: Ci proteggiamo anticipando le mosse di aggressori mediante l'implementazione di controlli preventivi volti a prevenire gli accessi non autorizzati ai nostri sistemi, la perdita o l'uso improprio di informazioni riservate e proprietarie e a ridurre il numero di incidenti;
- Rilevare: Ci proteggiamo limitando l'esposizione tramite l'implementazione di controlli rilevativi, tra cui il monitoraggio dei firewall, la protezione anti-spam e anti-virus, la gestione di identità e accessi e altre forme di monitoraggio; monitoriamo continuamente tutte le identità dei conti umani e non umani, le applicazioni, i dati, i sistemi e le reti;
- Mitigare: Ci proteggiamo mitigando gli incidenti mediante la capacità di reagire in modo agile e coordinato;
- Rispondere/Ripristinare: Ci proteggiamo migliorando il livello di sicurezza tramite solide capacità forensi, indagini e lezioni apprese, e affrontando al contempo eventuali problemi di conformità, indagini normative, azioni disciplinari o rivendicazioni legali.