INFORMATION SECURITY MONITORING NOTICE - EMEA

English Version

Effective: 3rd April 2023

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 to set out its 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. Appendix B should be referred to by Authorized Users in specific countries.

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, monitoring tools and processes 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 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 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.

[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.

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.

All Electronic Communications, including emails (encrypted 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.

Subject to applicable law, 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);**
- **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.

SENSITIVE PERSONAL DATA

The Company may collect and process certain special categories of Personal Data including Sensitive Personal Data as 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 Appendix A. In addition to those individuals as set out in the relevant DPN, access will be granted on a strict need-to-know basis, to limited members of the Global Information Security Department and where necessary Internal Enterprise Investigations.

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 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

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 (including but not limited to) the monitoring of telephone calls, emails and Internet or intranet use (including personal telephone calls, emails and Internet usage) 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.

Related Documents

Code of Conduct

Electronic Communications Retention – Enterprise Policy

Global Information Security Policy documents

Harassment & Discrimination Prevention – Enterprise Policy

Reputational Risk – Enterprise Policy

Violence Free Workplace – Enterprise Policy

Information Security Monitoring Notice - Flagscape

For additional policies, standards and guidelines, please see the Global Policy Source Flagscape page.

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 Communications and Records (both live and after the event) which we monitor on the Company's electronic systems and devices and from which we may collect Personal Data include, but are not limited to:

- Emails sent;
- Emails received;
- Web / internet usage, FTP, HTTP, HTTPS, Telnet;
- Print usage;
- 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;
- 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 logs and screen shots;
- Conferencing technologies;
- Cookies, Beacons, Sinkholes and Honeypots;
- GPS, Wi-Fi Tracking and Location Data;
- Swipe Card entry data;
- Text Messages sent and received.

The Purposes For Which We May Collect, Use, Transfer And Disclose Personal Data:

The Global Information Security Policy is designed to provide the necessary requirements to enable the Company to prepare, prevent, detect, respond and recover from increasing changes in the threat landscape. The Global Information Security Program provides solutions and uses advanced techniques to prevent information security threats from undermining customer confidence and disrupting business operations. Global Information Security protects the Company and its clients by using a risk-based and outcome-focused framework.

- 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 loss, misuse and inappropriate use of confidential and proprietary information and reduce the number of incidents;
- Detect: We protect by limiting exposure through the deployment of detective controls including firewall monitoring, anti-spam and virus protection, and other monitoring; continuously monitoring all bank teammates, 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.

APPENDIX B

Spain

In Spain, pursuant to the content of art. 20 of Real Decreto Legislativo 2/2015, de 23 de octubre, Texto Refundido del Estatuto de los Trabajadores (Legislative Royal Decree 2/2015, dated 23rd October, on the Spanish Workers' Statute), the Company reserves its right to use any means, provided such means are proportionate in order to verify the compliance by the employee with its labour obligations in connection with the use of computer equipment and Internet.

The Russian Federation

This Information Security Monitoring Notice is applicable insofar as it does not contradict legislation of the Russian Federation, including but not limited to the Federal Law # 152-FZ "On Personal Data" as of July 27, 2006 as well as OOO Merrill Lynch Securities data protection policies and regulations.

Greece

This Information Security Monitoring Notice is applicable insofar as it does not contradict to the laws and regulations in Greece in particular Greek law 2472/1997 "Protection of Individuals with regard to the Processing of Personal Data" and Greek law 3471/2006 "Protection of personal data and privacy in the electronic telecommunications sector and amendment of law 2472/1997" as well as specific case decisions issued from the Hellenic Data protection Authority.

Qatar

This Information Security Monitoring Notice is applicable insofar as it does not contradict to the laws and regulations in Qatar, including but not limited to the QFC Data Protection Regulations and Rules 2005 as well as Merrill Lynch International – QFC Branch data protection internal policies and requirements.

United Arab Emirates

This Information Security Monitoring Notice is applicable insofar as it does not contradict to the laws and regulations in DIFC, including but not limited to the Data Protection Law DIFC Law No. 5 of 2020 and DIFC Amendment Law DIFC Law No. 2 of 2022 as well as Merrill Lynch International (DIFC Branch) data protection internal policies and requirements.

KENNISGEVING INZAKE INFORMATIEBEVEILIGINGSTOEZICHT - Dutch

Nederlandse Versie

Ingangsdatum: 3rd April 2023

INLEIDING

De rechtspersoon die vermeld staat op de arbeidsovereenkomst van de Werknemer of de verbintenis van de Aannemer (het "**Bedrijf**") heeft deze Kennisgeving inzake informatiebeveiligingstoezicht[3] (de "**Kennisgeving**") opgesteld als aanvulling op de Kennisgeving inzake gegevensbescherming voor werknemers en aannemers (Data Protection Notice, de "**DPN**") die u als werknemer of aannemer ontvangt, om zijn praktijken uiteen te zetten met betrekking tot het toezicht van gegevens en andere materialen (met inbegrip van maar niet uitsluitend, zakelijke en persoonlijke[4] berichten, communicatie en informatie) verzonden, ontvangen, verwerkt en/of opgeslagen door de elektronische systemen en apparaten van het Bedrijf. Deze omvatten, maar zijn niet beperkt tot, infrastructuur voor netwerk, stem, computer, door het bedrijf verstrekte mobiele apparaten, instant messaging, webtoepassingen, mobiele toepassingen, sociale media, audioconferenties, videoconferenties en fax ('**Elektronische communicatie**'), gebruik van printers, het internet en fysieke toegangslogs.

Deze Kennisgeving geldt voor alle individuen of groepen aan wie toegang is verstrekt tot de systemen, faciliteiten en/of informatie van het Bedrijf voor een zakelijk doel of uit hoofde van toezicht, waaronder werknemers, consulenten, aannemers, niet-uitvoerende directeurs en andere medewerkers in het Bedrijf (elk een '**Geautoriseerde gebruiker**'). Bijlage A bevat een niet-limitatieve lijst van de communicatie en bestanden die wij monitoren en waaruit wij individueel identificeerbare informatie over Geautoriseerde gebruikers ("**Persoonsgegevens**") kunnen verzamelen, alsmede de doeleinden waarvoor wij Persoonsgegevens kunnen gebruiken, overdragen en bekendmaken. Bijlage B moet geraadpleegd worden door Geautoriseerde gebruikers in specifieke landen.

In het geval dat deze Kennisgeving in een andere taal dan het Engels wordt verstrekt aan een Geautoriseerde gebruiker, worden alle discrepanties, conflicten of tegenstrijdigheden tussen de twee taalversies geïnterpreteerd zoals uiteengezet in de desbetreffende DPN.

Ongeacht de locatie worden controletools en -processen routinematig door het Bedrijf ingezet op de elektronische systemen en apparaten van het Bedrijf voor zover dit niet verboden is onder lokale wet- en regelgeving. Alle controleactiviteiten die plaatsvinden op de elektronische systemen en apparaten van het Bedrijf worden uitgevoerd in overeenstemming met deze Kennisgeving.

Persoonsgegevens die in de loop van de toezichtsprocessen worden verzameld, zullen worden behandeld overeenkomstig de relevante DPN zoals van tijd tot tijd bekendgemaakt. De verwerking van Persoonsgegevens wordt verricht met behulp van handmatige en elektronische hulpmiddelen.

In deze Kennisgeving wordt verwezen naar belangrijke delen van relevant beleid van het Bedrijf, maar het bevat niet het volledige beleid en alle vereisten van het Bedrijf die van toepassing zijn op het gebruik van

[3] De Kennisgeving inzake Informatiebeveiligingstoezicht (Information Security Monitoring Notice - ISMN) was voorheen bekend onder de naam Kennisgeving inzake Cyberveiligheidstoezicht (Cyber Security Monitoring Notice - CSMN) en kan ook in andere bedrijfsdocumentatie als zodanig worden aangeduid

[4] In overeenstemming met de Gedragscode is het geautoriseerde gebruikers toegestaan beperkt persoonlijk gebruik te maken van door het bedrijf beheerde apparatuur en toepassingen, het internet en e-mail voor persoonlijke communicatie. Het gebruik van de middelen kan worden gecontroleerd en geïnspecteerd om de integriteit van de systemen te handhaven (bv. controle op het invoeren van malware of ongepaste gegevensoverdracht) en activiteiten te vermijden die aanleiding kunnen geven tot aansprakelijkheid of risico's voor het bedrijf.

Elektronische communicaties en het internet. Geautoriseerde gebruikers moeten zich houden aan de vereisten die staan vermeld in de Code of Conduct (Gedragscode), Electronic Communications Guide (Elektronische communicatiegids) en de Global Information Security Policy documents (documenten over Wereldwijd informatiebeveiligingsbeleid) van het Bedrijf en eventuele andere geldende normen die van tijd tot tijd worden uitgevaardigd door het Bedrijf. Alle met een hoofdletter geschreven termen die in deze kennisgeving worden gebruikt maar niet gedefinieerd zijn hebben de betekenis die daaraan is gegeven in de Global Information Security Policy documents (documenten over Wereldwijd informatieveiligheidsbeleid) van het Bedrijf.

Voor communicatie door bepaalde gereguleerde medewerkers van het Bedrijf gelden bijkomende specifieke vereisten qua toezicht en wij vragen Geautoriseerde gebruikers het relevante beleid en de relevante procedures die van toepassing zijn op hun bedrijfsonderdeel na te zien voor meer informatie.

Alle elektronische communicaties, waaronder e-mails (versleuteld en niet-versleuteld) en bezoeken aan internet- en intranetsites waarbij computers of het netwerk van het Bedrijf worden gebruikt zijn eigendom van het Bedrijf en kunnen onder toezicht worden gehouden of gecontroleerd worden.

Onder voorbehoud van de toepasselijke wetgeving, omvat dit onder meer:

- **Toezichtsactiviteiten uitvoeren zonder voorafgaande kennisgeving ('geheim toezicht'), in omstandigheden waar het is toegestaan dit te doen (bijvoorbeeld wanneer er een vermoeden bestaat van gegevensuitwisseling, criminele of andere onwettige activiteiten of inbreuk op het Nalevings- of Wereldwijde informatiebeveiligingsbeleid van het Bedrijf of enige andere verplichting jegens het Bedrijf);**
- **Toezicht houden op en/of blokkeren van in- en uitgaande e-mails en andere berichten, aangemerkt om aan te geven dat ze persoonlijk of privé zijn of anderszins van persoonlijke aard, waarbij er een vermoeden bestaat dat dergelijke e-mails en de inhoud of bijlagen ervan in overtreding of inbreuk zijn met de toepasselijke wetgeving of de Beleidsvoorschriften van het Bedrijf inzake Naleving of Wereldwijde Informatiebeveiliging of van gelijk welke andere aan het Bedrijf verschuldigde verplichting.**

INZAMELING VAN PERSOONSGEGEVENS EN GEBRUIKSDOELEINDEN

Bepaalde toezichtsactiviteiten van de elektronische systemen en apparaten van het Bedrijf worden in het hele Bedrijf uitgeoefend voor de doelstellingen zoals uiteengezet in Bijlage A van deze Kennisgeving.

De categorieën Persoonsgegevens die het Bedrijf kan verwerken bij het uitvoeren van de in deze Kennisgeving geschetste controle en de rechtsgronden voor een dergelijke verwerking (met inbegrip van toestemming, waar nodig) zijn zoals uiteengezet in de relevante DPN.

GEVOELIGE PERSOONSGEGEVENS

Het Bedrijf kan bepaalde speciale categorieën Persoonsgegevens verzamelen en verwerken, waaronder Gevoelige Persoonsgegevens zoals uiteengezet in de relevante DPN, in de loop van het uitvoeren van de in deze Kennisgeving beschreven activiteiten.

Toezichtsactiviteiten voor wereldwijde informatiebeveiliging houden niet actief toezicht op Gevoelige Persoonsgegevens, maar sommige Gevoelige Persoonsgegevens kunnen onvermijdelijk worden bekendgemaakt tijdens het toezicht op andere soorten gegevens.

TOEGANG DOOR PERSONEEL VAN HET BEDRIJF

De toegang tot Persoonsgegevens die overeenkomstig deze Kennisgeving worden verwerkt, is beperkt tot

de personen die deze toegang nodig hebben voor de in Bijlage A vermelde doeleinden. Naast de personen die in de desbetreffende DPN worden genoemd, wordt toegang verleend op basis van het strikte "need-to-know"-beginsel, en tot beperkte leden van de afdeling Wereldwijde Informatiebeveiliging en, waar nodig, Interne Bedrijfsonderzoeken.

BEKENDMAKING

De hulpmiddelen en processen voor toezicht beschreven in deze Kennisgeving kunnen gebruikt worden door de teams van Wereldwijde Informatiebeveiliging van het Bedrijf en haar filialen en kantoren, waaronder die in de VS, het VK, Singapore, Hongkong en India, evenals binnen het specifieke land/de regio waar de activiteiten plaatsvinden. Persoonsgegevens kunnen worden opgeslagen in het eigen rechtsgebied van de Geautoriseerde gebruiker en/of andere jurisdicties waar het Bedrijf vestigingen heeft.

Aangezien het Bedrijf wereldwijd actief is, kan het Bedrijf uw Persoonsgegevens overdragen naar landen buiten uw thuisland, zoals uiteengezet in de relevant DPN.

Het Bedrijf kan in overeenstemming met de toepasselijke wet relevante Persoonsgegevens aan haar filialen en kantoren bekendmaken, en deze kunnen dergelijke Persoonsgegevens verwerken voor de doeleinden die in deze Kennisgeving zijn uiteengezet. Daarnaast kan het Bedrijf, in overeenstemming met de toepasselijke wetgeving, relevante Persoonsgegevens bekendmaken aan bepaalde derden zoals uiteengezet in relevante DPN.

BEVEILIGING

Het Bedrijf treft de nodige technische en organisatorische maatregelen om de Persoonsgegevens te beschermen tegen onrechtmatige of onwettige verwerking en/of tegen onopzettelijk verlies, wijziging, bekendmaking of toegang of onopzettelijke of onwettige vernietiging of beschadiging van Persoonsgegevens.

MODALITEITEN VAN DE GEGEVENSVERWERKING EN -BEWARING

Bij de verwerking van Persoonsgegevens voor de in deze Kennisgeving uiteengezette doeleinden, maakt het Bedrijf geen gebruik van geautomatiseerde besluitvorming over processen van Geautoriseerde gebruikers, wanneer het besluit een juridisch of een soortgelijk significant effect zou hebben op de geautoriseerde gebruiker bij het uitvoeren van toezicht zoals beschreven in deze Kennisgeving. 'Geautomatiseerde besluitvorming' is het proces waarbij op geautomatiseerde wijze en zonder menselijke tussenkomst een besluit wordt genomen.

De bewaarperiodes voor elk type gegevens en rechtsgebied worden beschreven in het Global Records Retention Schedule op de pagina Global Records Management op Flagscape. De bewaarvereisten zijn op verzoek beschikbaar voor nieuwe Geautoriseerde gebruikers die nog geen toegang hebben tot de interne site. Het Bedrijf zal na de toepasselijke bewaarperiode de Persoonsgegevens wissen.

SANCTIES

Er kan onderzoek worden ingesteld naar Geautoriseerde gebruikers die het beleid overtreden waarnaar wordt verwezen in deze Kennisgeving. Tevens kan hen de toegang (tijdelijk) worden ontzegd en/of kunnen er sancties worden getroffen (met in het uiterste geval beëindiging van het arbeidscontract of de contractuele diensten). Geautoriseerde gebruikers die geen werknemers zijn, kunnen voor sancties worden doorverwezen naar hun werkgever. Geautoriseerde gebruikers die de toepasselijke wet- of regelgeving overtreden kunnen worden doorverwezen naar wetshandhavende en/of regelgevende instanties in overeenstemming met de wettelijke en regelgevende bepalingen. Gelijk welk materiaal of bewijs geïdentificeerd via (waaronder maar niet beperkt tot) het toezicht op telefoongesprekken, e-mails en

gebruik van internet of intranet (waaronder persoonlijke gesprekken, e-mails en gebruik van internet) kunnen gebruikt worden in gelijk welke sanctieprocedures en interne of externe onderzoeken. Geautoriseerde gebruikers worden, indien gevraagd, geacht hun medewerking te verlenen aan onderzoeken, inspecties en monitorings- en opnameactiviteiten. Het weigeren mee te werken aan een veiligheidsonderzoek kan leiden tot juridische of disciplinaire stappen, waaronder de beëindiging van het arbeidscontract of de gecontracteerde diensten.

CONTACTGEGEVENS

Voor vragen of om meer informatie over deze Kennisgeving of activiteiten van Wereldwijde Informatiebeveiliging, moeten Geautoriseerde gebruikers contact opnemen met Wereldwijde Informatiebeveiliging.

Mogelijk heeft u het recht een klacht in te dienen bij de Gegevensbeschermingsautoriteit van uw land; voor toepasselijkheid en nadere informatie wordt verwezen naar de relevante DPN.

Voor vragen over lokale wetten en beperkingen kunnen Geautoriseerde gebruikers contact opnemen met hun lokale nalevingsverantwoordelijke, functionaris voor Gegevensbescherming of de juridische afdeling.

WIJZIGINGEN AAN DEZE KENNISGEVING

Deze Kennisgeving houdt geen contractuele verplichting in en het Bedrijf behoudt zich het recht voor de Kennisgeving gelijk wanneer te wijzigen of in te trekken. Moest het Bedrijf substantiële wijzigingen aanbrengen aan deze Kennisgeving, zal het Geautoriseerde gebruikers zo snel als redelijk mogelijk daarvan op de hoogte brengen door een herwerkte Kennisgeving uit te geven en/of door andere stappen te nemen in overeenstemming met de toepasselijke wetten.

Gerelateerde documenten

Gedragscode

Bijhouden van elektronische communicatie - Ondernemingsbeleid

Beleidsdocumenten inzake Wereldwijde informatiebeveiliging

Harassment & Discrimination Prevention – Enterprise Policy (Bedrijfsbeleid intimidatie- en discriminatiepreventie)

Reputational Risk – Enterprise Policy (Bedrijfsbeleid reputatierisico)

Violence Free Workplace – Enterprise Policy (Bedrijfsbeleid geweldsvrije werkplek)

Kennisgeving inzake Informatiebeveiligingstoezicht - Flagscape

Ga voor bijkomende beleidsvoorschriften, normen en richtlijnen naar Global Policy Source Flagscape page. (Flagscape-pagina met wereldwijde beleidsregels).

BIJLAGE A

Raadpleeg de hier gelinkte matrix om de categorieën van gegevens te bekijken die kunnen worden verzameld voor elk gebruiksdoel, hieronder samengevat. De matrix is op verzoek beschikbaar voor nieuwe Geautoriseerde gebruikers die nog geen toegang hebben tot de interne site.

De Communicaties en Dossiers (zowel live als na het voorval) waar we toezicht op houden op de elektronische systemen en apparaten van het Bedrijf en waaruit we Persoonsgegevens kunnen verzamelen, omvatten, maar zijn niet beperkt tot:

- Verzonden e-mails;
- Ontvangen e-mails;
- gebruik web / internet, FTP, HTTP, HTTPS, Telnet;
- Afdrukgebruik;
- Bestanden die zich bevinden op het bureaublad (buiten Mijn documenten), samenwerkingssites, gedeelde openbare ruimtes, interne wiki's;
- verwijderbare media, apparaten die niet door het Bedrijf worden beheerd en die verbonden zijn met het systeem van het Bedrijf;
- Instant messaging;
- telefoongesprekken, VOIP-gesprekken, voicemails;
- logboeken en dossiers inzake toegang tot en gebruik van toepassingen;
- logboeken en dossiers inzake toegang tot en gebruik van systemen (waaronder dossiers die het verloop van het gebruik en gedrag tonen);
- faxen en scannen/beelden maken van documenten;
- gebruik en inhoud van sociale media (extern, niet van het Bedrijf);
- open-source en openbaar beschikbare informatie;
- beveiligingslogboeken;
- belangrijke logs en screenshots;
- Conferentietechnologieën;
- cookies, Beacons, Sinkholes en Honeypots;
- GPS, Wi-Fi tracking en locatiegegevens;
- swipe Card invoergegevens;
- verzonden en ontvangen tekstberichten.

De doeleinden waarvoor we Persoonsgegevens kunnen verzamelen, gebruiken, overdragen en bekendmaken:

Het Wereldwijd informatiebeveiligingsbeleid is ontworpen om de noodzakelijke vereisten te bieden die het Bedrijf in staat moeten stellen zich voor te bereiden op toenemende veranderingen in het bedreigingslandschap en deze te voorkomen, op te sporen, erop te reageren en ervan te herstellen. Het Wereldwijd informatiebeveiligingsprogramma biedt oplossingen en maakt gebruik van geavanceerde technieken om te voorkomen dat bedreigingen voor de informatiebeveiliging het vertrouwen van klanten

ondermijnen en de bedrijfsactiviteiten verstoren. Wereldwijde informatiebeveiliging beschermt het Bedrijf en zijn klanten door gebruik te maken van een op risico gebaseerd en resultaatgericht kader.

- Voorbereiden: We beschermen door het informatiebeveiligingsprogramma voortdurend bij te werken, waaronder het naleven van lokale of buitenlandse staats- en/of landspecifieke wetten om beter te anticiperen op potentiële bedreigingen en deze te identificeren;
- Voorkomen: We beschermen door tegenstanders voor te blijven door middel van preventieve controles om verlies, misbruik en ongepast gebruik van vertrouwelijke en eigendomsrechtelijk beschermde informatie te voorkomen en het aantal incidenten te verminderen;
- Opsporen: We beschermen door blootstelling te beperken door de implementatie van detectieve controles, waaronder firewalltoezicht, anti-spam- en virusbescherming en ander toezicht; continu toezicht van alle bankteamgenoten, toepassingen, gegevens, systemen en netwerken;
- Beperken: We beschermen door incidenten te beperken door middel van een flexibele en gecoördineerde responscapaciteit;
- Reageren/herstellen: We beschermen door de beveiligingsstatus te verbeteren door middel van robuuste forensische onderzoeken en geleerde lessen, terwijl we alle nalevingskwesties, regelgevende vragen, disciplinaire maatregelen of juridische claims aanpakken.

BIJLAGE B

Spanje

In Spanje, overeenkomstig de inhoud van art. 20 of Real Decreto Legislativo 2/2015, de 23 de octubre, Texto Refundido del Estatuto de los Trabajadores (wetgevend Koninklijk Besluit 2/2015, van 23 oktober, inzake het Spaanse arbeidersstatuut) behoudt het Bedrijf zich het recht voor om gelijk welke middelen te gebruiken, op voorwaarde dat dergelijke middelen proportioneel zijn om de naleving van arbeidsverplichtingen door werknemers inzake het gebruik van computeruitrusting en het internet te verifiëren.

De Russische Federatie

Deze Kennisgeving inzake Informatiebeveiligingstoezicht is van toepassing voor zover ze niet in strijd is met de wetgeving van de Russische Federatie, met inbegrip van maar niet beperkt tot de Federale Wet nr. 152-FZ "Persoonsgegevens" van 27 juli 2006 en het beleid en de voorschriften inzake gegevensbescherming van OOO Merrill Lynch Securities.

Griekenland

Deze Kennisgeving inzake Informatiebeveiligingstoezicht is van toepassing voor zover ze niet in strijd is met de wet- en regelgeving in Griekenland, in het bijzonder de Griekse wet 2472/1997 "Bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens" en de Griekse wet 3471/2006 "Bescherming van persoonsgegevens en de persoonlijke levenssfeer in de elektronische telecommunicatiesector en wijziging van wet 2472/1997", alsook specifieke besluiten van de Griekse Gegevensbeschermingsautoriteit.

Qatar

Deze Kennisgeving inzake informatiebeveiligingstoezicht is van toepassing voor zover ze niet in strijd is met de wet- en regelgeving in Qatar, met inbegrip van maar niet beperkt tot de QFC Data Protection Regulations and Rules 2005 en het interne beleid en de vereisten inzake gegevensbescherming van Merrill Lynch International - QFC Branch.

Verenigde Arabische Emiraten

Deze Kennisgeving inzake informatiebeveiligingstoezicht is van toepassing voor zover ze niet in strijd is met de wet- en regelgeving in DIFC, met inbegrip van maar niet beperkt tot de Data Protection Law DIFC Law No. 5 van 2020 en DIFC Amendment Law DIFC Law No. 2 van 2022, alsmede het interne beleid en de vereisten inzake gegevensbescherming van Merrill Lynch International (DIFC Branch).

AVIS DE SURVEILLANCE DE LA SÉCURITÉ DES INFORMATIONS - French

Version Française

Avec effet au: 3rd April 2023

INTRODUCTION

L'entité juridique désignée dans le contrat de travail de l'Employé, ou dans la mission du Sous-traitant (la « **Société** ») a rédigé le présent Avis de surveillance de la sécurité des informations[5] (l'« **Avis** ») pour compléter l'Avis de protection des données des employés et des sous-traitants (le « **DPN** ») que vous recevez en tant qu'employé ou sous-traitant pour exposer ses pratiques concernant la surveillance des données et autres éléments (y compris mais non exclusivement, les messages[6], communications et informations professionnelles et personnelles) transmis, reçus, traités et/ou stockés par les systèmes et appareils électroniques de la Société. Ceux-ci incluent, sans s'y limiter, le réseau, le système vocal, l'ordinateur, les appareils mobiles fournis par la Société, la messagerie instantanée, les applications web, les applications mobiles, les médias sociaux, l'audioconférence, la vidéoconférence et la télécopie (« **Communications électroniques** »), l'utilisation des imprimantes, Internet et les journaux d'accès physique.

Cet Avis concerne tous les individus ou groupes auxquels on a accordé l'accès aux systèmes, locaux et informations de la Société à des fins d'affaires ou pour des fonctions de supervision, y compris les employés, les consultants, les fournisseurs, directeurs non exécutifs et autres collaborateurs de la Société (chacun étant un « **Utilisateur autorisé** »). L'Annexe A présente une liste non exhaustive des communications et des documents que nous surveillons et à partir desquels nous pouvons recueillir des informations personnellement identifiables sur les Utilisateurs autorisés (« **Données à caractère personnel** »), ainsi que les fins pour lesquelles nous pouvons utiliser, transférer et divulguer ces Données à caractère personnel. Les Utilisateurs autorisés de pays spécifiques doivent consulter l'Annexe B.

Au cas où le présent Avis serait fourni à un Utilisateur autorisé dans une langue autre que l'anglais, tout écart, incohérence ou conflit entre les deux versions linguistiques doit être résolu comme indiqué dans le DPN concerné.

Indépendamment du lieu, les outils et processus de surveillance sont systématiquement appliqués par la Société à ses systèmes et appareils électroniques dans la mesure autorisée par la législation et réglementation locale. Toutes les activités de surveillance appliquées aux systèmes et appareils électroniques de la Société sont menées conformément au présent Avis.

Toutes les Données à caractère personnel recueillies dans le cadre des processus de surveillance sont traitées conformément au DPN concerné tel que publié ponctuellement. Le traitement des Données à caractère personnel s'effectue à l'aide d'outils manuels et électroniques.

Le présent Avis fait référence aux principaux volets des politiques de la Société concernées, mais ne contient pas toutes les politiques et exigences de la Société relatives à l'usage des Communications électroniques et

[5] L'Avis de surveillance de la sécurité des informations (Information Security Monitoring Notice, ISMN), s'intitulait auparavant « l'Avis de surveillance en matière de cybersécurité » (Cyber Security Monitoring Notice, CSMN) et peut également être mentionné comme tel dans d'autres documents de la Société.

[6] Conformément au Code de conduite, les utilisateurs autorisés sont en droit d'utiliser de manière limitée, à des fins personnelles, les appareils et applications gérés par la Société, ainsi que l'Internet et la messagerie électronique pour leurs communications personnelles. L'utilisation des ressources peut être contrôlée et inspectée pour veiller à ce que l'intégrité des systèmes soit préservée (par ex., contrôler l'introduction de logiciels malveillants ou de transmissions de données inappropriées) et éviter les activités susceptibles de donner lieu à une responsabilité ou à un risque de la part de la société.

de l'Internet. Les Utilisateurs autorisés se doivent de se conformer aux exigences énoncées dans les documents de la Société, Code de conduite, Guide des communications électroniques et Politique du Service international de sécurité des informations, ainsi qu'à toute autre norme applicable établie ponctuellement par la Société . Tous les termes débutant par une majuscule utilisés mais non définis dans le présent Avis ont la signification qui leur est attribuée dans les documents relatifs à la politique du Service international de sécurité des informations de la Société.

Les communications d'un certain personnel régulé de la Société sont sujettes à des exigences de suivi détaillées supplémentaires et les Utilisateurs autorisés sont priés de consulter les politiques correspondantes pour leur domaine d'affaires pour plus d'informations.

Toutes les communications électroniques, notamment les e-mails (chiffrés ou non) et les connexions aux sites Web et Intranet via les ressources informatiques et réseau de la Société sont la propriété de la Société et peuvent être soumises au suivi et à la surveillance.

Sous réserve des lois applicables, cela comprend notamment, sans s'y limiter:

- **mener des activités de surveillance sans avis préalable (« surveillance discrète »), dans des situations où cela est permis (en cas de soupçon d'exfiltration de données, d'activités criminelles ou illégales par exemple, ou de violation des Politiques de la Société relatives à la conformité ou au Service international de sécurité des informations, ou de toute autre obligation envers la Société) ;**
- **surveiller et/ou bloquer les courriels entrants et sortants et autres messages portant une indication de contenu personnel ou privé, ou sur présomption que lesdits courriels et leurs contenus ou pièces jointes enfreignent la législation en vigueur ou les Politiques de la Société relatives à la conformité ou au Service international de sécurité des informations, ou toute autre obligation envers la Société.**

COLLECTE DES DONNÉES À CARACTÈRE PERSONNEL ET FINALITÉS DE TRAITEMENT

Certaines activités de surveillance des systèmes et appareils électroniques de la Société sont exercées dans l'ensemble de la Société aux fins énoncées à l'Annexe A du présent Avis.

Les catégories de Données à caractère personnel que la Société peut traiter lors du processus de surveillance décrit dans le présent Avis, ainsi que les fondements juridiques de ce traitement (y compris le consentement, le cas échéant), sont définis dans le DPN concerné.

DONNÉES À CARACTÈRE PERSONNEL SENSIBLES

Dans le cadre des activités décrites dans le présent Avis, la Société peut recueillir et traiter certaines catégories particulières de Données à caractère personnel, notamment des Données à caractère personnel sensibles, comme indiqué dans le DPN concerné.

Le Service international de sécurité des informations ne surveille pas activement les Données à caractère personnel sensibles, mais certaines Données à caractère personnel sensibles sont fortement susceptibles d'être visibles dans le cadre de la surveillance d'autres types de données.

ACCÈS PAR LE PERSONNEL DE LA SOCIÉTÉ

L'accès aux Données à caractère personnel traitées conformément au présent Avis est limité aux personnes nécessitant ledit accès aux fins énumérées en Annexe A. Outre les personnes mentionnées dans le DPN concerné, l'accès sera accordé en cas de nécessité absolue aux membres du Service international de sécurité des informations et, le cas échéant, aux membres du service chargé des enquêtes internes de la Société.

DIVULGATION

Les outils et processus de surveillance décrits au présent Avis sont susceptibles d'être appliqués par les équipes du Service international de sécurité des informations de la Société ou de ses sociétés affiliées ou succursales, notamment celles situées aux États-Unis, au Royaume-Uni, à Singapour, à Hong Kong et en Inde, ainsi que dans le pays ou la région d'exploitation concernés. Les Données à caractère personnel peuvent être stockées dans la juridiction du pays de l'Utilisateur autorisé et/ou dans d'autres juridictions où la Société exerce ses activités.

Compte tenu de la nature internationale des activités de la Société, celle-ci est par conséquent susceptible de transférer les Données à caractère personnel vous concernant vers des pays situés en dehors de votre pays d'origine, comme indiqué dans le DPN concerné.

Conformément à la loi en vigueur, la Société pourra divulguer certaines Données à caractère personnel à ses sociétés affiliées et succursales, lesquelles pourront traiter lesdites Données à caractère personnel aux fins énoncées dans le présent Avis. En outre, la Société peut divulguer, conformément à la législation en vigueur, des Données à caractère personnel pertinentes à certains tiers, comme indiqué dans le DPN concerné.

SÉCURITÉ

La Société a mis en place les mesures techniques et organisationnelles appropriées afin d'empêcher le traitement non autorisé ou illicite des Données à caractère personnel, leur perte, destruction ou altération accidentelle, ainsi que l'accès et les dommages accidentels ou illicites à celles-ci.

MODALITÉS DU TRAITEMENT ET DE LA CONSERVATION DES DONNÉES

Lors du traitement des Données à caractère personnel aux fins énoncées dans le présent Avis, la Société ne recourt pas à la prise de décision automatisée pour les processus relatifs aux Utilisateurs autorisés lorsque la décision pourrait avoir sur ceux-ci des répercussions légales ou des effets d'importance similaire dans le cadre de la surveillance telle que décrite dans le présent Avis. La « prise de décision automatisée » est le processus de prise de décision par des moyens automatisés sans aucune intervention humaine.

Les périodes de conservation pour chaque type de données et de juridiction sont décrites dans le Calendrier mondial de conservation des documents consultable sur la page Gestion internationale des documents de Flagscape. Les exigences de conservation sont disponibles sur demande pour les nouveaux Utilisateurs autorisés qui n'ont pas encore accès au site interne. La Société supprimera les Données à caractère personnel après la période de conservation applicable.

MESURE DISCIPLINAIRE

Les utilisateurs autorisés qui enfreignent toute politique indiquée dans le présent Avis peuvent faire l'objet d'une enquête, une suspension du droit d'accès et/ou des procédures disciplinaires (allant jusqu'à la cessation d'emploi ou des services sous contrat). Les utilisateurs autorisés qui ne sont pas des employés peuvent faire l'objet d'un renvoi à leur employeur pour mesure disciplinaire. Les utilisateurs autorisés qui enfreignent les lois et les réglementations en vigueur peuvent être adressés aux responsables de l'application des lois et/ou des réglementations, conformément aux exigences des lois et des réglementations. Tout document ou preuve identifié [notamment mais sans s'y limiter) la surveillance des appels téléphoniques, des e-mails et de l'utilisation d'Internet ou de l'intranet (notamment les appels téléphoniques personnels, les e-mails et l'utilisation d'Internet] peut être invoqué lors de toutes mesures disciplinaires et d'enquêtes internes ou externes. Les utilisateurs autorisés doivent coopérer dans les activités d'enquête, de contrôle, de suivi et d'enregistrement si on leur demande. Le refus de coopérer dans une enquête de sécurité peut entraîner une action légale ou disciplinaire, y compris la cessation d'emploi ou de services contractuels.

COORDONNÉES

Pour toute question ou pour obtenir de plus amples informations sur cet Avis, ou sur les activités de surveillance de la sécurité globale des informations, les Utilisateurs autorisés doivent contacter le Département de Sécurité Globale des Informations.

Vous pourriez avoir le droit de déposer une plainte auprès de l'autorité chargée de la protection des données de votre pays. Pour connaître les modalités d'application et obtenir de plus amples informations, veuillez consulter l'Avis de protection des données (DPN) pertinent.

En cas de questions concernant les lois et les restrictions locales, les utilisateurs autorisés sont priés de contacter leur responsable de conformité, Responsable de la protection des données ou leur service juridique.

MODIFICATIONS AU PRÉSENT AVIS

Cet Avis n'est pas contractuel et la Société se réserve le droit de modifier ou de retirer l'Avis à tout moment. Si la Société apporte des changements substantiels à cet Avis, elle en informera les Utilisateurs autorisés dès que possible, en rediffusant un Avis revu et/ou en prenant d'autres mesures conformément aux lois en vigueur.

Documents associés

Code de conduite

Conservation des communications électroniques - Politique de l'entreprise

Documents de la Politique du Service international de sécurité des informations

Politique de l'entreprise relative à la prévention du harcèlement et de la discrimination

Reputational Risk – Enterprise Policy (Politique de l'entreprise sur le risque de réputation)

Violence Free Workplace – Enterprise Policy (Politique de l'entreprise pour un milieu de travail sans violence)

Avis de surveillance de la sécurité des informations - Flagscape

Pour consulter les politiques, les normes et les directives supplémentaires, veuillez vous rendre sur la page Global Policy Source Flagscape.

ANNEXE A

Reportez-vous à la matrice (cliquez sur le lien) pour afficher les catégories de données qui peuvent être collectées pour chaque objectif d'utilisation, résumées ci-dessous. La matrice est disponible sur demande pour les nouveaux Utilisateurs autorisés qui n'ont pas encore accès au site interne.

Les Communications et Dossiers (aussi bien en direct qu'après l'événement) que nous surveillons sur les systèmes et appareils électroniques de la Société et auprès desquels nous sommes susceptibles de collecter des Données à caractère personnel incluent sans s'y limiter :

- les courriels envoyés ;
- les courriels reçus ;
- l'utilisation du Web / Internet, FTP, HTTP, HTTPS, Telnet ;
- l'utilisation d'imprimantes ;
- les fichiers sont situés sur le bureau (hors de Mes documents), sur des sites de collaboration, des sites de partage, des Wiki internes ;
- les dispositifs amovibles, dispositifs non gérés par la Société se connectant au système de la Société ;
- la messagerie instantanée ;
- les appels téléphoniques, les appels VOIP, les messages vocaux ;
- les dossiers et journaux d'accès et d'utilisation des applications ;
- les dossiers et journaux d'accès et d'utilisation du système (notamment les dossiers indiquant le cours de l'utilisation et de la conduite) ;
- la télécopie et numérisation de documents / Imagerie ;
- l'utilisation et le contenu des médias sociaux (externe, hors Société) ;
- les informations open source et disponibles publiquement ;
- les journaux de sécurité ;
- les registres de clés et les captures d'écran ;
- les technologies de conférence ;
- les cookies, balises, Sinkholes (puisards) et Honeypots (pots de miel) ;
- les données GPS, de traçage Wi-Fi et de localisation ;
- les données de carte magnétique d'entrée ;
- les messages texte envoyés et reçus.

Nous pouvons collecter, utiliser, transférer et divulguer des Données à caractère personnel aux fins suivantes :

La Politique du Service international de sécurité des informations est conçue pour fournir les exigences nécessaires pour permettre à la Société de se préparer, de prévenir, de détecter, de répondre et de se rétablir des changements croissants en matière de menaces. Le Programme international de sécurité des informations fournit des solutions et utilise des techniques avancées pour empêcher les menaces à la sécurité des informations de nuire à la confiance des clients et de perturber les opérations commerciales. Le Service international de sécurité des informations protège la Société et ses clients en utilisant une

structure axée sur les risques et les résultats.

- Se préparer : nous protégeons en mettant continuellement à jour le Programme de sécurité des informations, qui comprend le respect des lois locales ou étrangères spécifiques à un État ou à un pays afin de mieux anticiper et identifier les menaces potentielles.
- Prévenir : nous protégeons en gardant une longueur d'avance sur nos adversaires grâce au déploiement de contrôles préventifs visant à réduire le nombre d'incidents et prévenir la perte, ainsi que l'utilisation abusive et inappropriée d'informations confidentielles et exclusives.
- Détecter : nous protégeons en limitant l'exposition par le déploiement de contrôles de détection, y compris la surveillance des pares-feux, les protections anti-spam et anti-virus, et d'autres fonctions de surveillance ; la surveillance continue de tous les collaborateurs, de toutes les applications, de toutes les données, de tous les systèmes et de tous les réseaux de la banque.
- Atténuer : nous protégeons en atténuant les incidents grâce à une capacité de réponse agile et coordonnée.
- Répondre/Se rétablir : nous protégeons en améliorant le dispositif de sécurité par le biais d'une solide criminalistique, d'enquêtes et d'enseignements tirés de l'expérience, tout en traitant tout problème de conformité, enquête réglementaire, action disciplinaire ou action en justice.

ANNEXE B

Espagne

En Espagne, conformément au contenu de l'art. 20 du Real Decreto Legislativo 2/2015, de 23 de octubre, Texto Refundido del Estatuto de los Trabajadores (Décret Royal Législatif 2/2015, du 23 octobre, sur le statut des travailleurs espagnols), la Société se réserve le droit de faire appel à tous les moyens nécessaires, à condition que ces moyens soient proportionnés, pour vérifier le respect par l'employé de ses obligations professionnelles en rapport avec l'utilisation du matériel informatique et de l'Internet.

La Fédération de Russie

Le présent Avis de surveillance de la sécurité des informations est applicable dans la mesure où il ne contredit pas la législation de la Fédération de Russie, notamment la loi fédérale n° 152-FZ sur les « Données personnelles » du 27 juillet 2006, ainsi que les politiques et réglementations de OOO Merrill Lynch Securities en matière de protection des données.

Grèce

Le présent Avis de surveillance de la sécurité des informations est applicable dans la mesure où il ne contredit pas les lois et réglementations grecques en vigueur, en particulier la loi grecque 2472/1997 « Protection des personnes à l'égard du traitement des Données à caractère personnel » et la loi grecque 3471/2006 « Protection des données à caractère personnel et de la vie privée dans le secteur des télécommunications électroniques et modification de la loi 2472/1997 », ainsi que les décisions rendues dans des cas spécifiques par l'Autorité hellénique de protection des données.

Qatar

Le présent Avis de surveillance de la sécurité des informations est applicable dans la mesure où il ne contredit pas les lois et réglementations du Qatar, y compris, notamment, les réglementations et règles de protection des données 2005 du QFC, ainsi que les politiques et exigences internes de la succursale QFC de Merrill Lynch International en matière de protection des données.

Émirats arabes unis

Le présent Avis de surveillance de la sécurité des informations est applicable dans la mesure où il ne contredit pas les lois et réglementations du DIFC, y compris, notamment, la loi sur la protection des données n° 5 de 2020 du DIFC et la Loi n° 2 modifiée du DIFC de 2022, ainsi que les politiques et exigences internes de protection des données de Merrill Lynch International (Succursale DIFC).

BİLGİ GÜVENLİĞİ İZLEME BİLDİRİMİ - Turkish

Türkçe Versiyon

Geçerli: 3rd April 2023

GİRİŞ

Çalışanın iş akdinde veya Yüklenicinin taahhüdünde adı belirtilen tüzel kişilik ("**Şirket**") işbu Bilgi Güvenliği İzleme Bildirimini[7] ("**Bildirim**") çalışan veya yüklenici olarak aktarılan, alınan, işlenen ve/veya Şirketin elektronik sistemlerinde ve cihazlarında saklanan verileri ve diğer materyalleri (iş ve kişisel[8] mesajlar, iletişimler ve bilgiler dahil ancak bunlarla sınırlı olmamak üzere) izlemek ile ilgili uygulamaları ortaya koyan Çalışan ve Yüklenici Veri Koruma Bildirimi ("VKB") belgesine ek olarak hazırlamıştır. Bu elektronik sistemler, ağ, ses, bilgisayar, şirket tarafından verilen mobil cihazlar, anlık mesajlaşma, web uygulamaları, mobil uygulamalar, sosyal medya, sesli konferans, görüntülü konferans ve faks altyapısı ("**Elektronik İletişimler**"), yazıcı kullanımı, İnternet ve fiziksel erişim günlüklerini içerir ancak bunlarla da sınırlı değildir.

Bu Bildirim, Şirketteki personel, danışmanlar, yükleniciler, icrada görevi olmayan yöneticiler ve diğer çalışanlar dahil olmak üzere (her biri "**Yetkili Kullanıcı**" olan), iş amacı için veya danışmanlık işleviyle Şirketin sistemlerine, tesislerine ve/veya bilgilerine erişim sağlanmış olan tüm kişiler ya da gruplar için geçerlidir. Ek A, izlediğimiz ve Yetkili Kullanıcılar hakkında kişisel olarak tanımlanabilir bilgileri ("**Kişisel Bilgiler**") toplayabileceğimiz iletişim ve kayıtların kapsamlı olmayan bir listesini ve kişisel verileri kullanabileceğimiz, aktarabileceğimiz ve ifşa edebileceğimiz amaçları ortaya koymaktadır. Ek B'ye, belirli ülkelerdeki Yetkili Kullanıcılar tarafından başvurulmalıdır.

Bu Bilgilendirmenin İngilizce dili dışında bir dilde bir Yetkili Kullanıcıya sağlanması durumunda, iki dil sürümü arasındaki herhangi bir farklılık, çatışma veya tutarsızlık ilgili VKB içerisinde belirtilen şekilde çözümlenecektir.

Konumdan bağımsız olarak, izleme araçları ve süreçleri Şirket tarafından rutin bir şekilde Şirketin elektronik sistemlerine ve cihazlarına yerel yasalar ve yönetmelikler kapsamında yasaklı olmadığı ölçüde kurulur. Şirketin elektronik sistemlerinde ve cihazlarında gerçekleştirilen tüm izleme faaliyetleri bu Bildirim uyarınca gerçekleştirilir.

İzleme süreçleri seyrinde toplanan her türlü Kişisel Bilgi, zaman zaman yayınlandığı şekilde ilgili VKB doğrultusunda ele alınacaktır. Kişisel Bilgilerin işlenmesi manuel ve elektronik araçlarla yürütülür.

Bu bildirim, Şirketin ilgili politikalarının önemli kısımlarına atıfta bulunur, ancak Şirketin Elektronik İletişimlerin ve İnternetin kullanımı için geçerli olan politikaları ve gerekliliklerinin hepsini içermez. Yetkili Kullanıcılar, Şirketin Mesleki Davranış Kuralları, Elektronik İletişimler Kılavuzu_ve Küresel Bilgi Güvenliği Politikası_belgelerinde yer alan gereklilikler ile beraber muhtelif zamanlarda Şirket tarafından yayınlanan diğer geçerli standartlara uymalıdır. Bu Bildirimde büyük harfle yazılan ancak tanımlanmış olmayan tüm terimler, kendilerine Şirketin Küresel Bilgi Güvenliği Politikası belgelerinde verilen anlamlara sahiptir.

Düzenlemeye tabi belirli Şirket personelinin iletişimleri ilave ayrıntılı denetleme gerekliliklere tabidir ve

[7] Bilgi Güvenliği İzleme Bildirimi (BGİB) daha önce Siber Güvenlik İzleme Bildirimi (SGİB) olarak adlandırılmaktaydı; dolayısıyla, şirketin diğer belgelerinde adı bu şekilde geçebilir

[8] Mesleki Davranış Kuralları doğrultusunda, yetkili kullanıcıların, şirket tarafından yönetilen cihazları ve uygulamaları, İnternet'i ve kişisel iletişimleri için e-postayı şahsi olarak kullanmalarına sınırlı şekilde izin verilir. Kaynakların kullanımı, sistemlerin bütünlüğünün sağlanması (ör. kötü amaçlı yazılımların kullanımının izlenmesi veya uygun olmayan veri aktarımı) ve şirketi sorumluluk ya da risk altına sokacak faaliyetlerin önlenmesi için izlenebilir ve denetlenebilir.

Yetkili Kullanıcılara daha fazla bilgi için kendi iş kollarına ait olan ilgili politika ve prosedürlere başvurmaları hatırlatılmaktadır.

Şirketin bilgisayar ve ağ kaynakları kullanılarak yapılan, e-postalar (şifrelenmiş veya şifrelenmemiş) ve İnternet ile İnternet web sitelerine bağlantılar dahil olmak üzere tüm Elektronik İletişimler Şirketin mülküdür ve izleme ile gözetime tabi tutulabilir.

Geçerli yasalara tabi olarak bu, aşağıdakileri içerir ancak bunlarla sınırlı değildir:

- **Bildirim vermeden izleme faaliyetleri gerçekleştirme ("örtülü izleme"), bu faaliyetlerin gerçekleştirilmesine izin verilen durumlarda, (örneğin, suç teşkil eden veya diğer ciddi yasa dışı faaliyetler ya da Bank of America'nın Uyum veya Küresel Güvenlik Politikalarının ihlali veya Şirkete karşı sorumlu olunan diğer yükümlülüklerin ihlali konusunda kuvvetli şüpheler olduğunda);**
- **E-posta ya da bunların içerikleri ile eklentilerinin yasaları ya da Bank of America'nın Uyum veya Küresel Güvenlik Politikalarının ihlali veya Şirkete karşı sorumlu olunan diğer yükümlülüklerin ihlali veya bunlara aykırı hareket edilmesine yönelik bir şüphe olduğunda şahsi ya da özel veya başka bir şekilde şahsi niteliğe sahip olduğunu belirtmek için işaretlenmiş olan gelen veya giden e-postaların ya da diğer mesajlaşmaların izlenmesi ve/veya engellenmesi.**

KİŞİSEL VERİLERİN TOPLANMASI VE KULLANIM AMAÇLARI

Şirketin elektronik sistemleri ve cihazlarında gerçekleştirilen belirli izleme faaliyetleri, Şirket genelinde bu Bildirimin Ek A'da düzenlenen amaçlar doğrultusunda uygulanır.

Bu Bildirimde belirtilen izlemeyi gerçekleştirirken Şirketin işleyebileceği Kişisel Verilerin kategorileri ve bu tür bir bilgi işleme için geçerli yasal dayanak (gerekli olduğu durumlarda olur da dâhil), ilgili VKB'de belirlenmiştir.

ÖZEL NİTELİKLİ KİŞİSEL VERİLER

Şirket, bu Bildirimde açıklanan faaliyetlerin yürütülmesi sırasında, ilgili VKB'de belirlenen şekilde, Hassas Kişisel Veriler de dâhil belirli özel Kişisel Veri kategorilerindeki verileri toplayabilir ve işleyebilir.

Küresel Bilgi Güvenliği izleme faaliyetleri, Hassas Kişisel Verileri aktif olarak izlemez, ancak bazı Hassas Kişisel Veriler diğer veri türlerinin izlenmesi sırasında engellenemeyen bir şekilde ifşa edilebilir.

ŞİRKET PERSONELİNİN ERİŞİMİ

Bu Bildirim uyarınca işlenen Kişisel Verilere erişim, Ek A'da sıralanan amaçlar doğrultusunda verilere erişim ihtiyacı olan bireylerle sınırlıdır. İlgili VKB'de belirtildiği gibi bu bireylere ek olarak, bilgileri kesin olarak bilmesi gereken kişilere, Global Bilgi Güvenliği Departmanı'nın belirli çalışanlarına ve Dâhili Kurumsal Soruşturmalarda gerekli olduğu durumlarda erişim sağlanacaktır.

AÇIKLAMA

Bu Bildirimde tarif edilen izleme araçları ve süreçleri, Şirketin ve iştiraklerinin ve şubelerinin herhangi birinin ABD, Birleşik Krallık, Singapur, Hong Kong ve Hindistan'da bulunanlar dahil bunlar ile birlikte faaliyet gösterilen belli başlı ülkelerde/bölgelerde bulunan Küresel Bilgi Güvenliği ekipleri tarafından kullanılabilir. Kişisel Veriler, Yetkili Kullanıcının ülke hukuki yetki alanında ve/veya Şirketin faaliyet gösterdiği diğer hukuki yetki alanlarında saklanabilir.

Şirketin küresel nitelikteki faaliyetleri göz önüne alındığında, Şirket Kişisel Bilgilerinizi, ilgili VKB'de belirtildiği şekilde kendi ülkeniz dışındaki ülkelere aktarabilir.

Şirket, yürürlükteki yasalara uygun şekilde ilgili Kişisel Verileri iştiraklerinin ve şubelerinin herhangi birine sunabilir ve bunlar söz konusu Kişisel Verileri bu Bildirim dahilinde belirtilmiş olan amaçlar doğrultusunda işleyebilir. Ek olarak Şirket, ilgili VKB'de belirlendiği şekilde, ilgili Kişisel Verileri üçüncü taraflara geçerli yasalar doğrultusunda ifşa edebilir.

GÜVENLİK

Şirket, Kişisel Verilerin yetkisiz ya da yasa dışı biçimde işlenmesine ve/veya kazara meydana gelen kayıp, değiştirme, açıklama veya erişim ya da Kişisel Verilerin kazara veya yasa dışı olarak yok edilmesi veya hasar görmesi durumlarına karşı onları korumak için uygun teknik ve kurumsal önlemleri alır.

İŞLEME VE VERİ SAKLAMA YÖNTEMLERİ

Kişisel Verilerin bu Bildirim içerisinde belirtilen amaçlar doğrultusunda işlenmesinde, bu Bildirim içerisinde açıklanan şekilde izleme faaliyeti gerçekleştirilirken yetkili kullanıcı üzerinde yasal veya benzer şekilde önemli bir etkisi olacak kararlar için Şirket, Yetkili Kullanıcı süreçlerine yönelik olarak otomatik karar verme süreçlerini kullanmaz. "Otomatik karar alma", insan faktörünün herhangi bir dahli olmaksızın, otomatik olarak karar verme sürecine denir.

Her veri türü ve yargı yetkisi için saklama süreleri, Flagscape'deki Global Kayıt Yönetimi sayfasında bulunan Global Kayıt Tutma Programında ana hatlarıyla belirtilmiştir. Saklama gereksinimleri, henüz kurum içi siteye erişim yapmamış yeni Yetkili Kullanıcılara talebe istinaden sunulur. Şirket yürürlükteki saklama döneminden sonra Kişisel Verileri silecektir.

DİSİPLİN İŞLEMİ

Bu Bildirimde atıfta bulunulan politikalardan herhangi birini ihlal eden Yetkili Kullanıcılar, soruşturmaya, askıya almaya ve/veya disiplin işlemlerine tabi olabilir (istihdamın veya sözleşme hizmetlerinin sonlandırılmasına kadar ve bunlar dahil olmak üzere). Personelden olmayan Yetkili Kullanıcılar, disiplin işlemleri için kendi işverenlerine yönlendirilebilir. Yürürlükteki yasaları veya yönetmelikleri ihlal eden Yetkili Kullanıcılar, yasal ve düzenleyici gereklilikler uyarınca kolluk kuvvetlerine ve/veya düzenleyici memurlara yönlendirilebilir. Telefon çağrıları, e-postalar ve İnternet ya da intranet (kişisel telefon çağrıları, e-postalar ve İnternet kullanımı dahil) kullanımının (bunlar dahil ancak bunlarla sınırlı olmamak üzere) izlenmesi ile tespit edilen herhangi bir materyal ya da kanıt herhangi bir disiplin işleminde veya harici soruşturmada dayanak olarak alınabilir. Yetkili Kullanıcıların, istenmesi halinde, sorgu, teftiş, izleme ve kayıt faaliyetlerinde iş birliği yapması beklenmektedir. Bir güvenlik araştırması sürecinde iş birliğinin reddedilmesi, iş akdinin ya da sözleşme hizmetlerinin sonlandırılması dahil olmak üzere yasal işlemler ya da disiplin işlemleri ile sonuçlanabilir.

İLETİŞİM BİLGİLERİ

Bu Bildirim ya da Küresel Bilgi Güvenliği izleme faaliyetleri hakkında sorular ya da daha fazla bilgi için, Yetkili Kullanıcılar Küresel Bilgi Güvenliği ile iletişime geçmelidir.

Ülkenizdeki Veri Koruma Makamına şikâyette bulunma hakkınız olabilir; uygulanabilirlik durumu ve daha detaylı bilgi için ilgili VKB'ye bakın.

Yerel yasa ve kısıtlamalarla ilgili sorular için, Yetkili Kullanıcılar yerel uyum görevlisi, Veri Koruma Yetkilisi veya hukuk departmanı ile iletişime geçmelidir.

BU BİLGİLENDİRMEYE YÖNELİK DEĞİŞİKLİKLER

Bu Bildirim sözleşme niteliği taşımaz ve Şirket herhangi bir zamanda Bildirimi değiştirme veya geri çekme

hakkını saklı tutar. Şirketin bu Bildirimde önemli değişiklikler yapması halinde, Banka, gözden geçirilmiş bir Bildirimi yeniden yayınlamak ve/veya yürürlükteki yasalara göre başka adımlar atmak yoluyla Yetkili Kullanıcıları makul olan en erken sürede bilgilendirecektir.

İlgili Belgeler

Mesleki Davranış Kuralları

Elektronik İletişimlerin Saklanması - Kurumsal Politika

Küresel Bilgi Güvenliği Politikası belgeleri

Taciz ve Ayrımcılığın Önlenmesi - Kurumsal Politika

İtibar Riski - Kurumsal Politika

Şiddet Bulunmayan İşyeri - Kurumsal Politika

Bilgi Güvenliği İzleme Bildirimi - Flagscape

Ek politikalar, standartlar ve yönergeler için lütfen Küresel Politika Kaynağı Flagscape sayfasına bakın.

EK A

Aşağıda özetlenen her bir kullanım amacı için toplanabilecek veri kategorilerini görüntülemek üzere burada bağlantılı matrise bakın. Matris, henüz kurum içi siteye erişim yapmamış yeni Yetkili Kullanıcılara, talebe istinaden sunulur.

Kişisel Verileri toplayabileceğimiz ve Şirketin elektronik sistemleri ve cihazları üzerinden izlediğimiz İletişim ve Kayıtlar (hem canlı hem de olaydan sonra) aşağıdakileri içerir ancak bunlarla sınırlı değildir:

- Gönderilen e-posta mesajları;
- Alınan e-posta mesajları;
- Web / internet kullanımı, FTP, HTTP, HTTPS, Telnet;
- Yazdırma işleminin kullanımı;
- Masaüstünde (Belgelerim dışında), iş birliği yapılan sitelerde, açık paylaşımlarda, dahili Wiki'lerde bulunan dosyalar;
- Çıkarılabilir medya, Şirket sistemine bağlanan Şirket Dışı yönetilen cihazlar;
- Anında mesajlaşma;
- Telefon görüşmeleri, VOIP çağrıları, sesli mesajlar;
- Uygulama erişimi ve kullanım günlükleri ve kayıtları;
- Sistem erişimi ve kullanım günlükleri ve kayıtları (kullanım ve davranışı gösteren kayıtlar dahil);
- Faks ve Belge Tarama/Görüntüleme;
- Sosyal medya kullanımı ve içeriği (harici, Şirket dışı);
- Açık kaynak ve kamuya açık bilgiler;
- Güvenlik günlükleri;
- Önemli günlükler ve ekran görüntüleri;
- Konferans görüşmesi teknolojileri;
- Çerezler, İşaretler, Sinkhole ve Sanal Sunucular;
- GPS, Wi-Fi İzleme ve Konum Verileri;
- Manyetik Kart Okuyuculu Kart giriş verileri;
- Gönderilen ve alınan Kısa Mesajlar.

Kişisel Verileri Toplama, Kullanma, Aktarma ve Açıklama Amaçları:

Küresel Bilgi Güvenliği Politikası, Şirketin tehdit hususlarında artan değişikliklere hazırlanmasını, bunları önlemesini, tespit etmesini, karşılık vermesini ve bunlardan kurtulmasını sağlamak üzere gereklilikleri yerine getirmek üzere sağlanmıştır. Küresel Bilgi Güvenliği Programı, bilgi güvenliği tehditlerinin müşteri güvenine zarar vermesini ve ticari faaliyetleri kesintiye uğratmasını önlemek için çözümler sunar ve ileri teknikler kullanır. Küresel Bilgi Güvenliği, Şirketi ve müşterilerini risk bazlı ve sonuç odaklı bir çerçeve kullanarak korur.

- Hazırlanma: Potansiyel tehditleri daha iyi bir şekilde öngörmek ve tanımlamak üzere yerel veya yabancı eyalet ve/veya ülkeye özel yasalar ile uyumu içeren Bilgi Güvenliği Programı'nı sürekli olarak güncelleyerek koruma sağlarız.

- Önleme: Gizli ve tescilli bilgilerin kaybını, kötüye kullanımı ve uygunsuz kullanımını önlemek ve olayların sayısını azaltmak üzere önleyici kontrollerin uygulanması yoluyla karşı tarafların bir adım önünde olarak koruruz.
- Tespit Etme: Güvenlik duvarı izleme, istenmeyen e-posta engelleme ve virüs koruma ve diğer izleme, bankadaki tüm ekip üyelerinin, uygulamaların, verilerin, sistemlerin ve ağların sürekli olarak izlenmesi dahil tespit etme amaçlı kontrollerin uygulanması yoluyla maruz kalmayı sınırlandırarak koruruz;
- Azaltma: Aktif ve koordine bir şekilde yanıt verme özelliği aracılığıyla olayları azaltarak koruruz;
- Yanıt Verme/Kurtulma: Güçlü adli incelemeler, soruşturmalar ve alınan dersler kapasitesini iyileştirerek ve aynı zamanda uyum hususlarını, düzenleyici sorgularını, disiplin tedbirlerini veya yasal iddiaları ele alarak koruruz .

EK B

İspanya

İspanya'da Real Decreto Legislativo 2/2015, de 23 de octubre, Texto Refundido del Estatuto de los Trabajadores (İspanya'daki Çalışanların Tüzüğü Hakkında 23 Ekim tarihli Yasa Hükmünde Kararname 2/2015) 20. Maddesi uyarınca, Şirket, bir aracın orantılı olması kaydıyla, çalışanın, bilgisayar donanımı ve İnternet kullanımı ile bağlantılı olarak iş yükümlülüklerine uyduğunu doğrulamak için herhangi bir aracı kullanma hakkını saklı tutar.

Rusya Federasyonu

Bu Bilgi Güvenliği İzleme Bildirimi, 27 Temmuz 2006 tarihli 152-FZ Kişisel Veriler Federal Yasası ve OOO Merrill Lynch Securities veri koruma politikaları ve düzenlemeleri dâhil ancak bunlarla sınırlı olmamak üzere Rusya Federasyonu mevzuatına aykırı olmadığı ölçüde geçerlidir.

Yunanistan

Bu Bilgi Güvenliği İzleme Bildirimi, özellikle 2472/1997 sayılı "Kişisel Verilerin İşlenmesine Dair Bireylerin Korunması" adını taşıyan Yunan yasası ve 3471/2006 sayılı "Elektronik telekomünikasyon sektöründe kişisel verilerin ve gizliliğin korunması ve 2472/1997 sayılı yasada değişiklik" adını taşıyan Yunan yasası olmak üzere Yunanistan'daki yasalarla ve düzenlemelerle olduğu kadar özel durumlara yönelik olarak Yunan Veri koruma Makamı tarafından ilan edilen kararlarla çelişmediği ölçüde geçerlidir.

Katar

Bu Bilgi Güvenliği İzleme Bildirimi, QFC Veri Koruma Düzenlemeleri ve Kuralları 2005 ile aynı zamanda Merrill Lynch International - QFC Şubesi dahili veri koruma politikaları ve gereklilikleri dahil ancak bunlarla sınırlı olmamak üzere Katar'da yürürlükte olan yasalar ve yönetmelikler ile çelişmediği ölçüde geçerlidir.

Birleşik Arap Emirlikleri

Bu Bilgi Güvenliği İzleme Bildirimi, 2020 tarihli ve 5 sayılı Veri Koruma Yasası DIFC Yasası ve 2022 tarihli ve 2 sayılı DIFC Yasası DIFC Değişiklik Yasası ile aynı zamanda Merrill Lynch International (DIFC Şubesi) dahili veri koruma politikaları ve gereklilikleri dahil ancak bunlarla sınırlı olmamak üzere DIFC'de yürürlükte olan yasalar ve yönetmelikler ile çelişmediği ölçüde geçerlidir.

إخطار مراقبة أمن المعلومات

النسخة العربية

اريخ السريان: 3 ابريل 2023

قام الكيان القانوني المذكور في عقد توظيف الموظف أو تعاقد المقاول ("الشركة") بإعدد إخطار مراقبة أمن المعلومات[9] هذا ("الإخطار") لاستكمال إخطار حماية بيانات الموظف والمقاول ("DPN") الذي تتلقاه كموظف أو مقاول لتحديد ممارساته فيما يتعلق بمراقبة البيانات والمواد الأخرى (بما في ذلك، على سبيل المثال لا الحصر، رسائل الأعمال والرسائل الشخصية[10]، والاتصالات والمعلومات) التي يتم نقلها

[9] كان إخطار مراقبة أمن المعلومات (ISMN) يُطلق عليه سابقًا إخطار مراقبة الأمن السيبراني (CSMN) ويمكن الإشارة إليه أيضًا على هذا النحو في وثائق الشركة الأخرى

[10] تماشيًا مع مدونة قواعد السلوك، يُسمح للمستخدمين المُصرّح لهم باستخدام شخصي محدود للأجهزة والتطبيقات التي تديرها الشركة والإنترنت والبريد الإلكتروني للاتصالات الشخصية. قد تتم مراقبة استخدام الموارد وفحصها للحفاظ على سلامة الأنظمة (على سبيل المثال، مراقبة إدخال برامج ضارة أو عمليات نقل بيانات غير سليمة) وتجنب الأنشطة التي قد تؤدي إلى تحمل الشركة لأي مسؤولية أو تعرضها لأي مخاطر.

و/أو استلامها و/أو معالجتها و/أو تخزينها بواسطة الأنظمة والأجهزة الإلكترونية للشركة. ويشمل ذلك، على سبيل المثال لا الحصر، الشبكة والصوت والكمبيوتر والأجهزة المحمولة التي تصدرها الشركة والرسائل الفورية وتطبيقات الويب وتطبيقات الهاتف الجوّال ووسائل التواصل الاجتماعي ومؤتمرات الصوت ومؤتمرات الفيديو والبنية التحتية للفاكس ("الاتصالات الإلكترونية") واستخدام الطابعة والإنترنت وسجلات الوصول المادي.

يسري هذا الإخطار على جميع الأفراد أو المجموعات التي تم تزويدها بإمكانية الوصول إلى أنظمة الشركة و/أو مرافقها و/أو معلوماتها لغرض تجاري أو وظيفة إشرافية، بما في ذلك الموظفين والمستشارين والمقاولين والمديرين غير التنفيذيين وغيرهم من العاملين في الشركة (يُشار إلى كل منهم باسم "**المُستخدم المُصرّح له**"). يحدد الملحق أ قائمة غير شاملة بالمراسلات والسجلات التي نراقبها والتي قد نجمع منها أي معلومات يمكن التعرف عليها بشكل فردي عن المستخدمين المُصرّح لهم ("**البيانات الشخصية**") والأغراض التي قد لأجلها نستخدم وننقل ونُفصح عن البيانات الشخصية. يجب الرجوع إلى الملحق ب من قبل المُستخدمين المُصرّح لهم في بعض الدول.

في حالة تقديم هذا الإخطار إلى مُستخدم مُصرّح له بلغة غير الإنجليزية، يتم حل أي اختلاف أو تعارض أو عدم اتساق بين نسختي اللغة على النحو الموضح في إخطار حماية البيانات ذي الصلة.

بصرف النظر عن الموقع، يتم تطبيق أدوات وإجراءات المراقبة بشكل روتيني من قبل الشركة على الأنظمة والأجهزة الإلكترونية للشركة إلى الحد الذي لا يحظره القانون أو اللوائح المحلية. ويتم إجراء جميع أنشطة المراقبة التي تتم على الأنظمة والأجهزة الإلكترونية للشركة وفقًا لهذا الإخطار.

سيتم التعامل مع أي بيانات شخصية يتم جمعها في سياق إجراءات المراقبة وفقًا لإخطار حماية البيانات ذي الصلة على النحو الصادر من وقت لآخر. تتم معالجة البيانات الشخصية باستخدام أدوات يدوية وأخرى إلكترونية.

يشير هذا الإخطار إلى الأجزاء الرئيسية من سياسات الشركة ذات الصلة، ولكنه لا يحتوي على جميع سياسات الشركة ومتطلباتها المُطبقة على استخدام الاتصالات الإلكترونية والإنترنت. يتعين على المستخدمين المُصرّح لهم الامتثال للمتطلبات المذكورة في مدونة قواعد السلوك ودليل الاتصالات الإلكترونية ووثائق السياسة العالمية لأمن المعلومات الخاصة بالشركة، إضافة إلى أي معايير أخرى معمول بها تصدرها الشركة من وقت لآخر. تحمل جميع المصطلحات المكتوبة بخط عريض المُستخدمة ولكن غير المُعرّفة في هذا الإخطار المعاني المُخصّصة لها في وثائق السياسة العالمية لأمن المعلومات الخاصة بالشركة.

تخضع الاتصالات التي يقوم بها بعض موظفي الشركة المُنظمين لمتطلبات إشرافية تفصيلية إضافية ويتم تذكير المُستخدمين المُصرّح لهم بالرجوع إلى السياسات والإجراءات ذات الصلة الخاصة بنوعية عملهم للحصول على مزيدٍ من المعلومات.

جميع الاتصالات الإلكترونية، بما في ذلك رسائل البريد الإلكتروني (المشفرة وغير المشفرة) والاتصالات بمواقع الإنترنت والإنترانت باستخدام موارد حوسبة أو شبكة الشركة هي ملك للشركة وقد تخضع للمراقبة والرصد.

وفقًا للقانون المعمول به، يشمل ذلك على سبيل المثال لا الحصر:

- **إجراء أنشطة المراقبة دون تقديم إخطار مسبق ("المراقبة السرية")، في الظروف التي يُسمح فيها بذلك (على سبيل المثال عندما يكون لديها شكوك بتسريب البيانات أو أنشطة جنائية أو غير قانونية أخرى أو انتهاك السياسات العالمية للامتثال أو أمن المعلومات الخاصة بالشركة أو انتهاك أي التزام آخر مستحق للشركة)؛**
- **مراقبة و/أو حجب رسائل البريد الإلكتروني الواردة والصادرة وغيرها من الرسائل الموسومة بما يفيد أنها شخصية أو خاصة أو ذات طبيعة شخصية عندما يكون هناك شك في أن رسائل البريد الإلكتروني هذه ومحتوياتها أو مرفقاتها تتعارض مع أو تنتهك القانون المعمول به أو السياسات العالمية للامتثال أو أمن المعلومات الخاصة بالشركة أو أي التزام آخر مستحق للشركة.**

جمع البيانات الشخصية وأغراض الاستخدام

تتم ممارسة أنشطة مراقبة مُعيّنة للأنظمة والأجهزة الإلكترونية الخاصة بالشركة في جميع أنحاء الشركة للأغراض المذكورة في الملحق أ من هذا الإخطار.

فئات البيانات الشخصية التي قد تعالجها الشركة أثناء إجراء المراقبة الموضحة في هذا الإخطار والأسس القانونية لهذه المعالجة (بما في

ذلك الحصول على الموافقة، عند الضرورة) ترد على النحو الموضح في إخطار حماية البيانات ذي الصلة.

البيانات الشخصية الحساسة

يجوز للشركة جمع فئات خاصة مُعيّنة من البيانات الشخصية ومعالجتها بما في ذلك البيانات الشخصية الحساسة على النحو الموضح في إخطار حماية البيانات ذي الصلة في سياق إجراء الأنشطة الموضحة في هذا الإخطار.

لا تراقب أنشطة مراقبة أمن المعلومات العالمية البيانات الشخصية الحساسة بفعالية، ومع ذلك قد يتم الكشف عن بعض البيانات الشخصية الحساسة حتمًا أثناء مراقبة أنواع أخرى من البيانات.

الوصول إلى البيانات من قبل موظفي الشركة

يقتصر الوصول إلى البيانات الشخصية التي تتم معالجتها وفقًا لهذا الإخطار على الأفراد الذين يحتاجون إلى هذا الوصول للأغراض المُدرجة في الملحق أ. إضافة إلى هؤلاء الأفراد على النحو الموضح في إخطار حماية البيانات ذي الصلة، سيتم منح الوصول على أساس الحاجة إلى المعرفة فقط، وللأعضاء المحدودين في إدارة أمن المعلومات العالمية وتحقيقات الشركة الداخلية عند الضرورة.

الإفصاح

يجوز نشر أدوات وإجراءات المراقبة الموضحة في هذا الإخطار من قبل فرق أمن المعلومات العالمية في الشركة وأي من الشركات التابعة لها وفروعها بما في ذلك تلك الموجودة في الولايات المتحدة والمملكة المتحدة وسنغافورة وهونج كونج والهند وكذلك داخل بلد/منطقة التشغيل المحددة. ويجوز تخزين البيانات الشخصية في نطاق الاختصاص القضائي المحلي للمُستخدمين المُصرّح لهم و/أو الاختصاصات القضائية الأخرى التي تعمل فيها الشركة.

نظرًا للطبيعة العالمية لأنشطة الشركة، قد تنقل الشركة بياناتك الشخصية إلى بلدان بخلاف بلدك الأم، وذلك على النحو الموضح في إخطار حماية البيانات ذي الصلة.

ووفقًا للقانون المعمول به، يجوز للشركة الإفصاح عن البيانات الشخصية ذات الصلة إلى أي من الشركات التابعة لها وفروعها ويجوز لها معالجة هذه البيانات الشخصية للأغراض الموضحة في هذا الإخطار. إضافة إلى ذلك، يجوز للشركة الإفصاح، وفقًا للقانون المعمول به، عن البيانات الشخصية ذات الصلة إلى أطراف ثالثة مُعيّنة على النحو الموضح في إخطار حماية البيانات ذي الصلة.

الأمن

تحتفظ الشركة بالتدابير الفنية والتنظيمية المناسبة للحماية من المعالجة غير المصرح بها أو غير القانونية للبيانات الشخصية و/أو من الفقدان أو التغيير أو الإفصاح أو الوصول أو الإتلاف العرضي أو غير القانوني للبيانات الشخصية.

طرق معالجة البيانات والاحتفاظ بها

عند معالجة البيانات الشخصية للأغراض الموضحة في هذا الإخطار، لا تستخدم الشركة عملية مؤتمتة لاتخاذ القرارات بشأن إجراءات المُستخدم المُصرّح له حيث يكون للقرار تأثير قانوني أو ما شابه ذلك من تأثير كبير على المُستخدم المُصرّح له عند إجراء المراقبة على النحو الموضح في هذا الإخطار. و"اتخاذ القرارات بصورة مؤتمتة" هي عملية استخدام وسائل مؤتمتة في اتخاذ القرارات دون أي تدخل بشري.

ويوضح الجدول الزمني العالمي للاحتفاظ بالسجلات فترات الاحتفاظ لكل نوع من البيانات والاختصاص القضائي على النحو المذكور في صفحة إدارة السجلات العالمية على Flagscape. تتوفر متطلبات الاحتفاظ عند الطلب للمُستخدمين المُصرّح لهم الجدد الذين لم يحصلوا بعد على إمكانية الوصول إلى الموقع الداخلي. وستحذف الشركة البيانات الشخصية بعد فترة الاحتفاظ المعمول بها.

الإجراءات التأديبية

قد يخضع المُستخدمون المُصرّح لهم الذين ينتهكون أيًا من السياسات المُشار إليها في هذا الإخطار للتحقيق و/أو تعليق الوصول و/أو الإجراءات التأديبية (بما يصل إلى ويشمل إنهاء الخدمة أو خدمات العقد). قد يخضع المُستخدمون المُصرّح لهم ممن ليسوا موظفين

للإحالة إلى صاحب العمل لاتخاذ إجراء تأديبي. يمكن إحالة المُستخدمين المُصرّح لهم الذين ينتهكون القوانين أو اللوائح المعمول بها إلى مسؤولي إنفاذ القانون و/أو المسؤولين التنظيميين وفقًا للمتطلبات القانونية والتنظيمية. ويجوز الاعتماد على أي مواد أو أدلة يتم تحديدها عبر (بما في ذلك على سبيل المثال لا الحصر) مراقبة المكالمات الهاتفية أو استخدام البريد الإلكتروني والإنترنت أو شبكة الإنترانت (بما في ذلك المكالمات الهاتفية الشخصية ورسائل البريد الإلكتروني واستخدام الإنترنت) في أي إجراءات تأديبية وتحقيقات داخلية أو خارجية. ويُتوقع من المُستخدمين المُصرّح لهم التعاون في أنشطة الاستعلامات والفحوصات والمراقبة والتسجيل إذا طُلب منهم ذلك. قد يؤدي رفض التعاون في إجراء تحقيق أمني إلى اتخاذ إجراء قانوني أو تأديبي، بما في ذلك إنهاء الخدمة أو خدمات العقد.

تفاصيل الاتصال

لطرح الأسئلة أو الحصول على مزيدٍ من المعلومات حول هذا الإخطار أو أنشطة مراقبة أمن المعلومات العالمية، يجب على المُستخدمين للأسئلة أو مزيد من المعلومات حول هذا الإشعار أو أنشطة مراقبة أمن المعلومات العالمية، يجب على المستخدمين المصرح لهم الاتصال بأمن المعلومات العالمي

قد يكون لك الحق في تقديم شكوى إلى سلطة حماية البيانات في بلدك، لمعرفة إمكانية التطبيق والحصول على مزيدٍ من المعلومات، يُرجى الرجوع إلى إخطار حماية البيانات ذي الصلة.

لطرح الأسئلة المتعلقة بالقوانين والقيود المحلية، يجب على المُستخدمين المُصرّح لهم الاتصال بمسؤول الامتثال المحلي أو مسؤول حماية البيانات أو إدارة الشؤون القانونية.

التغييرات في هذا الإخطار

هذا الإخطار ليس تعاقديًا وتحتفظ الشركة بالحق في تعديل الإخطار أو سحبه في أي وقت. إذا أجرت الشركة تغييرات جوهرية على هذا الإخطار، فسوف تخطر المُستخدمين المُصرّح لهم في أقرب وقت ممكن بشكل معقول عن طريق إعادة إصدار إخطار مُعدّل و/أو اتخاذ خطوات أخرى وفقًا للقوانين المعمول بها.

الوثائق ذات الصلة

مدونة قواعد السلوك

الاحتفاظ بالاتصالات الإلكترونية - سياسة الشركة

وثائق السياسة العالمية لأمن المعلومات

منع التحرش والتمييز - سياسة الشركة

مخاطر السمعة - سياسة الشركة

مكان عمل خالٍ من العنف - سياسة الشركة

إخطار مراقبة أمن المعلومات - صفحة Flagscape

للاطلاع على سياسات ومعايير وإرشادات إضافية، يُرجى الاطلاع على صفحة Flagscape لمصدر السياسة العالمية.

الملحق أ

راجع المصفوفة عبر الرابط هنا لعرض فئات البيانات التي قد يتم جمعها لكل غرض من أغراض الاستخدام، والملخصة أدناه. تتوفر المصفوفة عند الطلب للمُستخدمين المُصرّح لهم الجدد الذين لم يحصلوا بعد على إمكانية الوصول إلى الموقع الداخلي.

تشمل الاتصالات والسجلات (المباشرة وبعد الحدث) التي نراقبها على الأنظمة والأجهزة الإلكترونية للشركة والتي قد نجمع منها البيانات الشخصية، على سبيل المثال لا الحصر:

- رسائل البريد الإلكتروني المُرسلة.
- رسائل البريد الإلكتروني المُستلمة.
- استخدام الويب / الإنترنت، FTP وHTTP وHTTPS وTelnet.
- استخدام الطباعة.
- الملفات الموجودة على سطح المكتب (خارج مستنداتي)، ومواقع التعاون، والمشاركات المفتوحة، والويكي الداخلية.
- الوسائط القابلة للإزالة والأجهزة غير غير التابعة للشركة التي تديرها الشركة وتتصل بنظام الشركة.
- الرسائل الفورية.
- المكالمات الهاتفية ومكالمات VOIP ورسائل البريد الصوتي.
- تسجيلات وسجلات الوصول إلى التطبيق واستخدامه.
- تسجيلات وسجلات الوصول إلى النظام واستخدامه (بما في ذلك السجلات التي توضح مسار الاستخدام والسلوك).
- مسح/تصوير الفاكس والمستندات.
- استخدام وسائل التواصل الاجتماعي ومحتواها (خارجي، غير تابع للشركة).
- المعلومات مفتوحة المصدر والمعلومات المتاحة للجمهور.
- السجلات الأمنية.
- السجلات الرئيسية ولقطات الشاشة.
- تقنيات المؤتمرات.
- ملفات تعريف الارتباط، والإشارات، وحفر الإغراق، ومصائد مخترقي الشبكات.
- نظام تحديد المواقع العالمي GPS وتعقب Wi-Fi وبيانات الموقع.
- بيانات الدخول باستخدام البطاقات الممغنطة.
- الرسائل النصية المُرسلة والمُستلمة.

الأغراض التي قد نجمع من أجلها البيانات الشخصية ونستخدمها وننقلها ونفصح عنها:

صُممت السياسة العالمية لأمن المعلومات لتوفير المتطلبات اللازمة لتمكين الشركة من الاستعداد للتغييرات المتزايدة في بيئة التهديدات ومنعها والكشف عنها والاستجابة لها والتعافي منها. يوفر البرنامج العالمي لأمن المعلومات حلولاً ويستخدم تقنيات متقدمة لمنع تهديدات أمن المعلومات من تقويض ثقة العملاء وتعطيل العمليات التجارية. يحمي أمن المعلومات العالمي الشركة وعملائها من خلال استخدام إطار عمل قائم على المخاطر يركز على النتائج.

- الإعداد: نحمي من خلال التحديث المستمر لبرنامج أمن المعلومات، والذي يتضمن الامتثال للقوانين المحلية أو الأجنبية و/أو الخاصة بالدولة لتوقع التهديدات المحتملة وتحديدها بشكل أفضل.
- الوقاية: نحمي من خلال البقاء في صدارة المنافسين من خلال نشر الضوابط الوقائية لمنع فقدان المعلومات السرية والخاصة وإساءة استخدامها والاستخدام غير المناسب لها وتقليل عدد الحوادث.
- الكشف: نحمي بالحد من التعرض من خلال تطبيق الضوابط الاستكشافية بما في ذلك مراقبة جدار الحماية ومكافحة البريد العشوائي

والحماية من الفيروسات وغيرها من سبل المراقبة؛ المراقبة المستمرة لجميع الزملاء في البنك والتطبيقات والبيانات والأنظمة والشبكات.

- التخفيف: نحمي بتخفيف الحوادث من خلال قدرة استجابة سريعة ومنسقة.
- الاستجابة/التعافي: نحمي بتحسين الوضع الأمني من خلال الأدلة الجنائية القوية والتحقيقات والقدرة على الدروس المستفادة مع معالجة أي مشكلات تتعلق بالامتثال أو الاستفسارات التنظيمية أو الإجراءات التأديبية أو المطالبات القانونية.

الملحق ب

إسبانيا

في إسبانيا، وفقًا لمحتوى المادة 20 من Real Decreto Legislativo 2/2015, de 23 de octubre, Texto Refundido del Estatuto de los Trabajadores (المرسوم الملكي التشريعي رقم 2/2015، بتاريخ 23 أكتوبر، نص منقح بشأن قانون العمال الإسباني)، تحتفظ الشركة بحقها في استخدام أي وسيلة، شريطة أن تكون هذه الوسائل متناسبة من أجل التحقق من امتثال الموظف لالتزاماته العمالية فيما يتعلق باستخدام أجهزة الكمبيوتر والإنترنت.

الاتحاد الروسي

يسري إخطار مراقبة أمن المعلومات هذا طالما أنه لا يتعارض مع تشريعات الاتحاد الروسي، بما في ذلك على سبيل المثال لا الحصر القانون الاتحادي رقم 152-FZ "بشأن البيانات الشخصية" اعتبارًا من 27 يوليو 2006 وكذلك سياسات ولوائح حماية بيانات الأوراق المالية لشركة OOO ميريل لينش.

اليونان

يسري إخطار مراقبة أمن المعلومات هذا طالما أنه لا يتعارض مع القوانين واللوائح المعمول بها في اليونان وعلى وجه الخصوص القانون اليوناني 2472/1997 بشأن "حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية" والقانون اليوناني 3471/2006 بشأن "حماية البيانات الشخصية والخصوصية في قطاع الاتصالات الإلكترونية وتعديل القانون 2472/1997" وكذلك القرارات الخاصة بالقضية الصادرة عن هيئة حماية البيانات اليونانية.

قطر

يسري إخطار مراقبة أمن المعلومات هذا طالما أنه لا يتعارض مع القوانين واللوائح المعمول بها في دولة قطر، بما في ذلك، على سبيل المثال لا الحصر، لوائح وقواعد حماية البيانات الصادرة عن مركز قطر للمال لعام 2005 وكذلك السياسات والمتطلبات الداخلية لحماية البيانات لدى شركة ميريل لينش إنترناشيونال - فرع مركز قطر للمال.

الإمارات العربية المتحدة

يسري إخطار مراقبة أمن المعلومات هذا طالما أنه لا يتعارض مع القوانين واللوائح المعمول بها في مركز دبي المالي العالمي، بما في ذلك، على سبيل المثال لا الحصر، قانون حماية البيانات رقم 5 لسنة 2020 الصادر عن مركز دبي المالي العالمي وقانون تعديل مركز دبي المالي العالمي رقم 2 لسنة 2022 وكذلك السياسات والمتطلبات الداخلية لحماية البيانات لدى ميريل لينش إنترناشيونال (فرع مركز دبي المالي العا

INFORMATIVA SUL MONITORAGGIO DELLA SICUREZZA DELLE INFORMAZIONI - Italia

Data di decorrenza: 26 maggio 2023

INTRODUZIONE

La persona giuridica indicata nel contratto di lavoro del Dipendente o nell'incarico all'Appaltatore (la "**Società**") ha redatto la presente Informativa[11] sul monitoraggio della sicurezza delle informazioni (l'"**Informativa**") per integrare l'Informativa sulla protezione dei dati del Dipendente e dell'Appaltatore ("**DPN**") che gli utenti ricevono in qualità di dipendenti o appaltatori per definire le sue pratiche relative al monitoraggio di dati e altri materiali (inclusi, a titolo esemplificativo ma non esaustivo, messaggi[12], comunicazioni e informazioni aziendali e personali) trasmessi, ricevuti, trattati e/o archiviati tramite sistemi e 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. L'appendice B dovrebbe essere riferita agli Utenti autorizzati di Paesi specifici.

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 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 Informativa.

Tutti i Dati personali raccolti 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

[11] 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

[12] 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.

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.

Tutte le Comunicazioni elettroniche, ivi comprese le e-mail (crittografate 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.

Ai sensi della legge vigente, 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);**
- **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 descritto nella presente Informativa e le basi giuridiche per tale trattamento (incluso, ove necessario, il consenso) sono quelle indicate nella relativa DPN.

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 nell'Appendice A. Oltre alle persone indicate nella relativa DPN, l'accesso sarà concesso in base a una rigorosa necessità di conoscenza a membri limitati del Dipartimento globale per la sicurezza delle informazioni e, ove necessario, all'Ufficio per le indagini aziendali interne.

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 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 DEL TRATTAMENTO E DELLA CONSERVAZIONE DEI DATI

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. Qualsiasi materiale o prova individuati tramite (a mero titolo esemplificativo ma non esaustivo) il monitoraggio delle chiamate telefoniche, delle e-mail e dell'uso di Internet o Intranet (ivi comprese le chiamate, le e-mail e l'uso di Internet con carattere personale) possono essere utilizzati nell'ambito di procedimenti disciplinari e di indagini sia interne che 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 domande o ulteriori informazioni sulla presente Informativa o sulle attività di monitoraggio della Sicurezza globale delle informazioni, gli Utenti autorizzati devono contattare Global Information Security.

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 è contrattuale e la Società si riserva il diritto di modificarla o ritirarla 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.

Documenti correlati

Codice di condotta

Ritenzione delle comunicazioni elettroniche – Politica aziendale

Documenti relativi alla Politica globale sulla sicurezza delle informazioni

Harassment & Discrimination Prevention – Enterprise Policy (Prevenzione delle molestie e della discriminazione - Politica aziendale

Reputational Risk – Enterprise Policy (Rischi per la reputazione - Politica aziendale)

Violence Free Workplace – Enterprise Policy (Luogo di lavoro esente da violenza - Politica aziendale)

Informativa sul monitoraggio della sicurezza delle informazioni - Flagscape

Per altre politiche, standard e linee guida si prega di fare riferimento alla pagina Global Policy Source Flagscape (Flagscape fonti politiche globali).

APPENDICE A

Fare riferimento alla matrice qui collegata per visualizzare le categorie di dati che possono essere raccolti per ogni scopo 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.

Le Comunicazioni e la documentazione (sia in tempo reale che successive all'evento) che monitoriamo su sistemi e dispositivi elettronici della Società e tramite le quali potremmo raccogliere Dati Personali includono a titolo esemplificativo ma non esaustivo:

- E-mail inviate;
- E-mail ricevute;
- Utilizzo web/internet, FTP, HTTP, HTTPS, Telnet;
- Utilizzo della stampa;
- File posizionati su Desktop (al di fuori di Documenti), siti di collaborazione, condivisioni apertr, 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;
- 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;
- Registri degli accessi e screenshot;
- Tecnologie per conferenze;
- Cookie, Beacon, Sinkhole e Honeypot;
- Dati di monitoraggio e localizzazione GPS e Wi-Fi;
- 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 Global Information Security Policy (Politica sulla sicurezza delle informazioni globale) è progettata per fornire i requisiti necessari per consentire alla Società di preparare, prevenire, rilevare, rispondere e recuperare da cambiamenti crescenti nel panorama delle minacce. Il Programma globale per la sicurezza delle informazioni fornisce soluzioni e utilizza tecniche avanzate volte a evitare che le minacce alla sicurezza delle informazioni compromettano la fiducia dei clienti e interrompano le operazioni aziendali. La sicurezza globale delle informazioni protegge la Società e i suoi clienti utilizzando un quadro basato sul rischio e incentrato sui risultati.

- 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 potenziali minacce;
- Prevenire: Ci proteggiamo mantenendo il nostro vantaggio sugli avversari mediante l'implementazione di controlli preventivi volti a prevenire la perdita e l'uso improprio e illecito 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 e altre forme di monitoraggio; monitoriamo continuamente tutti i membri del team bancario, 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