CME Group *LEADING WITH CONVICTION AND INTEGRITY*

CONFIDENTIALITY AND DATA PROTECTION POLICY	**CME Group Policy Document No. and Version No.:**	**0009 Version 12.0**
	Policy Document Issued By:	**Corporate Compliance Information Governance and Privacy**
	Policy Document Owner Information:	**Corporate Compliance**
	Date Policy Document Originally Issued:	**November 2013**
	Date Policy Document Last Revised:	**August 2023**

PURPOSE AND STATEMENT OF POLICY

The CME Group organization, including those entities where CME Group has controlling ownership of the entity (collectively, ***"CME Group"*** or the ***"Company"***), is committed to protecting its proprietary, confidential and personal data, including information relating to its business, customers, vendors, strategic partners, employees and other third parties.

CME Group has adopted this Policy to set forth a framework so that:

- Information, including ***CME Group Information*** (defined below) is evaluated and properly classified based upon the sensitivity and criticality of the information;
- Information is protected and managed based upon its classification;
- ***Personal Data*** (defined below) is collected, used, maintained and disposed of in compliance with legal and regulatory requirements; and
- Additional considerations are taken into account for certain regulated businesses.

This policy sets forth the requirements related to the following:

- CME Group's Right to Monitor its Information Resources
- Data Classification Requirements and Security Controls
- Privacy Compliance and Personal Data
    - Subject Access Requests
- Additional Requirements for Certain Regulated Businesses
- Data Access Request (***"DAR"***) Process for Use and Access Approvals
- Secure Disposition
- Responsibilities Regarding Confidential Information
- Available Resources and Raising Concerns

APPLICABILITY AND SCOPE

This Policy applies to all employees, internal consultants, and temporary personnel of CME Group and any authorized third-party with physical or logical access to CME Group, collectively referred to as ***Colleagues***. The responsibility to protect CME Group Information continues even

after termination of employment or service to the Company. The Policy governs the handling of proprietary and confidential information relating to Colleagues, clients, vendors, strategic partners, distributors, subscribers, shareholders and other third parties.

Regardless of format (e.g., verbal, hardcopy, electronic), CME Group Information must be protected in a manner commensurate with its classification. For purposes of this Policy, the term ***"CME Group Information"*** means any information classified as **CME Group Internal, CME Group Confidential** and **CME Group Highly Sensitive**. These standards apply to any access to and/or use of CME Group Information regardless of the method or device used to access the information. Further guidance can be found in the Information Governance Functional Standard on the management of CME Group Information.

CME GROUP'S RIGHT TO MONITOR ITS INFORMATION RESOURCES

CME Group has implemented a number of policies and procedures consistent with applicable law to protect the confidentiality, integrity, and availability of CME Group's ***Information Resources*** (as defined in the **Information Technology Glossary**). To support these efforts, CME Group reserves the right to take possession, access, review, monitor, intercept, or conduct surveillance on any content or materials located on any CME Group Information Resource that may contain CME Group Information, in accordance with applicable law. CME Group resources should only be used for CME Group business-related purposes. Personal use of CME Group Information Resources is prohibited in Israel and should be limited to incidental use in all other locations. CME Group may actively monitor communications relating to regulated entities or to safeguard CME Group, in accordance with applicable law.

CME Group may record certain verbal (e.g. telephone, web conferencing) conversations, in accordance with regulations and applicable law. The purposes of such recordings are to provide verification of customer transactions entered in connection with CME Group business, to protect the organization against misconduct, to fulfill a regulatory requirement, or for general business operations (e.g. team meetings, trainings, etc.). Advance notification should be provided along with the purpose of the recording prior to the recording commencing.

In accordance with regulations and applicable law, CME Group may provide information obtained in the course of its monitoring activities to a third party, including regulators and law enforcement agencies.

DATA CLASSIFICATION REQUIREMENTS AND SECURITY CONTROLS

Data classification is the process of assigning a level of sensitivity to information and determining the controls and security measures required for each classification.

The Company has established the following **FOUR** classifications to apply controls and security measures in an efficient, repeatable and structured manner:

Public*[1]*: Information available to the general public and/or created with the intention for broad distribution outside the Company. This information may be freely disseminated inside and outside the Company.

→ **Examples of Public Information:** marketing brochures, advertisements, press releases, published annual reports and content published to www.cmegroup.com.

→ **Examples of Controls and Security Measures:** minimal security measures designed to ensure the availability and integrity of the information.

CME Group Internal*[2]*: Information belonging to the Company created in the normal course of business with the intention of broad, general distribution within the Company, but not externally. Information classified as CME Group Internal should not be shared publicly or outside the Company, except where there is a legitimate business need.

→ **Examples of CME Group Internal Information:** new employee training materials, compliance policies for the general population and all employee communications.

→ **Examples of Controls or Security Measures:** minimal security measures to ensure the information is not distributed outside of the Company unless such distribution is in accordance with a valid business need, in furtherance of the interests of the Company, in accordance with application licenses or subscriptions, or you have permission to do so based on your role.

CME Group Confidential*[3]*: Information not broadly made available to the organization, such as information maintained solely within a single Department or Division, should be classified as CME Group Confidential.

This includes information sensitive to the Company or a third party (e.g., a client) and should only be shared with individuals inside the Company on a "need to know" basis, meaning the individual needs access to the information to perform their assigned job functions. Improper disclosure of the information could harm or adversely impact the Company, its clients or employees, or could result in a breach of our regulatory or legal obligations. ***It is expected that most of the Company's information will be classified as CME Group Confidential and the security measures required will vary based on the sensitivity of the content of the information.***

→ **Examples of CME Group Confidential Information:** individual Department information, information made available through a license or subscription, information protected by confidentiality agreements, client contact information, annual budget, and strategic plans that are not material to the stock price.

→ **Examples of Controls and Security Measures:** Security measures must be designed to preserve the confidentiality and integrity of the information based on

[1] NEX legacy classification equivalent, Public.
[2] NEX legacy classification equivalent, Internal Use or Confidential-Sensitive.
[3] NEX legacy classification equivalent, Confidential or Confidential – Highly Sensitive

the degree to which the disclosure of the information or impairment of its integrity would harm or adversely impact the Company, its clients, employees or other stakeholders, or result in legal liability as discussed below. For example, do not leave **CME Group Confidential** information in hardcopy form unattended and/or unsecured. Electronic versions should be saved to designated repositories with limited access and/or password protection/encryption and transmitted using a secure company-approved method. It is the responsibility of the ***Information Asset Owner*** (as defined in the **Information Technology Glossary**) to determine the appropriate protections.

CME Group Highly Sensitive[4]: Information where the unauthorized internal or external access to, alteration or inappropriate destruction of the information could have significant harm or an impact on the Company, its clients, employees or other stakeholders. ***Data integrity is extremely vital, and the highest possible levels of confidentiality, restricted access and security measures are essential.*** Refer to the **Frequently Asked Questions – Confidentiality Policy** for additional information.

→ **Examples of CME Group Highly Sensitive Information:** transaction records including trade-related data, client or clearing firm position data and order and messaging data, Regulatory Data (defined below), credit card information, social security numbers, bank account information, employees' medical information or health insurance information and other sensitive Personal Data.

→ **Examples of Security Measures:** information classified as CME Group Highly Sensitive must be subject to the highest security protections available, such as encryption, and access controls that are implementable based on the information and system at issue.

Information classified as CME Group Confidential and CME Group Highly Sensitive may only be provided outside of CME Group in accordance with established authorization procedures and then only transmitted or shared through secure means, protected against tampering or alteration, and, as applicable, subject to legal protective measures, such as Non-Disclosure Agreements. If you need clarification on whether a transfer is authorized, contact **Privacy Compliance**.

If you need help determining the safest method to store or transfer Confidential or Highly Sensitive Information, contact Information Governance. For additional security measures refer to the **Confidentiality Policy FAQ**.

Every Colleague has responsibility for protecting CME Group's information. Those who create, maintain, control or manage access to CME Group Information Resources, such as certain applications, have accountabilities as Information Asset Owners and Information Asset Custodians (as defined in the **Information Technology Glossary**). Everyone must do their part to ensure information is classified and appropriate safeguards are applied to protect the integrity, availability and confidentiality of CME Group Information. All CME Group office spaces are secure and additional access limitations may apply within certain Departments or functions. Even in secure areas, extra precautions must be taken to protect confidential and highly sensitive information either electronically or physically.

[4] NEX legacy classification equivalent, Secret or Confidential – Extremely Sensitive

Please see the **Frequently Asked Questions - Confidentiality Policy** for additional guidance, including specific examples of the type of information belonging to each of the four classifications, security measures to safeguard information, reasonable steps you should take to ensure its protection, process for seeking approval for access to certain data or the transfer or copying of CME Group Confidential or CME Group Highly Sensitive Information.

If you are uncertain of the appropriate classification, assume at a minimum it is CME Group Confidential. You may contact the **Information Governance Team** if you have additional questions regarding the classification process or the classification of particular information.

Any disposal of CME Group Information should be conducted in accordance with the retention requirements of the **Records and Information Management Policy** and as discussed below under **Secure Disposition**.

PRIVACY COMPLIANCE AND PERSONAL DATA

Personal Data (also referred to as personal information or personally identifiable information) means any information that can be used to identify a person. This includes any direct identifiers such as a name and contact details, but also indirect identifiers such as information that may be collected from an electronic device or an alias.

Personal Data includes, but is not limited to, name, email address, phone number, address, birthdate, social security number, driver's license number, other government issued identification number, financial account information, medical and health information, usernames and passwords, IP address, employment information, demographic information, and geographical indicators. Examples of Personal Data held by CME Group about its Colleagues and other individuals such as candidates for employment are:

- Financial information
- Government issued identification documents
- Employment information
- Medical / Health information

Personal Data must be appropriately secured and retained based on its classification. CME Group adheres to the following privacy principles:

→ **Transparency:** Express or implied consent may be required before obtaining Personal Data. When required, the individual providing the Personal Data should be made aware of the type of Personal Data being collected and the relevant **Privacy Policy**;

→ **Purpose Limitation:** Personal Data should only be collected for specific, legitimate, and lawful purposes. Personal Data should only be collected if it is directly relevant and necessary to accomplish the specific business purpose(s);

→ **Data Minimization:** Personal Data should only be collected if it is directly relevant and limited to what is necessary to accomplish the specific purpose(s);

→ **Accuracy:** Personal Data should be accurate, complete, and current. Personal Data that is incomplete, inaccurate or outdated should be corrected;

→ **Storage Limitation:** Personal Data should only be maintained for as long as it is necessary to fulfill the specified purpose(s). Personal Data should be destroyed appropriately as specified by the **Records and Information Management Policy** and as discussed below under **Secure Disposition**;

→ **Confidentiality:** Appropriate security safeguards, in accordance with this Policy and the **Corporate Information Security Policy**, should be put in place to protect Personal Data from known and unknown threats and to minimize the risk of unauthorized access, disclosure, loss, or destruction; and

→ **Access:** Upon request, Personal Data should be made accessible to the individual. The individual should have the ability to correct any inaccuracies or request destruction of his or her Personal Data. Personal Data may not be destroyed if it is required to be maintained for legal, regulatory, or business purposes. Refer to **Global Privacy** – Data Subject Access Requests for further details.

Any unauthorized access, whether intentional or unintentional, of Personal Data should be reported to **Cyber Defense Monitoring** immediately. You may limit further exposure, but do not take any additional remediation actions until you have spoken to a CME Group privacy or information security representative.

CME Group may collect, use, maintain and disclose Personal Data about an individual to carry out its business activities. For more information about how CME Group collects, uses, discloses, and protects Personal Data, see the **Privacy Center**.

DATA SUBJECT ACCESS REQUESTS

Individuals, including those working for CME Group, third parties or clients, may ask CME Group to provide them with the information we collect, use and maintain about them. This is known as a Data Subject Access Request (***"DSAR"***) and must be handled promptly and in a specific manner to comply with relevant privacy laws.

DSAR's can take on different forms. Any written inquiry that asks for information held about the person making the request can be construed as a DSAR. DSAR's include requests to access, be provided copies of, modify, restrict further processing of, or delete Personal Data.

The following are likely to be considered a DSAR:

- "Please send me a copy of my employment records."
- "I have a right to see all the invoices issued to me for the last three years. Please send copies to me."

- "Please send me any documents or correspondences relating to any work you have completed with me."

Immediately forward all requests, even if you are not sure you have received a DSAR, to the **Privacy Compliance** team for review, particularly if it relates to a client or a third party. If the request involves a current or former Colleague, immediately forward the request to **Human Resources**.

If you receive a phone inquiry asking you to disclose any Personal Data (e.g. contact details relating to a third party or a Colleague), please be aware that you should only disclose this Personal Data once the following conditions have been met:

- The caller's identity has been verified to ensure that the information is only provided to someone who is authorized to receive it; and
- The scope of the requested data is reasonable based upon the business justification for requesting the data.

If you feel that you are unable to verify the identity of a caller, please take down his/her contact details and check internally. Alternatively, ask the caller to submit their request in writing.

Should you have any doubt or questions regarding a request, please direct your questions to **Privacy Compliance**.

ADDITIONAL REQUIREMENTS FOR CERTAIN REGULATED BUSINESSES

1. DATA COLLECTED FOR CFTC REGULATORY PURPOSES

CME Group currently operates four U.S. designated contract markets (***"DCMs"***)[5], global trade repositories (***"Trade Repositories"***) and a Swap Execution Facility (***"SEF"***). These businesses are subject to regulations that apply additional **use** restrictions to certain types of information collected by the DCMs, the Trade Repositories and the SEF.

Information that meets the definition of Regulatory Data may not be used for business or marketing purposes or distributed outside of the CME Group organization unless the market participant who provided it to the DCM, Trade Repository or SEF has clearly consented to the use of such data in such manner.

The definition of ***CFTC Regulatory Data*** for these purposes is limited to proprietary data or Personal Data collected, maintained or received by a DCM, Trade Repository or the SEF for the purposes of fulfilling its regulatory obligations. More specifically, Regulatory Data includes:

[5] CME Group's DCMs are permitted to share "Regulatory Data" with other DCMs or swap execution facilities registered with the Commodity Futures Trading Commission ("***CFTC"***) for regulatory purposes with or without customer consent.

- ***Derivatives Clearing Organization records*** – Records of all activities related to the clearing and settlement activities of the derivatives clearing organization, including all cleared transactions, margin levels, value and adequacy of financial resources, and the establishment of settlement prices.
- ***Detailed regulatory transaction data*** ─ Trade data maintained by the Market Regulation Department including order and messaging data at the specific account or customer level.
- ***Financial information*** ─ Financial records and other information collected by the Financial and Regulatory Surveillance Department during the course of regulatory and fee examinations, and member or participant due diligence reviews, and any information received by the Company from third-party depositories of clearing members in its capacity as a designated self-regulatory organization (***"DSRO"***).
- ***Investigative materials*** ─ Information collected by the Market Regulation Department as part of surveillance activities or investigations of potential rule violations.
- ***Position data*** ─ Reports of large positions collected pursuant to CME/CBOT/NYMEX/COMEX Rule 561 (Reports of Large Positions), records of requests for exemptions from position limits collected pursuant to Rule 559 (Position Limits), and records collected pursuant to Rule 560 (Position Accountability).
- ***Trade Repository data –*** Any information received or maintained by the Trade Repositories for the purposes of complying with applicable regulatory reporting requirements, that is not subject to public reporting. For avoidance of doubt, any data received or maintained in the regular course of business outside of a Trade Repository does not become Regulatory Data for purposes of this Confidentiality Policy merely because it is also received or maintained by a Trade Repository.

All CFTC Regulatory Data is classified as CME Group Highly Sensitive Information.

Note that the **use** restrictions that prevent Regulatory Data from being used for "business" or "marketing" purposes would not prevent appropriate internal uses of Regulatory Data by authorized personnel. "Business" purposes do not include: activity aimed at compliance with the Commodities Exchange Act or any other applicable law or regulation; market regulation; clearing; risk management; market operations; market and product research and development; and performance monitoring in connection with ensuring effective operations and integrity of the marketplace. For example, Regulatory Data collected by the Financial and Regulatory Surveillance Department could be shared with CME Clearing risk management staff for the purpose of operating CME Group's clearing house business function in compliance with CFTC Core Principles related to risk management. Other uses of Regulatory Data must be authorized by the CME Group **Data Access Review Team**.

Finally, the Regulatory Data received by the Trade Repositories is also subject to certain special **access** restrictions. This information can be accessed internally only by individuals who are duly authorized or who are otherwise operating pursuant to a documented Service Level Agreement, and in such cases only to the degree that such access is necessary for those individuals to perform their assigned job responsibilities. Additionally, in appropriate circumstances, counterparties to a trade (with certain limitations) housed by a Trade

Repository and certain approved regulators as set forth in the **Global Repository Services Access Policy** may also be allowed to access Regulatory Data received and maintained by a Trade Repository.

2. BROKERTEC AMERICAS LLC

BrokerTec Americas LLC (***"BTEC"***) operates as an alternative trading system (***"ATS"***)[6] registered with the U.S. Securities and Exchange Commission and has established and maintains safeguards and procedures limiting **access** to any confidential or highly-sensitive trading information of subscribers to those who are operating the ATS or responsible for its compliance with applicable rules.

Subscriber confidential trading information includes, but may not be limited to:

- Orders and order detail information;
- Trades and execution detail information; and
- Any information that cannot be ascertained by subscribers from directly looking at the ATS's screens at the time subscribers submit their information to the ATS.

Only Colleagues who provide services to assist BTEC's ongoing operations will be eligible to receive access to confidential trading information, to perform their job functions. If you are confirmed to be eligible to have access to BTEC confidential trading information, you may **not use** it for any other purpose other than for the business function for which access was provided and you may not share that information with unauthorized persons. Individuals who receive access may be subject to certain additional monitoring requirements.

Initial requests to receive confidential trading information of BTEC subscribers should be submitted through the **Data Access Review** process.

3. OTHER REGULATED BUSINESSES

CME Group has a number of additional regulated businesses, including those regulated by the Financial Conduct Authority and the Netherlands Authority for the Financial Markets. Each of our regulated entities have regulatory requirements limiting the access and use of information, and this Policy has considered the requirements under the relevant regimes. By protecting and preserving CME Group Information in accordance with this Policy, Colleagues help to ensure that the Company continues to meet its confidentiality obligations stemming from various regulations. If you have any questions about our regulatory obligations with regards to the use or access of information, please reach out to **Corporate Compliance**. Please refer to **Open Exchange** for additional guidance on data related to certain businesses and partnerships.

[6] SEC Regulation ATS Rule 301(b)(10).

DATA ACCESS REQUESTS (*"DAR"*) PROCESS FOR USE AND ACCESS APPROVALS

Access and use of CME Group Confidential or CME Group Highly Sensitive data should be strictly limited to Colleagues that have a business reason to access and/or use the information. If a Department, team, or Colleague requires access to CME Group Confidential or CME Group Highly Sensitive data for a new business purpose, requests should be submitted through the Data Access Request (***"DAR"***)[7] process for review and consideration. The DAR team is comprised of representatives from Legal, Corporate Compliance, Market Regulation, Information Security, and Data Management. DAR will determine if the request should be approved as is, approved with modifications, or declined, and will indicate what controls or other security measures are required to allow the use or access. In making its determination, DAR will assess the type of information the individuals proposed to obtain access to and how the information will be used and will consider any regulatory or contractual considerations. Please refer to **Open Exchange** for additional guidance on data related to certain businesses and partnerships.

Examples of requests that should be submitted to DAR include (but are not limited to) the following:

- a business need to use or combine datasets that have not previously been brought together, providing new insights which are not available when reviewing the datasets individually;
- access to data that has not previously been granted to a particular Department, team, or Colleague, specifically as it relates to the regulated businesses;
- a novel use of data of the regulated businesses, even if the Department or Colleague involved already has access to such data; or
- creation of a new report intended to be shared externally that is not available to the general public.

If a request is approved, Colleagues may not use the information for any other purpose beyond what was specified in the approval from DAR. Any access or use granted by DAR to a specific Department, team or Colleague may not be shared with others without first obtaining additional approval from DAR, even with Colleagues who are part of your same Department or team. When in doubt, please refer questions to **Privacy Compliance** or **DAR Admin**, who can assist with determining whether a DAR review is necessary.

SECURE DISPOSITION

To reduce the risk of exposing CME Group Information to unauthorized persons or for unintended purposes (e.g. data breaches, identity theft, fraud, software license violations, or exposure of proprietary or trade secret information), all Information Assets and Information Resources should be properly destroyed or cleansed of CME Group Internal, CME Group Confidential and CME Group Highly Sensitive data using methods that render the data unreadable and non-recoverable by any means.

[7] DAR requests should be submitted through Archer GRC, Information Governance – DAR: General User, Create New DAR.

This applies to ***Information Assets*** and ***Information Resources*** (both as defined in the **Information Technology Glossary**) such as computers, technology equipment and other electronic or physical media capable of displaying, collecting, or storing CME Group Information regardless of final disposition (e.g., destruction of devices or data, donations, recycling, returns, resale, and repurpose by internal or external parties).

CME Group has set forth a framework designed to ensure:

- Information Assets and Information Resources use methods for disposal that render the information irretrievable and incapable of being reconstructed by any reasonable means;
- Corporate assets and information are properly identified and have met the retention requirements as outlined within the **Records Retention Schedule** or applicable Legal Hold Notices; and
- Prior to final disposition reasonable attempts are made to secure the Information Assets and Information Resources at all times.

Disposal of physical materials:

- All CME Group owned and managed facilities are equipped with secure shredding consoles or electronic cross-cut shredders.
- CME Group materials should never be placed in recycling or garbage receptacles.
- Physical materials such as paper, photos, booklets, and some small media (flash drives, tapes, CDs, etc.) must be placed in secure consoles or shredders to ensure secure disposition.

If you have questions regarding the disposal of physical materials, contact the **Information Governance Team**.

Disposal of electronic assets & content:

- All CME Group owned and managed assets (laptops, desktops, mobile devices, servers, SAN, etc.) are to be securely destroyed by authorized personnel only.
- For disposal of assets or secure disposition of content, please contact Customer Support Group for assistance, at +1 312 930 3444 or e-mail.

RESPONSIBLITIES REGARDING CONFIDENTIAL INFORMATION

CME Group Colleagues

CME Group Confidential and CME Group Highly Sensitive information fall under the definition of ***"Confidential Information"*** as defined in the Acknowledgement and Acceptance of Confidentiality and Intellectual Property Policy and/or an applicable employment agreement (collectively, the ***"Confidentiality Agreement"***) signed at the beginning of employment with, or provision of services to, CME Group. Accordingly, you are obligated by your Confidentiality Agreement to hold all CME Group Confidential and CME Group Highly Sensitive information in the strictest confidence, and to take reasonable precautions to prevent the unauthorized disclosure of such information.

If you inadvertently send Personal Data, CME Group Confidential or CME Group Highly Sensitive information to an unintended third party, internal or external, contact **Cyber Defense Monitoring** immediately. We ask that you do not attempt to resolve the matter directly.

If you receive any subpoena or become subject to any legal obligation to disclose any CME Group Confidential or CME Group Highly Sensitive information that is not part of your regular responsibilities at CME Group, you must contact **Corporate Compliance** or a litigation attorney in the Legal Department and comply with any objections made by the Company regarding such disclosure obligations.

Certain employees are required to execute a Confidentiality, Non-Competition and Non-Solicitation Agreement that contains similar undertakings regarding the preservation and safeguarding of such information.

Third Parties

To the extent CME Group engages a third party vendor to provide services that include hosting or processing any information classified as CME Group Confidential or CME Group Highly Sensitive, the business owner of the relationship and representatives from Legal, Compliance and from the Third Party Risk Management (***"TPRM"***) Risk Assessment process (as appropriate) must review the vendor's process and controls against the standards of this Policy. **Corporate Procurement** can assist with arranging for the required reviews when engaging such vendors. Please allocate sufficient time for the completion of such reviews which will vary based on the complexity of the engagement.

AVAILABLE RESOURCES AND RAISING CONCERNS

Questions regarding this Policy should be directed to **Corporate Compliance**. Suspected violations of this Policy, including any inappropriate use, disclosure, destruction, theft or loss of CME Group Confidential or CME Group Highly Sensitive Information (including Regulatory Data and Personal Data) whether intentional or inadvertent, must be raised in accordance with the **Speak Up and Escalation Policy** and your obligations under your Confidentiality Agreement, including reporting to the CME Group Compliance & Ethics Helpline (www.ethicspoint.com). Your timely reporting is necessary and important to ensure the Company can appropriately respond to any inappropriate data disclosure or breach in accordance with applicable legal and regulatory requirements.

OVERSIGHT AND REVIEW OF POLICY

This Policy is subject to the oversight of the Global Corporate Compliance & Ethics Team. CME Group will periodically review and monitor compliance with this Policy as necessary and appropriate. Colleagues are required to execute periodic certifications of compliance with this Policy, as well as attend any required educational programs associated with this Policy. This Policy is subject to review on an annual basis.

PENALTIES AND CONSEQUENCES

Breaches of the Company's commitment to carefully protect CME Group Information can have serious repercussions on many levels, as well as damage the Company's reputation. Potential violations will be subject to investigation by the Company and/or its agents, and any failure to comply with this Policy may result in discipline, up to and including termination, referral to regulatory authorities, and potential civil and criminal exposure.

Revision History for Confidentiality and Data Protection Policy

Version	Date	Summary of Changes	Owner(s)
12.0	May 2023	• Added reference to the IG Functional Standard • Removal of the Department Record Controllers	Corporate Compliance Information Governance and Privacy
11.0	April 2022	• Addition of references to data sharing guidance and other administrative updates	Corporate Compliance Information Governance and Privacy
10.0	February 2021	• Updated Personal Information to Personal Data. Changed Privacy Policy to Privacy Center.	Corporate Compliance Information Governance and Privacy
9.0	November 2019	• Updated to incorporate NEX business and regulatory requirements.	Corporate Compliance Information Governance and Privacy
8.0	May 2018	• Updated the definition of Personal Information and modified the Privacy Principles to comply with General Data Protection Regulation.	Corporate Compliance Information Governance and Privacy
7.0	November 2017	• Updates to Regulatory Data business purposes. • Incorporation of additional subject access request types and requirements. • Other clarifying changes and updates based on changes in business processes.	Corporate Compliance Information Governance and Privacy
6.0	September 2016	• Updates to the definition of Regulatory Data. • Incorporation of additional information on how to securely dispose of CME Group information and associated assets. • Other clarifying changes.	Corporate Compliance Information Governance and Privacy
5.0	October 2015	• Updated to incorporate the revisions to Rule 537 regarding Regulatory Data. • Updated to incorporate additional provisions relating to the protection of Personal Information and secure disposition.	Corporate Compliance Information Governance and Privacy

Version	Date	Summary of Changes	Owner(s)
4.0	March 2015	• Incorporated additional data classification descriptions. • Incorporated examples of information within each data classification that require security measures to safeguard information.	Corporate Compliance Information Governance and Privacy
3.0	October 2014	• Incorporated clarification of access and use rights with respect to certain information collected in the discharge of designated self-regulatory responsibilities.	Corporate Compliance Information Governance and Privacy
2.0	June 2014	• Incorporated additional regulatory requirements providing for collection of account balance information.	Corporate Compliance Information Governance and Privacy
1.0	November 2013	• Incorporated the provisions of the separate Data Classification Policy which was retired. • Incorporated the provisions of the separate Confidentiality Policy for Market Regulation and Audit Departments and applied the confidentiality requirements to the entire organization. The separate policy was retired. • Incorporated additional regulatory requirements for the Company's regulated businesses such as CME Repository Services and the UK trade repository.	Corporate Compliance Information Governance and Privacy

Matrix of Approvals

Description of Required Approval	Date of Last Approval Relating to Current Version (Version 12.0)
Global Corporate Compliance & Ethics Team	March 08, 2023