CME Group *LEADING WITH CONVICTION AND INTEGRITY*

CONFIDENTIALITY AND DATA PROTECTION POLICY	**CME Group Policy Document No:**	**0009**
	Policy Document Issued By:	**Global Corporate Compliance & Ethics Team**
	Policy Document Owner Information:	**Global Chief Compliance Officer**
	Date Policy Document Originally Issued:	**November 2013**
	Date Policy Document Last Revised:	**November 2017**

PURPOSE AND STATEMENT OF POLICY

The CME Group organization, including its wholly-owned subsidiaries (collectively, ***"CME Group"*** or the ***"Company"***), is committed to protecting its proprietary, confidential and personal information, 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 designed to ensure:

- 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 preserved based upon its classification;
- ***Personal Information*** (defined below) is collected, used, maintained and disposed of in compliance with legal and regulatory requirements; and
- Any ***Regulatory Data*** (defined below), including any data received in connection with the Company's operation of ***Trade Repositories*** (as defined below), is used only for permitted purposes in accordance with applicable law.

APPLICABILITY AND SCOPE

This Policy applies to all employees, internal consultants, contractors, and temporary personnel resources of CME Group, including all of its wholly-owned subsidiaries and any agent or supplier with physical or logical access credentials to CME Group, referred to collectively as ***CME Group colleagues***. The responsibility to protect CME Group Information continues even after termination of employment with or service to the Company. The Policy governs the handling of proprietary and confidential information relating to CME Group colleagues, customers, vendors, strategic partners, distributors, subscribers, shareholders and other third parties.

CME Group Information regardless of format (e.g., verbal, hardcopy, electronic) 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 and regardless of whether it is collected in the ordinary course of business or in connection with the Company's regulated businesses.

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 **Corporate Information Security Policy**). 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 may record certain telephone conversations, including phone lines in the Global Command Center, in accordance with applicable law. The purposes of such recordings is to provide verification of customer transactions entered in connection with CME Group business, to protect the organization against misconduct, and to ensure the telephone lines are being used consistent with applicable CME Group policies. Consent to such recording and monitoring is presumed by the use of the recorded phone lines.

In accordance with 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 to what degree the information needs to be controlled and secured.

The Company has established the following **FOUR** classifications to identify and rank its information for the application of controls and security efforts in an efficient, repeatable and structured manner:

Public: 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 Security Measures:** version control, read only.

CME Group Internal: Information belonging to the Company created in the normal course of business with the intention of broad, general distribution within (but not outside) the Company.

Information classified as CME Group Internal should not be shared publicly or outside the Company, except where there is a legitimate business need to do so. Information not broadly made available to the organization such as information maintained solely within a single Department or Division is not considered CME Group Internal and should be classified as CME Group Confidential.

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

→ **Examples of Security Measures:** do not distribute outside of the company unless such distribution is in accordance with ordinary business practices, in furtherance of the interests of the Company and you have permission to do so based on your role.

CME Group Confidential: Information sensitive to the Company or a third party (e.g., a customer) should only be shared with individuals 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 significantly harm or adversely impact the Company, its customers or employees, or could result in a breach of our legal obligations under a contract. ***It is expected that the bulk 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, customer contact information, annual budget, strategic plans and M&A/transactions that are not material to the stock price.

→ **Examples of Security Measures:** Security measures must be designed to preserve the confidentiality and integrity of the information based on the degree to which the disclosure of the information or impairment of its integrity would harm or adversely impact the Company, its customers, 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 protected/encrypted and transmitted using a secure company-approved method. It is the responsibility of the ***Information Asset Owner*** as defined in the **Corporate Information Security Policy** to determine the appropriate protections.

CME Group Highly Sensitive: Information where the unauthorized internal or external access to, alteration or inappropriate destruction of, the information could have a material impact to the Company, its customers, employees or other stakeholders. ***For this information, 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, customer or clearing firm position data and order and messaging data, Regulatory Data, credit card information, social security numbers, bank account information, employees' medical information or health insurance information and other Personal Information.

→ **Examples of Security Measures:** information classified as CME Group Highly Sensitive must be subject to the highest security protections available, such as encryption in transit and at rest, and 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 subject to applicable legal protective measures, such as Non-Disclosure Agreements. If you need clarification on whether a transfer is authorized, contact an attorney in the Legal Department or Corporate Compliance.

Every CME Group 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 Custodians***, as defined in the **Corporate Information Security Policy,** and as Information Asset Owners. Everyone should do their part to ensure information is classified and appropriate safeguards are applied to protect *the integrity, availability* and *confidentiality* of CME Group Information.

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

If you are uncertain of the appropriate classification, assume at a minimum it is CME Group Confidential. You may contact **Global Information Security**, **Corporate Compliance** or 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 done in accordance with the retention requirements of the **Records and Information Management Policy** and as discussed below under **SECURE DISPOSITION**.

PRIVACY COMPLIANCE AND PERSONAL INFORMATION

CME Group may collect, use, maintain and disclose Personal Information about an individual to carry out its business activities. ***Personal Information*** (also referred to as personal data or personally identified information) is considered to be any recorded information which relates to or can reasonably identify an individual. Personal Information does not have to be confidential in nature – a simple list of employees on a public website will constitute personal information. Even a number, such as a telephone extension number, may qualify as personal information when an individual can be identified from that number, for example, where that number may be linked to his/her name in another database. Personal Information also includes expressions of opinion when it can reasonably identify the individual. Examples of Personal Information held by CME Group are:

- Financial information
- Government issued identification documents

- Employment information
- Medical / Health information

Personal Information must be appropriately secured and retained based on its particular classification.

When collecting or processing Personal Information, CME Group adheres to the following principles:

→ **Collection:** Personal Information should only be collected for specific and legitimate purposes. Prior to collecting or processing Personal Information, the individual providing the Personal Information should be made aware of the reasons for which the information is being collected;

→ **Choice:** Expressed or implied consent may be required before obtaining Personal Information based upon the type of Personal Information collected; the method in which it is collected, or the individual's place of residency;

→ **Usage:** Personal Information should only be used and disclosed for the intended purposes for which the information was originally collected;

→ **Access:** Upon request, Personal Information should be made accessible to the individual and they should have the ability to correct any inaccuracies or request destruction of their Personal Information. Information, however, may not be destroyed if it is required to be maintained for legal, regulatory or business purposes;

→ **Transfer:** Transfer of Personal Information between nations or countries is permissible when consent has been provided, agreements have been established that allow the transfer of data, or adequate guarantees have been made that the data will be protected. Transfers to non-CME Group companies is permissible provided there is a contract in place between the CME Group company and the third party that covers the data sharing and the Legal Department has approved the transfer. If you have any questions on the transfer requirements, contact privacycompliance@cmegroup.com;

→ **Integrity:** Personal Information should be accurate, complete and kept up-to-date and any incomplete or inaccurate data should be corrected;

→ **Maintain:** Personal Information should only be maintained to fulfill the business purposes for which it was collected and retained in compliance with the **Records Retention Schedule**;

→ **Protection:** Appropriate measures should be taken to ensure all Personal Information is secured to prevent unauthorized access, disclosure, loss or destruction. Personal Information requires additional protections; and

→ **Disposition:** Personal Information should be destroyed in accordance with the company's secure disposition procedures as described below.

Any unauthorized access of Personal Information should be reported to Privacy Compliance.

For more information about how CME Group collects, uses, discloses, and protects personal information, see the **Privacy Policy**.

For more information about how the UK entities comply with UK data protection laws, see the **UK Compliance Manual**.

SUBJECT ACCESS REQUESTS

Individuals, including those working for CME Group, third parties or customers, may ask CME Group to provide them with the information we collect, use and maintain about them. This is known as a subject access request. Subject access requests can take different forms. Any written inquiry that asks for information held about the person making the request can be construed as a subject access request. Subject access requests include requests to receive copies of their information, deletion of personal information, and complaints regarding the use or storage of their personal information.

The following are likely to be treated as subject access requests:

- "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 done with me."

For customer or third party subject access requests, forward immediately to the Privacy Compliance Team without delay. Certain privacy laws establish short timelines for fulfilling such a request.

Please direct employee requests, current or former to Human Resources.

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

- Verified the caller's identity to make sure that the information is given to someone who is authorized to receive it.
- 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 privacycompliance@cmegroup.com.

ADDITIONAL INFORMATION ON DATA COLLECTED FOR REGULATORY PURPOSES

CME Group currently operates four U.S. designated contract markets (***"DCMs"***), 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. The use restrictions discussed below do not apply to CME Clearing's use of any data for compliance with the Commodity Exchange Act (***"CEA"***) or any other applicable law or regulation. Further, these use restrictions apply only to Regulatory Data.

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[1] 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 ***Regulatory Data*** for these purposes is limited to proprietary data or Personal Information 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:

- ***Position data*** – Reports of large positions collected pursuant to CME/CBOT/NYMEX[2] 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).

- ***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"***).
- ***Detailed regulatory transaction data*** – Trade data maintained by the Market Regulation Department including order and messaging data at the specific account or customer level.
- ***Investigative materials*** – Information collected by the Market Regulation Department as part of surveillance activities or investigations of potential rule violations.
- ***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.

---

[1] 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.

[2] Trading on COMEX is governed by the NYMEX Rulebook.

All 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 CEA 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 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.

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 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.

This applies to ***Information Assets*** and ***Information Resources*** (both as defined in the **Corporate Information Security Policy**) 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).

The Company also expects persons working on our behalf, such as external consultants, third parties and business partners, to adhere to the standards set forth in this Policy in connection with the disposal, destruction, removal, and/or transfer of any CME Group Information.

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 at RIM@cmegroup.com or the Department Records Controller in your respective area.

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.

If you have questions regarding electronic disposal, contact Customer Support Group at +1 312 930 3444 or CustomerSupport@cmegroup.com.

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 services with 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 Information, CME Confidential or CME Group Highly Sensitive Information to an unintended third party, internal or external, contact Privacy Compliance or Cyber Defense Response 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 an attorney in the Legal Department and comply with any objections made by the Company regarding such disclosure obligations.

Certain employees are also 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 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.

AVAILABLE RESOURCES AND RAISING CONCERNS

Questions regarding this Policy should be directed to the Global Chief Compliance Officer or another compliance resource. 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 Information) 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. CME Group personnel may be 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 as needed basis, but at least every three (3) years.

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 Policy

Date	Revision
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.
June 2014	• Incorporated additional regulatory requirements providing for collection of account balance information.
October 2014	• Incorporated clarification of access and use rights with respect to certain information collected in the discharge of designated self-regulatory responsibilities.
March 2015	• Incorporated additional data classification descriptions. • Incorporated examples of information within each data classification that require security measures to safeguard information.
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.
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.
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.