Confidentiality and Data Protection Policy

Policy Number: 0009

Table of Contents

CME Group *LEADING WITH CONVICTION AND INTEGRITY*

CONFIDENTIALITY AND DATA PROTECTION POLICY	**CME Group Policy Document No. and Version No.:**	**0009 Version 15.1**
	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:	**December 2025**

PURPOSE AND STATEMENT OF POLICY

CME Group 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.

APPLICABILITY AND SCOPE

This policy applies to all employees and internal consultants 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. This policy governs the handling of proprietary and confidential information relating to colleagues, clients, vendors, strategic partners, distributors, subscribers, shareholders and other third parties.

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**. Regardless of format (e.g., verbal, hardcopy, electronic), CME Group Information must be protected in a manner commensurate with its classification. 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.

Questions regarding this policy should be directed to **Corporate Compliance**. Additional details on the requirements of this policy are set forth in the **Appendix**.

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 (as defined herein) and Personal Data) whether intentional or inadvertent, must be raised in accordance with the **Speak Up and Escalation Policy**, including reporting to the **CME Group Compliance & Ethics Helpline**. 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.

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:*** 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.
- ***CME Group Internal:*** 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.
- ***CME Group Confidential:*** Information not broadly made available to the organization, such as information maintained solely within a single Department or Division. 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.***
- ***CME Group Highly Sensitive:*** 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.***

Examples of the foregoing classifications, applicable security measures and guidance on determining which classification to apply are set forth in the **Appendix**.

You are responsible for protecting CME Group's Information. Colleagues who create, maintain, control or manage access to CME Group Information Resources, such as certain applications, have additional accountabilities as Information Asset Owners and Information Asset Custodians

(as defined in the **Information Technology Glossary**). You must do your part to ensure information is classified and appropriate safeguards are applied to protect the integrity, availability and confidentiality of CME Group Information regardless of your working environment (e.g., whether working in a secure area or remotely).

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.

RESPONSIBILITIES REGARDING CONFIDENTIAL INFORMATION

You are required 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.

Any unauthorized access, whether intentional or unintentional, of Personal Data or CME Group Confidential Information or CME Group Highly Sensitive Information should be reported to **Cyber Defense Monitoring** immediately. This includes inadvertently sending it to an unintended third party (internal or external). 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. 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.

Nothing in this policy prohibits you from communicating with any governmental authority or making a report in good faith and with a reasonable belief of any violations of law or regulation to a governmental authority, or from providing documentation, testifying or participating in a legal proceeding relating to such violations, including making other disclosures protected or required by any whistleblower law or regulation to the SEC, the Department of Labor, or any other appropriate government authority.

PRIVACY COMPLIANCE AND PERSONAL DATA

CME Group has established processes and procedures to comply with applicable privacy laws and regulations. If you have responsibility for collecting, processing, using or accessing any Personal Data, you must be familiar with the principles set forth in the **Appendix**. ***Personal Data*** (also referred to as personal information or personally identifiable information) means any information that can be used to identify a person, or if you live in California, your household. 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. Even when data points are not individually identifying, the combined informational value of such indirect identifiers can lead to data becoming personally identifiable. For example, a combination of name and geographical indicators could ultimately pinpoint a specific individual.

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**.

ADDITIONAL REQUIREMENTS FOR CERTAIN REGULATED BUSINESSES

CME Group's regulated businesses bring with them additional restrictions on how information and data related to their regulated activities may be accessed, shared and used. In general, by protecting and preserving CME Group Information in accordance with this policy, you help to ensure that the company continues to meet its confidentiality obligations stemming from these various regulations.

Some regulations are more prescriptive on who may access and use data. If your role involves support of any of our futures and options exchanges (CME, CBOT, NYMEX, COMEX), our clearing house, and our global trade repositories, BrokerTec Americas LLC or FanDuel Prediction Markets LLC and you have access to their sensitive data, you must be familiar with the requirements as set forth in the **Appendix**.

It is extremely important that the information we collect for regulatory purposes is not inappropriately used. All such data would be classified as CME Group Highly Sensitive.

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 **OpenExchange** for additional guidance on data related to certain businesses and partnerships and for the contact details of our **Regulatory Compliance Officers**.

PROCESS TO REQUEST ACCESS TO AND USE OF CME GROUP CONFIDENTIAL AND CME GROUP HIGHLY SENSITIVE INFORMATION

CME Group follows the principle that access and use of CME Group Confidential and CME Group Highly Sensitive data should be strictly limited to colleagues that have a business reason to access and/or use the information. To help ensure that CME Group Information is appropriately accessed and used, the company encourages consultation with **Privacy Compliance** to request access to CME Group Confidential or CME Group Highly Sensitive data for a new business purpose. Consult the **Appendix**, for further information.

When in doubt, please refer questions to **Privacy Compliance**, who can provide additional guidance.

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"***). To comply with relevant privacy laws, the company

has an established process for responding to a DSAR. Determining whether a request for information is a DSAR may not be readily apparent. DSARs 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 correspondence relating to any work you have completed with me.”

Immediately forward all such 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**.

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

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.

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).

Any disposal of CME Group Information should be conducted in accordance with the retention requirements of the **Records and Information Management Policy**. Refer to the **Appendix** for the requirements for securely disposing 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 may actively monitor communications relating to regulated entities or to safeguard CME Group, 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 should be limited to incidental use and you should not use CME Group resources to store personal artifacts (photos, documents).

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.

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 CME Group's commitments as set forth in this policy can have serious repercussions on many levels, including legal and regulatory consequences and damaging the company's reputation. Potential violations of this policy will be subject to investigation by CME Group, 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.

APPENDIX

ADDITIONAL INFORMATION ON DATA CLASSIFICATION REQUIREMENTS AND SECURITY CONTROLS

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

CME Group Internal: 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: Information not broadly made available to the organization, such as information maintained solely within a single Department or Division. 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 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: 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, FanDuel Predicts Sensitive Information (as defined below) 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.

Data classifications should be applied to all data and also must be applied to services and applications, where technically possible. When applying a classification to a service or application, the classification shall take on the highest level of classification associated with the data; e.g. if an application contains data that is Public and data that is CME Group Confidential, then the classification will be CME Group Confidential.

When determining the classification of a service or application, you should consider the sensitivity of all of the following data: any data that is held by the service or application, all data that passes through the service or application, all data that the service or application has control over permissions, and all data that the service or application oversees management of (including backup and recovery).

Information classified as CME Group Confidential and CME Group Highly Sensitive may only be provided outside of CME Group with prior management authorization 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 guidance as to whether a transfer is authorized, contact the **Information Governance Team**.

If you need help determining the safest method to store or transfer CME Group Confidential or Highly Sensitive Information, contact the Information Governance Team. For additional security measures refer to the **Frequently Asked Questions – Confidentiality Policy**.

ADDITIONAL INFORMATION ON PRIVACY COMPLIANCE AND PERSONAL DATA

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:** 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 Notice;

→ **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.

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. Refer to the **Guidelines for Suspicious Communications** page on Confluence in the event of a suspicious conversation.

ADDITIONAL INFORMATION ON REQUIREMENTS FOR CERTAIN REGULATED BUSINESSES

DATA COLLECTED FOR CFTC REGULATORY PURPOSES

Our exchanges (CME, CBOT, NYMEX, COMEX)[1], our clearing house, and our global trade repositories are subject to regulations that apply additional **use** restrictions to certain types of information they collect.

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 has clearly consented to the use of such data in such a manner.

The definition of ***Regulatory Data*** for these purposes is limited to proprietary data or Personal Data collected, maintained or received for the purposes of fulfilling our regulatory obligations. More specifically, Regulatory Data includes:

- ***Derivatives Clearing Organization records*** – Records of all activities related to the clearing and settlement activities of the cleaning house, 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

[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.

received by the company from third-party depositories of clearing members in its capacity as a designated self-regulatory organization.

- ***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).
- ***Global Trade Repository data –*** Any information received or maintained by our global 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 policy merely because it is also received or maintained by a trade repository.

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 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 should be directed to **Privacy Compliance**.

Finally, the Regulatory Data received by our global 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.

BROKERTEC AMERICAS LLC

BrokerTec Americas LLC (***"BTEC"***) operates as an alternative trading system (***"ATS"***)[2] registered with the SEC 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.

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

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 directed to **Privacy Compliance**.

FANDUEL PREDICTION MARKETS LLC

FanDuel Prediction Markets LLC (***"FanDuel Predicts"***) operates as a futures commission merchant (***"FCM"***) registered with the CFTC and has established safeguards and procedures to limit **access** to the non-public information of its customers to those who are running the FCM or who are responsible for its compliance with applicable rules.

Non-public customer information, referred to as ***FanDuel Predicts Sensitive Information***, includes but may not be limited to:

- Customer detailed position information;
- Customer personal information; and
- Customer balances or margin amounts.

Only colleagues who provide services to assist the FCM's ongoing operations will be eligible to receive access to FanDuel Predicts Sensitive Information, and only if access to such information is necessary to perform their job function at the FCM or supervising the FCM. If you are confirmed to be eligible to have access to FanDuel Predicts I Sensitive Information, you may **not use** it for any other purpose other than for the business function of the FCM 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 FanDuel Predicts Sensitive Information should be directed to **Privacy Compliance**.

ADDITIONAL INFORMATION ON THE PROCESS TO REQUEST ACCESS TO AND USE OF CME GROUP CONFIDENTIAL AND CME GROUP HIGHLY SENSITIVE 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 directed to **Privacy Compliance**.

The Privacy team will review the request and may consult with representatives from Legal, Compliance, Market Regulation, Information Security and Data Management. The Privacy team will notify the requestor 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 consultation with the teams, they will assess the type of information the individuals propose to access and how the information will be used and will consider any regulatory or contractual considerations. Please refer to **OpenExchange** for additional guidance on data related to certain businesses and partnerships.

Examples of requests that should be submitted 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. Any access or use granted to a specific Department, team or colleague may not be shared with others without first obtaining additional approval, even with colleagues who are part of your same Department or team.

ADDITIONAL INFORMATION SECURE DISPOSITION

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**.