



*INTERNATIONAL FINANCIAL*  
*DATA SERVICES*

## International Financial Data Services (Luxembourg) S.A.

Procedure Owner: Compliance

Procedure Name: Making a report under the Law of 16 May 2023  
(Whistle-blowing Law)



## Version Control and Revision History

Version	Effective Date	Author	Approver	Revision Details
1.0	1 <sup>st</sup> December 2023	IFDSL Compliance	IFDSL Conducting Officers	First draft



## Contents

1. Purpose.....	4
2. Scope .....	4
3. Regulatory Requirements.....	5
4. Key concepts and definitions.....	5
i. What is a Violation? .....	5
ii. Information on violations.....	5
iii. In a professional context.....	6
iv. Reasonable belief.....	6
v. What is Retaliation? .....	6
5. Process – Step by Step Procedure .....	8
i. When to raise a concern? .....	8
ii. Options on raising a concern.....	8
iii. Internal reporting.....	8
iv. External reporting .....	9
v. Public disclosure.....	10
vi. Protection of Identity .....	10
6. Privacy and confidentiality .....	11
7. Appendices .....	12
Appendix I – Making a report using Navex .....	12
Appendix II – Follow up on a Navex report.....	18

## 1. Purpose

The objective of the Procedure is to enable the confidential escalation of improper professional behaviour and protect those individuals reporting incidents. It also provides guidance to employees and non-employees (or “external reporting persons”) on how to raise concerns they have relating to improper professional behaviour. IFDSL (“the Company”) is committed to maintaining an open culture with the highest standards of honesty and accountability where employees and non-employees can report any concerns in confidence, without fear of retaliatory treatment. This procedure has been written with reference to the requirements of the Law of 16 May 2023 transposing Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law (“Whistleblowing Law”).

## 2. Scope

The procedure applies to all persons working in the private or public sector who have obtained information about violations, in a professional context, which have occurred or are very likely to occur within IFDSL’s organization. According to the Article 2 of the “Whistleblowing Law”, these reporting persons can be, among others, current and former employees, contractors and sub-contractors, interns, suppliers, vendors, volunteers, board members, shareholders and job candidates.

In scope:

- Matters noted under the definition of a violation (see section 4.i.).

Out of scope:

- This procedure does not apply to matters exclusively affecting personal grievances such as bullying, harassment or issues relating to terms of employment which are covered by specific HR processes and procedures. This procedure does not apply to disclosures which do not relate to a “violation”.

This document is not intended to act as a substitute for normal day to day operational reporting or HR procedures or policies.

### 3. Regulatory Requirements

List the regulations that are applicable to this procedure document.

No.	Regulatory Requirement	Details
i	Law of 16 May 2023 transposing Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union Law	Sets out the legal basis for disclosing concerns related to violation (“whistle-blowing”)

### 4. Key concepts and definitions

#### i. What is a Violation?

A violation, in the Law, consist of acts or omissions which:

(a) are unlawful; or

(b) are against the object or purpose of the provisions of national or European law applicable directly.

A violation can also relate to the failure to comply with internal governance, professional obligations and regulatory requirement which results to harm to the public interest or to the interest of others (e.g. clients, IFDSL’s shareholders).

IFDSL’s primary aim is to prevent workplace violation from occurring in the first place. If it happens, the objective is to prevent it from reoccurring. If appropriate, every effort will be made to take necessary steps to resolve the situation on a case by case basis.

#### ii. Information on violations

Employees and non-employees are informed that they are not required or entitled to investigate matters themselves to find proof of their suspicion and should not endeavor to do so.

All reporting persons should disclose any information on violations, i.e. information, including reasonable suspicions, concerning actual or potential violations, which have occurred or are very likely to occur in the organization in which the reporting person works or worked or in another organization with which the reporting person is or has been in contact with in the course of his work, and regarding attempts to conceal such violations.

### iii. In a professional context

A professional context means past or present professional activities in the public sector or private by which, regardless of the nature of these activities, people obtain information on violations and in connection with which these persons could be the subject of retaliation for reporting such information.

### iv. Reasonable belief

A reporting person must have a reasonable belief that the information disclosed shows, or tends to show, a violation. The term "reasonable belief" does not mean that the belief has to be correct. Reporting persons are entitled to be mistaken in their belief, so long as their belief was based on reasonable grounds.

It may be quite reasonable for a reporting person to believe that a wrongdoing is occurring on the basis of what he or she observes. A reporting person may not know all the facts of the case and as noted above, the reporting person is not obliged to find proof of their suspicion. In such a case the reporting person may have reasonable grounds for believing that some form of violation is occurring, but it may subsequently turn out that the reporting person was mistaken.

No reporting person will be subject to any form of retaliation simply for getting it wrong, so long as the reporting person had a reasonable belief that the information disclosed showed, or tended to show, violation.

### v. What is Retaliation?

"Retaliation" means any direct or indirect act or omission which occurs in a professional context, due to the making of an internal or external report or public disclosure (whistleblowing), and which causes (or may cause) unjustified detriment to an individual. In particular, the following forms of retaliation are prohibited (this is a non-exhaustive list):

- a) Suspension, lay-off or dismissal,
- b) demotion, loss of opportunity for promotion or withholding of promotion,
- c) transfer of duties, change of location of place of work, reduction in wages or change in working hours,

- d) the imposition or administering of any discipline, reprimand or other penalty (including a financial penalty),
- e) coercion, intimidation, harassment or ostracism,
- f) discrimination, disadvantage or unfair treatment,
- g) injury, damage or loss,
- h) threat of reprisal,
- i) withholding of training,
- j) a negative performance assessment or employment reference,
- k) failure to convert a temporary employment contract into a permanent one, where the worker had a legitimate expectation that he or she would be offered permanent employment,
- l) failure to renew or early termination of a temporary employment contract,
- m) harm, including to the worker's reputation, particularly in social media, or financial loss, including loss of business and loss of income,
- n) blacklisting on the basis of a sector or industry-wide informal or formal agreement, which may entail that the person will not, in the future, find employment in the sector or industry,
- o) early termination or cancellation of a contract for goods or services,
- p) cancellation of a licence or permit,
- q) psychiatric or medical referrals.

The reporting persons will not be subject to any form of retaliation, including harassment, victimization, or disciplinary action by IFDSL as a result of raising the concern, in accordance to the article 25, 26 and 27 of "Whistleblowing" law. They shall in no way be put at a disadvantage as a result of his report.

A fine of 1,250 to 25,000 euros can be imposed by authorities on persons exercising retaliation against the reporting persons.

## 5. Process – Step by Step Procedure

### i. When to raise a concern?

Employees or external reporting persons should raise concerns if they have a reasonable belief that a violation has occurred, is occurring or is likely to occur. This is to ensure that the Company can review the facts and take corrective action.

### ii. Options on raising a concern

Reporting persons have available to them a number of ways to disclose violations, internally, externally or with public disclosure. Reporting persons are strongly encouraged to report their concerns internally as set out below but there may be circumstances where an individual wants to make a disclosure externally or with a public disclosure.

The Company confirms that internal reports will be taken seriously, and that the reporting person will receive appropriate protection, in accordance with regulatory requirements.

**Note:** Reporting persons must make a report in the manner set out in this procedure in order to gain the protections of the Whistleblowing Law.

### iii. Internal reporting

Employees and external reporting persons have the possibility to report a violation through Navex, an independent firm which facilitates confidential reporting 24 hours a day, seven days a week. Reports can be made both orally, via a dedicated phone line, and in writing, via a web-form online.

Reporting persons may communicate with Navex on an anonymous basis. It is preferable, however, for reporting persons to identify themselves to enable the Company to obtain a complete report of the relevant facts as expeditiously as possible. Information that a reporting person provides the Company, will be handled confidentially to the extent permitted by law. The Company may not be able to investigate anonymous reports if there is insufficient detail or if it is not possible to obtain further information where required.

Reporting persons should note that important elements of the Company's report handling procedures (e.g., keeping the reporting person informed) may be difficult or impossible to apply unless the reporting person discloses their identity. Furthermore, a reporting person cannot obtain redress under the Law without identifying themselves as part of the process of seeking redress.



The initial recipients of confidential reports from Navex are the Chairman of the Board and the Head of Compliance ("Designated Persons"). The Designated Persons will investigate the reports and take appropriate actions depending on the circumstances, including notifying the appropriate internal or external functions (e.g., Managing Director or HR), without delay. The Designated Persons, if necessary and in consultation with the appropriate internal or external functions, will appoint a person responsible for investigating the disclosure and liaising with the employee or external person who raised the concern. Communications from Navex may be forwarded within the Company for further action as appropriate, in line with confidentiality and privacy requirements set out in section 6.

You can submit a report via Navex using the following communication methods:

**By telephone:**

From Luxembourg: Dial the Global Inbound Services (GIS) number: 8008-5259

**By Web-Form online:**

Open [ifdsluxembourg.ethicspoint.com](https://ifdsluxembourg.ethicspoint.com) with your Internet browser. Select the "Make a Report" link at the top of this web page and follow the instructions.

Please see detailed instructions in Appendix I.

Note: Users can follow up on a report made via Navex. See Appendix II for instructions.

#### iv. External reporting

Where an employee or external reporting person wishes to make a report externally to the CSSF they may make the disclosure through the following channels:

- **E-mail:** [whistleblowing@cssf.lu](mailto:whistleblowing@cssf.lu)
- **Phone:** +352 26251 2757
- **Online Web form:**
  - <https://whistleblowing.apps.cssf.lu/index.html?language=en> (for English version)
  - <https://whistleblowing.apps.cssf.lu/index.html?language=fr> (for French version)

Further details about utilising CSSF resources for whistleblowing could be accessed under the following link: [https://www.cssf.lu/wp-content/uploads/whistleblowing\\_EN.pdf](https://www.cssf.lu/wp-content/uploads/whistleblowing_EN.pdf)

Before contacting the CSSF, IFDSL employees and external reporting persons are encouraged to first use the whistleblowing internal reporting procedures described in section 5.iii of this document.

## v. Public disclosure

Besides the internal and external reporting options, IFDSL staff or external reporting persons can also decide to make a public disclosure, i.e. making available in the public sphere information about violations. This is generally the last viable option, after a person has already reported internally to the Company or externally to the authorities and did not receive an appropriate response.

## vi. Protection of Identity

### **IDENTITY OF REPORTING PERSON**

The Company shall ensure that the identity of the reporting person is only ever shared on a “need to know” basis and only where it is necessary to carry out proper follow-up of a report.

In other cases, the Company will seek the reporting persons consent before disclosing their identity. However, there are circumstances allowed by the Law, where the identity can be disclosed without consent, e.g., where disclosure is otherwise required by law or prevention of a serious risk to the security of the State, public health, public safety or the environment.

Reporting persons who are concerned that their identity is not being protected should notify the IFDSL Compliance team (LUX-IFDS-REGULATORY@statestreet.com). The Company is committed to assess / investigate such notifications, and to take appropriate action where necessary.

Any attempt to identify the reporting person should not be made by persons within IFDS to whom the identity has not been revealed as part of the receipt and follow-up of the report of a disclosure. If such attempts are made, whether successful or not, this will be dealt with under the HR disciplinary process.

### **IDENTITY OF PERSONS CONCERNED**

The person concerned is a person to whom the violation is attributed or associated with.

The Company shall protect the identity of a person concerned, while an investigation is ongoing, unless disclosure of the identity is necessary in accordance to the Law.

The reporting persons who have knowingly disclosed false information may be subject to prison sentence of eight days to three months in prison and a fine of 1,500 euros to 50,000 euros.

## 6. Privacy and confidentiality

IFDSL is committed to protect the privacy of the reporting persons involved to the fullest extent possible and in accordance with applicable laws. Any personal data obtained, as part of the whistleblowing report, shall be carried out in accordance with the General Data Protection Regulation (EU) 2016/679 and Law of 1 August 2018 and will only be provided to those persons who have a need to know these data for these purposes or to comply with the law.

The reports will be disclosed only to the members of staff who are concerned for the purpose of the investigations. The personal data in the whistleblowing report can relate to Whistleblower, the persons under investigation, witnesses or other individuals that are mentioned and remain subject to applicable data protection laws.

Where a report is received by IFDSL staff members other than those responsible for handling reports, the staff members who receive it are prohibited from disclosing any information that might identify the reporting person or the person concerned, and they should promptly forward the report without modification to the Head of Compliance. All staff involved in the whistleblowing process and having access to whistleblowing reports will maintain strictly confidential and secret the content of any reports made.

Personal data which is not relevant for the processing of a specific report shall not be collected or, if accidentally collected, will be erased without undue delay.

The person who is the subject of a whistleblowing report has the right to request access, correction, or erasure of personal data or to object to the processing or receive a copy of the personal data held through this process. Such requests must be made by contacting the IFDSL Privacy Office (IFDS\_PrivacyOffice@StateStreet.com) which will engage with IFDSL Compliance Department for fulfilment of the data subject request as applicable.

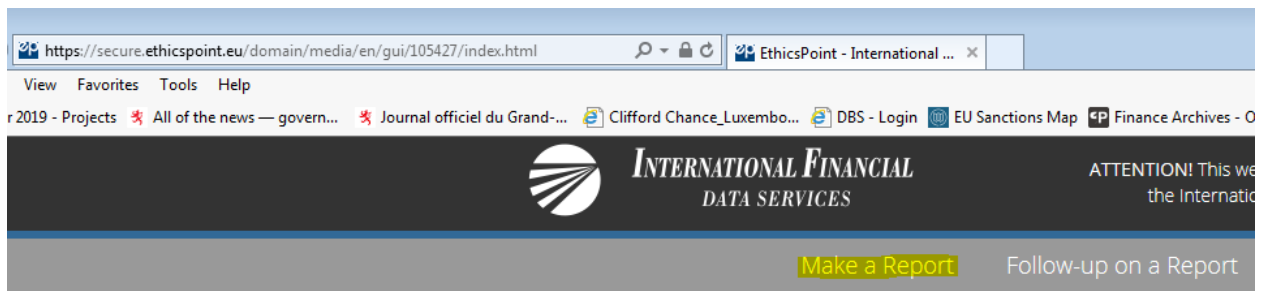
The report and the personal data there included will not be kept longer than 6 months from the conclusion of the investigation, which will be communicated to the reporting person as described in "Appendix II – Follow up on a Navex report" at the end of this document. Such period would be different when legal proceedings or disciplinary measures are initiated against the incriminated person or the reporting person in cases of false or slanderous declaration. In such cases, personal data will be kept until the conclusion of these proceedings and the period allowed for any appeal.

## 7. Appendices

### Appendix I – Making a report using Navex

#### Make a Report – Online

1. Go to the IFDS Luxembourg Whistleblowing website - [ifdsluxembourg.ethicspoint.com](https://ifdsluxembourg.ethicspoint.com)
2. At the Home page, click on the **Make a Report** link.



#### Our Commitment

INTERNATIONAL FINANCIAL DATA SERVICES (LUXEMBOURG) S.A. is an organization with strong values of responsibility and integrity. Our Standard of Conduct contains general guidelines for conducting business with the highest standards of ethics.

3. Select the type of report that you would like to make. The options are:

- Accounting and Auditing Matters
- Anti-Bribery
- Bank Secrecy Act (BSA) / Anti-Money Laundering Laws and Terrorism Financing
- Banking
- Discrimination or Harassment
- Embezzlement
- Falsification of Contracts, Reports or Records
- Sabotage or Vandalism
- Substance Abuse
- Theft
- Violation of Policy

- Violence or Threat
- Other

Users can click on the **Details** link of each option to reveal additional information about each type of report. For example, clicking on the **Details** link for Violation of Policy reveals:

Violation of Policy	Details
<p>Willful or innocent actions that are in direct violation of company policy, procedures, code of conduct, and/or implied contractual responsibilities. (Examples include: non- disclosure agreements, hiring standards, safety, Internet usage, corporate guidelines)</p>	

4. Once the user has selected the type of report that they wish to make, they will be presented with an information requesting screen. Below is a Test example for a **Violation of Policy** report:

ETHICSPPOINT IS NOT AN EMERGENCY SERVICE.  
 Do not use this site to report events presenting an immediate threat to life or property. Reports submitted through this service may not receive an immediate response. If you require emergency assistance, please contact your local authorities.

\* Yes - I agree to the [Terms and Conditions](#) of making this report.

**Please provide information as follows:**  
 ( \* Required fields )

Organization/Tier: **International Financial Data Services (Luxembourg) S.A.**

Location where incident occurred:

Physical address, branch and/or store number

City:  State/Province:

Zip/Postal Code:

Country:

**\* Relationship to the Company or Organization?**

In this example, the user has chosen to stay anonymous.

**\* Do you wish to remain ANONYMOUS for this report?**  
 Yes  No

The user will be asked additional questions (the answers included are for illustration purposes only):

**Report - Violation of Policy**

**\*Please identify the person(s) engaged in this behavior:**  
Example:  
John Doe, Director of Internal Audit  
Unknown, Unknown, Night Supervisor

	First Name	Last Name	Title
#1	Mr	Pink	Accounts
#2	Mrs	Black	Admin
#3	Mr	Blue	Facilities

**Do you suspect or know that a supervisor or management is involved?**  
 Yes  No  Do Not Know / Do Not Wish To Disclose

If yes, then who?

Mrs White, Director of Operations	Example: John Doe, Director of Internal Audit
-----------------------------------	--

Any persons mentioned here will be restricted by EthicsPoint from access to this reported information.

**Is management aware of this problem?**  
 Yes  No  Do Not Know / Do Not Wish To Disclose

**What is the general nature of this matter?**  
Work PCs are being used to print political material.

This should be a general description only, you will be asked for specifics later.

**where did this incident or violation occur ?**

In the kitchen which is turned in to an unofficial makeshift printing facility on Friday nights.

We recognize that this incident may not have occurred in a particular location. However, if this incident was observed in some documentation or business transactions, please indicate this accordingly.

**Please provide the specific or approximate time this incident occurred:**

Friday, April 27th, 2018  
Friday, April 20th, 2018

Examples:

Tuesday, May 3, 2002  
Two weeks ago  
Approximately a month ago

**\* How long do you think this problem has been going on?**

1 to 3 months

**\* How did you become aware of this violation?**

I observed it

If other, how?

**Please identify any persons who have attempted to conceal this problem and the steps they took to conceal it:**

Mr Blue, Facilities  
Told me that they had permission when I asked what was going on.

Examples:

Ignored it  
Changed documents  
Said it was not a problem  
Said they would look into it

Please identify by name and title.

In this example, the user has uploaded a file called **This is a test file.docx** – Note: The following file types are supported: Word, Excel, and PDF:

**If you have a document or file that supports your report, most common file types can be uploaded:**

[Click here to upload files](#)

**\* Please provide all details regarding the alleged violation, including the locations of witnesses and any other information that could be valuable in the evaluation and ultimate resolution of this situation.**

I was working late and went to get a glass of water in the kitchen and observed my colleagues engaged in desktop publishing and printing, using work PCs in the kitchen - etc. etc. etc. etc. etc.


Please take your time and provide as much detail as possible, but exercise care to not provide details that may reveal your identity unless you wish to do so. It may be important to know if you are the only person aware of this situation.

When you submit the report, you will be issued a Report Key. Please write it down and keep it in a safe place. We ask you to use this Report Key along with the password of your choosing to return to EthicsPoint through the website or telephone hotline in 5-6 business days. By returning in 5-6 business days, you will have the opportunity to review any Follow-up Questions or submit more information about this incident.

Users must choose a unique password for each report they submit. Once this has been completed, the user can click on the **Submit Report** button.

**Please choose a password for this report:**

\* Password:

\* Re-enter Password:  

Your passwords must match and be at least four characters long.

**Submit Report**

Immediately upon successful submission of an online report, the user will receive back a confirmation notification. It is vital that the user records the **Report Key** and notes their **Password** of the report for future reference.





You are now in an EthicsPoint Secure Area | [File a Report](#)

### YOUR REPORT KEY IS:

874043407202

### WRITE THIS DOWN AND KEEP THIS IN A SAFE PLACE!

You will need your report key and the password you selected to check on your report in the future or to make a follow-up.

### PLEASE ALLOW 5-6 BUSINESS DAYS FOR PROCESSING AND REVIEW

Begin checking after 5-6 business days and then continue to check periodically to see if the organization has any additional questions for you to answer regarding your report.

### HOW TO FOLLOW-UP ON A REPORT

Go to [www.ifdsgroup.ethicspoint.com](http://www.ifdsgroup.ethicspoint.com) OR Call our toll-free hotline at 844-222-1725

[Return to EthicsPoint home](#)



[Privacy Statement](#) | [Terms of Use](#)  
© 2018 NAVEX Global Inc., All Rights Reserved.



## Make a Report – Telephone

To make a telephone report, users can call Global Inbound Services (GIS). From an outside line dial the GIS number for Luxembourg:

8008-5259

This number can be called without any need for international / local prefixes.

After you complete your report you will be assigned a unique code called a "report key." Write down your report key and password and keep them in a safe place.

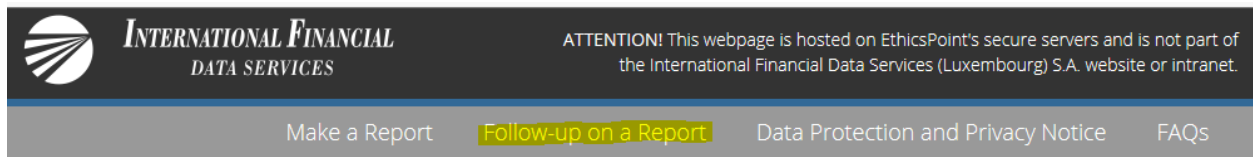
## Appendix II – Follow up on a Navex report

### Online

The member of staff or the external reporting person who has submitted the report will receive an acknowledgement of the receipt of that report within seven days. A diligent follow-up will be also provided by the Head of Compliance or Chairman of the Board to the reporting person.

Use your report key and password to check your report for feedback or questions.

To check an **online** report, logon to the IFDS Luxembourg Whistleblowing website and click on the **Follow-up on a Report** link ([ifdsluxembourg.ethicspoint.com](http://ifdsluxembourg.ethicspoint.com)).



### Our Commitment

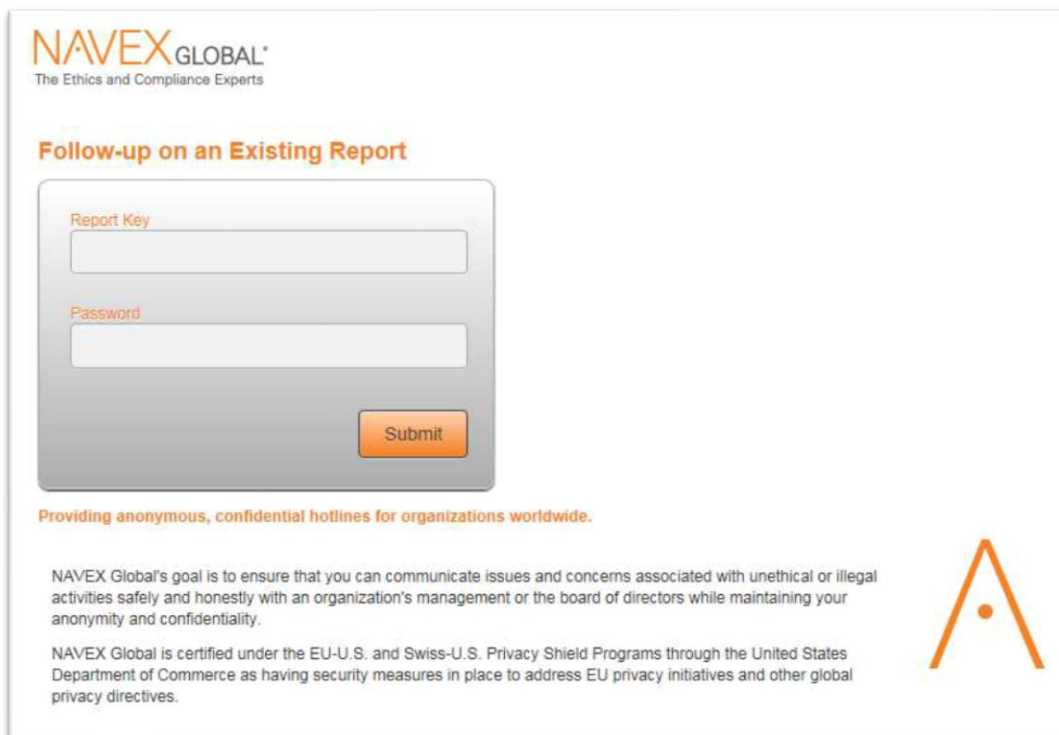
INTERNATIONAL FINANCIAL DATA SERVICES (LUXEMBOURG) S.A. is an organization with strong values of responsibility and integrity. Our Standard of Conduct contains general guidelines for conducting business with the highest standards of ethics.

### To Make a Report

You may use either of the following two methods to submit a report:

Online:

Then enter the relevant **Report Key** and **Password** in the screen below:



The user will be brought into the following screen and will be alerted to any Questions or Comments.

The screenshot displays the 'ethics-point' reporting interface. On the left, there is a sidebar with the following sections: 'Issue Type' (Violation of Policy), 'Report Actions' (Questions and Comments, Add Follow-Up Notes, Upload Files, Report Details, Print My Report, Join a Chat, Log Off), and the NAVEX GLOBAL logo. The main content area is titled 'Report Details' and contains the following information: Report Submission Date (5/3/2018), Reported Company/Branch Information (Location Bishop's Square, Redmond's Hill, City/State/Zip: Dublin, Dublin 2, Ireland), a list of persons engaged in the behavior (Mr Pink - Accounts, Mrs Black - Admin, Mr Blue - Facilities), a question about supervisor involvement (Yes), the name of the supervisor (Mrs White, Director of Operations), a question about management awareness (No), the general nature of the matter (Work PCs are being used to print political material), the location of the incident (In the kitchen which is turned in to an unofficial makeshift printing facility on Friday nights), and the specific or approximate time the incident occurred (Friday, April 27th, 2018 and Friday, April 20th, 2018). At the bottom of the page, there are logos for SAS70 Type II Certified, TRUSTe Certified Privacy, and the NAVEX GLOBAL logo with the text 'The Ethics and Compliance Experts' and '© NAVEX Global 2018. All rights reserved.'.

Furthermore, within three months from the receipt of the acknowledgement, the reporting person will receive feedback about how the report has been dealt with, whether any corrective measures or process improvements have been recommended, and if any further steps will be taken.

## Telephone

To follow up on a **telephone** report submission, users need to call **8008-5259**. Users will need to have their **Report Key** and **Password** ready for the operator, who will assist the user through the process.

## Miscellaneous

Please keep in mind that EthicsPoint is **NOT** an **Emergency Service!**

Do not use this web-page or the phone number provided there to report events presenting an immediate threat to life or property. Reports submitted through this service may not receive an immediate response. If you require emergency assistance, please contact local authorities.

Should you have any specific questions not covered here as to the EthicsPoint reporting system, hot-line or any other queries related to the Whistleblowing process within the Company please contact the Compliance Department directly or via email address [LUX-IFDS-Regulatory@StateStreet.com](mailto:LUX-IFDS-Regulatory@StateStreet.com).