syntrio

LAUNCHING THE LIGHTHOUSE WHISTLEBLOWER HOTLINE ACROSS EUROPE

Launching a Whistleblower Hotline Across Europe

Table of Contents

Abstract

Our hotlines are used by companies worldwide to uncover hidden business risks and address various issues such as loss prevention, ethics and integrity violations, HR related concerns, workplace safety, and other serious matters your stakeholders and employees would like to anonymously report.

Our program quickly brings you into compliance with multiple disparate regulatory requirements including:

- Sarbanes-Oxley Act
- Dodd-Frank Act
- Federal Acquisition Regulations
- American Recovery and Reinvestment Act of 2009
- Deficit Reduction Act of 2005
- Federal Sentencing Guidelines

While whistleblower hotlines are prevalent in the United States, attempts at hotline implementation by U.S. multinationals within their European operations have proven at times to be challenging. In general, Europeans tend to be more protective of their personal privacy than Americans, and more stringent data privacy laws are in place in many European nations.

Moreover, global companies face various restrictions regarding whistleblower programs across multiple jurisdictions within the European Union (hereinafter "EU") and surrounding European Economic Area (hereinafter "EEA").

Issues Faced by Multinationals When Launching a European Hotline

Many EU member states have constructed legal hurdles restricting the use of whistleblower reporting hotlines, in particular restricting the scope of topics that may be reported through the hotline, restricting who may be the subject of a report and disallowing anonymity of the reporter.

Over a dozen European jurisdictions interpret their local domestic data protection laws specifically to rein in employer hotlines. An EU advisory body called the Article 29 Working Party issued a persuasive but non-binding report that recommends all twenty-eight EU members embrace a particularly-restrictive interpretation of EU data law to restrict hotlines.

Issues Faced by Multinationals When Launching a European Hotline

Many EU member states have constructed legal hurdles restricting the use of whistleblower reporting hotlines, in particular restricting the scope of topics that may be reported through the hotline, restricting who may be the subject of a report and disallowing anonymity of the reporter.

Over a dozen European jurisdictions interpret their local domestic data protection laws specifically to rein in employer hotlines. An EU advisory body called the Article 29 Working Party issued a persuasive but non-binding report that recommends all twenty-eight EU members embrace a particularly-restrictive interpretation of EU data law to restrict hotlines.

The goal accordingly is to facilitate a framework for multinationals to establish compliance guidelines and whistleblowing reporting programs that are both effective and consistent across the entire organization, while simultaneously observing applicable data protection, privacy and labor laws in foreign countries.

Before offering a hotline in a particular EU state, companies should attempt to isolate the unique issues that pertain to local law. Organizations should refer to the country summaries included within this primer as well as consult their local data protection authority for guidance. Companies should then take steps necessary to develop their hotline reporting protocols and employee communications packages. Some multinationals have successfully dealt with these issues by developing various hotline communication protocols for each member state.

Among the specific issues in European jurisdictions, the most meaningful are:

1. Restrictions against hotlines accepting anonymous reports
2. Limits on the scope of infractions for which a hotline may accept reports
3. Limits on who can use a hotline to submit a report
4. Limits on who may be the subject of a report
5. Hotline registration requirements
6. Notices to employees, targets and witnesses explaining their rights
7. Complying with “sensitive” data restrictions for information received through the hotline
8. Rights to access, rectify, block or eliminate personal data processed via hotline
9. Restrictions against transferring hotline data outside of Europe
10. Deleting/purging data in hotline call files

Two-Step Process for Developing a Solution

The following are actions that a company should take when establishing a hotline in any EU or EEA business operation:

1 *Assess its position regarding EU data protection law issues.*

The issues relevant to implementing whistleblower hotlines regarding substantive compliance requirements as well as procedural data requirements for clients of Lighthouse include:

- Limiting the list of reportable offenses pertaining to the whistleblower hotline (i.e. scope of reporting)
- Discouraging anonymity (anonymous reporting)
- Allowing data subjects to access, correct, rectify and/or delete personal data collected
- Not requiring rank-and-file workers to report on colleagues' misconduct
- Cleary communicating due process rights, particularly the presumption of innocence
- Obtaining permission to implement a hotline where necessary, from the local data protection authority (some countries require a separate filing for hotlines in addition to the filing for general human resources data)
- Consult with and/or receive approval where applicable from the local works council or employee representative
- Translating hotline communications into the applicable local language

2 *Inform/Consult/Co-determine*

Before implementing a whistleblowing reporting program in Europe, companies should take the time to inform/consult/co-determine with worker representatives and also the local data protection authority (hereinafter "DPA") within the relevant country, prior to launching.

Employees should be informed regarding the details of the whistleblowing program including, but not limited to procedures for submitting and handling reports, as well as possible consequences for unfounded reports.

General Data Protection Regulation (GDPR)

In addition to data privacy regulations in individual countries within the EEA, the General Data Protection Regulation ("GDPR") became effective May 25, 2018.

GDPR is designed to strengthen and unify existing data protection for all EU citizens. The primary objectives are to ensure individuals have control over their personal data and to simplify the regulatory environment for businesses. The regulation affects not just companies located or operating within the EU, but all organizations that process personal data of EU citizens.

In the context of your relationship with Lighthouse, GDPR applies to you if Lighthouse's services are offered to data subjects in the EU. This may include but isn't limited to extending Lighthouse's hotline reporting services to affiliates, employees, vendors, contractors, customers or other data subjects.

In this respect, we request our customers to inform us when they intend to use our services in the context of any EU establishment or if they otherwise feel that the GDPR is applicable to their operations.

As defined under GDPR, Lighthouse is a processor of customer data. The customer is the controller of the data and must comply with applicable data privacy legislation accordingly.

To ensure GDPR compliance Lighthouse has undertaken the following measures:

- Lighthouse Services, Inc., is certified under the Privacy Shield which can be viewed at
- Lighthouse enters into data processing agreements with its customers if the GDPR applies to the processing of their data
- Lighthouse enters into sub-processing agreements with its providers as necessary
- Lighthouse implements up-to-date security measures and performs audits
- Lighthouse has enabled clients the ability to set Closed Report Notifications within our Case Management System ("CMS") allowing users to set country specific reminders helping to ensure compliance with GDPR Articles 13 through 17 relating to the rights of data subjects regarding storage and retention of data that is no longer necessary for the purpose that it was collected or otherwise processed
- Lighthouse has adopted policies in relation to security, data breaches, data protection impact assessment, prior consultation and other provisions of GDPR

In addition to GDPR, as previously mentioned, each European nation offers its own unique set of laws, rules and regulations pertaining to data privacy compliance, it is important to gain an awareness of the laws before launching a hotline in a particular nation. Lighthouse provides a one stop solution whereby our scripts are customized to meet each country's individual regulatory requirements.

The goal of the following individual country summaries is to facilitate a framework for analyzing and constructing multinational or global whistleblowing programs, with an eye towards consistency and adherence to local law.

PLEASE NOTE that this guide provides general information only. While this primer is not inclusive of all twenty-eight EU countries, its purpose is to provide a brief overview of legislation governing whistleblowing programs in each jurisdiction covered. If you have an inquiry regarding a country that isn't covered in this primer, you may contact counsel or the local DPA for guidance. This information is not comprehensive and is not intended as professional or legal advice, generally or in a given situation. This guide is an outline of country-specific obligations, which may change. Legal counsel and advice should routinely be obtained, including locally for any particular jurisdiction. Please consult your own counsel.

Preliminarily, it is important to note with regard to data privacy regulations, processing of data and cross border transfers, when implementing a whistleblower program, the following definitions generally apply across the EU/EEA:

Personal data means any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her identity. For example, in the context of a whistleblower hotline, personal data could pertain to the reporter and/or the subject of the report.

Sensitive personal data generally means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

Data controller means the person which alone or jointly with others determines the purposes and means of the processing of personal data (i.e. the employer).

Data processor means a person which processes personal data on behalf of a data controller (i.e. Lighthouse).

Data subject means an individual about whom personal data is being processed.

Standard processor obligations means obligations on the data processor to only act on instructions from the data controller and to comply with the general security obligations.

General data security obligations means the obligation to implement appropriate technical and organizational measures to protect personal data having regard to the state of the art, the risks represented by the processing and the nature of the data to be protected (Article 17(1), Data Protection Directive).

Standard conditions for processing personal data means the processing satisfies the general principles for data processing and is: (a) carried out with the data subject's consent ; or (b) necessary for the performance of a contract with the data subject; or (c) necessary for compliance with a legal obligation; or (d) necessary in order to protect the vital interests of the data subject; or (e) necessary for the public interest or in the exercise of official authority; or (f) necessary for the data controller's or recipient's legitimate interests, except where overridden by the interests of the data subject.

The general principles of data processing are that personal data is: (a) processed fairly and lawfully; (b) collected for specific, explicit and legitimate purposes and not processed in a manner incompatible with those purposes; (c) adequate, relevant and not excessive; (d) accurate and, where necessary, up to date; (e) kept in an identifiable form for no longer than necessary.

Standard conditions for processing sensitive personal data means the processing: (a) is carried out with the data subject's explicit consent; or (b) is necessary for a legal obligation in the field of employment law; or (c) is necessary to protect the vital interests of the data subject where the data subject is unable to give consent; or (d) is carried out by data subject a non-profit-seeking body and relates to members of that body or persons who have regular contact; or (e) relates to data made public by the data subject; or (f) is necessary for legal claims; or (g) is necessary for medical reasons.

Fair processing information means the provision of information about (a) the identity of the data controller and of his representative, if any; (b) the purposes of the processing for which the data are intended; and (c) any further information in so far as such further information is necessary, having regard to the circumstances in which the data are collected to guarantee fair processing.

Standard conditions for cross-border transfer means the cross-border transfer: (a) is to a whitelisted country; or (b) is made pursuant to a set of Model Contracts; or (c) is made pursuant to Binding Corporate Rules (if permitted in that jurisdiction); or (d) is made pursuant to the provisions of the Privacy Shield; or (e) is made with the data subject's consent; or (f) is necessary for the performance of a contract with, or in the interests of the data subject; or (g) is necessary or legally required on public interest grounds, or for legal claims; or (h) is necessary to protect the vital interests of the data subject; or (h) is made from a public register.

Model contracts (Standard contractual clauses) means the contractual clauses set out in Commission Decision C(2010) 593, Commission Decision C(2004) 5271 and Commission Decision C(2001) 1539 which can be utilized as a vehicle for cross-border transfers insuring an adequate level of data protection.

While the United States is not a whitelisted country, as mentioned previously, Lighthouse Services, Inc., is certified under the Privacy Shield, negating the need to utilize Model contracts for cross-border transfers from the EU to the United States within the context of our whistleblower program.

Austria

The Austrian data protection authority (hereinafter "DPA") is the supervisory authority for data protection.

Austrian Data Protection Authority
Hohenstaufengasse 3
1010 Vienna
Austria
www.dsb.gv.at

Notification to the DPA of a whistleblowing program is required and can be done by data application online.

Contrary to the standard definition of personal data, the definition of personal data under the DPA extends to data relating to both individuals and legal entities. Austria is one of the few countries to extend local data protection law to legal entities.

The DPA has approved the following scope for reporting: identification, contact, professional qualification, determination of the circumstances of the case, and data about possible consequent actions. Generally, that means the scope of the report is typically the employee's behavior at work, but also matters concerning accounting, corruption and financial crimes are acceptable reportable incidents.

All employees may be entitled to report. It is unclear whether external suppliers may also report under a whistleblowing program.

A data controller must provide fair processing information to data subjects. Additionally, he must provide the data subject, upon request, with a list of the processed data and a description of the origin of the data, the legal basis for the data processing and the recipients of the data (if any). Such information has to be given within eight weeks. Generally, this means that a person who has information collected about them as part of the whistleblowing program, has the right to know the identity of the company, Lighthouse and purposes for which the data is being processed.

Belgium

A whistleblower program has to comply with the provisions of the Belgian Act on the protection of privacy in relation to the processing of personal data (hereinafter "DPA").

The Commission for the Protection of Privacy is the supervisory authority for data protection (hereinafter the "Commission") and has addressed the specific issue of whistleblowing programs in its Recommendation 01/2006 regarding the compatibility of whistleblowing with the DPA in relation to the processing of personal data ("CPP Recommendation").

Commission for the Protection of Privacy
Rue de la Presse 35
1000 Brussels
Belgium
www.privacycommission.be

The CPP Recommendation provides guidelines as how the implementation of a whistleblowing program can comply with the principles and requirements of the DPA. Most of the provision of this Recommendation are inspired by the Article 29 Data Protection Working Party text approving whistleblowing programs in the fields of accounting, internal accounting controls, auditing matters, anti-bribery, banking and financial crime.

Belgian rules however, do not limit reporting systems to these categories so long as the conditions of the DPA are met.

The data controller must notify the Commission before the start of any wholly or partially automated processing operation. Such notification is a mere filing of information that can be made by electronic means.

Anonymous reports are in principle forbidden but the CPP Recommendation states that there must be promotion of identified and confidential reports versus anonymous reports.

Anonymous reports are exceptionally allowed in so far as:

- Anonymity is not mandatory;
- Anonymity is not encouraged as the usual way to make a complaint
- The company does not advertise that anonymous reports may be made through the program
- The program informs the whistleblower their identity will be kept confidential at all stages of the process

With regard to whistleblower hotlines, no specific limitation is provided for regarding scope of reporting, as long as all conditions of the Belgian Privacy Act are met. A legitimate interest for the company to install the system complies, provided that it is not overridden by interests, fundamental rights and freedoms of the concerned data subject.

When introducing a whistleblowing program the employer will need to inform the workers collectively (through the Works Council, the Prevention and Protection Committee or the unions) as well as individually. Ideally, the employer obtains the worker's consent, by making them sign a copy of the policy for approval.

A data controller must provide fair processing information to data subjects.

Upon request, the data controller must provide the subject access information to the data subject, free of charge.

Czech Republic

The supervisory authority for data protection in the Czech Republic is the Office for Personal Data Protection (hereinafter "DPA").

Office for Personal Data Protection
(Úad pro ochranu osobních údaj)
Pplk. Sochora 27,
170 00, Prague 7
Czech Republic
www.uoou.cz

Personal data may only be processed by a data controller that has submitted notification to the DPA.

A data controller must provide the fair processing information to data subjects including information about data subjects' rights.

There is no defined scope of reporting in the applicable Czech legislation which follows the Working Party Opinion expressly stating that the fields of accounting, internal accounting controls, auditing matters, anti-bribery, banking and financial crimes fall within the permitted scope for whistleblowing hotlines.

Anonymous reporting is not prohibited, however, even though Czech law does not specifically forbid anonymous whistleblowing, it is not advisable.

Data subjects may obtain their subject access information by written request to data controllers. The data controller is entitled to ask for reasonable payment not exceeding the costs associated with the provision of a response to a subject access request.

The data subject may ask the data controller to correct his personal data if they are untrue or inaccurate. The data subject is entitled to ask the data controller to inform him which of his personal data are being processed.

No specific security requirements exist for operation of a whistleblowing program, all of the characteristics of the program, including the periods for which the personal data may be retained, must be strictly adequate to the purpose of processing. Even though there are no specific data retention periods prescribed by law, the program must specify for how long the data shall be retained and the employer must be prepared to justify such a period to the DPA.

Denmark

The supervisory authority for data protection in Denmark is The Data Protection Agency (the "Agency")

The Data Protection Agency (Datatilsynet)
Borgergade 28, 5
DK-1300
Copenhagen K
Denmark
Phone +45 33 19 32 00
www.datatilsynet.dk

While Denmark has no specific whistleblower protection laws in place, sections of the Danish Financial Business Act state companies in the financial sector are obligated to implement a whistleblower program that enables employees and board members to anonymously report any violation of the financial regulations committed by the company or its employees.

In addition, the Danish Act on Processing of Personal Data ("DPL") contains the general rules applicable to all processing of personal data, including processing of personal data in connection with whistleblower programs.

Both notification and authorization from the Agency is required prior to implementation of a whistleblowing program.

No employee consent is required for implementation of a whistleblower program however they should be informed of its implementation and details thereof. A whistleblower policy should also be implemented prior to commencing the program.

Companies with more than thirty-five (35) employees must appoint a Works Council that must be consulted prior to implementing a whistleblower program, consisting of members representing the employees and the management.

Only serious matters (actual or imminent) that can influence the company or group as a whole or the life or health of individuals can be reported under the whistleblower program (i.e. fraud, bribery, falsification of documents, unlawful behavior in connection with accounting, internal accounting controls or auditing matters, corruption, and environmental violations). The Agency has specifically stated that all matters that may be reported under the U.S. Sarbanes Oxley Act may also be reported under a whistleblower program.

Reporting on minor misconduct, (i.e. bullying, absence, incompetency, issues relating to difficulties in cooperation, or violation of company guidelines) are generally not permitted.

Anonymous reports are generally permitted, however the company should make an effort to avoid anonymous reporting.

The data controller shall at the request of the data subject rectify, erase or block data which is inaccurate or misleading or in any other way processed in violation of law or regulations.

According to the DPL, the personal data processed in connection with the whistleblower program can only be stored for as long as needed for the purpose for which it has been collected, (i.e. if the report proves groundless, the personal data should be deleted immediately).

Finland

There is no special legislation involved with a whistleblower system but whistleblower programs have to fulfill the general requirements set forth in the Personal Data Act, the Act on Protection of Privacy in Working Life and the Employment Contracts Act. The Data Protection Ombudsman who serves as the data protection authority (“DPA”) has prepared guidelines for data controllers to help them in setting up such a system.

No prior notification to the DPA is required to set up a whistleblower program, however there is always an obligation to notify the DPA if any processing of personal data is being outsourced to a third-party service provider (i.e. Lighthouse).

The Office of the Data Protection Ombudsman (supervises the processing of personal data in order to achieve the objectives of the DPA) (the “Ombudsman”)
P.O. Box 800
00521 Helsinki
Finland
www.tietosuoja.fi

If a company has more than thirty (30) employees, an employer has to call a meeting in which the new procedure is explained and discussed with the employees or their representatives.

Besides the notification requirement, the data controller must draw up a description of each personal data file, in which the purpose and main principles of data processing are explained. The description of the data file must be kept available for review for all data subjects.

Reporting to the whistleblowing hotline is limited to the employees, managers and executives of the company. It does not include external suppliers, contractors or vendors.

There is no limit as to who can be the subject of a report.

Finnish law is unclear with regard to anonymous reporting. While no statute specifically prohibits anonymous reporting, a person has a right to be informed regarding the source of the information, which tends to exclude the possibility. The DPA recommends that anonymous reporting not be used.

The DPA recommends that data should be destroyed within two months of collecting it.

A data controller must provide the fair processing information to data subjects.

Data subjects may obtain their subject access information upon a signed request or otherwise comparably verified document or personal appearance at the premises of the data controller.

France

Whistleblowing programs are subject to the provisions of the French Data Protection Act. The Commission Nationale de l'Informatique et des Libertés ("CNIL") serves as the Data Protection Authority.

Commission Nationale de l'Informatique et des Libertés
3 Place de Fontenoy
TSA 80715
75334 Paris
Cedex 07
France
www.cnil.fr

CNIL published a decision (Single Authorization AU 004) that authorizes the processing of personal data implemented through a whistleblowing program, and that the processing meets the requirements set out in said decision.

Prior notification to CNIL is required before setting up a whistleblower program either by:

- making a declaration of conformity to the Single Authorization AU 004 (simplified declaration process)
- applying for approval if the company wishes to implement a whistleblowing program that does not precisely match these requirements (standard authorization process)

Whistleblowing programs permitted under the Single Authorization are those limited in scope to facts regarding the following fields, as long as the use of the data relates to the data controller's legal obligation or to its legitimate interests in these fields: Finance, accounting, banking (for financial institutions) and the fight against corruption; Antitrust law; Harassment and to address discrimination; Health, hygiene and security in the workplace; and Protection of the environment.

Whistleblowing programs not limited to this scope will not benefit from the simplified declaration process and will be reviewed by the CNIL on a case by case basis as to the legitimacy of the program's purposes and proportionality.

Consultation with a Works Council is also required and employees must be informed collectively and individually of the implementation of a whistleblower program.

There is no limit on who can make a report or who can be the subject of a report. However, the company's whistleblowing policy should define who is entitled to make a report.

Anonymous reporting is tolerated as long as it is not actively encouraged by the company.

A data controller must provide fair processing information to data subjects.

It is a general obligation under French law employers must use the French language when conducting business or dealing with consumers or employees in France. Therefore, in most instances, this will also apply to fair processing information. Though the DPA does not specify that the DPA itself must be mentioned in any fair processing information, all information samples proposed by the CNIL include a specific reference to the DPA.

Data subjects or a duly empowered representative may obtain subject access information by submitting a written request to data controllers.

Data relating to a report found to be unsubstantiated by the entity in charge of processing such reports must be deleted immediately.

Data pertaining to a given report and reporting of facts giving rise to an investigation (or "verification") must not be stored beyond two months, unless a disciplinary procedure or legal proceedings are initiated against the person incriminated in the report or the author of an abusive/false alert. In that case, data must be deleted at the end of the procedure/proceedings.

Germany

No specific whistleblower protection laws are in place, the German Federal Data Protection Act (Bundesdatenschutzgesetz) ("DPA") governs data protection.

There are eighteen (18) different federal and regional data protection authorities as well as further supervisory bodies responsible for monitoring the implementation of data protection. In Germany, legislative and administrative competence in data protection issues rests with the regional state level and not within the federal realm. Guidance indicates that companies should use a neutral independent party (i.e. Lighthouse), specialized companies or law firms to operate an external whistleblower hotline to reduce the risk of misuse.

Every private entity with: (i) more than nine persons permanently engaged in automated data processing; or (ii) at least twenty (20) persons engaged in non-automated processing, is obliged to appoint a data protection official. The data protection official must be appointed within one month following the beginning of the data processing.

In addition, the company is obliged to negotiate on the whistleblower hotline with a Works Council (where a Works Council has been established at the respective entity). Requirements for a Works Council's participation include information on the implementation of a whistleblower program, negotiation and conclusion of an agreement.

Under the DPA there are no legal restrictions regarding the scope of reporting in whistleblower programs. However, it is recommended that the program be restricted to reporting of serious offenses and misconduct such as discrimination, sexual harassment, bribery, corruption, betrayal of trade secrets and confidence, theft, and incorrect accounting and auditing.

There is no limit on who can make a report or who can be the subject of a report (i.e. employees, manager, suppliers, etc...)

Anonymous reporting is permitted but as a less preferred option only. The company must encourage all users to include their names with their submissions to the whistleblowing system.

Data subjects may obtain their subject access information by written request to data controllers and such information is generally provided free of charge.

There are no specific security requirements for operation of a whistleblower program, however, management must provide that personal data is deleted if no longer needed.

Ireland

The Data Protection Act 1988 ("DPA") establishes an implied right to privacy.

The national regulatory authority that enforces the DPA is the Office of the Data Protection Commissioner (the "DPC").

Office of the Data Protection Commissioner
Canal House
Station Road
Portarlington R32 AP23
Co. Laois
Ireland

and

21 Fitzwilliam Square
Dublin 2
D02 RD28
Ireland
www.dataprotection.ie

Additionally, the Protected Disclosures Act 2014 (the "2014 Act") introduced protection for workers who "blow the whistle" about wrongdoing at work. Under the 2014 Act, workers have a right not to be dismissed or suffer a detriment at work as a result of making a "protected disclosure".

No prior approval is required to implement a whistleblowing program. However, while under the DPA all data controllers and data processors are required to register with the DPC.

There is no legal requirement to appoint a data protection officer. However, the DPC recommends that data controllers appoint a co-ordinator to deal with subject access requests.

Information tending to show that one or more of the following is occurring, has occurred or is likely to occur is proper regarding scope of reporting under a whistleblowing program: Committal of an offense; Failure to comply with a legal obligation; A miscarriage of justice; Danger to health and safety of an individual; Damage to the environment; Unlawful or improper use of funds and/or resources of a public body or of other public money; An act or omission of a public body that is oppressive, discriminatory, grossly negligent or constitutes gross mismanagement; and The deliberate concealment of any of the above matters.

Anonymous reporting is permitted but not encouraged.

The 2014 Act provides that workers (which include employees, contractors and agency workers) can make a report under the whistleblowing program.

A data controller must provide the fair processing information to data subjects and a data controller is obliged to explain the fair processing information to data subjects.

Data subjects may obtain their subject access information by written request to data controllers. An application must be in writing.

Italy

Italy has issued specific provisions regarding whistleblower protection and guidelines exclusively with reference to the banking and financial sector by means of the approval of Legislative Decree No. 72 of May 12, 2015, in force from June 27, 2015.

There are no Italian general whistleblower protection laws in place so for the time being any whistleblowing program has to be governed by the existing and general privacy rules, including the Italian Privacy Code ("DPC")

The National regulatory authority in Italy is the Garante per la protezione dei dati personali (the "Garante")

The data controller has to submit a notification to the Garante before commencing processing however, no approval is required for implementation of a whistleblowing program.

Garante per la protezione dei dati personali (Italian Regulatory Authority)
Piazza di Monte Citorio 121
00186 Roma
Italy
www.garanteprivacy.it

There are no legal limits to the scope of reporting for a whistleblower program, however guidelines recommend restricting reporting to serious offenses and misconduct such as discrimination, sexual harassment, bribery, corruption, betrayal of trade secrets and confidence, theft, incorrect accounting and auditing. Reporting is not permitted in areas concerning private or intimate life.

There are no legal limits on who can make a report under a whistleblowing program and anonymous reporting is permitted.

The DPC applies to anyone who processes personal data in Italy including data controllers, data processors and any person in charge of the processing.

A data controller must provide the fair processing information to data subjects and data subjects may obtain their subject access information by making a request to the data controller, the data processor or the person in charge of the processing.

Data subjects may ask to have their personal data updated, amended or supplemented or have their personal data cancelled, transformed into anonymous data or blocked by the data controller.

Netherlands

The general data protection law is the Wet Bescherming Persoonsgegevens, the Data Protection Act ("WBP").

The Dutch Corporate Governance Code ("DCGC"), provides general rules in respect to whistleblowing programs in the private sector.

Whistleblower programs implemented by companies are assessed against the statutory requirements of the WBP and general principles of employment law, such as the concept of "good employership". In 2006 the Dutch Data Protection Authority ("DPA"), issued an opinion on the data protection aspects of whistleblowing. Its position is that in order for the processing of personal data in the context of a whistleblowing program to be lawful, the processing should be necessary for the legitimate interest of the company and the fundamental rights and interests of data subjects should not prevail.

A prior notification to the DPA is required with regard to the types of personal data (potentially) processed in the context of the whistleblower program. This notification does not entail approval.

Dutch Data Protection Authority (Autoriteit Persoonsgegevens) ("DPA")
Autoriteit Persoonsgegevens
Postbus 93374
2509 AJ Den Haag
The Netherlands

Visiting address:
Prins Clauslaan 60
2595 AJ DEN HAAG
The Netherlands
autoriteitpersoonsgegevens.nl/nl

There is no legal obligation to appoint a data protection officer. However, the appointment of a data protection officer can avoid the need to notify the DPA of new processing.

Additionally, a whistleblower program qualifies as a complaints procedure under the Works Council Act and the Works Council has a right of consent with regard to decisions on the establishment, amendment or cancellation of such procedures.

A data controller must provide the fair processing information to data subjects prior to obtaining the personal data from them or from third parties, unless this information is already known to the data subject. In other words employees should be notified by the employer of implementation and the details of the whistleblower program.

The DPA has stated that a whistleblowing hotline should be used only for reporting serious and substantial offenses. Financial reporting and corruption are most frequently mentioned as examples.

There is no limit on who can make a report under a whistleblowing program nor is there any restriction on who can be the subject of a report.

Anonymous reporting is permitted but the DPA has stated that confidential reporting is preferred.

Data subjects may obtain their subject access information by request to data controllers. Data subjects may ask the data controller to correct, supplement, delete or block the data processed about them in the event that such data is inaccurate, incomplete or irrelevant for the purposes of the processing, or is being processed in any other way that infringes a legal provision.

Norway

The Data Protection Directive has been implemented by the Personal Data Act (the "DPA") Although Norway is a member of the EEA, but not a member of the EU, the Act implements the EU Directive into Norway's national legislation.

In Norway there are both specific whistleblower legislation and data protection guidelines.

A data controller must notify the Data Protection Authority (the "Authority") before processing personal data by automatic means or establishing a manual personal data filing system which contains sensitive personal data. The DPA merely establishes an obligation to notify if a whistleblowing program is only available for employees. If the whistleblowing program will be used by others, such as consultants or customers, a license from the Authority is required.

The Data Protection Authority
P.O. Box 8177
Dep, N-0034
Oslo, Norway
www.datatilsynet.no

There are no specific requirements in relation to how the program has to be set up. The Personal Data Act and the Personal Data Regulations (collectively the "DPL") apply to the processing of personal data that is reported through and collected in whistleblowing programs.

There is an obligation for the employer to establish routines for internal notification or implement other measures that enable the employees to make use of the right to whistle blow but employee consent to implement is not a requirement. Consultation with a Works Council, union or other employee representative may be advisable to increase the credibility of the whistleblowing program.

Although there is no legal requirement, the appointment of a data protection officer provides an exemption from the obligation to notify if that officer is approved by the Authority.

There is no limit on who can make a report under a whistleblowing program and anonymous reporting is permitted.

A data controller must provide the fair processing information to data subjects. This also includes: (i) the categories of recipients of data; (ii) the fact that the provision of data is voluntary; and (iii) the existence of the right to access and to rectify the data concerning him.

The data subjects may obtain their subject access information by request to data controllers.

Personal data must be deleted when no longer necessary to carry out the purpose of the processing. According to administrative practices from the DPA, personal data in a whistleblowing program must be deleted two months after closing the investigation unless other purposes legitimize longer storage.

Poland

Currently in Poland, there are no specific laws concerning whistleblowing programs. The Act on the Protection of Personal Data ("DPA") is the applicable law.

The Inspector General for the Protection of Personal Data is the (the "GIODO")
The Inspector General for the Protection of Personal Data (the "GIODO")
ul. Stawki 2
00-193 Warsaw
Poland
www.giodo.gov.pl

The law does not require any kind of notification or approval to launch a whistleblowing program in a workplace. There is also no obligation to register the personal data information system containing the data of employees or service providers in involved in the whistleblowing procedure by a given data controller. However, if the personal data system contains the personal data of third parties (vendors, clients, employees of third parties, including affiliates), it is subject to regular registration.

Employees need to be informed about the introduction of a whistleblowing program, its purpose and function, as well as related internal regulations or policies.

There are no legal limitations as to the persons who are authorized to report as whistleblowers and there is no limitation as to who may be the subject of a report.

However, the scope of actions that may be reported should be defined within the company's written whistleblowing policy and limited accordingly.

Data subjects may obtain their subject access information and information regarding the identity of the data controller and the dates on which the data processing took place, by requesting such information from the data controller. This right may only be exercised once every six months and the data controller must respond within 30 days of the request.

No specific security requirements exist for a whistleblower program in Poland, however the data should be deleted within two months of the date the investigation reaches its conclusion, unless legal or disciplinary proceedings or archiving rules require a longer storage period.

Portugal

Portugal has no specific whistleblower protection laws in place. The implementation of a whistleblower program is subject to the Portuguese Data Protection Act ("DPA"). The National Regulatory Authority is the Comissão Nacional de Protecção de Dados (the "CNPD").

Comissão Nacional de Protecção de Dados (the "CNPD")
Rua de São Bento, n.° 148, 3°
1200-821 Lisboa
Portugal
www.cnpd.pt

Prior notification and approval from the CNPD is required to implement a whistleblower program. Advanced notification to the Works Council is also recommended.

Whistleblowers are only allowed to report on bookkeeping, internal accounting controls, auditing matters, corruption, banking and financial crimes.

Only employees are allowed to make a report and individuals who are the subject of the report under the whistleblowing program are limited to individuals who are involved in management decisions in bookkeeping, internal accounting controls, auditing matters, corruption, banking and financial crimes. Therefore, the whistleblower program cannot be used for the investigating of incriminating reports regarding personnel who have no involvement whatsoever in the company's management decisions.

Moreover, anonymous reporting is not permitted.

A data controller must provide the fair processing information to data subjects. The data subject has the right to obtain his/her subject access information by written request to data controllers at reasonable intervals.

The data subject has the right to obtain from the data controller the rectification, erasure or blocking of data, the processing of which does not comply with the DPA.

Russia

Russia has no specific whistleblower protection laws in place.

The Russian Federal Law "On Personal Data" (the "OPD Law") which contains similar provisions to those in the Data Protection Directive, along with the Labor Code of the Russian Federation provide the compliance for implementing a whistleblower program.

Personal data may be processed by a "data operator" (a concept similar to a data controller) only with prior written notification to the Roskomnadzor, unless the processing is exempt. The notification must occur prior to the first processing of personal data.

The Federal Service for Supervision of Communications,
Information Technology and Mass Media (the "Roskomnadzor")
Kitaygorodsky pr. 7, bld. 2
109074 Moscow
www.rsoc.ru

No approval is required if, as part of the whistleblowing program, the personal data is processed solely in connection with labor relations. However, any excessive operations with the employees' personal data may go beyond this framework and, therefore, the "general" notification on processing of personal data will be required.

It is recommended to limit the scope of the program only to the reports on employees' performance and facts within the scope of employment.

There is a legal requirement for a data operator (if a legal entity) to appoint a data protection officer.

The officer is responsible for ensuring compliance with the OPD Law including: (i) implementing appropriate internal controls over the data operator and its employees; (ii) making employees of the data operator aware of personal data related laws and regulations, internal (local) acts on data protection and other data protection requirements; and (iii) dealing with applications and requests from data subjects.

A prior written consent from each employee is required for the processing of their personal data in connection with the whistleblowing program (including consent for the data to be used by other employees for the purpose of whistleblowing); similarly, an employee's consent is required for the cross-border transfer of data and the transfer to third parties.

The OPD Law requires any consent to be in writing and that the consent is specific, informed and freely given.

Under Russian law an operator is allowed, with the consent of the data subject, to engage a third party to process personal data on the basis of an agreement, state or municipal contract or under the state or municipal legal act issued by the relevant authority (the "Operator's Instruction").

Under Russian employment law, a company must put in place a written data protection policy.

Data subjects may obtain their subject access information by a request to the data operator.

Slovak Republic

The Office for Personal Data Protection of the Slovak Republic is the data protection authority (the "Office").

Office for Personal Data Protection of the Slovak Republic(Úrad na ochranu osobných údajov)
Hraničná 12
SK-820 07 Bratislava 27
Slovakia
www.dataprotection.gov.sk

The Slovak Republic has no general whistleblower protection act. Slovak data protection legislation is incorporated in the Act on Protection of Personal Data ("DPA")

In general, data controllers must notify the Office of their processing unless it is subject to an exemption. The processing of data may commence upon submission of that notification.

The Office has discretion to require registration of a program to include personal data processed without the consent of the data subject based on the so-called 'legitimate interest exemption', i.e. processing with the aim of protecting the legally protected rights and interests of the data controller or a third party (for example, CCTV or whistleblowing hotlines).

The scope of reporting under a whistleblowing program is any antisocial activity of which the natural person has become aware in the exercise of his/her employment (i.e. specified crimes, administrative violations).

There is no limit on who can make a report or who can be the subject of a report under a whistleblowing program.

There is no obligation on data controllers to appoint a data protection officer but this does provide an exemption to the notification obligation.

A data controller must provide fair processing information to data subjects prior to the collection of their personal data. This includes: (i) the identity of data controller and data processor (if appointed); (ii) purpose of processing; (iii) list or scope of personal data and (iv) further information within the meaning of Article 10 of the Data Protection Directive such as information on; third parties and recipients of personal data, entitled persons, third countries where data is transferred, whether the provision of personal data is voluntary or compulsory, the form of publication should data be published or advice on data subjects' rights. The means of provision of fair processing information is not specifically provided for in the DPA.

Data subjects may obtain their subject access information by written request to data controllers.

Spain

Spain has no specific whistleblower protection laws in place. Whistleblower programs are regulated by the Data Protection Act ("DPA").

The national regulatory authority in Spain is the Agencia Española de Protección de Datos (the "AEPD")
Agencia Española de Protección de Datos
Jorge Juan, 6
28001 Madrid, Spain
Tel +34 901 100 099/ +34 91 266 35 17
www.agpd.es

Any person intending to create or modify personal data files is required to register with the AEPD by completing the forms prior to processing personal data. It is a mere filing of information that must take place prior to the creation of the data file. Approval is not required for implementation, however, there is always a general obligation

to (i) notify the DPA about the existence of a data file containing the personal data derived from the whistleblowing program and (ii) if there is a transfer of personal data outside the EU/EEA.

There are no restrictions on who can make a report under a whistleblowing program and companies are free to design their program as they deem appropriate.

Historically, anonymous reporting was not permitted. Criteria that had been set forth for whistleblower programs within Spain, required the reporter to identify themselves.

However, pursuant to Data Protection Law, LO 3/2018 adopted December 2018, anonymous reporting is now permitted.

Specifically, Article 24, pertaining to internal complaint information systems, references that acts or behaviors that could be contrary to the regulations of a private law entity, may be brought to the attention of the entity, including anonymously.

A link to the pertinent law is included here for translation and review:

Employees must be informed in advance and in detail about the implementation of a whistleblower program. Launching a whistleblower program also requires notification of the existing Works Council or union representative regarding the features of the program.

Data subjects must be informed in advance expressly, precisely and unambiguously of the fair processing information.

Data subjects may obtain their subject access information by written request to data controllers. The data subject shall be granted a free and simple means of exercising the right of access.

Once the contractual service has been completed, the personal data must be destroyed or returned to the data controller, together with any support or documents containing personal data processed.

Sweden

Sweden has no specific whistleblower protection laws in place.

The Swedish Personal Data Act (Sw. Personuppgiftslagen (1998:204)) (the “Act”) implemented the EU Directive and is the relevant legislation.

The national regulatory authority is Datainspektionen (the "Data Inspection Authority")
Datainspektionen
Box 8114
SE-104 20 Stockholm
Sweden
www.datainspektionen.se

There is a general duty to notify the Data Inspection Authority about the processing of personal data. This merely requires a filing of information and does not require any approval. The notification must occur prior to the first processing of personal data.

Whistleblowing reports may include data regarding violations of law and/or criminal allegations. According to section 21 of the Act, such data about violations or criminal allegations may only be processed by the Swedish authorities. Therefore, the implementation of some whistleblowing programs may violate Swedish law.

In general regarding a whistleblower program, the requirements for how companies manage and process personal data in the system are:

- The whistleblowing program must be limited to serious irregularities concerning accounting, internal accounting control, auditing matters, the fight against bribery and banking and financial crimes
- Anyone can make a report under the whistleblowing program but its use must be voluntary
- Only key personnel and employees in a management position may be reported on and only they may be processed in the system
- The company is obliged to ensure that the processing for which the company is responsible is in compliance with the Act, for example in relation to the processing of sensitive personal data, information to the employees and transmission of personal data to third countries.

There is no legal obligation to appoint a personal data representative. However, the appointment and registration with the Data Inspection Authority of such a person exempts the data controller from the obligation to notify.

The data controller is responsible for compliance with the Act. Data processors are subject to a reduced set of specific requirements.

A data controller must provide the fair processing information to data subjects. The data controller must also provide all other information necessary in order for the data subject to be able to exercise his/her rights in connection with the processing. Such information shall include, inter alia, information about the types of data that are processed, the recipients of the personal data and the data subject's rights. The Data Inspection Authority has stated that it cannot be expected that the data subject understands languages other than Swedish, hence the information should be provided in Swedish.

Every data subject is, once a year and free of charge, entitled to receive their subject access information upon written request to data controllers.

The data subject is entitled to obtain immediate rectification, blocking or erasure of any personal data that has not been legally processed under the Act.

Switzerland

Switzerland has no specific whistleblower protection laws in place.

The Swiss Federal Data Protection Act (the "DPA") is the relevant law. The DPA follows similar concepts as the Directive.

The Swiss Federal Data Protection and Information Commissioner (the "DPIC") is the national regulatory authority.

The Swiss Federal Data Protection and Information Commissioner
Feldeggweg 1
CH-3003 Berne
Switzerland
www.edoeb.admin.ch

An overview of various private whistleblowing programs reveals that employees are encouraged to report any misconduct, deplorable circumstances, deficiencies, etc.

There are no limits on who can make a report under a whistleblowing program nor on who can be the subject of a report. No employee consent is required to implement a program.

Data controllers which regularly process sensitive personal data or personality profiles or regularly disclose personal data to third parties must register their data collection with the DPIC. This registration does not require any approval and is, therefore, a mere notification system.

There is no legal requirement to appoint a data protection officer. However, doing so can exempt a data controller from the requirement to register.

The DPA extends the definition of personal data to include information not only about individuals, but also about legal entities (this is interpreted broadly to include partnerships and trusts). The processing of personal data of legal entities is subject to the same provisions as the processing of personal data of individuals. Under the revised DPA (i.e. 2018 and onwards), personal data of legal entities will likely no longer be protected.

The data subject may request the personal data to be rectified, marked as being disputed or deleted. The data subject may request that no personal data be disclosed to third parties or processed further.

United Kingdom

The U.K. has specific whistleblower protection laws in place. The Public Interest Disclosure Act ("PIDA"), which amends the Employment Rights Act 1996 provides protection for workers who report malpractices by their employers or third parties against detriment and/or dismissal.

To be a protected disclosure, the disclosure must be a "qualifying disclosure" of "information" made in accordance with one of the specified methods. Broadly, this is where there has been a disclosure of information that a worker reasonably believes is made in the public interest and tends to show malpractice is, has or is about to take place

within an organization. PIDA encourages disclosures to be made internally to the employer rather than externally to a third party. More stringent conditions must be met for an external disclosure to be protected.

Note that the whistleblowing legislation in the U.K. imposes no positive obligations on employers to encourage whistleblowing or to implement a whistleblowing policy, save for listed companies where there is a positive obligation to maintain a sound system of internal control under the U.K. Corporate Governance Code, and public bodies where the government expects these to be in place.

The Data Protection Act 1998 (the "DPA") which implements the EU Directive is the general law related to data protection.

The Information Commissioner is the national regulatory authority.

The Information Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF
United Kingdom
www.ico.org.uk

In the context of a whistleblower program, personal data may not be processed by a data controller unless it has submitted a notification to the Information Commissioner. No approval is required. The notification must occur prior to the first processing of personal data.

Reporting to a whistleblower hotline is permitted when, in the reasonable belief of the worker, one or more of the six specified types of malpractice has taken place, is taking place or is likely to take place and it is in the public interest to disclose this information: Criminal offenses; Breach of any legal obligation; Miscarriage of justice; Danger to the health and safety of any individual; Damage to the environment; and The deliberate concealing of information about any of the above.

There is no limit on who can make a report under a whistleblowing program and no limit on who can be the subject of a report so long as it is related to one of the six types of malpractice aforementioned.

Anonymous reporting is permitted provided that the organization's whistleblower policy as created allows for anonymous reporting.

There is no legal requirement to appoint a data protection officer.

A data controller must provide the fair processing information to data subjects.

Data subjects may obtain their subject access information by written request to data controllers.

In certain cases, the data subject may ask the court to order the data controller to rectify, block, erase or destroy the data. An individual may in writing require that the data controller cease processing either generally or for a specified purpose or in a specified manner data concerning the individual if such processing is likely to cause substantial damage or distress to the individual or a third party and that damage/distress would be unwarranted.

Lighthouse Services is here to help you. Please let us know if you have any additional questions or need assistance with your hotline.

ABOUT SYNTRIO

Syntrio is a global leader in governance, risk, compliance and human resource solutions that help 6,000 organizations manage risks, empower culture and accelerate performance in 50+ languages. Easy, affordable and innovative Syntrio solutions include the robust Lighthouse reporting hotline and more than 1,000 elearning courses in Employment Law, Ethics and Compliance, Diversity and Inclusion, Health and Safety, Business Skills and Cybersecurity.

For more information visit syntrio.com.

888.289.6670 | SYNTRIO.COM