Corporate Directive	Whistleblowing process	UPSA-CORP-DIR-HQ-007
		Version 6

Document History

Version	Effective date	Description of modifications
1	December 10th, 2019	First version.
2	August 10th, 2021	> Requirement 3: Alert e-mail address for Italy has been added > Requirement 6: details on the evaluation of the whistleblowing system > Change of the format to be aligned with Quality" format
3	December 11th, 2021	> Replacement of the French whistleblowing system by the new Taisho Group whistleblowing system > Add the process related to harassment referents (France) > Update of Requirements accordingly
4	*Cf. date CARA*	Modification of the Scope and Requirements 1, 3 and 4 following the new French laws on whistleblower protection, linked to the European Directive (EU) n°2019/1937 of 23 October 2019
5	*Cf. date CARA*	> Integration of the elements of the "Taisho whistleblowing system Compliance Hotline Privacy Notice" into the present Directive to create a single document > Clarifications made to Requirements 1, 2, 3, 5 and 6 to improve the clarity of the information provided > Modifications to Requirement 4 and Appendix 1 following the update of the internal alert management process within the UPSA Group and the Taisho Group
6	*Cf. date CARA*	Changes made to the procedure following the change in the tool used within the Group to manage the whistleblowing system (the TSUHO tool has been replaced by the DQ Helpline tool).

Purpose

To specify the context of alerts and reports of misconducts, the associated process and the guarantees providing protection for the originators of such alerts and reports.

Content

In scope

Who falls under this policy?

This directive applies to all current and former UPSA employees as well as external staff (intermediaries, consultants, service providers), temporary staff (employees of service providers with whom UPSA occasionally works) and candidates for employment at UPSA. It also applies to all current and former employees of any UPSA third-parties (suppliers, customers…).

References

- [French law] « Sapin 2 Law » - LAW No. 2016-1691 of December 9, 2016 on transparency, the fight against corruption and the modernization of economic life
- European Directive (EU) No. 2019/1937 of October 23, 2019 on the protection of persons who report violations of European Union law
- [French law] Organic law no. 2022-400 of 21 March 2022 aimed at reinforcing the role of the Defender of Rights with regard to whistleblowing, in force on 23 March 2022.
- [French law] Ordinary law n°2022-401 of March 21, 2022 aimed at improving the protection of whistleblowers, in force on September 1, 2022.
- « 231 Law » applicable in Italy - Decreto legislativo 8 giugno 2001, n. 231
- Global Compliance Guideline of Taisho Group

Requirements

UPSA uses the whistleblowing system implemented by Taisho Group. To report inappropriate actions or facts, you can access the Taisho hotline by connecting on the following website: **https://i365.dqhelpline.com/taishopharma/upsa07509**

Use the common ID and password belowto connect and fill in your report. (See Apprendix 1):

- ID: **alertUPSA**
- Password: **UPSA39466**

For Italy specifically, the 231 Law requires a specific hotline. You can use the following e-mail address to report the facts: complianceitaly@upsa-ph.com

Requirement 1: Definition of a whistleblower

- The whistleblower is a natural person, who:
  - had personal knowledge of the facts he/she reports, or obtained information in the course of his/her professional activities (including if he/she is not or is no longer an employee of UPSA: unsuccessful candidate, employee whose employment relationship with UPSA has ended, or employee of a company under contract with UPSA);
  - acts in a disinterested manner, without direct financial compensation, for his/her action;
  - acts in good faith : at the time he/she makes a report, the facts reported must appear to be inappropriate, so that the whistleblower cannot be accused of having sought to harm others.

Requirement 2: Facts which may lead to a report

- The information disclosed concerns facts that have occurred or are very likely to occur within the Group. These information may concern:
  - a crime or an offense;
  - the violation or attempted concealment of a law or regulation including international or European Union law;
  - the violation of a national or international legal act;
  - a threat or damage to the public interest;

- an infringement of the Taisho Group's Global Compliance Guideline, or situations/behaviors likely to constitute breaches of the rules of probity defined by the Group.

More precisely, the reportable facts are :

1. Matters relating to accounting or audit
2. Corruption situations or bribe
3. Antitrust violation
4. Conflict of interest
5. Discrimination; harassment (sexist / sexual / moral)
6. Embezzlement; fraud
7. Violation of environmental protection, health, or safety laws and regulations
8. Forgery or alteration of contracts, reports, or records
9. Data falsification or misappropriation
10. Insider trading
11. Acts of sabotage or destruction
12. Theft
13. Assault; intimidation
14. Behavior that violates whistleblower protection, cooperating individuals and privacy
15. Violation of the Group's Code of Conduct
16. Violation of internal rules and procedures which lead to any of the conduct listed above

- The report must provide facts, information, documents that can substantiate its content.
- Confidential information may be subject to a report, subject to compliance with certain legal constraints (e.g. Article 122-9 of the French Criminal Code). The alert cannot concern elements covered by national security, medical confidentiality or attorney-client privilege.

Requirement 3: The whistleblower is granted guarantees and special protection

Protection of the whistleblower

- The whistleblower is granted the following guarantees:
  - No civil liability for damage caused by the alert, provided the following cumulative conditions are met:
    - The whistleblower meets the definition of a whistleblower;
    - The whistleblower had reasonable grounds for believing that the warning was necessary to safeguard the interests in question.

- Immunity from prosecution:
  - when the alert jeopardizes a secret protected by law; and
  - when this disclosure is necessary and commensurate with the safeguarding of the interests at stake; and
  - when it takes place in accordance with the reporting procedures specified by law; and
  - when the originator of the alert meets the criteria defining a whistleblower.
- The absence of any disciplinary measures or retaliatory measure related to the alert, subject to the alert being made in good faith and with no personal interest, even if the facts end up being inaccurate or do not lead to any consequences.
- Elements that could identify the whistleblower cannot be disclosed, except to a judicial authority, without his or her consent.
- When the persons in charge of collecting and processing alerts within the Group are required to report the facts to the judicial authorities, information likely to identify the whistleblower may be communicated to these authorities. In this case, the whistleblower will be informed, unless such information would compromise the legal proceedings.
- The individual who is being reported can under no circumstance gain access to information concerning the identity of the individual making the report.

o The same guarantees apply to facilitators, i.e. any natural or legal person under private non-profit law who has helped the whistleblower to report and disclose information relating to the facts denounced (associations, unions, etc.).

o However, these protection measures are not applicable if the whistleblower does not comply with Requirements 1 and 2. Whistleblowers acting in bad faith (i.e. with knowledge of the false nature of the facts reported) may :

- lose the benefit of the protection and be subject to a disciplinary sanction that may go as far as dismissal for serious or gross misconduct in the presence of an intention to harm;

- be prosecuted for slanderous denunciation (for instance, under Sapin 2 law: potential penalty of 5 years imprisonment and 45,000 € fine (C. pén., art. 226-10));

- be held civilly liable and ordered to pay damages to compensate the victim.

Confidentiality of the whistleblower

- The identity of the whistleblower, of the individuals targeted in the alert, of any third party mentioned in the alert, as well as all information collected as part of this directive, are kept confidential.
- Management of the alert relies solely on objectively formulated data that reveal the presumed nature of the reported facts. Only data that are in direct relation to the scope defined in the Requirement 2 and that are strictly necessary to verify alleged facts are collected. Data concerning the whistleblower, the individuals being reported in the alert and those involved in the collection or handling of the alert are limited to their identities, their jobs and their contact information. Elements that could identify the individuals accused in a report can only be disclosed, except to a judicial authority, once the alert has been deemed legitimate.
- The individuals in charge of collecting and handling alerts are limited in number, and they are subject to a higher contractual confidentiality obligation. Their partial or full access to the processed data is dependent on the extent to which these data are necessary to carry out their duties and within the limits of their respective powers.
- Appropriate measures are taken to ensure data security, both during the collection of the data and during their communication or retention.
- For information, under Sapin 2 law, disclosing confidential information is punishable by 2 years of imprisonment and a €30,000 fine.

Data Protection

- ***Your rights:*** Under the General Data Protection Regulation 2016/679 of April 27, 2016 ("GDPR") and the French Data Protection Act of January 6, 1978, as amended, any person subject to these regulations has the right to access his or her data and the right to be informed of them, to oppose them and to limit their processing, and to request that his or her data are rectified, completed and/or erased. In order to exercise your data protection rights or for any questions you may have, please contact the UPSA France Data Protection Officer at the following address: EUDPO@upsa-ph.com.
- ***Data protection measures:*** Regarding the Taisho whistleblowing system, the Group takes appropriate measures to preserve the confidentiality and security of data processed in connection with the alert, in accordance with the provisions of the GDPR and the French Data Protection Act.
- ***Personal data processed:*** When using the Hotline, personal data may be provided by the whistleblower, by authorized persons involved in the investigation, or by persons interviewed during the investigation. Depending on the content of the alert, the following categories of data are processed:

- if the whistleblower decides not to remain anonymous, his/her name and e-mail address , as well as the name of the company to which he/she belongs and the country of his/her place of work;
- the identity of the persons concerned by the alert or of any third parties mentioned in the alert;
- the events reported in the alert and related information;
- information gathered in the course of the investigation and formalized in the investigation report;
- Measures taken in response to the investigation;
- Depending on the content of the alert, and only if necessary, the persons in charge of collecting and processing alerts within the Group may be required to process sensitive personal data according to the GDPR (such as health data, data revealing racial or ethnic origin, data concerning a person's sex life or sexual orientation, etc.).

  Whistleblowers are asked to report only factual information directly related to the subject of the alert.

- ***Recipients of the personal data and anonymity:***
  - For information on data recipients, please refer to Requirements 4 and 5 of this Directive.
  - The system allows whistleblowers to remain anonymous if they so wish, while enabling them to track their reports using the unique code given to them when they launch their alert in the D-Quest tool (this code enables whistleblowers, even if they remain anonymous, to check whether replies, updates or requests to provide details or additional information have been made to their report).

- ***Purposes and legal basis for the use of personal data:***
  - The purpose of the processing operations is to report and process alerts, including investigation of reported events, relating to the acts mentioned in Requirement 2 of this Directive. The Group will only process the data required to manage the alert.
  - The legal basis for the processing operations carried out is:
    - the whistleblower's consent pursuant to article 6§1 a) of the GDPR;
    - The compliance with the legal obligations to which the Group is subject pursuant to article 6§1 c) of the GDPR, in particular the legislation listed at the beginning of this Directive;

- The legitimate interest pursued by the Taisho Group through the performance of investigations targeting situations and acts contrary to the Group's Code of Conduct, pursuant to article 6§1 f) of the GDPR;
- It should be noted that sensitive data falling within the scope of article 9 of the GDPR will only be processed: on the basis of the consent of the data subject (pursuant to article 9§2 a) of the GDPR), or if they are necessary for the establishment, exercise or defense of legal claims (pursuant to article 9§2 f) of the GDPR).

- ***Transfer of personal data abroad:*** The fulfillment of these purposes involves transfers of personal data to Japan, since Taisho's Internal Affairs department is located in Japan and the administrator of the whistleblowing line (DQ Helpline) is also located in Japan. The compliance of these data transfers with the requirements of articles 44 et seq. of the GDPR is guaranteed by the European Commission's adequacy decision C/2019/304, which stated that Japan ensures an adequate level of protection within the meaning of article 45 of the GDPR.
  For the investigations' realization, any other transfer of personal data that may occur will be carried out in accordance with articles 44 et seq. of the GDPR and applicable law. Further information can be requested from EUDPO@upsa-ph.com.

- ***Personal data retention period:***
  - Data relating to alerts will only be kept for the time strictly necessary to process them.
  - When the alert is not followed by disciplinary or legal proceedings, the data relative to this alert are destroyed or archived after anonymization, within thirty (30) days after verification efforts have been completed.
  - When disciplinary or legal proceedings are initiated against the individual against whom allegations have been made or against the originator of a wrongful alert, the data relative to the alert shall be retained until the completion of the proceedings. The data being archived are kept, within the framework of a separate information system with limited access, for a period not exceeding the length of the litigation proceedings (expiration of the statute of limitations).

Any breach to these requirements exposes the originator to possible disciplinary action or prosecution.

Requirement 4: The process to follow in the event of a report

- Each employee remains free to use the whistleblowing line or to report a situation, question or difficulty through the following alternative channels:
  - through the whistleblowing system of Taisho Group, via the following website **https://i365.dqhelpline.com/taishopharma/upsa07509** by using the common ID and password
    - ID: **alertUPSA**
    - Password: **UPSA39466** ; or
  - to a direct or indirect superior (for UPSA staff); or
  - for specific cases related to the legal entity UPSA Italy, to the Italian Supervisory Body members : complianceitaly@upsa-ph.com; or
  - for specific cases related to harassment in the legal entity UPSA France, to the harassment referents appointed within the French work councils of Rueil or Agen (if you have any questions about this process, please contact the Human Resources Department); or
  - to Legal and Compliance Department;
  - to the Human Resources Department;
  - to the competent authorities outside UPSA (e.g. the Defender of Rights in France).

- The whistleblowing system of Taisho Group is available 24/7 in several languages (including French, English, Italian and Spanish).
- The steps of the whistleblowing system of Taisho Group are detailed in Appendix 1. In order to ensure that every whistleblower has the necessary guarantees of fair treatment, this system is managed by Taisho Internal Affairs Department (which is the department in charge of the Taisho Pharmaceutical Headquarters), via an external and independent company,DQ Helpline. It enables you to directly report facts so that investigations can be carried out in a confidential and impartial manner by the people in charge of the whistleblowing system within this Department of the Taisho Group and, where appropriate regarding the content of the alert, UPSA's Legal and Compliance Department or UPSA's Human Resources Department.
- The originator of the alert can, if he/she wishes, identify him/herself, and his or her identity is kept confidential.
- As an exception, an alert originated by someone who wishes to remain anonymous may be handled under the following conditions:

- the severity of the facts mentioned is evident, and the factual elements are sufficiently detailed;
- special caution must be used in the handling of this type of alert, such as an assessment by its initial recipient prior to its dissemination as part of this directive.
- In the event of an anonymous alert, the originator of the alert must be aware that the alert may not be handled if it does not meet the conditions listed above.

- The whistleblower can forward any information, in any form or on any medium, to support the facts of the alert.

Requirement 5: Handling process

- Originators of an alert receive a unique code when they send in their report, enabling them to retrieve the information they have provided, and also to check whether replies, updates or requests to provide details or additional information have been made to their report.
- The whistleblower may be asked to provide any additional information required to verify the receivability of the alert or the accuracy of the facts reported.
- The originator of the alert is informed of any measures planned or taken, within 3 months of acknowledgement of receipt of his alert.
- The individual(s) named in the alert are informed of the report. When precautionary measures are necessary, mainly to prevent the destruction of evidence relevant to the alert, the individual(s) may be informed after these measures are taken.
- Management of the alert, particularly the verification efforts, is entrusted to the most competent person in the field concerned by the report within the Human Resources Department or the Compliance and Legal Department.
- UPSA Governing Body is informed of the most sensitive situations (except when the CEO is implicated or likely to be implicated).
- In order to carry out investigations, information gathered through the alert may be disclosed to experts (such as in the financial, accounting, IT or legal fields), to police or government authorities, if necessary to comply with legal requirements or in connection with legal proceedings, and to other legitimate recipients, where required by law or in connection with any legal proceedings.

  The number of persons involved in an investigation will be limited to the extent compatible with a full and complete investigation and in compliance with applicable legislation.
- During the investigation, insofar as this is necessary to remedy and/or punish the misconduct established, the line manager(s) of the person(s) concerned by the alert will be informed, depending on the seriousness and nature of the facts.

- The originator of the alert is informed of the follow-up action given taken regarding the report by the alert system, the Compliance Manager, or the Human Resources Director, depending on the case. If the alert is considered as inadmissible, the originator of the alert is informed of the reasons of this inadmissibility.
- The originator of the alert and the individuals targeted within are informed of the alert's closure.

Requirement 6: *Other general principles for users of this directive*

- This alert directive is voluntary, and its non-use does not have any consequences for employees.
- Wrongful use of this directive exposes the originator to possible disciplinary action or prosecution.
- The quality and effectiveness of this whistleblowing system is evaluated at least annually by the Taisho Internal Affairs Department and the UPSA Legal and Compliance Department, using indicators (in particular: number of alerts received, closed without action or dealt with, processing times, issues raised). These indicators are presented to the UPSA General Management on a regular basis.
- A copy of this directive is given to any potential user of the alert procedure (staff members, external and temporary staff). A copy of this directive is also given to anyone being reported in an alert unless he or she has already received one.
- The whistleblower may choose to send his or her report, directly or after having made an internal report, to one of the following competent external authorities:
    - to one of the authorities listed in the appendix to decree no. 2022-1284 of October 3, 2022, depending on the subject of the alert;
    - In France, to the "Défenseur des droits", who will be responsible for directing the author of the alert to the authority or authorities best placed to deal with it, except in cases where he himself is designated as the competent authority;
    - to the judicial authority;
    - to a European Union institution, body, office or agency competent to collect information on violations falling within the material scope of Directive (EU) 2019/1937 of October 23, 2019.

Roles and Responsibilities

See Requirements.

Definitions

N/A

Related documents

N/A

Contact information

Direct questions about this document to: Legal & Compliance Department.

APPENDIX 1 – Description of Taisho whistleblowing system