Information notice on the processing of personal data, pursuant to Articles 13 and 14 of EU Reg. 2016/679 in relation to 'whistleblowing' reports_Rev.01

With this information notice Fidia Farmaceutici S.p.A (Company in the following) describes how it processes the data collected and what rights are granted to the Data Subject, pursuant to EU Reg. 2016/679 (GDPR) and Legislative Decree 196/2003 in relation to 'Whistleblowing' reports.

1. Controller

Controller of personal data processing is FIDIA FARMACEUTICI SPA, with registered office in Via Ponte della Fabbrica, 3 / A, 35031 Abano Terme (PD), Italy.

2. Data Protection Officer and contact details

The Company's Data Protection Officer is domiciled at the registered office of the Company and can be contacted by writing to the Company c/o Legal Department or by e-mail at dpo@fidiapharma.it.

3. Purpose of processing

The Company makes personal data processing described in this notice for the purpose of protecting persons who report violations of national or European Union laws that harm the public interest or the integrity of the public administration or private entity, of which they have become aware in a public or private work context, as provided for by Legislative Decree 24/2023 (Decree in the following) which transposes European Directive 1937/2019 into Italian law.

4. Useful definitions

Listed below the description of the main terms used here on the matter 'whistleblowing'; full definitions can be found in Legislative Decree 24/23.

Violations: conduct, acts or omissions that harm the public interest or the integrity of the public administration or private entity;
Reporting (whistleblowing): the written or oral communication of information on violations; internal reports in oral form are made through telephone lines or voice messaging systems or, at the request of the reporting person, through a in face to face meeting set within a reasonable period of time. The Reporting Person may make the report either through the channels set up internally by the Company or through an external report addressed to the competent authority ANAC, National Anti-Corruption Authority, see the specific company procedure on whistleblowing (Procedure below);
Public dissemination: making information about violations publicly available through newspaper or electronic media or otherwise through means of dissemination able of reaching a large number of people;
Reporting Person: the natural person who makes a report or public disclosure of information on violations acquired in the context of his/her work context;
Facilitator: a natural person who assists a Reporting Person in the reporting process, operating within the same work context and whose assistance must be kept confidential;
Involved Person: the natural or legal person mentioned in the report or in the public disclosure as the person to whom the violation is attributed or as a person otherwise implicated in the reported or publicly disclosed violation;
Follow-up: the action taken by the person entrusted with the management of the reporting channel to assess the existence of the reported facts, the outcome of the investigation and any measures taken

The data directly provided by the Reporting Person in order to report alleged unlawful conduct of which he/she has become aware by reason of his/her employment, service or supply relationship with the Company, as well as the data referring to the Reporting Person himself/herself, and to any Facilitator or Involved Person, shall be processed by the Company exclusively for the purpose of managing and follow-up the Report. The personal data are therefore acquired insofar as they are contained in the Report and/or in documents annexed thereto, they refer to the Reporting Person and may also refer to persons indicated as possibly responsible for the unlawful conduct, as well as to those involved in various ways in the events reported. The information acquired through the Report is then used to carry out the necessary investigative activities aimed at verifying the validity of the reported matter, as well as, if necessary, taking appropriate corrective measures and taking the appropriate disciplinary and/or judicial action against those responsible for the unlawful conduct.

5. Type of data processed

The receipt and management of Reports gives rise to the processing of 'common' personal data (name, surname, job role, date on which the Report was acquired), as well as may give rise, depending on the content of the Reports and of the acts and documents attached to them, to the processing of 'special' personal data (such as data relating to health conditions, sexual orientation or trade union membership, as specified in detail in Article 9(1) of the GDPR).
Personal data that is clearly not useful for processing a specific reporting is not collected or, if accidentally collected, is deleted immediately.

6. Data source

In the event that the Data Subject is the:

Reporting Person - his/her personal data is received as directly provided to the Company by the Reporting Person himself/herself with his/her Report;

Possible Facilitators or Involved Persons - their personal data is received as directly provided to the Company by the Reporting Person or in the course of the Follow-up to the Report, where the presence of such roles might become apparent later;

Involved Person- personal data referring to him/her is received as directly provided to the Company by the Reporting Person.

Since the regulations set out in Legislative Decree 24/23 provide for the possibility that a Reporting Person may make a Public Report or even an External Report directly to the ANAC Authority, the Company may receive the data referring to the above-mentioned roles through another entity: the ANAC Authority, the entities that publish the Public Report as received by the Reporting Person on their online or paper resources; this is also without prejudice to any other communications that the Company may receive from competent public authorities and in the course of a lawsuit.

7. Legal bases of processing

Taking into account the reference legislation, the processing of data is based on the legal obligation to which the Company is subject as Controller (Art. 6(1)(*c)* of the GDPR)) in order to comply with the requirements of Legislative Decree 24/23, and, with regard to any particular data voluntarily reported by the Reporting Person, the enabling condition is to be found in the reasons of relevant public interest on the basis of the law of the Union and of the Member States in relation to the reason for which the whistleblowing legislation was enacted (Art. 9, par. 2, lett. *g)* of the GDPR and Art. 2 sexies par. 1 of Legislative Decree 196/03), as well as in the fulfilment of obligations and on the exercise of specific rights of the Controller and the Data Subject in matters of labour law (Art. 9, par. 2, lett. *b) of the* GDPR). With reference to any personal data relating to criminal convictions and offences, the processing is based upon Art.10 of the GDPR, to the extent that said processing is necessary to comply with the requirements of Legislative Decree 24/23.

Further clarifications on legal bases

The prior consent of the Reporting Person will be required on a case-by-case basis (Art. 6(1*)*(*a)* of the GDPR) as provided for by the Decree, in particular:

- where the Follow-up to the Report involves disciplinary proceedings by the Company, and where the charge is based, in whole or in part, on the Report received and knowledge of the identity of the person making the report is indispensable for the defence of the accused, such Report shall only be usable for the purposes of disciplinary proceedings if the person making the report expressly consents to the disclosure of his/her identity;
- when the Report is made by means of a recorded telephone line or other recorded voice messaging system (as provided for in the Procedure), in order to allow, by the staff in charge, the relevant documentation by means of recording on a device suitable for storage and listening or by means of a verbatim transcription. In the case of transcription, the Reporting Person may verify, rectify or confirm the content of the transcript by signing it;
- when, at the request of the person making the report, the report is made orally during a meeting with the staff member in charge, whereby, with the consent of the person making the report, the report is documented by the staff member in charge by means of a recording on a device suitable for storage and listening or by means of minutes (as provided for in the Procedure). In the case of minutes, the reporting person may verify, rectify and confirm the minutes of the meeting by signing them.

8. Persons authorised to process data

The Company has authorised the persons entrusted with the task of handling the reports in question. The internal reporting channel is operated by service providers contracted as Data Processors pursuant to Article 28 GDPR. Where the Follow-up of Reports involves further activities, these will be conducted, each for its share of responsibility, by the competent internal departments of the Company. These persons are all formally authorised to process data and are specially instructed and trained to do so, and they are required to keep confidential all the data they became aware of it in the course of their duties, without prejudice to their reporting and notification obligations under Article 331 of the Code of Criminal Procedure.

9. Categories of recipients of personal data and possible data transfers outside the European Economic Area (EEA)

The data of the persons indicated as possibly responsible for the unlawful conduct, as well as of the persons involved in various ways in the reported events, will not be disseminated, however, if necessary under the laws in force, they may be transmitted to the Judicial Authority and to ANAC. These subjects are all autonomous Controllers.

In the context of any criminal proceedings that may be instituted, the identity of the reporter will be covered by secrecy in the manner and within the limits provided for in Article 329 of the Code of Criminal Procedure.; the identity of the Reporting Person shall not be disclosed in all cases where the allegation of the disciplinary charge is based on investigations that are separate from and additional to the report, even if consequent to the report itself, whereas it may be disclosed where three conditions are met, namely (*a)* that the allegation is based, in whole or in part, on the report, (*b)* that knowledge of the Reporting Person's identity is indispensable for the defence of the accused person and (*c) that* the Reporting Person has given his/her specific consent to the disclosure of his/her identity.

As a rule, personal data processing is carried out in Italy, with databases within the EEA. Should it become necessary to involve service providers, connected to the management of whistleblowing reports, established in countries outside the EEA, for the relevant transfer of data abroad the appropriate applicable safeguards will be adopted on a case-by-case basis in terms of adequacy decisions issued by the European Commission, standard contractual clauses always defined by the Commission or by the competent National Data Protection Authority or exceptions provided for by the GDPR. Further information on any data transfers to non-EEA countries and the relevant safeguards adopted, as well as on the companies appointed as Processors, may be requested from the DPO.

10. Modalities of processing

Personal data will also be processed by automated tools for the time strictly necessary to achieve the purposes for which it is collected. The Company adopts appropriate measures so that the data is processed in a manner that is adequate and conforms to the purposes for which it is managed, in accordance with the provisions of Articles 4, 12 and 13 of Legislative Decree 24/23, which also include, with regard to the IT platform, the encrypted Internet communication channel using advanced protocols as well as data stored in an encrypted format at data centres certified in accordance with ISO/IEC 27001 (Information Security Management System).

11. Data retention period

Reports and related documentation are kept for as long as necessary to process them, and in any case no longer than five years from the date of the communication of the final outcome of the reporting procedure , without prejudice to additional time periods in the event of the establishment, exercise or defence of a right in court.

12. Nature of data provision and consequences of failure to provide data

The report will only be taken into account if it is adequately substantiated, with details capable of bringing to light facts and situations relating them to specific contexts.

However, it is up to each Reporting Person to decide which personal data to provide. In this respect, there is the possibility of making anonymous reports as contemplated by Legislative Decree 24/23 provided that they are adequately substantiated as indicated above.

13. Rights of Interested Parties

As a general rule, Data Subjects have the right, at any time, to obtain confirmation of the existence or non-existence of the data provided, to request, in the forms provided for by law, the rectification of inaccurate personal data and the integration of incomplete data, and to exercise any other right under Articles 15 to 22 of the GDPR, by addressing their request to: DPO@fidiapharma.it.

If, on the other hand, the Data Subjects consider that the processing has been carried out in a manner that does not comply with the GDPR and Legislative Decree 196/2003, they may appeal to the Italian Data Protection Authority (Garante Privacy, www.garanteprivacy.it), pursuant to Article 77 of the GDPR.

With specific reference to the data processing carried out by the Controller as required by the applicable regulations on whistleblowing, pursuant to Article 13 paragraph 3 of Legislative Decree 24/23, it should be noted that it will proceed in compliance with the limits of the provisions of Article 2-undecies of Legislative Decree 196/03, which provides that the rights referred to in Articles 15 to 22 of the GDPR may not be exercised by making a request to the Data Controller or by lodging a complaint pursuant to Article 77 of the GDPR to the Garante Privacy if the exercise of such rights may result in actual and concrete prejudice to the confidentiality of the identity of the person reporting violations of which he/she has become aware by reason of his/her employment relationship or functions performed, pursuant to Legislative Decree 24/23.

Pursuant to Article 2-undecies paragraph 3 of Legislative Decree 196/03, the Controller informs Data Subjects that, in the aforementioned cases, rights shall be exercised in accordance with the provisions of the law or regulations governing the sector, which must at least contain measures aimed at regulating the areas referred to in Article 23(2) of the GDPR. The exercise of the same rights may, in any case, be delayed, limited or excluded by reasoned notice given without delay by the Controller to the Data Subject, unless such notice would jeopardise the purpose of the limitation, for the time and to the extent that this constitutes a necessary and proportionate measure, taking into account the fundamental rights and legitimate interests of the data subject, in order to safeguard the interests referred to in the confidentiality of the identity of the data subject. In such cases, the data subject's rights may also be exercised through the Garante Privacy in the manner set out in Article 160 of Legislative Decree 196/03. In such cases, the Garante Privacy shall inform the Data Subject that it has carried out all the necessary verifications or that it has conducted a review, as well as the Data Subject's right to lodge a judicial appeal.

If the Data Subject has given consent in the cases set out in the section 'Further clarifications on legal bases' above, he or she has the right to revoke that consent at any time, without, however, affecting the lawfulness of the processing, based on consent, carried out prior to the revocation.

These rights under Articles 15 to 22 of the GDPR, as well as the revocation of consent where given, may be exercised by making a request addressed to: DPO@fidiapharma.it.

Policy Rev. 01 published on 31st July 2023
Previous publication on 14th July 2023