farmaindustria

Code of Conduct Regulating the Processing of Personal Data

in Clinical Trials and Other Clinical Research and Pharmacovigilance Activities

February 2022

These texts are a non-official translation of the Spanish version of texts approved by FARMAINDUSTRIA.
The Spanish versions shall always prevail.

Contents

farmaindustria
Código de Conducta
DATOS PERSONALES

INTRODUCTION

Code of Conduct Regulating the Processing of Personal Data in Clinical Trials and Other Clinical Research and Pharmacovigilance Activities

February 2022

I

FARMAINDUSTRIA is the national trade association of the pharmaceutical industry in Spain. It brings together more than a hundred member companies that account for practically all prescription medicine sales in Spain.

FARMAINDUSTRIA's mission as an association is focused on the following objectives:

- Working with government agencies to design a stable economic and regulatory framework that fosters balanced growth, expansion of R&D and the development of the pharmaceutical industry.
- Enhancing the public perception of the pharmaceutical and drug industry, conveying to citizens, opinion leaders and public official the valuable contribution medicines make to our quality of life and social progress.
- Providing our member companies with value added services in the areas of information, consultancy and business partnerships.
- Representing the Spanish pharmaceutical industry, nationally and internationally.

II

In the pursuit of its objectives, while fully protecting the rights and freedoms of persons, FARMAINDUSTRIA has considered it necessary to adapt its activities in the clinical research and pharmacovigilance areas to the safeguards laid down in the legislation regulating the fundamental right to the protection of personal data, taking into account the crucial importance of those activities for scientific progress and the need to balance that progress with the rights of individuals.

As a consequence of that adaptation, on 17 June 2009 the FARMAINDUSTRIA Standard Code on Personal Data Protection in Clinical Research and Pharmacovigilance (the "**Standard Code**") was published and entered in the General Register of the Spanish Data Protection Agency (Agencia Española de Protección de Datos).

In addition, on 4 May 2016 the Official Journal of the European Union published Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the "**GDPR**"), effective as from 25 May 2018 and repealing at that date Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. As a consequence of the approval of the GDPR, Spain approved Organic Law 3/2018 of 5 December 2018 on the Protection of Personal Data and Guarantee of Digital Rights (Ley de Protección de Datos personales y garantía de los derechos digitales – the "**LOPDGDD**") to transpose the provisions of the GDPR into Spanish law.

The GDPR and LOPDGDD both contain provisions of special bearing on the activities of the member companies of FARMAINDUSTRIA and, in particular, on clinical research and pharmacovigilance. Those provisions, moreover, are complemented by the guidance issued by the Spanish

Data Protection Agency (Agencia Española de Protección de Datos – "**AEPD**") and by the European Data Protection Board ("**EDPB**").

In particular, the GDPR includes specific rules on data processing in clinical research that are implemented in the LOPDGDD. Of special importance in this regard is Additional Provision 17.2 of said statute, which regulates data processing in clinical health research.

III

Both the GDPR and LOPDGDD place central importance on establishing systems of self-regulation to complement the content of their provisions, adapting them to the specific characteristics of the processing carried out in a specific sector of activity and thus completing the general regime laid down by said law and regulation.

Whereas recital 98 of the GDPR specifies that "*[a]ssociations or other bodies representing categories of controllers or processors should be encouraged to draw up codes of conduct, within the limits of this Regulation, so as to facilitate the effective application of this Regulation, taking account of the specific characteristics of the processing carried out in certain sectors and the specific needs of micro, small and medium enterprises. In particular, such codes of conduct could calibrate the obligations of controllers and processors, taking into account the risk likely to result from the processing for the rights and freedoms of natural persons*". The GDPR itself has posited encouraging the drawing up of codes of conduct as one of the tasks or functions of the competent supervisory authorities, providing an opinion on and approving those that provide sufficient safeguards according to GDPR Article 57(1)(m). Article 40 of the GDPR stipulates that the Member States, supervisory authorities, the Board and the Commission should encourage the drawing up of codes of conduct intended to contribute to the proper application the Regulation.

IV

Not only does data protection legislation refer to the important role self-regulation can play in the legislation's enforcement, but it also specifies concrete benefits that can arise from the approval of codes of conduct that meet the requirements laid down in the legislation.

- Article 24(3) of the GDPR provides, first of all, that "*[a]dherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller*".

As is known, the GDPR establishes a system of compliance based on proactive responsibility or "accountability" of the persons obliged by the regulation, who must be in a position to demonstrate they have adopted the safeguards needed to ensure compliance. The GDPR considers that compliance with the provisions of a code of conduct can be a key determinant for finding that those obligations have been met.

- In this regard, Article 35(8) of the GDPR considers compliance with codes of conduct an essential element that should be taken into account favourably when assessing the impact of the processing operations for the purposes of a data protection impact assessment.
- Likewise, the adherence of a processor to a code of conduct is considered in Article 28(5) of the GDPR "*as an element by which to demonstrate sufficient guarantees*" of compliance with data protection legislation.
- Under Spanish law, Article 54(2) of the LOPDGDD envisages the possibility of the supervisory bodies for the codes of conduct collaborating with the AEPD in adopting mandatory guidelines as a result of the audit plans carried out.
- Also in relation to enforcement rules, Article 83(2)(j) of the GDPR includes adherence to a code of conduct as an element to be taken into account when quantifying the fines to be imposed for breaches of data protection rules.
- In addition, Article 65(4) of the LOPDGDD expressly provides for the possibility of the AEPD —before admitting for consideration a claim filed by a data subject— forwarding that claim to the supervisory body for the code of conduct to which the entity against which the claim has been brought has adhered, so that it can give an opinion on the issue and the claim can be settled before a proceeding is initiated by the supervisory authority.

V

From the standpoint of the activity of entities that have adhered to a code of conduct, their adherence facilitates their compliance with data protection regulations in the regulated areas. In this way:

- The adhering entities will have Protocols that allow the application of uniform criteria in the data processing in activities relating to clinical research and pharmacovigilance activities.
- Individuals participating in clinical investigations will enjoy the greatest safeguards in relation to the processing of their data.

- In pharmacovigilance matters, the effort to standardise procedures will allow a uniform and appropriate response to reports of adverse events, regardless of the channel through which the reports are received, offering maximum legal safeguards for consumers, physicians and pharmaceutical companies.

- There will be a lessening of the uncertainty felt by the adhering entities regarding the interpretation of the GDPR and LOPDGDD and their application to the most common daily situations seen in the pharmaceutical industry.

- The Spanish pharmaceutical industry will offer the different players in the market, and especially the consumers of its products, an image of unity, sensitivity and corporate effort and respect for the fundamental rights of citizens regarding the processing of personal data of individuals who participate in clinical research or in pharmacovigilance activities, in accordance with the applicable laws.

VI

Taking into account the important repercussions the Standard Code's implementation had in the pharmaceutical industry, and the unquestionable advantages that a system of self-regulation offers the adhering entities, both for dealing with the complex issues posed by data protection rules and in the undeniable benefits for fulfilment of the accountability obligations and the application of those rules by supervisory authorities, FARMAINDUSTRIA believes it is indispensable that the Standard Code (*Código Tipo*) in force to date be adapted to the provisions of the GDPR and LOPDGDD.

That adaptation culminates with the adoption of a new Code of Conduct Regulating the Processing of Personal Data in Clinical Trials and Other Clinical Research and Pharmacovigilance Activities (the "**Code of Conduct**"). The Code incorporates the substantive and formal requirements of the new data protection regulations, facilitates compliance with those rules by the Code's adherents and allows them to enjoy the benefits offered by the adoption of this instrument of self-regulation.

Mirroring the structure of the Standard Code, the Code of Conduct includes a general protocol on its scope and the mechanisms for monitoring compliance, as well as two specific protocols on the processing of personal data in clinical research and in pharmacovigilance activities.

VII

The most important aspects introduced by the Code of Conduct on data processing in scientific research may be summarised as follows:

- It only regulates processing of coded data by sponsors, given that the general practice of the sector is that sponsors engage in no processing of uncoded personal data.

- The legal basis for the data processing in this area is the fulfilment of legal obligations, without the consent of the research subject being needed for the processing of his or her data, without prejudice to the informed consent that must be given to participate in a clinical trial.

- The Code establishes the requirement to provide the data protection information separately from the information contained in the disclosure document that clinical trial rules require be provided to patients.

- Clarification of the roles of the different parties involved in the processing, specifying that the research sponsor and the healthcare centre or principal investigator will be the controllers of their respective processing, with each assuming the obligations that pertain to its activity, such that liability for breaches by any one of them will not be shared jointly with the others.

- The secondary use of the research data obtained in future research is regulated, without requiring, as a general rule, the consent of the participants in the research.

- The Code defines the concept of trusted third party, whom may be contracted to carry out the coding of the personal data of the participants in the research, such that the sponsor cannot on its own or with the mere assistance of the investigator re-identify the participants.

- The accountability obligations that must be fulfilled in relation to data processing in research activities are regulated. In particular, the Code resolves certain questions concerning notification of data breaches by third parties whose services were engaged by the sponsor.

- There are clarifications regarding international transfers of personal data, specifying that the rules on those transfers matters will not apply where it is completely impossible for a data transfer recipient located in another country or international organisation to re-identify the participants in the research because the data were previously anonymised by the sponsor who transferred the data. Nevertheless, where re-identification is possible, adequate safeguards will have to be adopted if the country of final destination does not offer a comparable level of protection to that of the GDPR.

- Different model clauses are included that will govern the legal relations between the different parties involved. The content of those models, however, may be modulated provided the final text offers equivalent safeguards.

VIII

In pharmacovigilance activities, the main novelties are:

- The differentiation is maintained between situations in which pharmaceutical companies process personal data that have been previously coded or not, clarifying the rules that apply in each case. In this regard, the Protocol begins with the regulation of the processing of identifying information and then addresses the specific provisions applicable to pharmacovigilance activities with coded data.

- The rules that apply to data processing in this area are adapted to the provisions of the regulations now in force, with special reference to the disclosure obligations laid down in Spanish law and in the European Union.

- The legal basis for the processing is defined having regard to those laws and regulations, as well as to the need to comply with a legal obligation, tied to the duty to ensure high levels of quality and security in healthcare, medicines and healthcare products.

- A uniform pharmacovigilance protocol is set out, differentiating the various channels through which reports may be received and the reporting party. A novelty on this point is that the Protocol also covers situations in which the information on adverse events becomes known through social networks.

- Disclosures of personal data relating to pharmacovigilance activities are regulated in detail, with special reference to the sharing of personal data within the same corporate group, taking into account the rules laid down in the applicable European regulations.

- The accountability obligations of adherent entities are detailed in order to guarantee compliance with the provisions of Chapter IV of the GDPR.

- A detailed protocol is included for managing and processing requests for exercise of the rights of access, rectification, erasure and restriction of processing.

IX

Together with those specific rules on clinical research and pharmacovigilance, the Code of Conduct, as already noted, includes a general first part that discusses the Code's scope of application, adherence procedure and implementation mechanisms. In that first general part, special reference should be made to the provisions regarding the following issues:

- Mechanisms are set out for disseminating the Code of Conduct and training.

- An independent control body is set up, which will have the powers and comply with all the requirements required by the AEPD and EDPB.

- An alternative procedure is regulated for out-of-court settlement of disputes that will allow an agile response with all safeguards to possible claims that may be brought by data subjects, as an alternative for pursuing those claims before the AEPD. This will reduce the possible litigiousness that could arise from the processing operations regulated by the Code of Conduct.

- Adequate guarantees are established for supervising compliance with the Code of Conduct by means, for example, of compliance audits and reviews and holding enforcement proceedings in cases of significant breaches.

X

In short, the Code of Conduct is intended to equip the entities that adhere to it an instrument to facilitate compliance with their data protection obligations in two particularly sensitive areas, allowing them to enjoy the undeniable benefits that personal data protection regulations confer upon self-regulation systems duly approved by data protection authorities.

In any event, to achieve this objective, there is express provision for the possibility of periodic review of the content of the Code of Conduct, at least every four years, so that it can be amended and incorporate the modifications needed to facilitate compliance with data protection rules in clinical research and pharmacovigilance activities in a constantly changing environment. Those periodic reviews are without prejudice to the possible review of the Code whenever required by new legislative or case-law developments.

XI

Lastly, we must add that the Code is not a static instrument, but one that may undergo successive modifications to adapt it to new interpretative criteria in the decisions of supervisory authorities, the latest case-law precedents and to the needs that may be raised by the adherent entities as a consequence of technological and scientific development in the fields regulated by the Code.

XII

This Code of Conduct is not adopted for the purpose of regulating international data flows and should therefore not be considered as a Code aimed at implementing adequate safeguards for international transfers of data.

1 GENERAL PROVISIONS AND GOVERNANCE OF THE CODE OF CONDUCT

1. Definitions

For the purposes of this Code of Conduct, the following definitions shall be taken into consideration, along with the definitions laid down in the regulations on the guarantees and rational use of medicines and medical devices, clinical research and biomedicine and the fundamental right to personal data protection.

1. **Adverse Event:** Any untoward medical occurrence in a subject administered a pharmaceutical product and which does not necessarily have to have a causal relationship with this treatment.

2. **Serious Adverse Event:** Any untoward medical occurrence that at any dose requires inpatient hospitalisation or prolongation of existing hospitalisation, results in persistent or significant disability or incapacity, results in a congenital anomaly or birth defect, is life-threatening or results in death.

3. **Auditor:** Any natural or legal person responsible for the independent and systematic examination of the activities and documents related to a clinical research project in order to determine whether the activities evaluated in connection with the study were conducted and the data were correctly recorded, analysed and reported in accordance with the study protocol, Standard Operating Procedures (SOP), Good Clinical Practice Guidelines and regulatory requirements.

4. **Master File for the Pharmacovigilance System:** Detailed description of the pharmacovigilance system used by the holder of the marketing authorisation for one or more authorised medicinal products.

5. **Clinical Trial Master File:** File that shall at all times contain the essential documents relating to the clinical trial which allow verification of its conduct and the quality of the data obtained, taking into account all characteristics of such trial, in particular if it is a low-intervention clinical trial.

6. **CEIm:** Ethics Committees for Investigation with medicinal products. An independent body with a multidisciplinary composition whose main purpose is to oversee the protection of the rights, safety and well-being of subjects participating in a biomedical research project and to offer public assurance in this respect by giving an opinion on the relevant research project documentation, taking into account the views of laypersons, in particular patients or patient organisations, and which is accredited to issue an opinion on a clinical study involving medicinal products.

7. **Research Site:** Any private or public entity or medical or dental facility where clinical research is being conducted.

8. **CRF:** Case Report Form. Printed, optical or electronic document designed to record all protocol-required information to be reported to the Sponsor on each clinical research participant.

9. **CRO:** Clinical Research Organisation. Natural or legal person contracted by the sponsor to perform the sponsor's duties or functions in connection with the clinical trial.

10. **Real-World Data:** Information relating to patient health status and/or the delivery of health care, collected in routine clinical practice from sources such as, but not exclusively: patient's records (including laboratory data), clinical studies other than clinical trials, medicine and disease registries, patient-generated data or data gathered from other sources such as mobile devices.

11. **Identifying information:** Any information concerning individuals that makes it possible to learn their identity. Identifying data is considered to include first and last names, initials, telephone, address, identification document (identity card number, foreigner's identification number or passport), social security number, patient's record number or similar information assigned by the government.

12. **Pharmacovigilance Department:** Department responsible for receiving, managing and registering adverse events.

13. **Clinical Research Department:** Department responsible for start-up, monitoring and other activities relating to clinical studies.

14. **Data Processor:** Natural or legal person, public authority, agency or other body processing personal data on behalf of the controller due to a provision of services.

15. **Observational Study With Medicinal Products:** All research involving the collection of individual data relating to human health, provided that it does not meet any of the conditions required to be considered a clinical trial established in Article 2(1)(i) of Royal Decree 1090/2015, of 4 December, regulating clinical trials with medicinal products, the Ethics Committees for investigation with medicinal products and the Spanish Clinical Studies Registry, and that is carried out for any of the following purposes:

1.º To determine the beneficial effects of medicinal products, as well as their modifying factors, including the perspective of patients, and their relationship with the resources used to achieve them.

2.º To identify, characterise or quantify adverse reactions to medicinal products and other risks to patient safety related to their use, including possible risk factors or effect modifiers, as well as to measure the effectiveness of risk management measures.

3.º To obtain information on the patterns of use of medicinal products in the population.

Observational studies with medicinal products should be aimed at complementing the information already known about the drug without interfering with routine clinical practice.

16. **Information Source or Data Source:** Origin of the data used to conduct the study. Data are considered primary when the information is obtained directly from participating subjects or from the health care professional for the purposes of the study. Data are considered secondary when the information is gathered from already existing data, such as the participating subject's medical history.

17. **Patient's record:** Set of documents containing the data, assessments and information of any kind on a patient's situation and clinical course throughout the health care process.

18. **Principal Investigator:** Investigator responsible for a team of investigators who conduct a clinical trial at a Research Site.

19. **Adhered Entities or Adherents:** Pharmaceutical companies (marketing authorisation holders or their local representatives) or other companies conducting research (sponsors) who may or may not be members of Farmaindustria, and CROs that are separately committed in writing to compliance with the provisions of this Code, in accordance with the procedure established herein.

20. **Monitor:** Qualified professional with the necessary training and clinical and/or scientific competence, chosen by the sponsor, who is responsible for direct follow-up of the conduct of the trial. The monitor is the link between the sponsor and the principal investigator when they are not the same person. In no case should the monitor be part of the investigator team.

21. **Good Clinical Practice Guidelines:** International ethical and scientific quality standard for designing, recording and reporting trials that involve the participation of human subjects.

22. **Sponsor:** Individual, company, institution or organisation taking responsibility for the initiation, management and setting up of the financing of the clinical research.

23. **Protocol:** Document describing the objectives, design, methodology, statistical considerations and organisation of a clinical trial. The term "protocol" encompasses successive versions of the protocol and protocol modifications.

24. **Record of Processing Activities:** File in which the processor or controller maintains a detailed list of the different kinds of processing carried out, including at least the information established in Article 30 of the GDPR.

25. **Trusted Third Party:** Natural or legal person not involved in performing the clinical research who is contracted by the Sponsor for the purpose of carrying out the coding process of the personal data of participants therein.

26. **Marketing authorisation holder:** Natural or legal person responsible for marketing the medicine for which the prescribed marketing authorisation has been granted.

2. Glossary

1. **AEMPS:** Spanish Agency of Medicines and Medical Devices (Agencia Española de Medicamentos y Productos Sanitarios).
2. **AEPD:** Spanish Data Protection Agency (Agencia Española de Protección de Datos).
3. **CC:** FARMAINDUSTRIA Code of Conduct for the protection of personal data in clinical research and pharmacovigilance activities.
4. **Civil Code:** Royal Decree of 24 July 1889 which published the Spanish Civil Code (Código Civil).
5. **DPO:** Data Protection Officer.
6. **DPIA:** Data Protection Impact Assessment.
7. **EDPB:** European Data Protection Board.
8. **EDPS:** European Data Protection Supervisor.
9. **Biomedical Research Law:** Law 14/2007 of 3 July 2007 on Biomedical research.
10. **HCP(s):** Healthcare professional(s).
11. **LOPDGDD:** Spanish Organic Law 3/2018 of 5 December 2018 on the Protection of Personal Data and Guarantee of Digital Rights (Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales).
12. **CCGB:** CC Governance Body.
13. **RDEC:** Spanish Royal Decree 1090/2015 of 4 December 2015 regulating clinical trials with medicines, medical product research ethics committees and the Spanish clinical studies registry.
14. **RDEO:** Spanish Royal Decree 957/2020 of 3 November 2020 regulating observational studies with medicinal products in humans.
15. **RDF:** Spanish Royal Decree 577/2013 of 26 July 2013 regulating pharmacovigilance of medicinal products for human use.
16. **CTR:** Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use.
17. **Implementing Regulation:** Commission Implementing Regulation (EU) No 520/2012 of 19 June 2012 on the performance of pharmacovigilance activities provided for in Regulation (EC) No 726/2004 of the European Parliament and of the Council and Directive 2001/83/EC of the European Parliament and of the Council.
18. **GDPR:** Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
19. **EU:** European Union.

3. General provisions

3.1 PURPOSE OF THE CODE OF CONDUCT

The purpose of this CC is to set out the rules that will govern the behaviour of marketing authorisation holders or their representatives in Spain and other sponsors of clinical studies with medicines who adhere to the Code, whether or not they are members of FARMAINDUSTRIA (the "**Adherents**"), in processing personal data of clinical trial subjects, patients and healthcare professionals carried out:

- As part of clinical research.
- In fulfilment of pharmacovigilance obligations laid down in the laws and regulations on medicinal products.

The Code will likewise apply to adhering CROs, solely in regard to the personal data processing they carry out in relation to the two points specified above and as a result of the engagement of their services by pharmaceutical companies adhered to the Code of Conduct.

The CC also sets out the rules for oversight and control of its provisions, including:

- The nature, composition, structure and functions of the Code of Conduct Governance Body (CCGB).
- The enforcement rules that apply to Adherents to the CC.
- The alternative dispute resolution procedure, both for cases involving a claim brought by an affected party and for those where the AEPD instructs the CCGB to act.

The terms of the CC supplement, and in no event substitute, the applicable laws on the protection of personal data.

3.2 TERRITORIAL SCOPE OF APPLICATION

This Code of Conduct shall only apply to the adhered entities mentioned in section 3.1 in relation to processing carried out in Spain and subject to the provisions of the specific legal provisions thereon. It does not apply to processing conducted outside of Spanish territory. It is thus designed as a National Code, subject solely to the authority of the Spanish Data Protection Agency and drawn up only in Spanish.

3.3 EFFECTIVE DATE AND REFORM OF THE CODE OF CONDUCT

This CC will enter into full effect, for an indefinite term, on the day following the date of the AEPD resolution on its approval and entry in the Register referred to by Article 38(5) of the LOPDGDD.

The provisions of the Code will not apply to research begun prior to the Code's effective date. Nevertheless, subsequent adoption of the measures deemed appropriate to allow full application of the Code to those investigations will be regarded as a good practice.

Data processing contracts made prior to 25 May 2018 under Article 12 of Organic Law 15/1999 of 13 December 1999 on the Protection of Personal Data will be governed by the provisions of Transitional Provision Five of Organic Law 3/2018 of 5 December on the Protection of Personal Data and Guarantee of Digital Rights.

The CCGB Secretary will propose to the CCGB whenever necessary and at least every four years that the CCGB issue a report on the need, where such is the case, to modify the CC to adapt or update it to possible changes in the regulations governing the activities covered by the CC and in the laws on the protection of personal data or their interpretation by the courts or in resolutions of supervisory authorities or the European Data Protection Board.

Where modification of the CC is deemed necessary, the CCGB will propose to FARMAINDUSTRIA the changes it considers appropriate. FARMAINDUSTRIA, in collaboration with the Code Adherents, will bring before its Executive Board for approval a draft proposal for the modified Code, accompanied by a memorandum explaining:

a) The reasons why the modification is considered necessary.

b) The changes to be made to the Code.

After being approved by the FARMAINDUSTRIA Executive Board, the proposed modification will be submitted to the AEPD for approval and entry in the Register referred to in Article 38(5) of the LOPDGDD, with effect as from the date of said registration.

3.4 ADHERENCE AND CANCELLATION OF ADHERENCE TO THE CODE OF CONDUCT

3.4.1 ADHERENCE PROCEDURE

The entities defined in section 3.1 on the purpose of the Code of Conduct may adhere to the CC provided they demonstrate their compliance with the obligations imposed by data protection regulations.

Those wishing to adhere to the CC must so state by completing the adherence application attached hereto as Annex 1 and submitting it to the CCGB. The application shall be signed by the entity's legal representative and accompanied by the representative's authorisation document. The application will be accompanied by information demonstrating the applicant's compliance with the GDPR and LOPDGDD, with express acceptance of the obligations contained in the CC and stating the applicant's intention to comply with those obligations. Compliance with the GDPR and LOPDGDD may be demonstrated, among other means, by submitting the results of the report on adaptation to the new data protection regulatory framework or the most recent data protection audit carried out in relation to the processing conducted by the applicant.

Applicants who are marketing authorisations holders or CROs adhering to the FARMAINDUSTRIA Standard Code on Personal Data Protection in Clinical Research and Pharmacovigilance registered in the Data Protection General Register of the AEPD shall so state in the application.

The CCGB will review the application and sworn statement and may ask the applicant to submit other documents it deems relevant for deciding on the application.

The CCGB will approve or deny adherence within a maximum of three months reckoned from the date all of the aforesaid documents have been received. A denial of adherence must state the grounds and how the errors or deficiencies detected can be corrected.

Approval of the request for adherence will entail publication of the information on the Adherent in the list of adhered entities that FARMAINDUSTRIA makes public on its website.

This CC will be binding on Adherents as from the date the CCGB gives notice of the approval of the adherence.

The governance bodies of FARMAINDUSTRIA will approve the system of annual dues for adherence to the Code and its updates.

3.4.2 CANCELLATION OF ADHERENCE

Adherence to the CC may be cancelled:

a) Voluntarily. Cancellation by the Adherent must be communicated in a written notice signed by the legal representative of the entity and sent to the CCGB, at least two months in advance of the effective termination of adherence, stating the intention to cancel adherence.

b) By a CCGB resolution adopted in an enforcement procedure.

3.5 ACCREDITATION OF ADHERENCE

In clinical research activities, the sponsor will state in the clinical trial protocol and in the rest of the documentation for the clinical trial that it adheres to the CC and complies with the applicable data protection obligations.

In pharmacovigilance activities, the pharmaceutical company will state in the consent request form, where consent is required, and in the rest of the documentation, that it adheres to the CC and complies with the applicable data protection obligations.

3.6 DISSEMINATION AND INTERPRETATION OF THE CODE OF CONDUCT

FARMAINDUSTRIA will post the CC on the self-regulation area of its website, allowing access to the full content of the CC and to the up-to-date list of Adherents. Those entities will provide a link on their websites to the CC area set up by FARMAINDUSTRIA.

The CCGB will address doubts and queries submitted by the Adherents in relation to the implementation and practical application of the CC.

It shall also keep Adherents periodically informed of legislative developments and new interpretations of data protection rules arising from decisions or reports of the AEPD and EDPB or from rulings handed down by Spanish and EU courts.

3.7 TRAINING

Adherents to this CC must conduct training on data protection matters for their personnel and professionals who process personal data.

FARMAINDUSTRIA will likewise conduct training activities on general data protection questions and on the CC in particular. Where the publication of a new regulation or an issue raised by an Adherent to the CC requires that specific data protection issues be addressed, FARMAINDUSTRIA will take the necessary measures to make those new developments known to the CC Adherents as soon as possible.

FARMAINDUSTRIA will also inform the Adherents to this CC of all data protection training sessions that may be of interest to them.

4. Governance body of the code of conduct

4.1 NATURE AND INDEPENDENCE

The Code of Conduct Governance Body (CCGB) is set up as oversight body for compliance with the Code on the terms laid down in Article 41 of the GDPR. The CCGB will be set up once the AEPD has approved the CC.

The CCGB will represent FARMAINDUSTRIA before the AEPD pursuant to its oversight and supervisory powers for the processing of personal data provided for in this CC by the Adherents. Toward that end, it will provide the AEPD will all information and documents requested by the latter for the performance of its functions, allow the AEPD to exercise its investigative powers and submit to the AEPD the resolutions and documentation of proceedings in relation to CC adherents.

In the discharge of its duties, the CCGB will be fully independent of FARMAINDUSTRIA and of the CC Adherents, subject to no instruction, supervision or control of its activity of any kind, and be governed by the principles of full organisational autonomy and independent judgment.

4.2 COMPOSITION

The CCGB will be composed of three members appointed by the FARMAINDUSTRIA Executive Board and Secretary.

The FARMAINDUSTRIA Executive Board will also appoint a maximum of three alternates, who will replace, in the stipulated order, the designated CCGB members whenever required and, in all events, with respect to a specific case, where there is a situation of conflict of interests, on the terms described further below. The alternates will likewise stand in for a CCGB member who has been appointed Mediator in an alternate dispute resolution procedure initiated as a consequence of enforcement proceedings.

The CCGB members shall elect one of them as President. The President will have the deciding vote in the case of deadlocked votes.

The CCGB members, whether principals or alternates, will be appointed for an initial term of four years, and may be reelected for terms of the same duration.

CCGB members and alternates must have proven experience and knowledge in data protection law and practice, in particular, in relation to the processing of data subject to regulation by this CC. Those qualifications can be demonstrated by providing curriculum vitae that show demonstrated experience performing functions involving the interpretation and application of data protection rules, or by submitting the relevant certificates and certifications.

Once they have been appointed, the members of the CCGB, in the pursuit of their activities therein, will be subject to what is provided for Data Protection Officers in Article 36(2) of the LOPDGDD.

The office of Secretary will be held by the head of the Legal Department in FARMAINDUSTRIA, assisted by the personnel from said Department. In the event of absence, vacancy or illness, the Secretary may be replaced by a person who works in that Department. The Secretary will also be responsible for hearing enforcement proceedings.

The Secretary will participate and speak in CCGB meetings but not vote. The responsibilities of that office include organising the CCGB meetings, monitoring its activities, drawing up and signing the meeting minutes and any other activity entrusted thereto by the Governance Body.

The CCGB will act with the assistance of an External Advisor, who shall be considered data processor in relation to the date to which he or she may have access in the provision of his or her services. If a conflict of interests is observed, the External Advisor will be subject to the provisions of section 4.5.

4.3 FUNCTIONS OF THE CCGB

As required by the GDPR, the CCGB will be responsible for the following functions in relation to optimum development of the CC:

a) Analysing applications for adherence to this CC, deciding on whether to accept or deny the application and keeping the list of Adherents to the Code up to date.

b) Disseminating, interpreting, complying with and monitoring the application of the CC, actively collaborating with the Adherents and enforcing compliance with the CC.

Toward this end, the CCGB may issue the guidelines to be followed by the Adherents to ensure proper compliance with the CC.

c) Handling queries by the Adherents in relation to compliance with the CC.

d) Promoting, developing and executing training initiatives on the CC for Adherents and their personnel, without prejudice to what is provided in the section on training.

e) Obtaining information from the Adherents on the CC's functioning and its effectiveness and degree of compliance, as well as the doubts and suggestions they may raise.

f) Issuing a report every four years on the need, where such is the case, for modification of the CC, proposing the changes deemed appropriate.

g) Preparing an annual report on its activities to be submitted to the Executive Board of FARMAINDUSTRIA.

h) Any other function that is needed or useful for proper application of the CC.

The CCGB will also have the following powers in relation to monitoring and supervising compliance with this CC:

a) Observing and controlling compliance with the provisions of this Code, scheduling an annual programme of systematic and random audits and reviews.

The purpose of this activity is to verify that Adherents are fulfilling the commitments made in this CC.

After the review is completed, the CCGB will issue a report for the audited Adherent, specifying incidents detected and proposals for remedying any possible breaches. In no event will the content of the report be shared with other Adherents.

b) Carrying on the proceedings provided for in section 6 and adopting the pertinent measures to enforce the resolutions.

4.4 RULES OF PROCEDURE AND DUTY OF SECRECY

The CCGB shall meet whenever necessary in relation to the proceedings regulated in this CC and at least every three months. Minutes will be taken of the meetings.

Valid adoption of resolutions will require the presence of the three members of the CCGB, replaced, where appropriate, by their alternates.

FARMAINDUSTRIA personnel whose presence is needed for a fuller understanding of the questions to be discussed and decisionmaking may attend and speak, but not vote, at the CCGB meetings.

The CCGB members shall have no access to individual and disaggregated data of the Adherents, except where such access is indispensable for performing their duties. In any event, its members shall preserve the secrecy of any information, including personal data, to which they have access in the performance of their duties, for which purpose they will sign a confidentiality undertaking.

4.5 CONFLICT OF INTERESTS

If a member of the CCGB or the Secretary believes there is a conflict of interests with the Adherent with whom a proceeding regulated by this CC is being pursued, said person must abstain from participating in the proceeding, giving immediate notice thereof to the Secretary of the CCGB.

The rest of the members of the CCGB or the entity with whom the proceeding is being pursued may likewise challenge said member, and the challenge will be resolved by the rest of the members of the CCGB after hearing the person challenged.

In either case, one of the alternates shall be designated in relation to the matter to replace the member who asked to abstain or who was challenged. If the Secretary is challenged, the Secretary shall be replaced by a person working in the Legal Department of FARMAINDUSTRIA.

Also, a party who has brought a claim before the CCGB that is to be handled as provided in section 6.2 may move to challenge the CCGB member who was named as Mediator to hear and resolve the claim. The challenge will be resolved by the rest of the members of the CCGB after hearing the challenged person.

If the challenge is upheld in this case, the challenged member will be replaced in the functions of Mediator by the CCGB member designated by turn of assignment.

The challenged member shall not have access to the case file for the proceedings in which a conflict of interests was held to exist for so long as the grounds for his or her abstention or challenge continue to exist.

4.6 FUNDING OF THE CCGB

FARMAINDUSTRIA will make a specific budget allocation for maintenance and operation of the CCGB in order to ensure its full financial independence. The budget allocation should be in the amount needed to fund the functions and responsibilities of the CCGB. FARMAINDUSTRIA shall not use the funds of that allocation for other purposes during the term of the annual budget.

The annual budget will be set by the governance bodies of FARMAINDUSTRIA and be funded in all events by the dues of its members and, if applicable, by the dues of Adherents who are not members of FARMAINDUSTRIA.

At the end of each year a review will be conducted of the amount of the budget allocation mentioned in the preceding paragraph and of the dues that will have to be paid to maintain it. An increase or decrease in that allocation will be decided according to the deficit or surplus, respectively, recorded at the close of the year, also taking into account the ordinary increase in the costs of maintaining CCGB.

5. Enforcement

Adherents will be subject to the enforcement rules set out in this CC, without prejudice to and independently of such liability as may arise from their actions vis-à-vis the AEPD.

The enforcement regime regulated here is established without prejudice to the sanctioning powers that the GDPR, the LOPDGDD and other applicable data protection provisions grant to the AEPD.

5.1 BREACHES OF THE CC

The infringements defined in Article 83 of the GDPR and in this article will be considered breaches of this CC. The minor, serious or very serious nature of the breaches will be determined as provided in Articles 72 to 74 of the LOPDGDD.

In addition to those provided for in Article 83(5) of the GDPR and Article 72 of the LOPDGDD, the following will be considered **very serious breaches**:

a) The commission of two serious breaches within a period of one year or less.

b) Failure to comply or delay in complying with sanctioning resolutions of the CCGB.

c) Repeated and unjustified refusal by Adherents to submit to the systematic reviews or audits envisaged in this CC.

d) Breach of the duty of secrecy that applies in clinical research or pharmacovigilance activities.

e) Disclosures or transfers of data other than in the permitted cases.

In addition to those provided for in Article 83(4) of the GDPR and Article 73 of the LOPDGDD, the following will be considered **serious breaches**:

a) The commission of two minor breaches within a period of one year or less.

b) Refusal or unjustified delay in abiding by resolutions adopted by the CCGB in the alternate dispute resolution system.

c) Impeding audits by the CCGB, except where such conduct qualifies as a very serious breach.

d) Refusal to submit to the systematic and random reviews by the CCGB regulated by this CC, except were such conduct qualifies as a very serious breach.

e) Processing the personal data of participants in clinical research projects or consumers, legal representatives or other reporters who contact the pharmacovigilance service for purposes (such as commercial and promotional purposes, etc.) that are incompatible with the purposes for which the data were obtained.

f) Impeding or hindering the exercise of the rights of access, rectification, erasure and objection or refusal to provide the requested information.

g) Failing to eliminate data or to anonymise data, beyond the expiry of the storage period stipulated in the laws and regulations applicable to the sector as necessary for complying with the objectives of the clinical research or pharmacovigilance, without prejudice to the possible storage and secondary uses of the data envisaged in this CC.

h) When working with pseudonymised or coded data, processing personal data that have not been previously coded with respect to the participants in the clinical research projects, legal representatives or other reporters who contact the pharmacovigilance service together with evaluations, comments, statistics, conclusions or any other data.

i) Where the data have not been coded, access by unauthorised personnel to the areas where the identifying information of consumers, legal representatives or other persons making reports to the pharmacovigilance service are stored.

j) Where the data have been coded, failing to take the necessary preventative measures to avoid reversal of the coding process, leading to access to identifying information in clinical research or in pharmacovigilance activities.

k) In pharmacovigilance activities where it has been decided to submit consumer data to coding, recording the identifying information of a consumer.

l) In pharmacovigilance activities where the data are coded, including identifying information of consumers, legal representatives or other reporting parties in the reports made.

In addition to those provided for in Articles 83(4) and 83(5) of the GDPR and Article 74 of the LOPDGDD, the following will be considered **minor breaches**:

a) Undue delay by the Adherent in answering CCGB requests for information or documents, where such delay does not constitute a serious breach.

b) Hindering the CCGB in the performance of its functions in relation to systematic reviews or the alternative dispute resolution system.

c) Failing to complete or cancel and substitute ex officio, for formal reasons, the personal data of participants in clinical research projects or of consumers/legal representatives or other reporters who have suffered or report an adverse event, where the data are found to be inaccurate or incomplete.

d) Failing to inform the participant in a clinical research project, the consumer, their legal representative or other reporters of the provisions of this Code regarding clinical research and pharmacovigilance.

e) Failing to subscribe with a CRO or other natural or legal person with access to data by virtue of the provision of a service a data processing contract in accordance with the provisions of this Code on clinical research and pharmacovigilance matters.

5.2 PENALTIES

Without prejudice to the sanctioning power of the AEPD, the following penalties may be levied by the CCGB:

a) Penalties for minor breaches: Written reprimand.

b) Penalties for serious breaches: Written reprimand and temporary suspension of adherence to the CC until the remedy of the breach has been confirmed.

c) Penalties for very serious beaches: Written reprimand, publication of the penalty imposed and temporary suspension of adherence to the CC for one to three years.

By way of exception, in the case of very serious breaches, where the unlawfulness or culpability is severely aggravated, the penalty will be exclusion from the CC and consequent loss of status as Adherent.

Each of the penalties will carry the obligation to remedy or correct the defects or irregularities observed and rectify the improper conducts or situations.

6. Proceedings carried on by the CCGB

6.1 COMPUTING TIME PERIODS

Unless otherwise specified, in time limits given in days, only business days will be counted.

6.2 PRELIMINARY OUT-OF-COURT DISPUTE RESOLUTION PROCEDURE

6.2.1. DESCRIPTION AND COMPETENCE

A voluntary, free, out-of-court procedure is established for claims regarding data protection matters brought by data subjects against Adherents to the Code.

Data subjects may use this alternative procedure and submit a claim to the CCGB if they believe their personal data protection rights have been infringed by an Adherent to the Code.

They may likewise file a claim if they believe that requests to exercise their rights of access, rectification, erasure, objection, restriction of processing and portability recognised by the GDPR, LOPDGDD and this CC have not been handled properly.

The proceedings will be conducted and resolved by a member of the CCGB (the "**Mediator**"). For this purpose, a system of rotating assignments will be established for conducting the proceedings. Where necessary, the Mediator may request the presence of the CCGB Secretary and the External Advisor. The Mediator will perform these duties with full respect for the principles of independence, impartiality, transparency, equity, effectiveness, legality and freedom.

6.2.2 PROCEDURE

Claims may be filed with the CCGB, which shall immediately forward them to the Mediator designated by turn of assignment.

Farmaindustria will set up an e-mail address for filing claims and post that address visibly on its website.

Claims must be made in writing, using the template included as Annex 2 hereto and which will be available on the Farmaindustria website. The claim shall include at least the following:

a) Full legal name of the claimant, his or her identity document, tax ID or identifying document, address and, if acting through a representative, the identifying detail of the representative and evidence of representative capacity.

b) An e-mail address for notices.

c) The identity of the Adherent against whom the claim is filed.

d) The facts on which the claim is based and the relief sought.

e) Specification, if applicable, of the harm or losses occasioned to the claimant as a consequence of the actionable conduct.

f) Supporting documents and evidence of the facts and, if applicable, the harm and losses claimed.

g) Statement that the claimant has on the basis of those same facts neither filed a complaint with the AEPD nor brought a civil suit for reparation of damages occasioned by the actionable conducts.

Claims will not be admitted for consideration if a complaint has already been filed with the AEPD regarding the same facts, even where no proceedings have yet been initiated as a result of the complaint, without prejudice to proceedings conducted as a result of claims forwarded by the AEPD. Nor will claims seeking damages be admitted if a claim has already been filed for those damages in a civil court.

Upon receiving the claim, the Mediator will forward it to the Adherent against whom the claim was filed in order for said entity to submit the pleadings it deems fit within 15 business days.

Solely within said time limit the procedure may also be terminated, with the Mediator resolving to close the case and so notifying the data subject and the Adherent, in the following events:

- Where the Adherent states in writing that it accepts the claim and commits to satisfying the relief sought by the claimant in full.

- Where the claimant and the Adherent against whom the claim was brought notify the Mediator that they have reached an agreement on the issue raised.

At the end of the 15-day period for submitting pleadings, the Mediator will have a further 15 days to resolve on the claim:

a) Upholding or rejecting the claim.

b) Specifying, if applicable, the corrective measures that should be taken to ensure the fundamental right of the claimant is not harmed.

c) Resolving as appropriate on the existence of the pecuniary and non-pecuniary harm claimed, as applicable, and the appropriateness of awarding damages.

The Mediator's decision will be binding on the Adherent.

The resolution will be served on the parties in order for them to comply with the terms of the resolution within the time limit stipulated therein. It will be posted on the relevant area of the Farmaindustria website, in all cases eliminating the data of the parties involved and any metadata or other data associated with the resolutions.

The Mediator must be notified of the actions taken by Adherents to comply with the decisions reached in the dispute resolution procedure.

6.3 ENFORCEMENT PROCEDURE

The CCGB may decide to open enforcement proceedings in the following cases:

a) Where a resolution has been handed down in a preliminary dispute resolution procedure imposing an obligation on an Adherent and the latter fails to comply with the obligation within the time limit specified in the resolution.

b) By initiative of the CCGB itself where it sees indicia of breaches or learns of their existence by any means, in particular, as a result of the systematic and random reviews and audits it conducts under this CC.

c) Enforcement proceedings may likewise be initiated where the CCGB learns of the existence of a large number of requests to exercise rights that have gone unattended by a given Adherent.

The enforcement proceedings will be divided into the examining phase, which shall be conducted by the CCGB Secretary, and the resolution of the case, which shall be done by the CCGB. In the case of proceedings brought under subparagraph (a) above, the CCGB member who acted as Mediator in the preliminary dispute resolution procedure will abstain from participating.

Where the CCGB sees fit to initiate enforcement proceedings, it shall so notify the Secretary, who, after taking the relevant actions, will prepare a report briefly setting out the facts known or detected and the breaches possibly committed by the Adherent. The Secretary will forward the report to the Adherent so that it may oppose the adoption of enforcement measures and submit the pleadings it deems fit within 20 business days.

After the time limit for submission of pleadings has ended, the Secretary may resolve to take such other actions as he or she deems appropriate to better establish the facts. The time limit for said further actions shall run no longer than one month.

To carry out those actions, the Secretary may use all means he or she considers appropriate to establish the facts and may call on the assistance of the External Advisor. The Adherent affected by the proceeding will be obliged to fully cooperate with the Secretary and for whomever acts on behalf of the Secretary.

The Secretary may likewise at any time propose to the CCGB the adoption of interim measures to preserve the rights of third parties. Where such interim relief is proposed, the CCGB will have 10 calendar days within which to resolve on the proposal.

At the conclusion of the period for conducting the pertinent investigative actions, the Secretary will draw up, within a maximum of one month, a proposed decision setting out the facts and an opinion as to whether they may constitute a breach, as well as their characterisation, and the proposed penalty deemed appropriate. The proposal, together with the case file, will be brought before the CCGB for assessment and resolution.

Within a maximum of one month after receiving the proposal, the CCGB will decide if a breach has been committed and the appropriate penalty, and, if applicable, the measures the Adherent must adopt to cease the misconduct. The resolution admits of no appeal and will be notified to the Adherent so that the Adherent can proceed to comply.

The CCGB resolution will be posted on the relevant area of the Farmaindustria website, in all cases eliminating the data of the parties involved and any metadata associated with the resolutions except, in the case of very serious breaches, the data identifying the penalised party.

Enforcement of the resolutions handed down in enforcement proceedings will rest with the CCGB, except for resolutions entailing the Adherent's suspension or exclusion from the CC, which will be enforced by the Farmaindustria Executive Board on the terms provided in the CCGB resolution.

6.4 HANDLING OF CLAIMS FORWARDED BY THE AEPD

Where the AEPD forwards to the CCGB a claim filed with the AEPD under Article 65(4) of the LOPDGDD, the same procedure as provided for resolution of disputes will apply. In this case, the CCGB Secretary will give immediate notice of the forwarded claim to the Mediator who by turn of assignment is to carry on the proceedings on the general terms of section 6.2.2, except for the time period for submitting arguments, which will be seven business days.

Annex 1:
Application to adhere to the code of conduct

TO THE GOVERNANCE BODY OF THE Farmaindustria CODE OF CONDUCT

REGULATING THE PROCESSING OF PERSONAL DATA IN CLINICAL TRIALS AND OTHER CLINICAL RESEARCH AND PHARMACOVIGILANCE ACTIVITIES

Mr/Ms [***], of legal age, with business address in [***], at Calle [***] and holding national / taxpayer identity document number [***], acting for and on behalf of *[complete with registered name of the applicant company]* ("**the Applicant**"), having its registered office in [***] and taxpayer identification number [***], as evidenced in the accompanying documentation [the power of attorney must be submitted].

The person appearing herein represents that the power of attorney under which he or she is acting has not been revoked or limited and is sufficient to bind his or her principal and, to such effect,

STATES

I. That the Applicant employs the utmost diligence to comply with the personal data protection laws in its ordinary activities, in accordance with the terms of Regulation (EU) No 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (the "**GDPR**"), and of Organic Law 3/2018 of 5 December 2018 on the Protection of Personal Data and Guarantee of Digital Rights (Ley de Protección de Datos personales y garantía de los derechos digitales – the "**LOPDGDD**").

II. That the Applicant wishes to adhere to the Farmaindustria **Code of Conduct** Regulating the Processing of Personal Data in Clinical Trials and Other Clinical Research and Pharmacovigilance Activities (the "Code of Conduct"), which was approved by the Executive Board of Farmaindustria at its meeting of ** December 2019 and was entered in the General Register of the Spanish Data Protection Agency (Agencia Española de Protección de Datos) under the resolution of [***] [***] 20[**]. Toward that end the Applicant has approved the internal resolutions, bylaws provisions and all other types of documents required to submit this application.

III. That the Applicant expressly agrees to comply with the obligations set out in the Code of Conduct and undertakes to implement the measures, procedures and actions required to adapt its organisation and functioning to the commitments and obligations it contains.

IV. That the Applicant submits expressly and without reservation to the procedures envisaged in the Code of Conduct for monitoring compliance therewith.

V. [Include in case of adherence to Standard Code previously registered with the AEPD] Whereas the Applicant was adhered to the FARMAINDUSTRIA Standard Code on Personal Data Protection in Clinical Research and Pharmacovigilance previously registered in the Data Protection General Register of the Spanish Data Protection Agency.

Now therefore, the Applicant hereby **REQUESTS** that the Governance Body of the Code of Conduct deem this application of adherence to the Code of Conduct to have been filed, admit it for consideration and accept said request.

Done in [***], on [***] [***] 20[**]

[Complete with the registered name of the Applicant entity]

Signed.:

[Position]

In accordance with the rules on protection of personal data, the Code of Conduct Governance Body will process your personal data in order to manage the application. You may exercise before said body the rights of access, rectification, erasure, objection, restriction of processing and portability laid down in the personal data protection regulations.

III. That the Applicant has adopted the necessary technical and organisational measures to ensure full compliance with the GDPR, the LOPDGDD and the Code of Conduct and has entered in its Record of Processing Activities the data processing carried out in the activity regulated by the Code of Conduct.

IV. That the following supporting documents are submitted herewith for the assertions made in this statement.

[complete as indicated in Section 3.4]

In witness whereof and for the relevant purposes, I sign this statement in [***], on [***] [***] 20[**]

[Complete with the registered name of the Applicant entity]

Signed.: _____

[Position]

Appendix: SWORN STATEMENT

I, Mr/Ms [***], of legal age, holding national / taxpayer identity document number [***], for and on behalf of [*Complete with registered name of the Applicant entity*] (("**Applicant**"), having its registered office in [***] and holding taxpayer identification number [***], do hereby

DECLARE UNDER MY OWN LIABILITY

I. That the Applicant complies with the provisions of personal data protection rules and, in particular, with Regulation (EU) No 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (the "**GDPR**"), and of Organic Law 3/2018 of 5 December 2018 on the Protection of Personal Data and Guarantee of Digital Rights (Ley de Protección de Datos personales y garantía de los derechos digitales – the "**LOPDGDD**").

II. That the Applicant is in full conformity with the terms of the FARMAINDUSTRIA Code of Conduct Regulating the Processing of Personal Data in Clinical Trials and Other Clinical Research and Pharmacovigilance Activities (the "**Code of Conduct**").

Annex 2:
Template for claims filed with the code of conduct governance body

TO THE GOVERN ACE BODY OF THE FARMAINDUSTRIA CODE OF CONDUCT

REGULATING THE PROCESSING OF PERSONAL DATA IN CLINICAL TRIALS AND OTHER CLINICAL RESEARCH AND PHARMACOVIGILANCE ACTIVITIES

PARTICULARS OF THE DATA SUBJECT

Mr/Mrs		Document / Passport
Address		
Town	Province	P.C

PARTICULARS OF THE REPRESENTATIVE (if applicable)

Mr/Mrs		Document / Passport
Address		
Town	Province	P.C

E-mail address for notices:

Code Adherent against whom the claim is brought:

Basis for the claim and relief sought

▶ next page

Basis for the claim and relief sought

Detail the facts on which the claim is based and the harm and losses claimed, which must be evidenced with the appropriate supporting documents

Documents and evidence submitted:

☐ Declare that I have not filed a complaint with the AEPD based on these same facts.

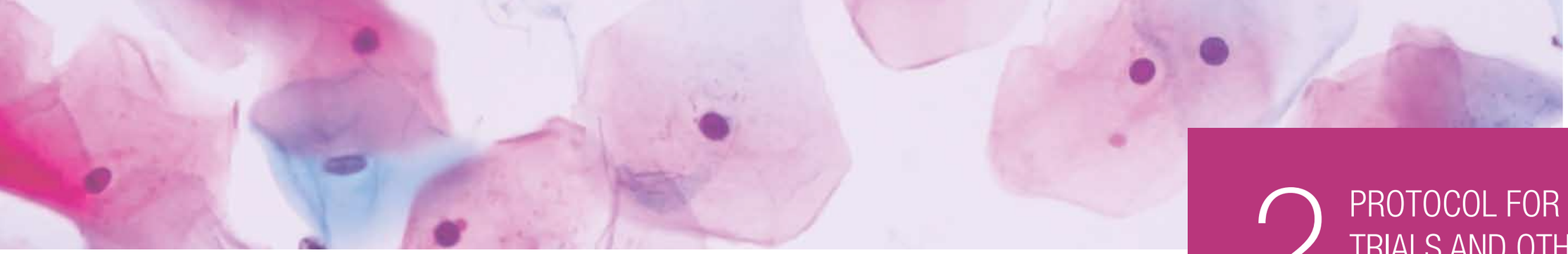
☐ Declare that I have brought no claim in civil court for the damages sought in this claim.

Done in on 20 .

Signature of the claimant

Signature of the representative (if applicable)

In accordance with the rules on protection of personal data, the Code of Conduct Governance Body will process your personal data in order to handle your claim. You may exercise before said body the rights of access, rectification, erasure, objection, restriction of processing and portability laid down in personal data protection regulations.



2 PROTOCOL FOR CLINICAL TRIALS AND OTHER CLINICAL RESEARCH

* The Annexes should be considered guides or illustrative models to aid in preparing the documents that apply to the respective topics.

1. Data protection principles

The different parties taking part in the clinical research must ensure compliance with the data protection principles enshrined in the GDPR and LOPDGDD over the course of the research.

In any event, the application of those principles needs to be modulated according to the circumstances in which the personal data will be accessed by each of those parties. In particular, it must be borne in mind that the Sponsor will only access coded data, such that even when processing personal data it will not be able to identify the participants in the trial directly and this will affect the application of some of the data protection rules.

That being said, the data protection principles that must be guaranteed during the processing are:

1.1 PRINCIPLE OF PURPOSE LIMITATION

The GDPR provides that personal data must be processed for the explicit, legitimate, specific purposes that justify their processing. In clinical investigations, the purpose is determined by the nature of the investigation. In this respect, having regard to the nature of the investigation, one must consider the definitions of “clinical study”, “clinical trial”, “low-intervention clinical trial” and “observational study” set out in the REC and RDEC, as well as those coined in the Biomedical Research Law and RDEO.

Once the investigation has concluded, the data should only be processed by the Sponsor and the Site for purposes compatible with the investigation conducted. A compatible purpose in this sense is the inclusion of the data by the Site in the patient’s record of the participant, as that processing is required by the very laws that regulate patient’s records.

The Sponsor and the Investigator may likewise process data obtained from the scientific research, once concluded, to carry out new research in those cases allowed by the applicable rules and, in particular, in accordance with the provisions of the Biomedical Research Law and Additional Provision 17 of the LOPDGDD. These secondary uses are analysed in detail in section 3.9, differentiating between processing involving personal data, in the case of the Investigator, and processing of coded data by the Sponsor.

In all events, the information may be used if, after the investigation ends, safeguards to avoid re-identification of the participants are reinforced. For example, subsequent use will be possible, without limitation, of data obtained if the data are coded and then submitted to a process rendering it impossible to associate each personal datum with an individual participant. In this case the data will have been anonymised and thus not be considered personal data, so that they can be used for other purposes after the investigation without the need to examine the compatibility of this new purpose of the processing.

1.2 PRINCIPLE OF LAWFULNESS AND FAIRNESS IN PROCESSING

The Sponsor and Principal Investigator must process the personal data of participants pursuant the legal basis set out in Article 6 of the GDPR. According to section 3.3 the processing will be justified in this case by the legal obligation that it be carried out in accordance with the legislation regulating the guarantees and rational use of medicinal products and medical devices (Article 6(1)(c) of the GDPR), in connection with the limitation of the prohibition of processing health data for reasons of public interest in the area of public health and for ensuring high standards of quality and safety of medicinal and healthcare products (Article 9(2)(i) of the GDPR), as well as for conducting scientific research (Article 9(2)(j) of the GDPR). The processing is not justified by the data subject's consent, without prejudice to the informed consent that is required in order to participate in the clinical research. That informed consent does not refer to the processing.

The Sponsor and Site shall adopt measures to ensure that the clinical research is pursued according to the applicable national and EU rules cited in section 2.2 of this Protocol.

1.3 PRINCIPLE OF TRANSPARENCY

The transparency principle speaks to the right of participants to be informed of the manner in which their personal data are to be processed and to be provided the information referred to by Article 13 of the GDPR.

This means that even where the participants' consent does not need to be obtained to process their data in scientific research activities, the data subjects must be informed of the processing of the data and provided with the requisite information at the time they are asked to give their informed consent to participating in the research. The content of the information that must be disclosed to the participant is given in section 2.4.2.

1.4 PRINCIPLE OF DATA MINIMISATION

The data processed must be adequate, relevant and limited to what is necessary for achieving the stated purposes of the processing.

This means that processing operations should only involve information without which it would not be possible to achieve the results pursued by the clinical research in relation to the utility of the medicine, device or medical treatment, without including any additional information that is not relevant for that purpose. Toward this end, the CRF for the clinical research must be devised to limit the information collected, especially health data of participants, to the data necessary for achieving the purpose of the investigation, without including any unnecessary information.

The information gathered must also be as objective as possible to ensure that all data obtained are necessary and strictly conform to the purpose of the clinical research are obtained. Toward this end there should be maximum parameterisation of the information included in the CRF, without prejudice to the possibility of including additional information where indispensable for ensuring the result of the clinical research.

It bears emphasis that the principle of data minimisation in processing by the Sponsor is reinforced by the requirement that only previously coded data will be accessed by the Sponsor. Thus, even where the Sponsor could legitimately process data not previously coded, the fact that coding is always done lends greater robustness to the measures adopted and thus allow the use of the data obtained during the research in subsequent activities by the Sponsor relating to the medicine or the medical treatment studied in the clinical research.

1.5 PRINCIPLE OF ACCURACY

The data must be accurate and, where necessary, kept current and up to date. In this case, the accuracy and updating of data related to the evolution of the participant's health are essential for being able to guarantee proper fulfilment of the purpose of the clinical research.

Responsibility for ensuring compliance with the accuracy principle rests with the Principal Investigator, who must ensure that the data recorded in the CRF accurately reflect the participant's evolution. Toward this end, as already indicated in relation to the data minimisation principle, it is essential that the information contained in the CRF be parameterisable, whenever possible, so that it is based on objective criteria and maximally reduces the introduction of subjective criteria that could distort the accuracy and currency of the information.

The information received by the Principal Investigator and the investigator team regarding completion of the CRF must be clear and accurate, ensuring the input of objective data and narrowing the margin for input of subjective or erroneous information.

The Principal Investigator must also adopt measures to ensure continuous review of the information included in the CRFs in order to ensure the accuracy of the information and avoid errors, discrepancies or inconsistencies with the participant's information that may be entered in other systems at the same Site, such as the medical history systems. Where discrepancies are detected, the erroneous or inconsistent data in the CRF must be corrected immediately, giving notice thereof to the other parties involved in the investigation so that all of them have accurate and current information.

Requests to rectify or eliminate personal data that could affect the accuracy and currency of the health data of participants in the clinical investigation must likewise be attended to as swiftly as possible, without prejudice to what is provided in section 3.7.

1.6 PRINCIPLE OF STORAGE LIMITATION

The data must be retained as long as necessary to achieve the purpose of the data processing.

On this question, EU legislation and Spanish law lay down specific retention periods for clinical research data. These are detailed in section 3.6 and are of mandatory compliance.

In any event, the limitation periods do not affect use and processing of data for reuse or for secondary uses in subsequent research. Nor do they affect possible retention of information that has been anonymised so that the data subjects cannot identified and are thus no longer subject to data protection legislation.

1.7 PRINCIPLE OF INTEGRITY AND CONFIDENTIALITY

Technical and organisational measures have to be adopted to ensure the availability, integrity and confidentiality of the information. Those measures will be the outgrowth of a prior data protection impact assessment performed as described in section 2.1. Section 2.2 clarifies the security measures that must be implemented in relation to the processing of clinical research data.

Together with these obligations, the LOPDGDD imposes on the different parties involved in clinical research a duty to maintain the confidentiality of the data processed in the research activity. This duty of the Principal Investigator's team complements and does not substitute the duty of secrecy imposed on the medical profession.

2. Preliminary phases of a clinical investigation

2.1 PERFORMING A PERSONAL DATA PROTECTION IMPACT ASSESSMENT

Before the clinical research begins, a data protection impact assessment (DPIA) must be performed to the extent that, in accordance with the provisions of Article 28 of the LOPDGDD, the nature, scope, context and purposes of the processing are likely to result in a high risk for the fundamental rights and freedoms of the participants in the research.

In this regard, one single DPIA may be performed for all of the clinical investigations carried on by the Sponsor. Without prejudice to the above, in those cases where some additional action is taken in a specific clinical investigation the nature, scope, context and purposes of which are likely to result in a high risk to the fundamental rights and freedoms of the participants, a DPIA must be performed and the results annexed to the comprehensive DPIA report.

In addition, where a specific DPIA is carried out, collaboration in performing the DPIA may be requested from the Monitor, the CRO, the Principal Investigator's team and from any other processor of data of the clinical research participants.

In this connection, the aforementioned Article 28 of the LOPDGDD provides that one of the factors to consider when determining the presence of a high risk is the processing of health data, i.e., precisely the data processed in a clinical investigation.

Each data controller (that is, both the Site and the Sponsor in their respective areas of processing) must perform its own DPIA according to the processing done by each. Those DPIAs may be performed inhouse or by engaging an outside professional. The DPO for the Site and the Sponsor should participate in conducting the respective DPIA with advice and recommendations.

In the case of the Sponsor, the DPIA must include an analysis of the coding process that will be used, primarily taking into consideration the risks and consequences of unauthorised reversal of the coding.

In addition, where a specific assessment is performed for a given investigation, collaboration in the conduct of the DPIA may sought from the Monitor, the CRO, the Principal Investigator's team and from any other processor of data of the participants in the clinical investigation.

In those cases where during the course of a clinical investigation there is a substantial modification of the protocol that affects the processing of the participants' personal data, the previous DPIA must be reviewed and updated.

The Site and Sponsor must establish a methodology for performing their respective DPIA that covers all relevant aspects that are to be assessed and in particular:

- The necessity and proportionality of the proposed processing, specifying the data that are to be processed and the compliance with the principles set out in section 1; analysing the purpose and the lawfulness of the processing, the use of data processors, storage of the data processed and the procedure for managing the rights of participants.

- The risks that may be posed by the processing, including an analysis of the possible consequences for participants of access to or accidental loss or modification of their data, and of the effects such risks could have on their rights and freedoms.

- The technical, organisational and legal measures that must be implemented to manage the risks detected.

- The advice of the DPOs and determination of the need to consult the AEPD.

- The conclusions reached, charting the plan of action to be undertaken.

Compliance with this CC should be taken into account when performing the DPIA and assessing the consequences of the processing operations that will be carried out in the clinical research.

The DPIA methodology may be established using others that have been published and approved by supervisory authorities from time to time[1].

If the DPIA concludes that the processing activities to be carried out in the clinical research are likely to result in a high risk to the rights and freedoms of the participants that cannot be mitigated by adopting adequate measures, the Site and Sponsor shall consult the competent national data protection authority before initiating the clinical research in question.

For these purposes, the Site and Sponsor must provide the competent data protection authority with the information specified in Article 36 of the GDPR.

In any event, without prejudice to the implicit risk of re-identification, that risk should be managed with technical, organisational and other measures and a periodic reassessment conducted of the residual risk that exists in order to introduce parameters for improving the coding process used.

2.2 SECURITY MEASURES

The security measures that should be adopted by the Site and Sponsor will be determined having regard to the DPIA conducted as provided in section 2.1 above.

The Site and Sponsor must document in writing the measures adopted for each processing activity carried out in connection with the clinical research, including:

- A description of the security measure implemented, specifying its type and classification.

- Specification of the processing activity to which the security measure applies.

- The frequency with which each security measure will be reviewed and the party responsible for the review.

Both the Site and Sponsor must include in the Record of Processing Activities referred to by section 3.5 the basic information on the security measures adopted or the standard applied.

Also, contracts entered into with the data processors must included the processor's obligation to adopt comparable security measures to those the Site and Sponsor have set up in their systems.

Insofar as the Sponsor will only process previously coded of the participants, the Sponsor will have already adopted a preliminary security measure, i.e., the coding, so that the intensity of the remaining measures can be modulated when working with personal data that has already been protected as regards the identity of the patients.

In this connection, the Sponsor must adopt security measures primarily aimed at ensuring that there is no re-identification of the participants in the clinical research.

Those security measures will include, among others, the following:

- Measures to prevent any access by the Sponsor's personnel to the identifying information of the clinical research participants, including training activities that inform personnel of their obligations in the processing of coded information.

- Obtaining the Monitor's commitment not to provide the Sponsor with information on the participants that could allow their identification.

- Inclusion in the contract with the Trusted Third Party of the points set out in section 3.1.

- Performance of periodic internal audits to check that the coded information is being used properly in accordance with the guidance given by the Sponsor.

- Having a confidentiality undertaking signed by all employees who process the coded data.

- Obtaining the Site's warranty that it will not provide the Sponsor with any type of information that could imply re-identification of the participants.

2.3 DATA BREACHES

A data breach is any situation that compromises the integrity, confidentiality or availability of the personal data of clinical research participants.

In particular, any situation in which the Site and/or the Sponsor run into constraints on their access to the personal data of participants (e.g. significant interruption of the systems in which the personal data are stored) should be considered a data breach, as well as any loss, destruction

1 Valid guidance in this respect can be obtained from the AEPD's "*Guía práctica para las Evaluaciones de Impacto en la Protección de Datos*" (Practical Guide for Data Protection Impact Assessments), the "*Privacy Impact Assessment*" document published by the Commission Nationale de l'Informatique et des Libertés (CNIL) in France or "*The Standard Data Protection Model*" of Germany's federal personal data authority.

or removal of media containing the personal data (e.g. where an external storage device containing personal data is missing) or unauthorised access thereto (e.g. detection of access to personal data storage systems by a third party with insufficient credentials).

Both the Sponsor and the Site must take all necessary steps to avoid data breaches and, where such breaches occur, to respond swiftly and diligently. Toward that end, they shall draw up internal protocols with guidance on how to respond to the occurrence of a data breach.

In accordance with Article 33 of the GDPR, the AEPD must be notified without undue delay and, in all events, no later than 72 hours after having become aware of a data breach that can result in a risk to the rights and freedoms of the participants. The notification should include all information on the data breach set out in the reporting templates provided by the AEPD for these purposes.

If not all of the information can be provided within the time limit specified above, the Sponsor and/or the Site must notify the AEPD of the reason why and inform the AEPD that they will submit the prescribed information as soon as it is available.

In this connection, considering the type of data of participants processed in the clinical research, a data breach in that processing shall be deemed to affect the rights and freedoms of the participants if the breach entails loss of control over the data or loss of the confidentiality of the data protected under obligations of secrecy.

In addition, the clinical research participants must be notified of a data breach without undue delay and, if necessary, the cooperation of the AEPD shall be requested. The only exception to this obligation will be for the circumstances provided for in Article 34(3) of the GDPR.

The Site shall conduct the notification by contacting the participants using the information they gave for communication purposes in clinical research.

The language used in the notification to participants must be the same as used, in accordance with section 2.4.2, to inform them of all matters regarding the clinical research in which they are participating.

In the case of minors or incapacitated persons, the notification will be addressed to the persons who signed the informed consent to participate in the clinical research.

Other channels may also be used, such as posting the information on the data breach on the website of Site and/or the Sponsor or in media with nationwide dissemination in order to maximise the likelihood of the participants becoming aware of the data breach.

For data breaches in the Sponsor's systems, the Sponsor will notify the AEPD, expressly noting in the prescribed template that the data affected by the breach were coded.

The severity of the breach may be determined by reference to the relevant documents issued by different authorities, for example, among others, "*Recommendations for a methodology of the assessment of severity of personal data breaches*" published by the European Union Agency for Network and Information Security (ENISA)" or la "*Guía para la gestión y notificación de brechas de seguridad*" (Guidelines on Personal Data Breach Notification) published by the AEPD.

In any event, the following factors are to be taken into account to determine the severity of the data breach:

- Consequences for the systems compromised by the data breach;
- Nature of the data involved in the breach;
- Possibility of identifying the participants from the data that were breached;
- Consequences of the data breach for the participants;
- Number of participants affected by the data breach.

Without prejudice to the severity of the data breach, all relevant information must be recorded, including the measures implemented in relation to the breach.

Notification to the AEPD and to the clinical research participants shall be the responsibility of the respective data controller for the affected data processing. In particular, if the data breach occurs in a processor's systems, the notification shall be made to the data controller who engaged that processor under Article 28 of the GDPR[2].

Without prejudice to the above, where the data breach is suffered by the Monitor, the latter will provide the Sponsor with all of the information needed for notification of the breach, but without disclosing data that allows the Sponsor directly or indirectly to identify the participants in the clinical research. The notification will be done by the Sponsor solely with the information provided by the Monitor and in no event with access to information that could entail a risk of re-identification of the participants. If the data breach must be notified to the data subjects, the notification will be done directly by the Monitor in collaboration with the Site and/or Principal Investigator, acting on behalf of the Sponsor, so

2 By way of example, where a data breach occurs as a consequence of actions of the Principal Investigator's team, the Site will be responsible for carrying out the notifications; nevertheless, in cases that involve a courier subcontracted by the Sponsor, the latter shall be responsible for the notifications.

that the Sponsor has no access to the identifying personal information of the participants in the clinical research. The contract between the Sponsor and Monitor shall expressly specify these conditions.

The contract between the Site and Sponsor for performing the clinical research must include the rules for determining who is responsible for (i) carrying out the prescribed notifications of data breaches and for (ii) coordinating and directing the actions in relation to the breaches.

2.4 RECRUITMENT OF PARTICIPANTS

2.4.1 ENROLMENT OF PARTICIPANTS

Participants in clinical investigations are selected by the Principal Investigator or, as applicable, by the members of the investigator's team. The enrolment criteria that the Principal Investigator must follow are determined by the clinical trial Protocol, which shall have been previously approved by the competent authorities.

To enrol participants, the Principal Investigator must access the patient's records of the candidates for participation in the clinical research to the extent that the Principal Investigator has to assess their suitability according to the terms of the Protocol. That access is done by the Principal Investigator or by members of the team and is thus tied to the provision of medical care or treatment, without prejudice to the subsequent processing of the patients' data in the clinical trial or investigation. This will also apply where the participant' data are obtained from previous clinical investigations, in accordance with the provisions of section 3.9.

2.4.2 INFORMATION

Once the participants in the clinical research have been selected the Principal Investigator must provide those participants with full disclosure of the possible implications of their participation. In this regard, the Principal Investigator must inform the participants both of the possible clinical consequence of their participation and of aspects relating to the processing of their personal data.

Thus, in addition to the information that must be disclosed to the participant in accordance with the provisions of the RDEC, the participant must be given an additional separate document that expressly includes clear, precise and unequivocal information on the processing of his or her personal data.

In this respect, though Article 11 of the LOPDGDD envisages the possibility of establishing a multi-layered disclosure procedure, given the special characteristics of the processing carried out as a result of the trial and the fact that the data subjects must receive clear and detailed information on that processing and give their informed consent to participate in the clinical research, the fundamental right of protection of personal data will be more intensely guaranteed by including all of the information required by the GDPR in that document.

In particular, the following information must be given to the participants:

- The identity and contact information of the Sponsor and of the Site and/or Principal Investigator, as well as the contact information of their DPOs. To avoid re-identification of participants by the Sponsor, mention must be made of the fact that contacting the Sponsor will entail a risk of re-identification;
- The application of the process that will be used to code their personal data;
- The purposes of the processing operations on the personal data, which must be specific, explicit and legitimate. In particular, if the data will be subsequently used for research purposes, that circumstance must be disclosed;
- The legal basis for the processing, which will be the fulfilment of a legal obligation, in accordance with Article 6(1)(c) of the GDPR, with the processing likewise authorised by articles 9(2)(i) and (j) of the GDPR;
- The recipients or categories of recipients of the personal data. This must include:
  - Third parties who access the data in connection with the provision of services, for example, the Monitor or the CRO. In these cases the entity with access to the data as a result of its provision of a service to the controller need not be expressly identified and a generic reference to the services provided by the entity may be included instead.
  - The disclosures of the data, including to the AEMPS and the CEIm, that will be made, specifying in each case the justification for the personal data disclosure and its purpose;
  - Insurers with whom insurance has been contracted to whom the data will be disclosed in the event of an adverse reaction, in order to take the necessary steps in accordance with the insurance contract.

- The mandatory or optional nature of the replies and the consequences of declining to provide the data;

- The possibility of asking the Site and/or the Principal Investigator for access, rectification, erasure of their personal data, as well as restriction of their processing, all in accordance with the terms of section 3.7 below and taking into account the limitations provided there;

- The right to bring a claim before the CCGB or, as applicable, before the AEPD;

- If applicable, the intention of the Site and/or the Sponsor to transfer the personal data to a third country or international organisation, specifying whether said country is considered to have a comparable level of protection or, if applicable, the safeguards adopted;

- The period during which the personal data will be retained or, if that is not possible, the criteria for determining said time period; and

- The Sponsor's adherence to this CC, specifying where the clinical research participants can consult the CC on the Sponsor and AEPD's websites.

Annex 1 sets out the minimum personal data protection content that must be included in the informed consent section for clinical research with coded data.

3. Clinical research

3.1 CODING PROCEDURE

The identifying information of the participants is normally not significant for achieving the objectives of the clinical research. Accordingly, the identifying particulars of clinical research participants is coded so that the Sponsor of the clinical research does not have access to said data.

The data coding may be done directly by the Principal Investigator or through a Trusted Third Party contracted by the Sponsor. In either case, the procedure ensures that the Sponsor cannot identify the participants other than in exceptional situations.

In particular, it bears emphasis that if a Trusted Third Party is engaged to do the coding, said party must not be involved in the clinical research and shall confine its role to coding the identifying data contained in the information sent to it by the Site before it is received by the Sponsor.

The coding procedure used must in all events ensure elimination of the patient identification chain so that the Sponsor is not able directly or indirectly to identify the patients. The procedure must allow, however, that all information referring to the same participant be stored under the same code in order to afford a real vision of the evolution of the clinical trial in each patent, but with the Sponsor not being able to make a direct identification in any case.

Sound robust techniques should be used for the coding. Valuable references in this respect are the guidelines and approaches to coding contained in the Good Clinical Practice Guidelines for clinical trials or the document "*Introduction to the hash function as a personal data pseudonymisation technique*" jointly issued by the AEPD and the EDPS[3].

Those techniques render direct identification by the Sponsor impossible as from the time a code is assigned to the participant and effectively block Sponsor access to the participant's identifying information.

Nevertheless, in order to avoid the possibility of indirect identification as a result of using information from one or more sources that allows the participant's re-identification, whether separately or in combination with other factors[4], the coding procedure must include mechanisms aimed at ensuring that indirect identification cannot take place.

With respect to the coding protocol, it must first be considered that, as already noted in section 2.4.1, responsibility for gathering, recording and notifying the participants' data correctly and for ensuring their veracity rests with the Principal Investigator. This means that it is the Principal Investigator who will enter that data in the CRF.

As stipulated in the Good Clinical Practice Guidelines, the CRF is the document used in clinical research to convey to the Sponsor all information on the participants in a clinical investigation that is needed according to the terms of the Protocol.

Before being passed on to the Sponsor, the identifying information contained in CRFs must therefore be coded, by applying the mechanisms and techniques deemed suitable according to the state of the art at the time the coding is carried out, in order to fulfil the ultimate purpose of the coding procedure, i.e. that the Sponsor is not able to re-identify the participants through other sources.

Information on the procedure employed and data needed for exceptional re-identification of participants shall only be kept by the Principal Investigator or the Trusted Third Party who does the coding, adopting technical and organisational measures to block access by the Sponsor to that information.

3 Available at https://edps.europa.eu/sites/default/files/publication/19-10-30_aepd-edps_paper_hash_final_en.pdf.

4 For example, the combination of various data such as blood type, sex, illness suffered and site where the clinical investigation is conducted could allow indirect identification.

In this connection, the contract between the Sponsor and Site or, as applicable, the Trusted Third Party, must include provisions for at least the following:

- Obligation of the Principal Investigator or Trusted Third Party to conduct the coding process so that the Sponsor cannot re-identify the participants, not even indirectly, without the intervention of the Principal Investigator or Trusted Third Party.

- Express undertaking by the Sponsor not to ask the Principal Investigator or Trusted Third Party for information on the participants that allows their re-identification.

- Compliance by the Principal Investigator or Trusted Third Party in the coding process with the GDPR, the LOPDGDD and the guidelines on anonymisation publicly issued by data protection authorities[5].

- Covenant by the Principal Investigator or Trusted Third Party to not provide the Sponsor with indications on the coding operations performed on the participants' data.

- Warranty by the Principal Investigator or Trusted Third Party that the post-coding operations or processing do not entail alteration of the real data.

Annex 2 sets out the minimum content that must be included in the contract between the Sponsor and Trusted Third Party where the latter is engaged by the former.

3.2 LEGAL POSITION OF PARTICIPANTS

3.2.1 RULES ON THE RESPECTIVE LIABILITY OF THE SITE (AND/OR, AS APPLICABLE, THE PRINCIPAL INVESTIGATOR) AND SPONSOR IN THE PROCESSING

As already noted, in clinical trials the Sponsor will only receive participants' data in coded form, so that its liability will therefore be modulated in comparison with the liability of the Site (and/or, if applicable, the Principal Investigator) that processes the identifying information of the participants.

Without prejudice to the above, as provided in the RDEC, both the Sponsor and the Site (and/or, if applicable, the Principal Investigator) have their respective liability in relation to the management of the clinical investigation.

Thus, over the course of a clinical investigation there will be constant communication between the Principal Investigator and the Sponsor in order for the clinical investigation to be managed properly.

Considering the above, we find ourselves with different parties sharing liability for the purposes of personal data protection rules in relation to the processing of personal data of participants. The Sponsor is the party responsible for establishing the criteria for enrolling participants in the clinical investigation and, the Site and/or, as applicable, the Principal Investigator are responsible for material fulfilment of most of the obligations laid down in the Protocol, and must complete the CRFs with all of the clinical information generated over the course of the investigation.

Insofar as the Sponsor determines the criteria regarding the participants whose coded data must be included in the CRF for the clinical investigation, it will be considered the controller of the processing operations on said data, and the Site (and/or, as applicable, the Principal Investigator) will be the controller of the processing of the participants data for the purpose of providing the participants with the appropriate medical care in the clinical investigation.

Without prejudice to the above, the respective liability of the Site (and/or, as applicable, the Principal Investigator) and the Sponsor will differ, taking into consideration that the latter does not have access to the identifying information of the participants, but only accesses data that have been previously coded.

In this regard, although the Sponsor will be considered controller of the processing given that it determines the participant selection criteria, establishes the guidelines for preparing the reports and, in short, oversees all of the clinical research activities, its liability in the processing of personal data will be modulated to the extent that it only processes coded data of the participants in the clinical investigation.

As a consequence of the above, the contract between the Sponsor and the Site (and/or, as applicable, the Principal Investigator) must clearly specify the liability assumed by each party in relation to the processing of personal data of participants, duly reflecting the functions undertaken by each and how their relations with the participants are organised.

In particular, that contract will provide that the Site (through the Principal Investigator) or, as applicable, the Principal Investigator, is responsible for complying with the disclosure duty laid down in Article 13 of the GDPR, ensuring that all participants are provided with the specific document that includes the information on the processing of personal data.

It will also set out the prohibition on the Sponsor participating in the collection of personal data of participants and on accessing archives and documents held by the Site and/or the Principal Investigator that contain identifying information of the participants in the clinical investigation.

5 At present the following documents have been published: "*Orientaciones y garantías en los procedimientos de anonimización de datos personales*" (Guidance and Guarantees in the Process of Personal Data Anonymisation) from the AEPD, "*Anonymisation: managing data protection risk code of practice*" from the Information Commissioner's Office and Opinion 05/2014 on Anonymisation Techniques of the Article 29 Data Protection Working Party.

In addition, to ensure that the Site (and/or, as applicable, the Principal Investigator) does not provide the Sponsor with any type of information that allows the Sponsor directly or indirectly to identify the clinical research participants, the contract shall expressly stipulate that the Site and/or, as applicable, the Principal Investigator has the obligation to send the Sponsor the CRFs without identifying information of the participants, such that all data sent are associated with the corresponding code.

And the contract shall specify that the contact point for participants is the Principal Investigator and include the pertinent particulars (e-mail address, telephone, etc.) that allow the participants to contact the Principal Investigator for any queries they may have regarding the processing of their personal data in the clinical research activities.

The contract also needs to set out the rules on subcontracting, expressly including which third parties must be contracted by the Sponsor, such as, for example, the CRO or the Monitor, and which will be contracted by the Site and/or, as applicable, the Principal Investigator, such as, among others, the members of the Principal Investigator's team if they do not belong to the Principal Investigator's organisation.

In summary, the Site (and/or, as applicable, the Principal Investigator), as the controller of the processing who accesses the identifying information of the clinical research participants and who processes data in the research activities, is the party who assumes the obligations related to that processing.

Annex 3 sets out the minimum content of the personal data protection clause that must be included in the contract between the Site and the Sponsor (and, as applicable, the Principal Investigator) to carry out a clinical investigation[6].

In order to reinforce compliance with the transparency principle regulated in the GDPR, the essential terms on personal data processing of the contract between the Site (and/or, as applicable, the Principal Investigator) and the Sponsor should be made available through the Data Protection Officer to participants who wish to see those terms. The procedure for requesting access to those essential terms may be included in the document on protection of personal data that is provided to the data subject together with the informational sheet at the time the participant's informed consent to participate in the clinical investigation is obtained on the terms required by the applicable rules.

Sponsors not established in the European Union must designate in writing a representative in accordance with Article 27 of the GDPR and said representative will be responsible for managing data subject requests to exercise their rights.

Lastly, all references to the Site where the clinical research is conducted will be understood to refer to all sites in which multisite trials are conducted. References to the Sponsor include all sponsors where there are more than one.

3.2.2 PROCESSORS

Clinical research involves access to the personal data of the participants by third parties acting for and on behalf of the Sponsor or of the Site or Principal Investigator, who act in their respective capacity as controllers of the data processing.

In these cases, the controller on whose behalf the data processor is acting must enter into a contract or agreement with those third parties on the terms of Article 28 of the GDPR.

In particular, the contract must include the security, technical and organisational measures that have to be implemented by the processor of the personal data of participants. Those measures must at least match those implemented by the controller.

Also, given that the controller has the obligation to report to the AEPD within a maximum of 72 hours any breach that could occur of the participants' personal data, the contract shall include the processor's obligation to notify the controller on whose behalf it is acting, within a maximum of 36 hours, of any security incident that affects the participants' data. This will afford the controller a reasonable time period for carrying out all necessary actions for complying with the aforesaid time limit for the report to the AEPD.

In addition to the provisions contained in Article 28 of the GDPR, the controller on whose behalf the data processor is acting will include in the contract or agreement with the processors: (i) representations regarding compliance with the of personal data protection regulations;

(ii) the obligation to submit to periodic audits by the controller or by another party designated by the controller; (iii) the obligation to collaborate with the controller if the controller decides to perform a DPIA on the terms of section 2.1; and (iv) the rules on liability in the event the processor breaches the contract.

It will furthermore be considered good practice for the processor to be required to contract insurance covering its possible liability in the event of data breaches and to maintain the insurance throughout the entire life of the contract.

There follows a description of the main processors who will participating in processing operations on the data in clinical research activities:

6 The content of this Annex is understood without prejudice to the criteria that may be established by supervisory authorities other than the Spanish Data Protection Agency (e.g. in multisite trials in different countries).

3.2.2.1 Monitor

The Monitor is selected by the Sponsor and must in no event be part of the investigator team. The Monitor's functions are to oversee that the clinical research is carried on properly in accordance with the terms of the Protocol and act as link between the Sponsor and the Principal Investigator.

In particular, the Monitor has the following obligations:

- Perform its functions according to the standard operating procedures established by the Sponsor;
- Meet with the Principal Investigator to ascertain that it is complying with the terms of the Protocol;
- Corroborate that the clinical research data are recorded in the CRF correctly and completely and that all patients have signed the informed consent form before the clinical investigation is started;
- Verify that the Principal Investigator and all members of his or her team who take part in the clinical investigation have all necessary information on the investigation and are qualified to perform it;
- Act as intermediary between the Sponsor and Principal Investigator, mainly as regards aspects relating to supervision of security in the clinical research;
- Check that the storage, distribution, return and documentation of the medicines being investigated are secure and appropriate;
- Issue reports on its visits for the Sponsor.

In performing its functions, the Monitor on behalf of the Sponsor accesses the personal data of the participants in the investigation and is thus considered a processor for the Sponsor. The Monitor is nevertheless obliged not to provide identifying information of the participants in the clinical research to the Sponsor. The security measures the Monitor must implement should be similar to those in place at the Site given that the Sponsor will access the same personal data as the Site.

If the Monitor performs its functions remotely, accessing the information by that means, it must comply with the conditions and measures established by the Site or the Principal Investigator for such purpose, even where the Monitor is not acting as processor on their behalf.

Annex 4 sets out the minimum content of the data protection clause to be included in the contract with the Monitor.

3.2.2.2 CRO

The Sponsor may delegate responsibilities to a CRO by subscribing a service contract whereunder the CRO acts for and on behalf of the Sponsor in relation to those services.

The CRO will be considered data processor for the Sponsor in the following events:

- Where the CRO carries out monitoring tasks. Nevertheless, in accordance with what is provided in the preceding section, the data protection clause included in the contract between the Sponsor and CRO must include a provision prohibiting the CRO from providing the Sponsor with the identifying information of the participants.
- Where the Sponsor subcontracts other tasks to the CRO that involve the latter's access to coded data of the participants contained in the CRFs. In this case, the contract must specify that the data which it accesses are coded.

Attached as Annex 5 for these purposes is the minimum content of the data protection clause to be included in the contract with the CRO where the CRO provides services other than monitoring and accesses coded data of the participants.

3.2.2.3 Auditor

In general terms, the Auditor is responsible for corroborating that all actions carried out in a clinical investigation are done in accordance with the applicable laws and regulations, the standard operating procedures established by the Sponsor, the Protocol and the Good Clinical Practice Guidelines.

To conduct those audits, the Auditor accesses identifying information of the participants in the clinical research insofar as, among other tasks, it must verify that said information has been properly recorded and analysed.

The role of the Auditor therefore includes acting as processor for the Sponsor and the audit service contract must include the clause set out in Annex 4.

3.2.2.4 Principal Investigator's Team

The customary practice is for the Principal Investigator's team to be personnel of the Site where the clinical research is conducted. In this case, the provisions of the section on the Site will apply to the Principal Investigator's team, whose members should be simply considered as users who belong to the Centre.

Without prejudice to the above, where a member of the Principal Investigator's team is not an employee of the Site, the member will be considered as a processor for the Site, and the contract with the Site must include a data protection clause with the provisions laid down in Article 28 of the GDPR.

3.2.2.5 Trusted Third Party

Where the coding process involves a Trusted Third Party, the latter will be a processor for the Sponsor and its contract must contain the clause set out in Annex 2.

The contract shall in all events include safeguards to avoid access to the data or to the coding procedure by the Sponsor, as well as the obligation to adopt measures to allow access traceability in the event of accidental access to the data.

3.2.2.6 DPO

If the Sponsor has an external DPO, the actions the latter must carry out in a clinical investigation will be in the capacity of processor. Without prejudice to the above, as in the case of the CRO it should be noted that the data of the clinical research participants to which the DPO may have access are coded.

3.2.2.7 Other Service Providers

On occasion the Sponsor outsources certain accessory clinical research services such as, for example, customer care services, collection and transport of samples.

The Sponsor may likewise contract a third party to locate patients who withdraw from the clinical investigation before its conclusion if they need to be found in order to give them information that may be of importance to their health and relates to their participation in the clinical investigation.

In all of these cases, the contracts with said third parties must include the data protection clause contained in Annex 6, which shall expressly specify that those service providers will only have access to data that are indispensable for rendering the contracted services[7].

3.2.3 THIRD PARTIES

Clinical research activities also involve disclosures of personal data to the CEIm and to the AEMPS (or other competent health authorities). Those disclosures are made on the basis of the applicable legal and regulatory provisions that stipulate, on the one hand, that the CEIm must monitor the clinical study from its start until the final report is received, and on the other, that the AEMPS may conduct inspections on the Site to check that the clinical research is being performed in accordance with the applicable laws and the Good Clinical Practice Guidelines.

Both the disclosures to the CEIm and to the AEMPS are made under Article 6(1)(c) of the GDPR, that is, in compliance with a legal obligation that applies to the Sponsor.

In addition, insofar as the Sponsor only processes coded data of the participants, it may disclose said data to third parties, including enterprises in its Group, without having to comply with any further requirement.

The content of this section is summarised in the accompanying chart that identifies the different parties that take part in a clinical investigation with coded data and the role played by each in the terms of personal data protection regulations:

Position	Site (and /or, as applicable, the Principal Investigator	Sponsor	CRO perfoming monitoring tasks	Monitor	Auditor	Principal Investigator's team[8]	Trusted Third Party	DPO	Other Service Providers
CONTROLLERS	X	X							
PROCESSOR FOR THE SPONSOR			X	X	X		X	X	X
PROCESSOR FOR THE SITE						X			

7 For example, providers of customer care services should only have access to the given name, surnames and telephone number.

8 If not an employee or personnel of the Site.

3.3 LEGAL BASIS FOR THE PROCESSING

The mandatory disclosures that must be made to participants in clinical research include information on the legal basis for the processing.

To the extent that a clinical investigation involves processing of health data, two requirements must be met to determine the legal basis for the processing:

- The legal basis must be one of those set out in Article 6(1) of the GDPR.
- The processing of the health data must be captured by one of the exceptions to the general processing of such data, namely those provided for in Article 9(2) of the GDPR.

Therefore, the legal basis for processing the data of clinical research participants is the existence of a legal obligation (Article 6(1)(c) of the GDPR) in connection with what is provided in Article 9(2)(i) and (j). Indeed, the processing, on the one hand, has as its purpose compliance with the legal obligations to ensure a high level of quality and security on the medicinal product and, on the other, it is carried out for scientific research purposes on the basis of Spanish and European Union legal rules regarding guarantees and rational use of medicinal products and medical devices that impose the legal obligation to conduct investigations before marketing a medicine, as well as to conduct studies after the medicine has been authorised.

The processing is thus carried out to comply with legal obligations imposed by the laws on medicinal products and medical devices, without requiring that data subjects give their consent to the processing of their personal data once they have agreed to enrol in an investigation.

Thus, although the laws and regulations on clinical research do require that the informed consent of the participants be obtained to take part in a specific clinical investigation, their consent need not be obtained for the processing of their data, given that the processing is based on compliance with the legal obligations of the Sponsor.

In particular, the specific provisions of the laws on clinical research that imply the Sponsor must process personal data of the participants include, among others, the obligations to:

- Generate reliable and robust data (Articles 3(b) of the REC and 3(1)(a) of the RDEC).
- Report the results of the investigation once it has concluded (Articles 37(4) and 37(8) of the REC, and Article 39(3)(l) del RDEC).
- Issue safety notices and reports (Articles 41-43 of the REC and 50-53 of the RDEC).
- Allow the authorities to conduct inspections and provide them with all information they request (Articles 78 of the REC and 44 of the RDEC).
- Maintain the master file of the clinical research as provided in section 3.6 (Articles 58 of the REC and 44 of the RDEC).

Consequently, a participant who consents to form part of a clinical investigation does not need to give his or her consent, once enrolled in the investigation, to the processing of his or her personal data as part of that investigation for the purposes and in accordance with the terms of the laws on clinical research.

So specific consent is not needed for the processing of the participant's data; the participant need only be informed of the processing on the terms del Article 13 of the GDPR through the document prepared for that purpose.

For this reason, should a participant decide to withdraw from the clinical investigation, the Sponsor and the Site may continue processing the data obtained from that participant before the withdrawal for the purposes and in accordance with the terms of the laws on clinical research, given that the patient's consent is not required and subsequent revocation is not possible.

The data subject's consent will be necessary, however, if it is proposed to process the data of participants in a clinical investigation for purposes not related to that investigation, unless that processing also finds some specific legal basis other than the consent.

Examples where there is a legal basis not grounded in the consent are cases where it is proposed to use a participant’s data in future investigations on the terms specified in section 3.9.

Also of note within those cases are where the Sponsor needs to locate a participant who has withdrawn from the clinical investigation to verify some question related to the investigation that could have bearing on the participant's health. In those instances, the need to locate the participant would be based on Articles 6(1)(d) and 9(2)(c) of the GDPR insofar as the processing is carried out to protect the vital interests of the data subject.

3.4 TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

It should first of all be borne in mind that this section applies both to when a third party accesses data as a result of providing a service to a controller and when a controller discloses data to a third party.

As a general rule, personal data cannot be transferred to countries that do not provide an adequate level of protection unless the requirements of Chapter V of the GDPR are fulfilled.

Without prejudice to the above, it should be kept in mind that the Sponsor only processes coded data of the participants. So if the Sponsor demonstrates that the information in its control has been submitted to techniques that render impossible the re-identification of the data subjects by the recipient of the information located in a third country, such that the information that may be transferred to other parties will in no instance permit the recipients of the information to know directly or indirectly the identity of the participants in the research because they have neither direct nor indirect access to the identifying information of the patients obtained prior to the coding[9], that information will be considered to have been anonymised.

Accordingly, given that the information send to the recipient is anonymised data and can therefore not be considered personal data, the rules governing international transfers of data to third countries or international organisations will not apply and the Sponsor may give access to and/or disclose the anonymised data to third parties irrespective of where they are located.

The anonymisation of the personal data must be done using solid and robust techniques. Valid reference in this respect are the AEPD's "*Orientaciones y garantías en los procedimientos de anonimización de datos personales*" (Guidance and Guarantees in the Process of Personal Data Anonymisation)[10] and "*Opinion 05/2014 on Anonymisation Techniques*"of the Article 29 Data Protection Working Party[11].

Where it is not possible to demonstrate that the anonymisation procedure has been performed or that the data are anonymised, if the country where the recipient of the data is located cannot be considered to have a comparable level of protection to that provided in the GDPR, the Sponsor must adopt one of the safeguards laid down in Article 46 of the GDPR. In this case the Sponsor must also carry out a prior analysis of the regulatory framework of the destination country and, if necessary, adopt measures supplementing those set out in that article, in accordance with the terms of "*Recommendations 1/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*" of the EDPB[12].

3.5 RECORD OF PROCESSING ACTIVITIES

Both the Site (and/or, as applicable, the Principal Investigator) and the Sponsor, in their capacity as controllers, must maintain a physical or electronic record of processing activities that contains all of the information provided for in Article 30 of the GDPR. The record must be maintained in a format that allows easy access and swift modification where changes need to be made.

To the extent that processing operations carried out in clinical research are similar, that is, the data processed and the purposes of the processing are similar, a single record may be kept that covers the shared basic purpose of managing clinical investigations.

The Sponsor must note in the record of processing activities that it only processes coded data of the clinical research participants and likewise include that circumstance among the security measures applied to the data.

Annex 7 contains the form for the Record of Processing Activities that must be completed in each case with the information on each specific processing.

3.6 STORAGE

As a general rule, clinical research data (that is, the content of the master file) must be stored by the Sponsor and by the Site (and/or, as applicable, the Principal Investigator) for a minimum period of 25 years after the end of the clinical investigation, and that period will be lengthened according to the regulations that apply in each case.

Without prejudice to the above, there are certain situations in which that period may be extended, for example:

- Where an applicable rule stipulates a longer period, as is the case, among others, in the regulations on advanced therapy medicinal products.

- A longer storage period is agreed between the Sponsor and the Site (and/or, as applicable, the Principal Investigator).

9 AIn this case there should be taken into account the existence of what the AEPD document "Orientaciones y garantías en los procedimientos de anonimización de datos personales" (Guidance and Guarantees in the Process of Personal Data Anonymisation) terms "anonymisation by layers", such that the information received by the data importer must be considered anonymised data in which re-identification of the investigation data subjects is impossible.

10 Available in Spanish at https://www.aepd.es/sites/default/files/2019-12/guia-orientaciones-procedimientos-anonimizacion.pdf

11 Available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

12 Available at https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf

- The medicine must comply with Annex I of Royal Decree 1345/2007 of 11 October 2007.

Furthermore, the storage periods for the master file documents retained by the Site (and/or, as applicable, the Principal Investigator) may differ based on the respective responsibilities undertaken by each in the contract between them.

The storage medium must, as a general rule, be electronic and ensure the authenticity of the documents and that they are not modified, and a record shall be included of any modification made, specifying the original datum and the modified datum and identifying the person who has made the modification.

For these purposes, the Sponsor shall designate the persons in its organisation who are responsible for custody of the stored documents and limit access to those persons only.

The content of the master file shall be preferably stored by protocols and in such way as allows it to be made available to the competent authorities who so request in compliance with the applicable laws and with the Good Clinical Practice Guidelines.

In any event, the storage period for clinical research data and, where applicable, the criteria used to determine said period must be disclosed in the informational document provided to the participants.

It should furthermore be taken into account that, where certain data are to be reused for purposes other than managing the clinical investigation in accordance with the provisions of section 3.9, the storage periods that apply for each purpose must be differentiated.

Lastly, retention of the Patient's records of the patients by the Site (and/or, as applicable, the Principal Investigator) will be governed by the provisions of the applicable laws.

3.7 EXERCISE OF RIGHTS

Since the Sponsor has no material access to the identifying information of the participants in the clinical research, it will not be able to carry out the requests by participants to exercise their rights.

Without prejudice to the above, even though it cannot handle those requests, the Sponsor does have the obligation to reply to the participants, inform them that their data are not contained in its records and instruct them to address their requests to the Principal Investigator of the clinical investigation using the contact information contained in the specific information document they were given on the processing of their personal data.

Annex 8 contains the form for responding to participants who send their requests to exercise their rights to the Sponsor.

3.8 ADVERSE EVENTS

3.8.1 CLINICAL TRIALS

The Principal Investigator must record and document all Adverse Events that arise in a clinical investigation and report them to the Sponsor with the timing stipulated in the Protocol.

The Sponsor shall likewise keep a record of all Adverse Events notified to it by the Principal Investigator that will be provided to the AEMPS upon the latter's request.

The communications regarding Adverse Events and Serious Adverse Events between the Principal Investigator and the Sponsor that are referred to in section 3.8 must be stripped of identifying information of the participant and only include the codes assigned to the participant.

Where information on participants has to be provided to the insurer with whom the Sponsor has contracted the prescribed insurance covering possible harm arising from the clinical investigation, that disclosure will be made by the Principal Investigator. Upon receiving that information, the insurer will be considered controller of said data. For this purpose, the Trusted Third Party will be asked to decode the data solely for purposes of their disclosure to the insurer.

All disclosures of personal data of clinical research participants envisaged in this section are made under Article 6(1)(c) of the GDPR, that is, for compliance with a legal obligation to the extent that the applicable health regulations lay down the obligation of the Principal Investigator and of the Sponsor to make those disclosures.

3.8.2 OBSERVATIONAL STUDIES

In prospective Observational Studies, the Sponsor will be obliged to report the Adverse Event to the contact point designated by the competent pharmacovigilance body of the Autonomous Community where the activity of the Principal Investigator is carried on within a maximum of 15 days after learning of the suspicion of a Serious Adverse Event or 90 days in the case of a minor Adverse Event.

Toward this end, the Principal Investigator will be obliged to notify the Sponsor of any Adverse Event in accordance with the provisions of Protocol for the clinical research in question.

In Observational Studies where the Sponsor is not the Marketing Authorisation Holder, the Sponsor will not be obliged to report the case to the authorities. It must, however, send the information on the Adverse Event to the holder of the marketing authorisation for the suspected medicinal product if it is known, in all cases specifying that the case involves a post-authorisation observational study and the code of the study in Spain. In these cases it will be the Marketing Authorisation Holder who reports the case to the authorities via the ordinary channels and indicating the code of the study in Spain in the notification.

These notifications are done on the basis of Article 6(1)(c) of the GDPR insofar as it is an obligation that rests with the Sponsor who conducts a study of these characteristics.

As studies of this type do not require that the Sponsor contract insurance, Sponsors will, generally speaking, not have to disclose personal data to an insurer. Nevertheless, if an insurance contract is subscribed, there may be disclosure of the data of the participants who suffered the Adverse Event under Article 6(1)(b) of the GDPR.

3.9 COMPATIBLE PURPOSES, REUSE AND SECONDARY USES

As indicated in section 3.3, where there is an intention to use a participant's data in future research, that future processing must be grounded in one of the lawful basis laid down in personal data protection laws and regulations.

In this regard, where the intended reuse involves coded data only, it may be carried out without having to obtain the consent of the participants, provided the legal and regulatory requirements are met. In particular, the investigator team in the successive investigations shall in no event be able to access the information of the team that carried out the initial coding; it will have to sign an undertaking not to carry on any activity that could lead to re-identification and specific security measures will have to be adopted to such effect.

This will allow the coded personal data to be used in future research projects without requiring the consent of the participants, provided the following requirements are met:

- The Principal Investigator and the members of his or her team cannot access the identifying information of the participants. For these purposes, the coding must be done by a third party outside the investigator team who will retain the necessary information for re-identifying the participants.

- All members of the investigator team must sign a confidentiality undertaking and accept the obligation not to carry on any activity aimed at re-identifying the participants.

  Attached as Annex 9 for these purposes is the minimum content to be included in the document signed by the members of the investigator team who participate in the research.

- The Site must implement all necessary security measures to prevent re-identification of participants and access by unauthorised third parties.

If during the course of the clinical research there is perceived a real and specific risk to the safety or health of an individual or group of individuals, a serious threat to their rights or the need to identify a data subject to ensure he or she is given proper medical care, the patient will be re-identified using the data at source.

The re-identification referred to in the preceding paragraph must only be done on an exceptional basis after carrying out an analysis to ascertain that the objective pursued cannot be achieved without reversing the coding.

In addition, where consent is to be obtained, it should be taken into account that the GDPR defines consent as any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Consent can therefore not be obtained in the negative, for example, by a participant not ticking a box indicating that he or she does not consent to the processing of his or her data; instead, a box must be included for informed consent that is to be ticked by those participants who expressly accept such processing.

Without prejudice to the above, as stipulated in the GDPR, in clinical research activities it is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of the data collection. Data of participants who have given their consent for a research project may thus be used for purposes or other research areas related to the scientific area of the initial study.

Consent may therefore be sought from participants in relation to a broad area of investigation, e.g., oncological research or for even broader areas. And the consent previously given by the data subject may likewise be interpreted in that broader sense.

In these cases, the Site must provide participants with the information contained in section 2.4.2 on the new clinical research, sending them an e-mail with that information or, where that is not possible, a letter sent by a means that allows acknowledgement of receipt (e.g. certified post).

That information must also be posted on the website of the Site where the new clinical research is to be conducted and on the Sponsor's website.

Lastly, it bears emphasis that in these situations the principles of personal data protection regulations must respected in accordance with section 1 and authorisation from the CEIm must be requested.

3.10 OTHER DATA SOURCES

Real word evidence is obtained from the analysis and/or synthesis of real life data. There is a wide array of sources of real world data, although the term is often used to refer to data that are already available to the extent they have been collected routinely for other purposes (e.g., electronic patient's records, records of patients/illnesses, hospital and administrative records, etc.). This evidence is pivotal for developing innovative products that meet uncovered medical needs and to support the safe and effective use of medicines once they are available in the market.

Nowadays, real world evidence provides important information throughout a medicine's life cycle, from studying the populations to be included in a clinical trial, to generating evidence that can be taken into account for regulatory purposes, a point that has been underscored in recent laws, regulations and initiatives of leading medicine evaluation agencies.

The Sponsor must make sure that the information sources selected in its studies have mechanisms to guarantee the quality of the information so that it is reliable, valid and adequate for responding to the specific questions that must be resolved in the investigation in question.

In addition, real world studies must be designed and carried out in accordance with good practice standards and recommendations in pharmacoepidemiology and pharmacovigilance and adhering to the local regulations that apply to observational studies.

Depending on the type of observational study that generates the real world evidence, processing of individual personal data by the Sponsor or a third party may or may not be necessary. Where necessary, as indicated above, the personal data processing will require consent.

Annex 1:
Minimum content of the specific document disclosing information on the processing of personal data in research in which the principal investigator is employed by the site

Data Controller

TBoth the Site where the clinical research is conduct and the Sponsor are considered controllers of the processing of your personal data and each is responsible for fulfilling their respective legal obligations on personal data protection matters.

The Site where you go to participate in the clinical research processes the data obtained in that investigation, which may include data on your medical history, for the purposes of carrying out that research.

The Sponsor, in turn, will also be considered controller in respect of the data generated in the clinical research. The Sponsor, however, will only process coded data as provided in the relevant section of the CC and will therefore not know your identity.

Lawfulness of the Personal Data Processing

The legal basis for processing your personal data is compliance with the legal obligations laid down in the regulatory provisions on medicinal products and medical devices in relation to (i) the public interest in the pursuit of scientific research; and (ii) enhancing and ensuring the standards of quality and safety of a medicinal product so that it may in the future be marketed, pursuant to the purposes described in the next section.

Purposes of the Processing

The purposes for which your personal data will be processed in the clinical research activities are:

- To generate reliable and robust data in relation to the medicinal product.
- To provide medical care as part of the clinical investigation.
- To report the results of the clinical research once it has concluded.
- To issue notices and reports on the safety of the medicinal product.

Encoding

The Sponsor only accesses your personal data in coded form and therefore does not know and cannot ascertain your identity.

The encoding is done by [the Principal Investigator / a third party engaged by the Sponsor for that purpose] and consists of random assignment to each patient of a number or alphanumerical code (the “Unique Code”) so that the patient cannot be directly identified by the Sponsor.

The information linking the Unique Code to the patient's identity will be kept solely by [the Principal Investigator/ the third party engaged by the Sponsor], securely and confidentially.

Therefore, the Unique Code is what the Site and Sponsor will use in all information they share in the clinical research and in all communications relating to that information. In this respect, the information received by the Sponsor will be associated with that Unique Code and include no identifying information, which will only be available to the Principal Investigator and his or her team.

Nevertheless, there are events in which other third parties will have access to your identifying information, whether by virtue of the applicable laws or because they provide services to the Site or to the Sponsor. Those third parties are described in the next section and have signed confidentiality and secrecy undertakings in relation to your personal data to ensure that no unauthorised third parties access your identifying information and that the Sponsor does not know your identity.

Who has access to your personal data?

Where necessary to manage the clinical research, different persons or entities will access your personal data for the purposes specified below:

- The **Principal Investigator**, who is the person that leads the clinical trial and who knows your identity at all times. You will find the contact information for the Principal Investigator in section [*].
- The **Principal Investigator's Team**, who are HCPs that work with the Principal Investigator in managing the clinical investigation and likewise know your identity.
- The Clinical Research Organisation ("**CRO**"), which is the entity engaged by the Sponsor to carry out certain activities relating to the management of the clinical investigation on behalf of the Sponsor. The Sponsor signs a contract with the CRO laying down the obligations that the latter must comply with in relation to your personal data; the CRO only has access to the Unique Code, unless it carries out monitoring activities, in which case it will have access to your identifying information.
- The **Monitor**, which is the entity that supervises that the clinical investigation is being conducted correctly and makes sure that the information is obtained properly. To perform those functions the Monitor has to have access to your identifying information.
- The **Auditor**, which is the entity that corroborates that all actions carried out in a clinical investigation are done properly and must have access to your identity in order to carry out those audits.
- **Other service providers** involved in the clinical investigation such as [complete as applicable], who, generally speaking, only have access to the Unique Code.

To whom are your personal data disclosed?

Clinical research requires the disclosure of certain personal data to Ethics Committees and the competent health authorities, as the Sponsor must comply with the obligations in that respect laid down in the applicable laws.

As a result, your personal data may be disclosed to Ethics Committees, for their monitoring of the clinical research, and to health authorities if they conduct an inspection.

In addition, in the event of an adverse reaction, your identifying information may be disclosed by the Site to the competent health authorities and to insurers with whom insurance has been contracted in order for them to take the necessary actions.

Both types of disclosure are done in order for the Sponsor to comply with its legal obligations on clinical research manners.

Data transfers to third countries or international organisations

[*Include if personal data are transferred to third countries or international organisations and the safeguards adopted, which must be made available to the data subjects if they so request*].

Storage

The Sponsor must retain the information generated during the clinical research in order to comply with a series of legal obligations, e.g., keeping the master file in clinical trials. The Sponsor thus stores your personal data, in all cases identified exclusively by means of the Unique Code, for a period of [*complete according to the specific clinical investigation*] years.

Rights

In accordance with data protection regulations, you have the right to access your personal data, request the rectification of inaccurate data or, as applicable, ask for such data to be erased where, among other situations, the data are no longer needed for the purposes for which they were obtained. You may also request to have the processing of your personal data limited to the events provided for in the applicable laws.

In certain situations, however, the exercise of those rights may be limited, for reasons such as the existence of a legal provision to such effect in European Union law or in the laws of the country where the clinical research is to be conducted or for health-related reasons of public interest.

As already indicated, the Sponsor does not access your identifying information, but only has access to the clinical research information associated with a Unique Code. Therefore, to exercise your rights you should contact the Principal Investigator whose contact information is given in section [*].

Lastly, we inform you that you may submit a claim to the Governance Body of the Code of Conduct Regulating the Processing of Personal Data in Clinical Trials and Other Clinical Research and Pharmacovigilance Activities approved by FARMAINDUSTRIA, as well as to the Spanish Data Protection Agency (Agencia Española de Protección de Datos) at its website **www.aepd.es**.

Annex 2: Sponsor – trusted third party contract clause

"The Service Provider represents and warrants that it will process all data relating to clinical research activities, including data relating to both the participants in those activities and to the HCPs who manage those activities (the "**Personal Data**") in accordance with the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and Organic Law 3/2018 of 5 December 2018 on the Protection of Personal Data and Guarantee of Digital Rights, and in accordance with the anonymisation guidelines issued by data protection authorities from time to time.

Access by the Service Provider to Personal Data is necessary in order to be able to provide the Services. The Service Provider will therefore be a processor of such data. Such access will not be considered a disclosure of Personal Data, but access required to provide the services subject to this Contract.

Without prejudice to the above, the Personal Data will be provided to the Service Provider by the [Site/Principal Investigator] without the Sponsor having access to said Personal Data before they are coded by the Service Provider.

The Personal Data processed will relate to the following categories of data subjects [complete] and the following categories of data [complete].

The Service Provider will process the Personal Data exclusively for the purposes of providing coding services to the Sponsor in accordance with the instructions issued in writing by the latter and shall under no circumstances use that data for any other purposes. Without prejudice to the above, the Sponsor will in no event provide the Service Provider with instructions that could imply its access to or knowledge of the identifying information of the participants in the clinical research. The Service Provider will immediately notify the Sponsor if it considers that an instruction provided by the latter infringes a provision of personal data protection laws and, in particular, if an instruction may imply access by the Sponsor to identifying information of the participants in the clinical research.

The Service Provider shall not disclose the Personal Data to any third party, not even for storage, unless such disclosure has been previously authorised by the Sponsor expressly.

The Service Provider shall keep a written record (including in electronic form) of processing activity carried out on behalf of the Sponsor pursuant to this contract.

If the Sponsor decides to carry out a data protection impact assessment evaluating, in particular, the origin, nature, particularity and severity of processing which could involve a risk for the rights and freedoms of natural persons as envisaged in the legislation, the Service Provider undertakes to actively assist and cooperate with the Sponsor in carrying out such an assessment taking into account the nature of the processing and the information at its disposal.

The Service Provider shall adopt technical and organisational security measures to ensure an adequate level of security, including confidentiality, taking into account the state of the art and the costs of implementation with respect to the risks to which the Personal Data are exposed as a result of their processing by the Service Provider.

By way of illustration and without implying any limitation, the Service Provider undertakes to adopt measures that allow it to know the traceability of all access to the Personal Data in the event of accidental access.

When assessing the risk in relation to the security of the Personal Data, the Service Provider shall take into account the risks arising from the processing of the Personal Data, such as accidental or unlawful destruction, loss or alteration of the Personal Data transmitted, stored or otherwise processed, or the unauthorised disclosure of, or access to, the Personal Data which could give rise to physical, material or non-material loss or damage. For these purposes, the Service Provider shall take as reference the security measures implemented at the Site where the clinical investigation is conducted.

In the event of (i) loss or undue use of the Personal Data, (ii) unauthorised or unlawful processing, disclosure, access, alteration, corruption, transfer, sale, rental, destruction or involuntary use of the Personal Data or (iii) any other event which compromises or could compromise the security, confidentiality or integrity of the Personal Data (a "**Security Breach**"), the Service Provider shall notify the Sponsor of such event without undue delay and, in all cases, no later than thirty-six (36) hours after becoming aware of the Security Breach. If the Sponsor is not notified within that time limit, the Service Provider shall give the Sponsor a reasoned explanation of the failure to notify.

If, in accordance with personal data protection laws, the Security Breach must be notified to the data subjects, the Service Provider shall provide such notification, expressly indicating that it is being provided on behalf of the Sponsor. Without prejudice to the foregoing, the Sponsor may determine the correction mechanisms to be implemented by the Service Provider with respect to the reasons for the Security Breach.

If the Sponsor authorises the Service Provider to subcontract certain services to a third party, the Service Provider shall enter into a contract with the personal data protection obligations contained in this clause with that third party.

If the Service Provider receives a request from the data subjects in relation to the exercise of their rights of access, rectification, erasure or restriction of processing of the Personal Data, it shall give them the necessary instructions for them to address their requests to the site where the clinical research in which they are participating is being conducted using the contact information contained in the informed consent document they were provided.

The Service Provider shall, after finishing the provision of services, return to the [Site/Principal Investigator] or destroy, as requested by the Sponsor, any Personal Data to which it has had access in the form in which it is held at that time. The Service Provider may, however, retain the Personal Data, duly blocked, for as long as necessary to deal with possible liability that may arise from the processing or for compliance with any legal obligations to which the Service Provider may be subject.

The Service Provider shall make available to the Sponsor all information necessary for the latter, whether directly or through a third party, to verify the degree of compliance by the Service Provider with the obligations in this clause and shall cooperate actively to achieve this.

The Service Provider shall not provide the Sponsor with Personal Data that have not been previously coded so that the Sponsor can in no case identify the data subject.

For these purposes, the Service Provider must use a procedure that ensures the information received by the Sponsor and, in particular, the information contained in the case report forms, contains no identifying information of the participants in the clinical research. The Service Provider undertakes to in no case provide information to the Sponsor in relation to the coding process used that could allow the Sponsor, whether directly or indirectly, to access the identifying information of the participants in the clinical research.

The Sponsor likewise undertakes in no event to access clinical research documents that contain identifying information of the participants, unless necessary for compliance with the obligations imposed on the Sponsor by the applicable laws and regulations.

The Service Provider warrants that the coding process used will not entail alteration of the real data provided to it by the [Site/Principal Investigator] so that the Sponsor may use said data in the clinical research."

Annex 3:
Data protection clause in the sponsor – site/principal investigator contract

The Parties agree that the Sponsor shall not take part in collecting the data of the participants in the clinical research.

Consequently, the [Site/Principal Investigator] shall be responsible for complying with the information and disclosure duty in relation to the participants in the clinical research, providing them at the time it gives them the informed consent form a specific document containing all information on the processing of their personal data in relation to the clinical research activities.

The Parties agree that the [Site/Principal Investigator/ Sponsor] shall be responsible for carrying out the coding of the personal data of the clinical research participants.

[Option A, where the obligation rests with the Site/ Principal Investigator]

For these purposes, the Site/Principal Investigator must use a procedure that ensures the information received by the Sponsor and, in particular, the information contained in the case report forms, contains no identifying information of the participants in the clinical research. The [Site/Principal Investigator] undertakes not to provide the Sponsor with information that allows it to access and know, directly or indirectly, identifying information of the participants in the clinical research, in particular, but without implying limitation, the [Site/Principal Investigator] shall in no event provide information on the process it used to code the data.

In addition, the Site/Principal Investigator shall adopt measures that allow traceability of all access to the personal data in the event of accidental access.

[Option B, where the obligation rests with the Sponsor]

For these purposes, the Parties agree that the Sponsor shall subcontract a third party to perform the coding of the data of the clinical research participants using a procedure that guarantees the Sponsor will in no event access identifying information of the participants in the clinical research. The [Site/Principal Investigator] must provide that third party with the information it may need to carry out the coding. The Sponsor must enter into a data processing contract with that third party in accordance with the requirements of Article 28 of the GDPR, with the particularity that the contract will lay down the Sponsor's express covenant not to give the processor any instruction that could allow the Sponsor to access or know the identifying information and the consequent obligation of the third party to not provide that identifying information unless required for compliance with its legal obligations.

The [Site/Principal Investigator] warrants that it will provide no information to the Sponsor that allows it to identify the participants in the clinical research. In particular, the [Site/Principal Investigator] undertakes to send the Sponsor the case report forms without the identifying information of the participants in the clinical research, and with no information that could allow the Sponsor to know that data, and only associating the data with the code assigned to each participant as provided in this Clause.

The Sponsor, in turn, undertakes not to access documents relating to the clinical research that contain identifying information of the participants unless required for compliance with its legal obligation or with the good clinical practice guidelines.

The [Site/Principal Investigator] will act as contact point for the participants in the clinical research and therefore undertakes to handle all queries that may be made by the participants in relation to the processing of their personal data, and to process their requests to exercise their right of access, rectification, erasure and restriction of processing with the timing stipulated for that purpose in the personal data protection laws that apply from time to time.

The Sponsor shall be responsible for contracting the Monitor and the Auditor and shall enter into a data processing contract with each of them in accordance with the terms of Article 28 of the GDPR.

In the event a member of the investigator team that takes part in the clinical research is not an employee of the Site, the Site will be responsible for contracting said member and will execute a confidentiality and secrecy undertaking, as well as a data processing contract, on the terms described in the preceding section.

Annex 4:
Clause to be included in the sponsor's contract with the monitor and auditor

"The Service Provider represents and warrants that it will process all data relating to the clinical research activities, including data relating to both the participants in those activities and to the HCPs who manage those activities (the "**Personal Data**") in accordance with the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and Organic Law 3/2018 of 5 December 2018 on the Protection of Personal Data and Guarantee of Digital Rights, and in accordance with the provisions of the Convention on Human Rights and Biomedicine.

Access by the [Monitor/Auditor] to Personal Data is necessary in order to be able to provide the Services. The [Monitor/Auditor] will therefore be a processor of such data. Such access will not be considered a disclosure of Personal Data, but access required to provide the services subject to this Contract.

The Personal Data processed will relate to the following categories of data subjects [complete] and the following categories of data [complete].

The [Monitor/Auditor] will process the Personal Data exclusively for the purposes of providing [monitoring/ audit] services to the Sponsor in accordance with any instructions issued in writing by the latter and shall not under any circumstances use such data for any other purposes. The [Monitor/Auditor] shall give the Sponsor immediate notice if it considers that an instruction given by the Sponsor infringes the provisions of the applicable personal data protection rules.

The [Monitor/Auditor] shall not disclose the Personal Data to any third party, not even for storage, unless such disclosure has been previously authorised by the Sponsor expressly.

The [Monitor/Auditor] shall keep a written record (including in electronic form) of processing activity carried out on behalf of the Sponsor pursuant to this contract.

If the Sponsor decides to carry out a data protection impact assessment evaluating, in particular, the origin, nature, particularity and severity of processing which could involve a risk for the rights and freedoms of natural persons as envisaged in the legislation, the [Monitor/ Auditor] undertakes to actively assist and cooperate with the Sponsor in carrying out such an assessment taking into account the nature of the processing and the information at its disposal.

The [Monitor/Auditor] shall adopt technical and organisational security measures to ensure an adequate level of security, including confidentiality, taking into account the state of the art and the costs of implementation with respect to the risks to which the Personal Data are exposed as a result of their processing by the [Monitor/Auditor].

When assessing the risk in relation to the security of the Personal Data, the [Monitor/Auditor] shall take into account the risks arising from the processing of the Personal Data, such as accidental or unlawful destruction, loss or alteration of the Personal Data transmitted, stored or otherwise processed, or the unauthorised disclosure of, or access to, the Personal Data which could give rise to physical, material or non-material loss or damage. For these purposes, the [Monitor/Auditor] shall take as reference the security measures implemented at the Site where the clinical investigation is conducted.

In the event of (i) loss or undue use of the Personal Data, (ii) unauthorised or unlawful processing, disclosure, access, alteration, corruption, transfer, sale, rental, destruction or involuntary use of the Personal Data or (iii) any other event which compromises or could compromise the security, confidentiality or integrity of the Personal Data (a "**Security Breach**"), the [Monitor/ Auditor] shall notify the Sponsor of such event without undue delay and, in any event, no later than thirty-six (36) hours after becoming aware of the Security Breach. If the Sponsor is not notified within that time limit, the [Monitor/ Auditor] shall give the Sponsor a reasoned explanation of the failure to notify.

If, in accordance with personal data protection laws, the Security Breach must be notified to the data subjects, the [Monitor/Auditor] shall provide such notification, expressly indicating that it is being provided on behalf of the Sponsor. Without prejudice to the foregoing, the Sponsor may determine the correction mechanisms to

be implemented by the [Monitor/Auditor] with respect to the reasons for the Security Breach.

If the Sponsor authorises the [Monitor/Auditor] to subcontract certain services to a third party, the [Monitor/Auditor] shall enter into a contract with the personal data protection obligations contained in this clause with that third party.

If the [Monitor/Auditor] receives a request from the data subjects in relation to the exercise of their rights of access, rectification, erasure or restriction of processing of the Personal Data, it shall give them the necessary instructions for them to address their requests to the site where the clinical research in which they are participating is being conducted using the contact information contained in the informed consent they were provided.

The [Monitor/Auditor] shall, after finishing the provision of services, return to the Sponsor or destroy, as requested by the latter, any Personal Data to which it has had access in the form in which it is held at that time. The [Monitor/Auditor] may, however, keep the Personal Data, duly blocked, for as long as necessary to deal with possible liability which may arise from the processing or for compliance with any legal obligations to which the [Monitor/Auditor] may be subject.

The [Monitor/Auditor] shall make available to the Sponsor all information necessary for the latter, whether directly or through a third party, to verify the degree of compliance by the [Monitor/Auditor] with the obligations in this clause and shall cooperate actively to achieve this.

The [Monitor/Auditor] shall not provide the Sponsor with Personal Data that have not been previously coded so that the Sponsor can in no case identify the data subject."

Annex 5:
Clause to be included in the sponsor's contract with the CRO when the CRO provides services other than monitoring

"To provide the Services the CRO needs to access previously coded personal data of clinical research participants (the "**Personal Data**"). The CRO will therefore be a processor of such data. Its access will not be considered a disclosure of Personal Data, but access required to provide the Services subject to this Contract.

The Personal Data processed will relate to the following categories of data subjects [complete] and the following categories of data [complete].

The CRO will process the Personal Data exclusively for the purposes of providing [complete] services to the Sponsor in accordance with any instructions issued in writing by the latter and shall under no circumstances use such data for any other purposes. The CRO shall give the Sponsor immediate notice if it considers that an instruction given by the Sponsor infringes the provisions of the applicable personal data protection rules.

The CRO shall not disclose the Personal Data to any third party, not even for storage, unless such disclosure has been previously authorised by the Sponsor expressly.

The CRO shall keep a written record (including in electronic form) of processing activity carried out on behalf of the Sponsor pursuant to this contract. That record shall note that the Personal Data accessed have been previously coded.

If the Sponsor decides to carry out a data protection impact assessment evaluating, in particular, the origin, nature, particularity and severity of processing which could involve a risk for the rights and freedoms of natural persons as envisaged in the legislation, the CRO undertakes to actively assist and cooperate with the Sponsor in carrying out such an assessment taking into account the nature of the processing and the information at its disposal.

The CRO shall adopt technical and organisational security measures to ensure an adequate level of security, including confidentiality, taking into account the state of the art and the costs of implementation with respect to the risks to which the Personal Data are exposed as a result of their processing by the CRO.

When assessing the risk in relation to the security of the Personal Data, the CRO shall take into account the risks arising from the processing of the Personal Data, such as accidental or unlawful destruction, loss or alteration of the Personal Data transmitted, stored or otherwise processed, or the unauthorised disclosure of, or access to, the Personal Data which could give rise to physical, material or non-material loss or damage. In particular, the measures implemented by the CRO must prevent inasmuch as possible re-identification of the data subjects whose Personal Data the CRO accesses.

In the event of (i) loss or undue use of the Personal Data, (ii) unauthorised or unlawful processing, disclosure, access, alteration, corruption, transfer, sale, rental, destruction or involuntary use of the Personal Data or (iii) any other event which compromises or could compromise the security, confidentiality or integrity of the Personal Data (a "**Security Breach**"), the CRO shall notify the Sponsor of such event without undue delay and, in any event, no later than thirty-six (36) hours after becoming aware of the Security Breach. If the Sponsor is not notified within that time limit, the CRO shall give the Sponsor a reasoned explanation of the failure to notify.

If, in accordance with personal data protection laws, the Security Breach must be notified to the data subjects, the CRO Provider shall provide such notification, expressly indicating that it is being provided on behalf of the Sponsor. Without prejudice to the foregoing, the Sponsor may determine the correction mechanisms to be implemented by the CRO with respect to the reasons for the Security Breach.

If the Sponsor authorises the CRO to subcontract certain services to a third party, the CRO shall enter into a contract with the personal data protection obligations contained in this clause with that third party.

If the CRO receives a request from the data subjects in relation to the exercise of their rights of access, rectification, erasure or restriction of processing of the Personal Data, it shall give them the necessary instructions

for them to address their requests to the site where the clinical research in which they are participating is being conducted using the contact information contained in the informed consent they were provided.

The CRO shall, after finishing the provision of services, return to the Sponsor or destroy, as requested by the latter, any Personal Data to which it has had access in the form in which it is held at that time. The CRO may, however, keep the Personal Data, duly blocked, for as long as necessary to deal with possible liability which may arise from the processing or for compliance with any legal obligations to which the CRO may be subject.

The CRO shall make available to the Sponsor all information necessary for the latter, whether directly or through a third party, to verify the degree of compliance by the CRO with the obligations in this clause and shall cooperate actively to achieve this."

Annex 6:
General clause of the sponsor's contract with service providers

"Access by the Provider to Personal Data is necessary in order to be able to provide the Services. The Provider will therefore be a processor of such data. Such access will not be considered a disclosure of Personal Data, but access required to provide the services subject to this Contract.

The Personal Data processed will relate to the following categories of data subjects [complete] and the following categories of data [complete].

The Provider will process the Personal Data exclusively for the purposes of providing coding services to the Sponsor in accordance with any instructions issued in writing by the latter and shall not under any circumstances use such data for any other purposes. The Provider shall give the Sponsor immediate notice if it considers that an instruction given by the Sponsor infringes the provisions of the applicable personal data protection rules.

The Provider shall not disclose the Personal Data to any third party, not even for storage, unless such disclosure has been previously authorised by the Sponsor expressly.

The Provider shall keep a written record (including in electronic form) of processing activity carried out on behalf of the Sponsor pursuant to this contract.

If the Sponsor decides to carry out a data protection impact assessment evaluating, in particular, the origin, nature, particularity and severity of processing which could involve a risk for the rights and freedoms of natural persons as envisaged in the legislation, the Provider undertakes to actively assist and cooperate with the Sponsor in carrying out such an assessment taking into account the nature of the processing and the information at its disposal.

The Provider shall adopt technical and organisational security measures to ensure an adequate level of security, including confidentiality, taking into account the state of the art and the costs of implementation with respect to the risks to which the Personal Data are exposed as a result of their processing by the Provider.

When assessing the risk in relation to the security of the Personal Data, the Provider shall take into account the risks arising from the processing of the Personal Data, such as accidental or unlawful destruction, loss or alteration of the Personal Data transmitted, stored or otherwise processed, or the unauthorised disclosure of, or access to, the Personal Data which could give rise to physical, material or non-material loss or damage.

In the event of (i) loss or undue use of the Personal Data, (ii) unauthorised or unlawful processing, disclosure, access, alteration, corruption, transfer, sale, rental, destruction or involuntary use of the Personal Data or (iii) any other event which compromises or could compromise the security, confidentiality or integrity of the Personal Data (a "**Security Breach**"), the Provider shall notify the Sponsor of such event without undue delay and, in any event, no later than thirty-six (36) hours after becoming aware of the Security Breach. If the Sponsor is not notified within that time limit, the Provider shall give the Sponsor a reasoned explanation of the failure to notify.

If, in accordance with personal data protection laws, the Security Breach must be notified to the data subjects, the Provider shall provide such notification, expressly indicating that it is being provided on behalf of the Sponsor. Without prejudice to the foregoing, the Sponsor may determine the correction mechanisms to be implemented by the Provider with respect to the reasons for the Security Breach.

If the Sponsor authorises the Provider to subcontract certain services to a third party, the Provider shall enter into a contract with the personal data protection obligations contained in this clause with that third party.

If the Provider receives a request from the data subjects in relation to the exercise of their rights of access, rectification, erasure or restriction of processing of the Personal Data, it shall handle those requests for and on behalf of the Sponsor, complying with the provisions of the applicable data protection rules.

The Provider shall, after finishing the provision of services, destroy to Personal Data to which it has had access in the form in which it is held at that time. The Provider may, however, keep the Personal Data, duly blocked, for as long as necessary to deal with possible liability which may arise from the processing or for compliance with any legal obligations to which the Provider may be subject.

The Provider shall make available to the Sponsor all information necessary for the latter, whether directly or through a third party, to verify the degree of compliance by the Provider with the obligations in this clause and shall cooperate actively to achieve this.

The Provider shall not provide the Sponsor with personal data that have not been previously coded so that the Sponsor can in no case identify the data subject whose data it has been provided."

Annex 7:
Record of processing activities form

NAME AND CONTACT DETAILS	
Data Controller	[*] TAXPAYER ID (CIF):
Address	[*]

THE CONTACT DETAILS OF THE DPO

DESCRIPTION OF PROCESSING
[*]

PURPOSE OF PROCESSING
[*]

LEGAL BASIS FOR THE PROCESSING

FORMAT IN WHICH RECORD IS KEPT
[Digital/paper] format

DESCRIPTION OF CATEGORIES	
Of data subjects	[*]
Of personal data	[*]

RECIPIENTS	
Identification	[*]

▶ next page

ENVISAGED TIME LIMITS FOR THE ERASURE OF DIFFERENT CATEGORIES OF DATA
[*]

TRANSFERS OF DATA TO THIRD COUNTRIES	
Name of country or international organisation	[*]

GENERAL DESCRIPTION OF TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

Duty of confidentiality and secrecy

- *[Describe measures which seek to avoid access by unauthorised persons to personal data collected, for example, restrict access to hard drives and servers storing images to authorised personnel.]*

Rights of data holders

- *[Describe procedure employed by the organisation to deal with requests by data subjects to exercise their rights.]*

Security breaches relating to personal data

- *[Describe procedure employed by the organisation to deal with security breaches.]*

Safeguarding duty

- *[Describe technical measures adopted to ensure the safeguarding of personal data, for example, security copies, technical measures to avoid external access to organisation's systems, computer anti-virus updates, data encryption, etc.]*

Identification

- *[Describe organisational measures adopted to ensure that those accessing data are authorised to do so, for example, description of the functions of personnel who may access that data, passwords, etc.]*

Annex 8:
Form for responding to requests received by the sponsor for exercise of rights

Dear Sir/Madam,

We are aware that you have exercised your [right of access, contained in Article 15 / right to object to the processing of your personal data, contained in Article 21 / right to rectification, contained in Article 16 / right to erasure, contained in Article 17 / right to restriction of processing, contained in Article 18] of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

We hereby inform you that we cannot satisfy your request given that, as was specified in the data protection document you were given before your participation in the clinical investigation, we process coded data only and we can therefore not identify you.

You may contact the principal investigator to exercise your rights in the manner specified in the section of the informed consent document regard the protection of your personal data.

Please do not hesitate to contact us if you need any clarification regarding the above. We hereby inform you of your right to lodge a complaint with the Spanish Data Protection Agency (Agencia Española de Protección de Datos).

Sincerely,

Signed _____

(Position)

Annex 9:
Confidentiality undertaking of the investigator team

Given the characteristics of the work to be done by the investigator in the performance of his or her functions, the investigator may need to access confidential information which, moreover, may contain personal data owned or controlled by [*] (the "**Site**").

Access by the investigator to such information shall take place solely and exclusively pursuant to the guidance and instructions given by the Site and provided in protocols, documents or guidelines. The confidential information shall only be used by the investigator for the purpose of carrying out work related to the investigator's position and provided its use is strictly necessary for that work. Including in those cases, the investigator shall have the following obligations in relation to the data to which the investigator has access in connection with the use of the confidential information:

a) Not to use the personal data for purposes other than for performing the tasks assigned to the investigator, and not disclose or make them public in any way, not even for purposes of their storage by third parties.

b) Maintain professional secrecy in relation to the data. This obligation will not end even when the investigator's relationship with the Site has terminated, and the investigator is not allowed to keep the data or a copy of the data in any type of medium or format that contains them.

c) Comply with and respect all technical and organisational security measures implemented by the Site, and with any others that may be conveyed to the investigator from time to time. The investigator will also be obliged to act diligently at all times to ensure the ensure the confidentiality of the data and keep them secure so that there is no security breach that leads to their destruction, accidental or illicit alteration or unauthorised access or disclosure.

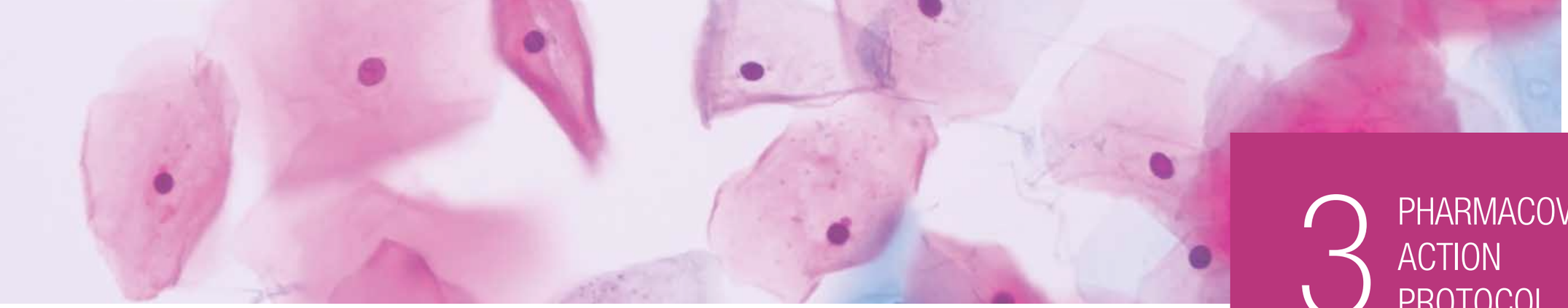
The above undertakings, and all those which, though not expressly mentioned, are to be expected from all reasonable, diligent and good faith compliance with the laws that apply from time to time, will be mandatory and binding for the entire life of the relationship between the investigator and the Site and continue after termination of that relationship.

Received and agreed,

Name:

ID document number.:

Signature: _____



3 PHARMACOVIGILANCE ACTION PROTOCOL

* The Annexes should be considered guides or illustrative models to aid in preparing the documents that apply to the respective topics.

INTRODUCTION

Applicable legislation provides that the objective of pharmacovigilance is the identification, quantification, assessment and prevention of the risks of using medicinal products, thereby permitting the monitoring of possible adverse effects which they may produce.

Of fundamental importance among pharmacovigilance activities is the adoption of measures designed to detect and report adverse reactions which may arise as a result of treatment with products sold by pharmaceutical companies.

Although the legislation governing the guarantees and the rational use of medicinal products and medical products, in particular Royal Decree 577/2013, of 26 July 2013, on the pharmacovigilance of medicinal products for human use, includes within the Spanish pharmacovigilance system only the competent authorities, such as the AEMPS and the competent bodies of the Autonomous Communities, as well as healthcare professionals and patients, it also imposes obligations on pharmaceutical companies.

Pharmaceutical companies have an obligation to report to the health authorities in charge of pharmacovigilance any suspected adverse reactions of which they become aware, and which may have been caused by medicinal products produced, distributed or sold by them, in accordance with the provisions of the European Union guidelines on Good Pharmacovigilance Practices.

In addition, pharmaceutical companies must keep a pharmacovigilance system master file, whether of a unified nature or with separate systems for different categories of medicinal products. The master file must include a description of the location of, functionality of and operational responsibility for computer systems and databases used to receive, collate, record and report safety information and an assessment of their fitness for purpose, as well as a description of the system for monitoring the performance of the pharmacovigilance system and the record management and data storage system in relation to the performance of pharmacovigilance activities.

In relation to suspected adverse reactions, pharmaceutical companies are required by pharmacovigilance rules to:

- Electronically record suspected adverse reactions produced in Spain, the EU or a third country of which they become aware from any source, which includes both those notified spontaneously by HCPs or citizens and those gathered during a post-authorisation study or clinical research.
- Electronically transmit to the Eudravigilance database reports of:
  - All suspected serious adverse reactions occurring in the European Union or third countries, no later than 15 calendar days following the day on which they become aware of them.
  - All suspected non-serious adverse reactions occurring in the European Union, no later than 90 calendar days following the day on which they become aware of them.

European legislation on pharmacovigilance (Commission Implementing Regulation (EU) No 520/2012 of 19 June 2012 on the performance of pharmacovigilance activities provided for in Regulation (EC) No 726/2004 of the European Parliament and of the Council and Directive 2001/83/EC of the European Parliament and of the Council) establishes that marketing authorisation holders must, when reporting adverse reactions to Eudravigilance, include information on the following matters (among others):

- Information identifying the patient (and mother in the case of a mother-child report), including age at the time of the onset of the first reaction, age group, gestation period (when the reaction/event was observed in the foetus), weight, height, sex, last menstrual date and/or gestation period at time of exposure.
- Relevant medical history and concurrent conditions.
- Concomitant medicinal products, identified in accordance with the Implementing Regulation, which are not suspected to be related to the occurrence of the adverse reaction and past-medical drug therapy for the patient (and for the mother), where applicable.
- Information on the suspected adverse reaction(s): start date and end date of the suspected adverse reaction or duration, seriousness and outcome of the suspected adverse reaction at the time of last observation, time intervals between suspect medicinal product administration and start of adverse reactions, the original reporter's words or short phrases used to describe the reactions and Member State or third country of occurrence of the suspected adverse reaction.
- Results of tests and procedures relevant to the investigation of the patient.
- Date and reported cause of death, including autopsy determined causes, in the event of death of the patient.
- A case narrative, where possible, providing all relevant information for individual cases with the exception of non-serious adverse reactions.

All of this information will, to the extent associated with an identified or identifiable person, include personal data. This will occur if the identifying information of the patient referred to in the first bullet point is provided, linked to the rest of the matters referred to.

European legislation also imposes an obligation on authorisation holders to establish mechanisms enabling the traceability and follow-up of adverse reaction notifications.

This means that pharmaceutical companies must be able to obtain additional information about a specific reaction, which will require singularisation in order to carry out the traceability required by legislation. Therefore, even if identifying information relating to the patient is not provided, pharmaceutical companies must be able to single out each patient who has suffered an adverse event to a medicinal product through a coding procedure.

Although pharmaceutical companies should, as a general rule, in accordance with the minimisation principle, codify personal data relating to adverse reactions notified to them, in view of (i) European reporting rules and pharmacovigilance ethical rules and (ii) the need to guarantee better traceability and to ensure the suitable monitoring of the patient, it is advisable to process identifying information relating to patients, and this will require the adoption of additional measures ensuring full compliance with data protection laws.

European legislation establishes that "*the fundamental right to protection of personal data should be fully and effectively guaranteed in all pharmacovigilance activities. The purpose of safeguarding public health constitutes a substantial public interest and consequently the processing of personal data should be justified if identifiable personal data are processed only where necessary and only where the parties involved assess this necessity at every stage of the pharmacovigilance process. National competent authorities and marketing authorisation holders may apply pseudonymisation where appropriate, thereby replacing identifiable personal data with pseudonyms.*"

Processing of patient data in the context of pharmacovigilance will take place, in particular, for the following purposes:

- Reporting information relating to the adverse event to the competent Spanish and European authorities using the systems established for this purpose (Fedra and Eudravigilance).
- Analysing information relating to the reaction and its evolution in order to be able to assess the risk/benefit balance of the medicinal product.
- Compensating the patient who has suffered an adverse event if the relevant requirements are met.

1. Processing of data relating to adverse events containing identifying information

As mentioned above, in many cases pharmaceutical companies will choose to process identifying information relating to a patient who has suffered an adverse event, in order to ensure compliance with the reporting, traceability and monitoring obligations contained in pharmacovigilance laws.

It is also possible that, on exceptional occasions when a pharmaceutical company has chosen not to spontaneously collect identifying information relating to a patient (generally using a coding procedure), it will nevertheless access data that allow it to directly identify patients, those data having been provided by the person reporting the adverse event without having been asked to do so by the pharmaceutical company.

In both cases, the pharmaceutical company should observe the provisions of this section when processing personal data in relation to pharmacovigilance.

1.1 LEGAL BASIS FOR THE PROCESSING

Given that pharmacovigilance activities involve the processing of health data, the processing must not only have one of the legal basis established in Article 6(1) of the GDPR, but also benefit from one of the exemptions from the general prohibition on the processing of this category of data contained in Article 9(2) of the GDPR.

Article 9(2)(i) of the GDPR exempts from the general prohibition on the processing of sensitive data (which includes data relating to the health of patients who suffer an adverse event) any processing which is necessary for reasons of public interest in the area of public health, as well as any processing aimed at ensuring high standards of quality and safety of health care and of medicinal products or medical devices.

It should be noted that not only do European Union rules on pharmacovigilance consider that pharmacovigilance, as a safeguard of public health, is in the public interest, but they also impose on holders of marketing authorisations of medicinal products a legal obligation to record and report the circumstances in which any adverse events to such products occur. The processing of personal data would therefore be lawful if necessary to comply with these legal obligations, which, moreover, arise from the need to safeguard the public interest.

The processing of data relating to a suspected adverse event by any of the means described below is therefore lawful under Article 6(1)(c) of the GDPR, and it is not necessary to obtain the consent of the patient, although the obligations contained in the GDPR, in particular those relating to guaranteeing the right to information, still apply.

On the other hand, it is possible that the information relating to a suspected adverse event is not collected directly from the person suffering the reaction, but from a third party such as, for example, a healthcare professional or a person related to the patient or close to the patient at the time the reaction occurs.

In relation to the former, usually, in accordance with Spanish pharmacovigilance laws, the reaction is reported not to the pharmaceutical company but to the competent authority of the Autonomous Communities or to the AEMPS, given that, as members of the Spanish pharmacovigilance system, such reporting is a requirement.

It is, nevertheless, possible for the pharmaceutical company to also be notified by a third party other than the patient suffering the alleged adverse event. This could be the case of parents, guardians or legal representatives of minors or incapacitated persons. It is also possible that the reaction be reported by a third party who does not represent the patient due to the fact that the patient cannot report the reaction precisely because of the symptoms presented.

In these cases, the pharmaceutical company will be able to continue processing on the basis of compliance with a legal obligation, but may ask itself whether it should wait, if notification is not given by the patient, until the patient is in a position to be informed directly in relation to the processing of his or her personal data.

The answer to this question should be no. It is not necessary to delay processing for these reasons given that, in addition to the legal basis referred to in Article 6(1)(c), that contained in Article 6(1)(d) would apply since the data would be processed for the purpose of protecting a vital interest of the patient suffering the adverse event, the patient not being in a condition to be directly informed of the processing. Although this article refers literally to the circumstances in which the data subject should be able to give his or her consent, if the patient is unable to do so, a balanced and reasonable interpretation of the article would support the view that data should be collected immediately, without waiting for the patient to have recovered sufficiently to be able to understand the information which has to be provided to him or her, given that the patient's health (or even life) could be in danger.

1.2 DATA COLLECTION

A possible adverse event in the use of a medicinal product can be reported through different channels. It can also be reported by different individuals, whether the patient him or herself, or a third party (either acting on behalf of the patient or happening to be close to the patient suffering the event) or a healthcare professional looking after the patient.

Each time data is collected, the data protection principles established in Article 5 of the GDPR must be observed. It must therefore be ensured that:

- The information is collected by personnel responsible for pharmacovigilance activities, in accordance with the contents of the pharmacovigilance system master file of the marketing authorisation holder.

- All information necessary to properly understand the circumstances surrounding the reported event is collected, with the aim of achieving its proper reporting in accordance with the law.

- Information which is irrelevant for the purposes of proper reporting and analysis of related information is not collected.

- The accuracy of the information collected is verified, and confirmation of as many matters as may be required to ensure such accuracy is requested.

- Technical and organisational measures necessary to ensure that the data collected are stored in systems in a way that ensures their confidentiality, integrity and availability are adopted.

Set out below are guidelines on the procedures which pharmaceutical companies should follow when collecting identifying information relating to patients through different channels, describing the different rules to be followed depending on who reports the adverse event. For this purpose, the different channels for collecting information will be differentiated (telephone, electronic, social media, ordinary post or in person).

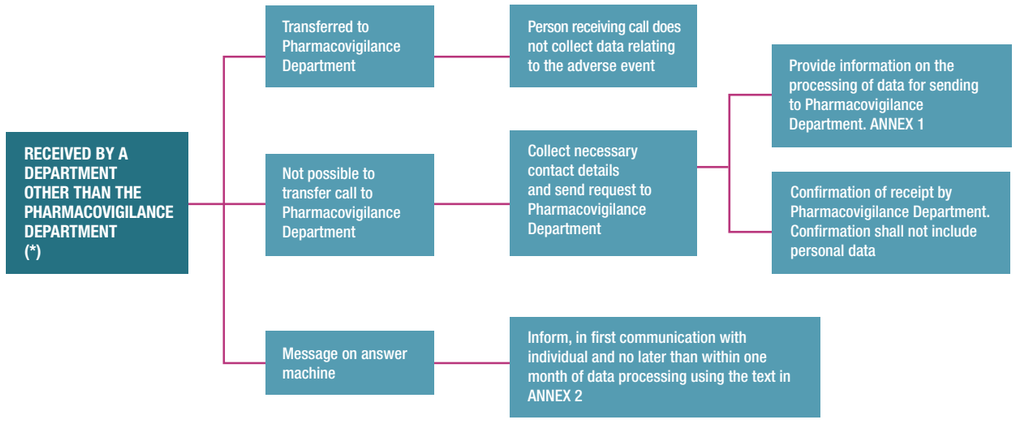
In view of the range of circumstances which can arise in the event of receiving information by telephone or electronically or through social media, we have chosen to provide a graphic description of the protocol to be followed depending on how information is received, establishing the steps to be followed in each case and how to comply with the duty to provide information:

- By telephone

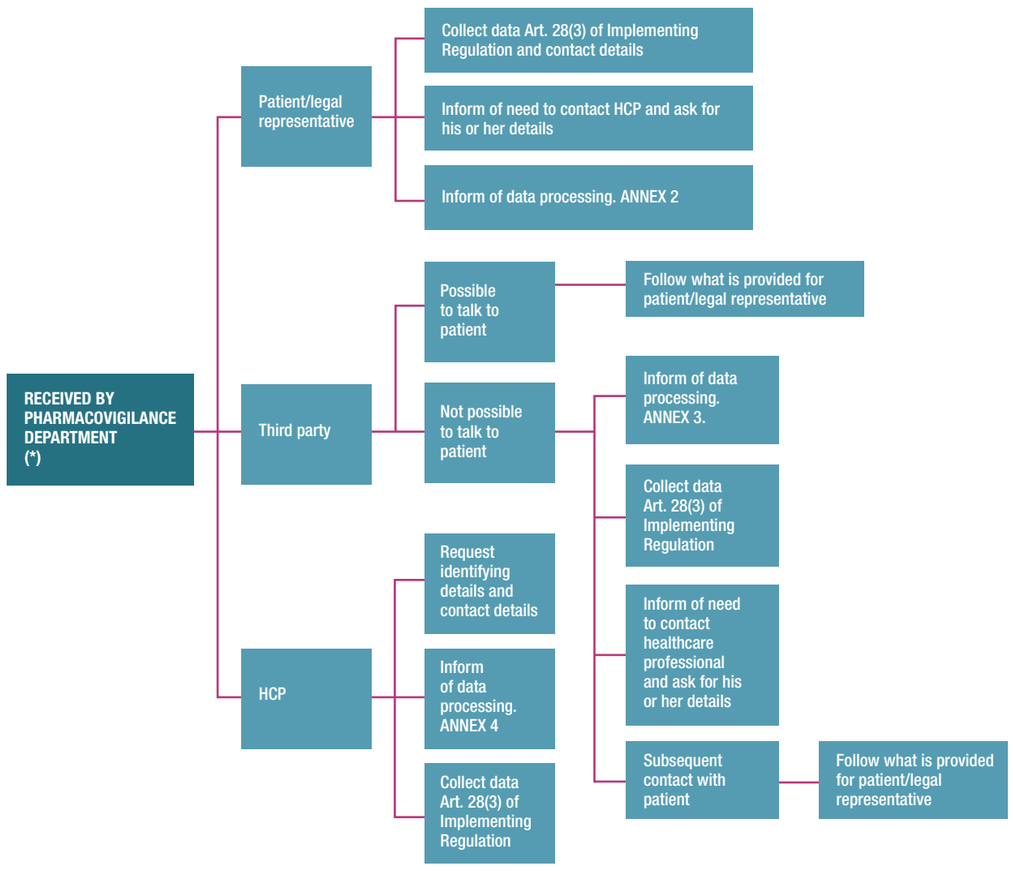
- By electronically

- Through social media

1.2.1 BY TELEPHONE

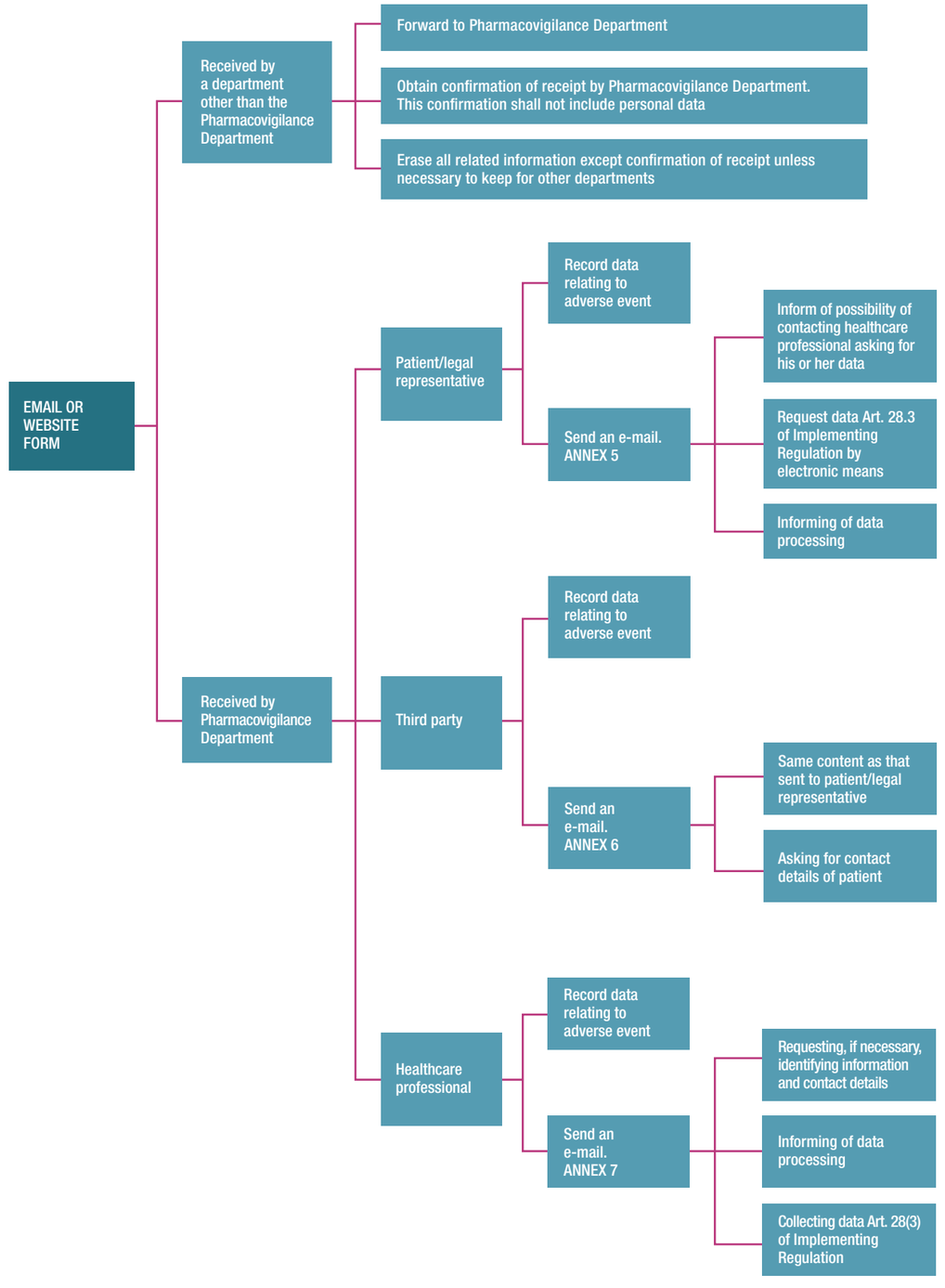


(*) If there is a pre-recorded message prior to the receipt it will not be necessary to repeat the information on the processing of personal data.

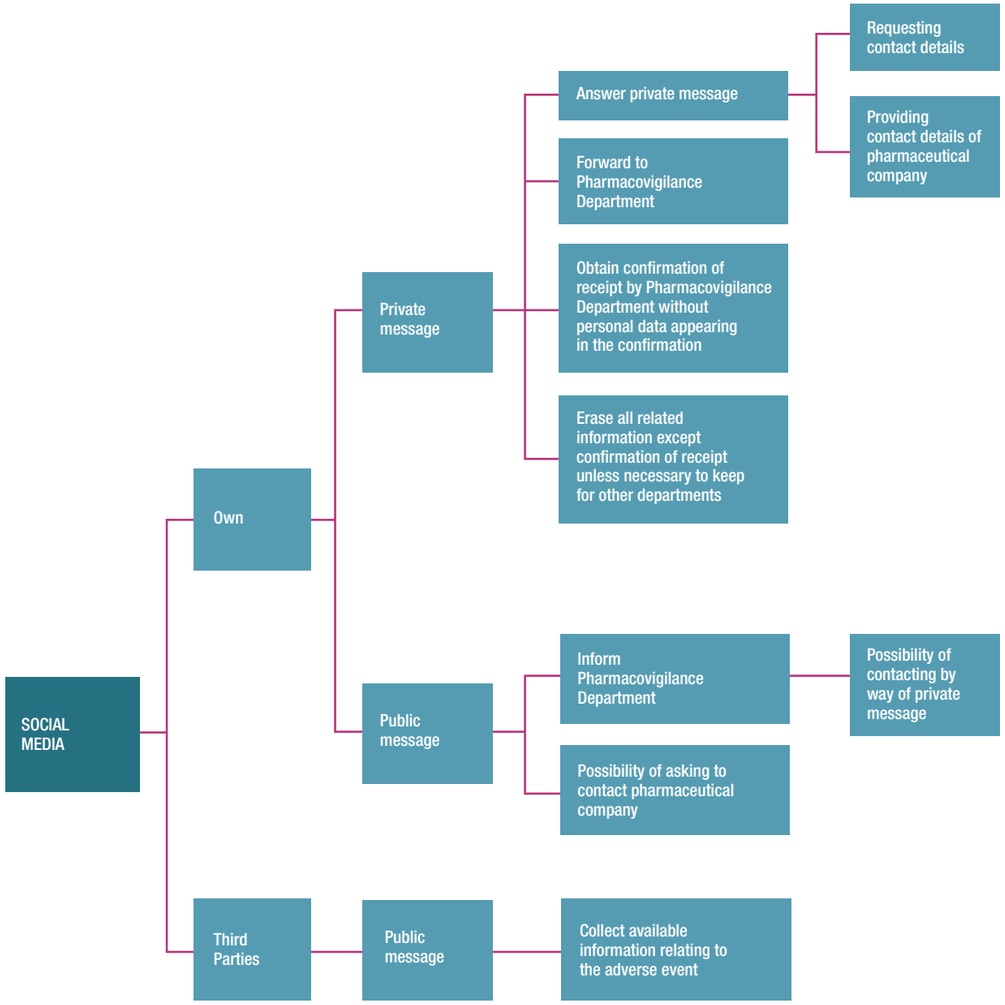


(*) If there is a pre-recorded message prior to the receipt it will not be necessary to repeat the information on the processing of personal data.

1.2.2 ELECTRONICALLY



1.2.3 TROUGH SOCIAL MEDIA



1.2.4 COLLECTION BY ORDINARY POST

Although the development of information technology has meant that the reporting of adverse reactions by way of ordinary or conventional post is exceptional, this method of reporting cannot be ruled out altogether.

In these circumstances, the guidelines to be followed would be similar to those provided for electronic reporting.

In order to ensure the adequate monitoring of the adverse event, a mechanism which ensures that information relating to the adverse event is provided to the department responsible for handling it (and enables this to be verified) must be used.

Pharmaceutical companies must include in their first communication the wording in Annexes 5, 6 or 7, depending on who reported the adverse event.

1.2.5 COLLECTION OF DATA IN PERSON

It is also possible that on occasion the patient or the patient's representative or a HCP will relay information to delegates or representatives of laboratories or will appear in person at the headquarters of the pharmaceutical company to report an adverse event.

In these circumstances, as well as any others in which data is collected in person, all of the information provided by the reporting person must be collected, as well as the minimum data required to process the adverse event and the contact details of the reporting person so that the Pharmacovigilance Department can get in touch and provide information in relation to data processing if it has not been possible to provide the data subject with that information at the time the adverse event was reported.

1.3 RECORD OF PROCESSING ACTIVITIES

Pharmaceutical companies, in their capacity as data controllers, must maintain a record of processing activities relating to their pharmacovigilance activities, which must include all the information referred to in Article 30 of the GDPR. This record must be kept in a format which allows both straightforward access to it and rapid modification if any changes are required to be made.

There may be a single pharmacovigilance and adverse event monitoring record, which will refer to all processing carried out in accordance with this CC. Nevertheless, it will be possible to differentiate, for organisational purposes, between the different medical products for which the pharmaceutical company is the holder of the marketing authorisation.

Pharmaceutical companies are advised to specify in their record of processing activities that the department in charge of managing processing will be the Pharmacovigilance Department.

Annex 23 contains a form of record of processing activities for pharmacovigilance, which must be completed with the information relating to each specific processing activity.

1.4 RECIPIENTS OF DATA

Pursuant to Articles 13 and 14 of the GDPR, data subjects must be informed of the recipients of their personal data, including both data processors and third parties.

In the course of a pharmaceutical company's pharmacovigilance activities, there may be both disclosure of data and access to data by data processors. Disclosure of data will include disclosure which must be made in relation to Spanish and European pharmacovigilance or disclosure to insurance companies for the purpose of handling any compensation cases. The pharmacovigilance tasks of a data processor may also be contracted to a CRO.

It should be noted that members of the group of companies to which a pharmaceutical company belongs will be considered recipients for the purposes of this CC.

Information regarding all these recipients must be included in the information provided by a pharmaceutical company to a reporting person and to the patient informing them of the processing of their personal data.

Set out below are possible recipients of data:

1.4.1 ACCESS BY THIRD PARTIES

In relation to data processors, it is not necessary to expressly identify the entity which accesses the data as a result of the provision of a service to a pharmaceutical company, it being possible to include a generic reference to the services provided by that entity.

The pharmaceutical company must have entered into a contract with the data processor including the requirements set out in Article 28 of the GDPR. In particular, the regime governing the storage of data by the data processor must be specified, in order to respect the guarantees required of pharmacovigilance processing activities.

If the contracted services consist of the collection of data on behalf of the Pharmacovigilance Department, the contract must include the obligation to comply with the procedures established in this CC.

In these circumstances, the processor shall not at any time address the person reporting the event on its own behalf, making clear at all times that it is acting on behalf of the pharmaceutical company.

1.4.2 DISCLOSURES

1.4.2.1 Disclosure to Pharmacovigilance Authorities

As mentioned in the introduction, Spanish and European pharmacovigilance laws, in particular in circumstances giving rise to an adverse event as a result of the use of a specific medicinal product, impose upon pharmaceutical companies the obligation to report a series of personal data for inclusion in the Eudravigilance database, the single European database for monitoring these cases.

There also exists an obligation to monitor adverse reactions recorded in the Spanish pharmacovigilance system, with the holder of the marketing authorisation being obliged to cooperate with the system in order to avoid duplication.

These laws therefore establish a series of obligations to disclose information to the competent pharmacovigilance authorities, whether at a domestic or European level, by way of the relevant networks established at each level. This therefore constitutes disclosure of data based on the existence of a legal obligation.

Reporting persons, HCPs and patients should be informed of such disclosures in the information provided by the pharmaceutical company.

1.4.2.2 Disclosure to Group Companies

Pharmacovigilance laws impose on the holder of a marketing authorisation the obligation to appoint a person responsible for pharmacovigilance in the European Union who will be responsible for the establishment and maintenance of the system.

In the case of multinational groups, there may therefore be, in addition to Pharmacovigilance Departments in each company, a single person responsible for the system, who may belong to another member of the group and not necessarily be located in Spain, although he or she must be located in the EEA.

The duties of the person responsible for pharmacovigilance in the European Union require that person to have access to information regarding adverse reactions occurring in any Member State of the European Union, which may involve the centralisation of pharmacovigilance information systems within the group and the exchange of information between the various companies forming part of the group.

This transmission of data between group companies will be based on the need to comply with each company's obligations and to comply with the obligations imposed by European Union law in relation to the centralisation of responsibility in this area and the legitimate interest of the group in transmitting such information within the group for administrative purposes, expressly recognised in Recital 48 of the GDPR.

The fact that the entity which constitutes the main establishment of the group in the European Union (or its holding company, if the group is European) must comply with the reporting obligations established in European legislation also justifies the disclosure of data to the holding company for such purposes on the basis of the existence of a legal obligation.

Thus, disclosure of data to other members of the group for the purposes set out in Articles 6(1)(c) and 6(1)(f) of the GDPR will be possible, without the need to obtain the consent of the patient or other person reporting the adverse event. In any event, the processing of data based on legitimate interests shall require a prior report evaluating its prevalence over the rights and interests of data subjects.

1.4.2.3 Insurance Companies

A pharmaceutical company, may, in the circumstances established by law, have contracted a civil liability insurance to cover possible losses which may arise from the consumption of a medicinal product prescribed to a patient.

In such cases, data regarding the patient suffering the adverse event may be transmitted to the insurance company in order to guarantee the payment of relevant compensation.

This disclosure would be based on the existence of a legal obligation, given that the law governing civil liability insurance contracts grants the party suffering loss a direct action against the insurer.

1.4.3 LICENSEES

There may be circumstances in which the pharmaceutical company (licensee) is not the holder of the marketing authorisation for the medicinal product and enters into a licensing agreement for the sale of a specific product with a third party based in the EEA which is the holder of the marketing authorisation (licensor). In these cases, the licensor is obliged to monitor adverse reactions produced by the medicinal product for which it holds the marketing authorisation.

The licensee pharmaceutical company will therefore process the data necessary to carry out pharmacovigilance activities on behalf of the licensor company, and section 1.4.1 shall apply given that the licensor would be the entity effectively obliged to comply with relevant laws in respect of the monitoring of adverse reactions.

The foregoing paragraph will also apply where a pharmaceutical company enters into a contract for the sale of a product to a third party.

1.5 INTERNATIONAL TRANSFERS OF DATA

It should first of all be borne in mind that this section applies both to when a third party accesses data as a result of providing a service to a controller and when a controller discloses data to a third party.

In the case of medicinal products, pharmacovigilance laws require, both for the performance of clinical trials and the sale of medicinal products, that the sponsor of the trial or the holder of the marketing authorisation, as applicable, be based in the EEA, therefore they must comply with the relevant legislation. Nevertheless, it may be necessary to transfer data to third countries in certain relevant circumstances for research or safety of the medicinal product at a global level.

As a general rule, personal data may not be transferred to third parties or organisations which do not provide an adequate level of protection unless the safeguards established in the GDPR are adopted.

Therefore, as an initial premise, such transfers may take place in circumstances in which the country or destination has been declared by the European Commission to be a country offering comparable protection[13].

If the recipient country does not offer an adequate level of protection, one of the following additional safeguards must be adopted:

- Standard data protection clauses adopted by the European Commission.
- Binding corporate rules approved by the competent supervisory authority.
- Standard data protection clauses adopted by the AEPD and approved by the European Commission.
- Approved codes of conduct, together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.
- Approved certification mechanisms, together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

A series of derogations is also established in Article 49 of the GDPR which must be used in a strictly limited manner, with pharmaceutical companies giving priority to the abovementioned mechanisms.

In this case the Sponsor must also carry out a prior analysis of the regulatory framework of the destination country and, if necessary, adopt measures supplementing those set out in that article, in accordance with the terms of the EDPB's "*Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*"[14].

In any event, if the possibility of an international transfer is envisaged before reporting the adverse event, a reference to the fact that a transfer of data to a third country may take place and the safeguards which have been adopted, as well as the possibility of accessing their content, must be included in the information provided to patients or reporting persons.

In relation to the last point, the same channel may be used as that provided to patients to access the privacy policy of the pharmaceutical company in relation to pharmacovigilance activities, as mentioned in section 1.2.

In general, if the transfer is based on the adoption of contractual clauses, these shall be incorporated as an addendum to the main contract, in which all the terms of the relationship between the pharmaceutical company and the entity located in a third country are established. In this way, patients shall have access to the contents of these clauses relating to the international transfer of data, although such access shall not be applicable by extension to the whole of the contract entered into with the recipient of the data. For this reason, the adoption of that addendum to the main contract is recommended, including all of the contractual clauses applying to the international transfer of data, but limited, in terms of its scope, to such clauses, such that access to them does not involve providing the entire contents of the contract or the specific technical and organisational measures agreed between the parties.

Without prejudice to the provisions of this section, if the pharmaceutical company must disclose data to the health authorities of a third country which does not provide a comparable level of protection, provided it is necessary for compliance with an obligation expressly established

13 Countries currently enjoying this status are Switzerland, Andorra, Israel, Canada, Argentina, Guernsey, the Isle of Man, Jersey, the Faroe Islands, Uruguay, New Zealand and Japan.

14 Available at: https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf

in the applicable health laws, it must do so without the need to use any of the abovementioned mechanisms, such transfer falling under important reasons of public interest in the area of health, in accordance with Article 49(1)(d) of the GDPR.

1.6 STORAGE LIMITATION PRINCIPLE

Article 12(2) of the Implementing Regulation provides that marketing authorisation holders shall arrange for the information contained in the pharmacovigilance system master file to be kept for at least five years after the system has been formally terminated. It also provides that pharmacovigilance data and documents relating to individual authorised medicinal products shall be retained for at least 10 years after the global marketing authorisation has ceased to exist unless the documents are required to be retained for a longer period where national law so requires.

In this regard, as already mentioned, the processing of patient data in pharmacovigilance has a series of specific purposes, such as:

- Reporting information relating to the adverse event to the competent Spanish and European authorities using the systems established for this purpose (Fedra and Eudravigilance).
- Analysing information relating to the reaction and its evolution in order to be able to assess the risk/benefit balance of the medicinal product.
- Compensating the patient who has suffered an adverse event if the relevant requirements are met.

Once all information relating to the adverse event and its evolution up to patient discharge is collected and reported to the pharmacovigilance systems, civil liability claims against the pharmaceutical company are possible. This right of action prescribes a year later, in accordance with Article 1968.2 of the Civil Code.

Pharmaceutical companies must therefore retain the information relating to adverse events for at least ten years to the extent necessary to meet these liabilities.

This retention period is considered separate from the retention period for data in the medical history of the patient for which the HCP or centre looking after the patient will be responsible.

1.7 EXERCISE OF RIGHTS

1.7.1 GENERAL CONSIDERATIONS

Chapter III of the GDPR contains, under the heading of "Rights of the data subject", certain aspects of the rights of data subjects, such as those relating to periods and procedures. In particular, the GDPR recognises the rights of access, rectification, erasure, objection, restriction of processing and portability. Similarly, Chapter II of Title III of the LOPDGDD contain certain provisions in relation to the exercise of these rights.

Nevertheless, given that the right to portability of data only operates if processing is based on consent or the performance of a contract, it would not apply to the processing of data in the context of pharmacovigilance activities given that these activities are based on compliance with a legal obligation. Similarly, the right to object would not apply, given that this only operates when the processing is based on the performance a task carried out in the public interest or the controller's legitimate interests.

It should also be pointed out that the rules governing rights in this CC relate to the processing of data carried out by a pharmaceutical company in the context of its pharmacovigilance obligations. Thus, the rights specifically established in health legislation relating to the processing of health data carried out by health centres or professionals looking after patients are not governed by this code and are subject in full to the rules on patient's records, which are not applicable to the Adherents.

The following are salient common features of all the rights:

- The rights are independent of each other, therefore the exercise of one right is not conditional upon prior exercise of another right.
- Sufficiently descriptive information relating to the means available for exercising the rights must be made available to data subjects. In the context of pharmacovigilance activities, this information must be provided to data subjects in accordance with the provisions of section 1.2 of this CC.
- The rights shall be dealt with preferably by electronic means unless the data subject requests a response by other means.
- Article 12(5)(a) of the GDPR, based on the free nature of the rights, provides that where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either charge a reasonable fee taking into account the administrative costs or refuse to act on the request[15]. In particular, in deciding whether a request is excessive or abusive, regard shall be had to data protection laws and to applicable sector laws. In these circumstances, a fee may be charged for attending to the rights.
- Given the very personal nature of these rights, they must be exercised directly by the data subject or by the data subject's legal representative, in the case of persons under the age of 14 years or incapacitated persons. Additional information may be requested on behalf of data controllers for the identification of the data subject if there are reasonable doubts as to the identity of the natural person making the request. Rights may also be exercised through a voluntary representative, provided it can be demonstrated that this power is conferred expressly upon the representative, as well as the identity of the representative and the person represented. Generic powers will not be admissible.
- If the request does not adequately identify the data subject, the data subject's representative or the power conferred or does not fulfil the requirements described below in relation to each of the rights, then a request to correct this must be issued.
- Attached as Annex 8 is a form of response requesting that the request be amended.
- Article 12(3) of the GDPR establishes a period of 1 month to take action on a request, which may be extended by two further months where necessary, taking into account the complexity and number of the requests, provided that the data subject is informed of any such extension within the general 1-month period, and is expressly informed of the reasons for the delay.

  Attached as Annex 9 is a form of response to the data subject when it is necessary to extend the period established by law.
- Data controllers are responsible for proving compliance with the duty to take action on the exercise of these rights, therefore it would be advisable to send responses by any means which provides evidence of sending and receipt at any time.
- If a pharmaceutical company subcontracts to a CRO services relating to pharmacovigilance, but not the handling of requests for the exercise of rights, and the latter receives a request to exercise rights, it must forward the request to the pharmaceutical company within 48 working hours to enable the pharmaceutical company to respond to the data subject.
- Attached as Annex 10 is a form of notice to be sent by the CRO to the data subject informing them that their request has been notified to the pharmaceutical company which is the data controller so that the latter can provide a response.
- If suitable action is not taken on a request for the exercise of rights, the data subject will be entitled to lodge a complaint with the CCGB or, as appropriate, the AEPD.

In accordance with the GDPR and the LOPDGDD, there may be exceptions to the rights of access, rectification, restriction of processing and objection if:

- The rights are exercised directly before the pharmaceutical company if anonymised or coded data are use, it being impossible to re-identify the patient.
- The exercise of the rights refers to conclusions reached in relation to the Adverse Event and not to data relating to the patient exercising the right.
- The purpose of the management of the Adverse Event is an essential public interest relating to national security, defence, public security or other important public interest objective, provided that in this case the exception is expressly covered by a legislative provision, as provided in Article 23 of the GDPR.

1.7.2 RIGHT OF ACCESS

Pursuant to this right, data subjects may request and obtain free of charge confirmation about the processing of their personal data, as well as detailed information regarding the categories of personal data undergoing processing; the source of the data; the specific uses and purposes of processing; the recipients or categories of recipients to whom the data is disclosed, including transfers to third countries or international organisations; the period for which data will be stored or the criteria used to determine that period; the existence of other rights and the right to lodge a complaint with a supervisory authority.

For these purposes, Annex 11 provides a form of response to a data subject's request to exercise his or her right of access.

If a pharmaceutical company processes a large volume of information relating to the data subject which is unrelated to pharmacovigilance activities and the data subject exercises his or her right of access without specifying whether this relates to all of the data or only part of the data, the data subject may be requested, prior to providing the information, to specify the data or processing activities to which the request relates. In particular, the data subject

15 For these purposes, Article 13.3 of the LOPDGDD provides that the exercise of the right to access more than once in six months can be considered repetitive unless there is a legitimate reason for it.

will be asked to specify whether the right is being exercised in respect of data relating to pharmacovigilance activities.

Attached as Annex 12 is a form of notice to be sent to the data subject in these circumstances.

The data controller shall provide a copy of the personal data undergoing processing. In addition, if the data subject makes an electronic request, unless he or she otherwise requests, the information shall be provided in a commonly used electronic form.

The copy referred to above shall be provided in a legible and intelligible form, regardless of the form in which it is provided.

The right of access may be denied, as well as in the circumstances mentioned above, if (i) the request is made by a person other than the data subject or his or her legal representative or a duly accredited volunteer; or (ii) the request is repetitive, in accordance with the abovementioned criteria.

Attached as Annex 13 is a form of response denying the right of access.

The data subject may request more than one copy, but in these circumstances the pharmaceutical company will be able to charge a reasonable fee based on administrative costs.

Persons related to a deceased person by family or de facto ties, as well as their heirs, provided they duly evidence their status by any legally recognised means, may request access to the personal data of the deceased person unless the latter expressly prohibited this, or this is expressly prohibited by law.

If the person requesting access is not in the databases of the pharmaceutical company, it will be sufficient to send him or her a notice informing him or her of the absence of any processing of personal data relating to that person by the pharmaceutical company.

In addition, as provided in the previous section, information relating to the Adverse Event such as, for example, the conclusions reached by the pharmaceutical company in relation thereto, shall not be covered by the right of access and, therefore, such information should not be included in the response to the data subject.

1.7.3 RIGHT TO RECTIFICATION

The exercise of the right to rectification is governed by Article 16 of the GDPR and Article 14 of the LOPDGDD. This right exists when the data subject requests that certain personal data processed by the pharmaceutical company be corrected or amended.

The data subject has the right to have his or her data rectified if they are inaccurate or incomplete, therefore the data controller has an obligation to ensure that such data are updated without undue delay.

This is particularly relevant in the context of pharmacovigilance activities given that the person affected by an adverse event may not request the pharmaceutical company to amend any data unless such data are inaccurate or incomplete. This represents a significant limitation on the exercise of this right since it operates in very specific circumstances such as, for example, in relation to the contact details of the person affected.

Persons related to a deceased person by family or de facto ties, as well as their heirs may, provided they duly evidence their status by any legally recognised means, request the rectification of the personal data of the deceased.

Attached as Annex 14 and Annex 15, respectively, are the responses to be sent by a pharmaceutical company in the event of granting or denying the right to rectification.

1.7.4 RIGHT TO ERASURE

The erasure of data involves data being erased “without undue delay”. Although the GDPR provides six grounds on which the right to erasure exists, some of these do not apply in the case of pharmacovigilance activities.

Thus, the right to erasure based on the withdrawal of the data subject’s consent shall not apply, given that the processing of data is not based on consent but on compliance with a legal obligation.

Nor shall erasure on the grounds of the exercise of the right to object apply, given that the latter is linked by the GDPR to the legal basis contained in points (e) and (f) of Article 6(1) and is not applicable when the legal basis for processing is compliance with a legal obligation, as in the case of pharmacovigilance activities.

Therefore, in the case of pharmacovigilance activities, the right to erasure only applies in the following circumstances:

- If the data are no longer necessary in relation to the purposes for which they were collected.
- If the data have been unlawfully processed.
- If erasure is necessary for compliance with a legal obligation.

Nevertheless, even if the data cease to be useful or necessary in relation to the purposes for which they were collected, they shall not be erased if processing is necessary:

- For exercising the right of freedom of expression and information.
- For complying with a legal obligation[16] which requires processing / retention in accordance with section 1.6 of data imposed by Union or Member State law or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- For reasons of public interest in the area of public health.
- For archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in so far as the right is likely to render impossible or seriously impair the achievement of the objectives of that processing.
- For the establishment, exercise or defence of legal claims.[17]

In the context of pharmacovigilance activities, this right may therefore only be exercised in respect of data not forming part of an Adverse Event in circumstances falling under one of the abovementioned exceptions.

In terms of the consequences of erasure, Article 32 of the LOPDGDD provides that in these circumstances the data shall be blocked, remaining available exclusively to the competent authorities, in particular the data protection authorities, for the enforcement of possible liability arising from processing during the relevant prescription period. The LOPDGDD considers blocking an accountability obligation of the kind envisaged in Article 24 of the GDPR.

While blocked, data must not be modified, processed or manipulated in any other way, and access to its place of storage should be kept restricted.

Finally, it should be noted that the LOPDGDD provides that persons related to a deceased person by family or de facto ties, as well as their heirs, are also entitled to request the erasure of the deceased person’s data.

Attached as Annex 16 and Annex 17, respectively, are the responses to be sent by a pharmaceutical company in the event of granting or denying the right to erasure.

1.7.5 RIGHT TO RESTRICTION OF PROCESSING

This right is contained in Article 18 of the GDPR and in Article 16 of the LOPDGDD.

This right consists of the restriction of the processing of a data subject’s data by the data controller. In view of the characteristics of pharmacovigilance activities, this right can only be exercised if:

- The data subject contests the accuracy of the personal data, in accordance with section 1.7.2 above, for a period enabling the controller to verify the accuracy of the personal data.
- The processing is unlawful, and the data subject opposes the erasure of the personal data and requests the restriction of their use instead.
- The controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims.

If a pharmaceutical company receives a request to restrict processing, it shall transfer the selected data to another processing system, for the purpose of preventing access by users normally authorised to access that data.

In the case of automated processing, restriction of processing shall, in principle, take place by technical means, such that the personal data cannot undergo subsequent processing or be modified, and this shall be made clear in that system.

The right to restriction of processing is an obligation of the data controller. That is to say, the pharmaceutical company must automatically adopt this measure without the need to request and obtain the prior express consent of the data subject, if the abovementioned conditions set out in Article 18(1) of the GDPR are met.

Attached as Annex 18 and Annex 19 are forms for responding to data subjects to notify them of the grant or denial of the right to restriction of processing.

1.7.6 PROCEDURE FOR HANDLING REQUESTS FOR THE EXERCISE OF RIGHTS

Receipt of request to exercise the right of access, rectification, erasure, objection or restriction of processing.

Notification within 24 hours of receipt of the request to the employee or department of the pharmaceutical company

16 Laws on pharmacovigilance activities must be taken into account.

17 During the prescription periods for possible claims by the person concerned or if necessary to claim on behalf of the pharmaceutical company.

responsible for handling such requests of the existence of a request. That employee or department shall assign a number to the request for the purposes of following up and managing.

Verification by the employee or department responsible for handling requests that the request contains the documentation and/or content required by data protection laws. Depending on the right requested, the request must include the following documentation and/or content:

a) Common to all rights:

- Name, surnames and a photocopy of the ID card of the data subject and, if applicable, of the person representing the data subject, as well as documentation proving such representation. The photocopy of the ID card may be substituted by any other legally valid proof of identity.
- The specific request.
- Means for taking any action on the request, including a postal or electronic address for such purposes.
- Date and signature of the person making the request.
- Any documentary evidence relating to the request.

b) Common to the rights of access, rectification and erasure:

- To request the right of access of a deceased person, the heirs, as well as persons related to a deceased person by family or de facto ties, must provide documentation proving their status as such. For this purpose, heirs must attach to the request a copy of the extract of the will of the deceased in which the person making the request appears as an heir or a copy of the extract of the public deed of declaration of heirs in which the status of the person making the request appears. If the person making the request is a person related by family or de facto ties, documentation proving the existence of such ties with the deceased must be provided.

c) Specific to the right to rectification:

- The data subject must specify the inaccurate data and the desired correction.

d) Specific to the rights to erasure and restriction of processing:

- The data subject must specify the reason justifying the erasure or restriction of processing.
- Determination by the person responsible for managing the rights of the merits of the request sent by the data subject.
- Action on the request to erase data or restrict treatment in the period of one month from receipt of the request. Departments having personal data of the person making the request shall be asked to provide the information required to prepare the response. If the need to use the extension provided by the GDPR is anticipated, this should be communicated to the data subject within that period.
- If the request to exercise the rights of erasure or restriction is granted, this shall be made known to the relevant Department in order to carry out the request of the data subject in the systems. The exercise of the right by the data subject should also be made known to recipients to whom the personal data has been disclosed. This shall take place within one month.
- Drafting of response to data subject[18], and sending of notice by any means providing evidence of compliance with the obligation to respond to the exercise of these rights (e.g., certified post, registered fax), unless the pharmaceutical company is obliged to send it by the means requested by the data subject.

18 A response must be given to the data subject in any event, independently of the right exercised by the data subject, of the merits of the request or of the existence/non-existence of the processing of personal data relating to the data subject by a pharmaceutical company.

2. Processing of data relating to adverse events containing coded data

2.1 REPORTING PROCEDURE

2.1.1 REPORTING OF ADVERSE REACTIONS BY HEALTHCARE PROFESSIONALS

If the pharmaceutical company does not take part in the collection of identifying information by HCPs, it shall avoid, as far as possible, access to documentation which could contain identifying information relating to a person affected by an adverse event.

The pharmaceutical company shall prepare internal documentation making its employees aware of the internal methods and procedures relating to its policy of not collecting identifying information relating to those affected by adverse events, as well as how to proceed depending on the communication channel chosen by the HCP.

The employees of the pharmaceutical company who are responsible for collecting information relating the adverse event shall be suitably instructed and informed so that they are aware of:

- The need to avoid the disclosure of identifying information relating to the person affected which could help identify that person (for example: name, surnames, address, telephone number, email, social media nickname, among others).
- The categories of data which are necessary to evaluate and adequately monitor the adverse event experienced by the person affected in accordance with Article 28 of the Implementing Regulation, for example:
  - Place of residence of the reporter and date of the adverse event.
  - Biological data of the person affected which could be necessary to evaluate the adverse event (for example: age, weight, body fat, sex, body mass index, among others).
  - Relevant patient's record (for example: other past or concurrent illnesses, previous adverse reactions, family history, genetic tests, among others);
  - Description of reaction suffered.
  - Time frames relating to the adverse event and consequences suffered or expected.
  - Treatment administered for the adverse event and concomitants.
  - Clinical evolution following treatment.
  - Contact details of HCP.

The personnel of the pharmaceutical company responsible for the external management and handling of information relating to the systems for obtaining and collecting secondary effects shall adapt their action methodology depending on the means of communication employed by the HCP reporting the adverse event:

2.1.1.1 By Telephone

The personnel of the pharmaceutical company shall, whenever possible, initiate the conversation, alerting the HCP to the impossibility of collecting identifying information relating to persons affected by an adverse event. If necessary, the personnel of the pharmaceutical company should advise the HCP as to what data can be collected and what data should be omitted from the description of the event.

If the pharmaceutical company uses automatic voice recording and locution systems, it would be advisable to include a generic warning explaining to the HCP the conditions for describing the adverse event.

If, notwithstanding the above, the HCP provides any identifying information relating to the person affected, the personnel of the pharmaceutical company shall take the following action:

- If the pharmaceutical company does not have recording systems, its personnel shall limit themselves to not recording identifying information of the person affected.
- If the pharmaceutical company does have recording systems for telephone calls, its personnel shall choose to either (a) delete the recording of the call once they have assured themselves that all information required to be able to follow up the adverse event has been collected; or (b) using specialised software, apply noise to those parts of the recording in which the HCP mentions identifying information relating to the person affected and thereafter delete the original recording.

If, despite not having collected identifying information relating to patients who have suffered an adverse event, the pharmaceutical company has recorded the contact details

of the HCP, it must comply with the relevant information obligations in relation to such details.

For these purposes, the HCP should be provided with the information contained in Annex 21.

2.1.1.2 Electronically

Upon receiving an email, t pharmaceutical company personnel must delete any identifying information relating to the person affected using a system that allows such deletion.

The pharmaceutical company personnel shall be instructed to delete any identifying information contained in emails, ensuring that original emails do not remain stored in temporary or sent items folders.

If the pharmaceutical company has its own instant messaging systems, social media or social communication systems on its website or in platforms owned by it (e.g., customer service chats), it must keep a team of administrators responsible for deleting any kind of message or communication which could represent the collection of identifying information relating to a person affected by an adverse event.

Pharmaceutical companies are advised to maintain visible policies for not collecting identifying information relating to persons affected by adverse reactions and to appropriately channel possible notifications. The use of closed files preventing the inclusion of identifying information relating to the person affected shall be considered good practice.

As in the case of notifications received by way of telephone call, pharmaceutical companies must inform HCPs of the processing of their data, as described in Annex 21.

2.1.1.3 Through Social Media

Pharmaceutical company personnel must keep strict control of possible incidents and notifications arising from the company's activity on its own private social media:

- If the information is received by way of private communication from the HCP, he or she must be informed of the pharmaceutical company's guidelines for action in relation to the collection of identifying information, namely, avoiding identifying information relating to the person affected. If the HCP includes a type of identifying information which allows his or her identification, the personnel of the pharmaceutical company must collect and record those data which are necessary for the notification and follow-up of the adverse event.
- If identifying information are collected because the HCP places an enquiry in the public part of the social media network controlled by the pharmaceutical company, the latter shall privately contact the HCP offering him or her information regarding the pharmaceutical company's data collection policy and suggesting that he or she contacts the pharmaceutical company.

In all of these circumstances, the pharmaceutical company shall include the wording contained in Annex 21 in its first communication with the HCP, informing him or her of the processing of his or her personal data.

- If private channels do not exist, the pharmaceutical company shall instruct its personnel to:
  - Collect the data necessary to perform pharmacovigilance tasks.
  - Consider contacting the HCP publicly (for example, by way of a public mention) offering the possibility of contacting the pharmaceutical company.
- If the personnel of the pharmaceutical company are aware of the HCP having made comments in relation to an adverse event in public profiles to third parties, it shall record the data necessary to perform pharmacovigilance tasks.

2.1.1.4 Collection by Ordinary Post

Upon receipt of the letter, the personnel of the pharmaceutical company shall delete any identifying information relating to the person affected or use a mechanism that renders the original message illegible.

It shall be considered good practice to also delete the identifying information of the person affected which appears on the envelope or container of the message, if such envelope or container contains such data.

In compliance with the duty to provide information, the text in Annex 22 should be included in the response acknowledging receipt of the letter sent by the HCP.

2.1.1.5 Collection of Data in Person

Similarly, if an adverse event is reported in person by a HCP, a data collection form may be provided, avoiding the collection of identifying information, or personnel may be instructed to record only information that is necessary for performing pharmacovigilance activities.

In these circumstances, the HCP should be provided with the information in Annex 22.

2.1.2 REPORTING OF ADVERSE EVENTS BY PERSONS AFFECTED BY ADVERSE EVENTS OR THEIR REPRESENTATIVES AND/OR THIRD PARTIES

Pharmaceutical companies must inform their personnel of the policy of not collecting identifying information relating to those affected by adverse reactions.

Pharmaceutical companies shall prepare internal documentation allowing their employees to be familiar with the internal methods and procedures in relation to the policy of not collecting identifying information relating to those affected by adverse reactions or their representatives and/or third parties, as well as how to proceed depending on the channel of communication chosen by the person affected.

Employees of pharmaceutical companies who are in charge of collecting data relating to adverse events shall be suitably instructed and informed so that they are aware of:

- The need to avoid the disclosure of identifying information relating to the person affected which could help identify that person (for example: name, surnames, address, telephone number, email, social media nickname, among others).
- That all enquiries relating to an adverse event made by a person affected, representative or third party should be re-directed to a HCP, whenever possible.
- That, if it is not possible to re-direct the person affected, representative or third party reporting the event to a HCP, contact details of the HCP shall be requested in order to better evaluate the adverse event suffered by the person affected and to follow up the case.
- The list of categories of data which are necessary to evaluate and adequately monitor the adverse event experienced by the person affected, for example:
  - Place of residence of person reporting the adverse event and date of the adverse event.
  - Biological data of the person affected which could be necessary to evaluate the adverse event (for example: age, weight, body fat, sex, body mass index, among others).
  - Relevant patient's record (for example: other past or concurrent illnesses, previous adverse reactions, family history, genetic tests, among others);
  - Description of reaction suffered.
  - Time frames relating to the adverse event and consequences suffered or expected.
  - Treatment administered for the adverse event and concomitants.
  - Clinical evolution following treatment.
  - Contact details of HCP.
- He or she will be required to contact his or her relevant HCP or to contact the pharmaceutical company again, if relevant. For these purposes, and to be able to locate the initial record of the adverse effect, a code may be assigned to him or her in order to be identified in the event of having to make another communication.
- The personnel of the pharmaceutical company responsible for the external management and handling of information relating to the systems for obtaining and collecting secondary effects shall vary their action methodology depending on the means of communication employed by the person affected, representative or third party reporting the adverse event:

2.1.2.1 By Telephone

The personnel of the pharmaceutical company shall, whenever possible, initiate the conversation, alerting the person affected, legal representative or third party reporting the adverse event to the impossibility of collecting identifying information of the persons affected by an adverse event. If necessary, the personnel of the pharmaceutical company should advise the person affected, legal representative or third party reporting the adverse event as to what data can be collected and what data should be omitted from the description of the event.

If the pharmaceutical company uses automatic voice recording and locution systems, it would be advisable to include a generic warning explaining to the person affected, legal representative or third party reporting the adverse event the conditions for describing the adverse event.

If, notwithstanding the above, the person affected, legal representative or third party reporting the adverse event provides any identifying information relating to the person affected, the personnel of the pharmaceutical company shall take the following action:

- If the pharmaceutical company does not have recording systems, its personnel shall limit themselves to not recording the identifying information of the person affected.

- If the pharmaceutical company does have recording systems for telephone calls, its personnel shall choose either to (a) delete the recording of the call once they have assured themselves that all data necessary to follow up the adverse event have been collected; or (b) apply noise, using specialised software, to those parts of the recording in which the person affected, legal representative or third party reporting the adverse event mentions identifying information and, once this system has been applied, delete the original recording.

2.1.2.2 Electronically

Upon receiving an email, a pharmaceutical company's personnel must delete identifying information relating to the person affected or use a mechanism that renders the original message illegible.

The personnel of the pharmaceutical company shall then delete any identifying information contained in emails. They must check that original emails do not remain stored in any temporary or sent item folders and must remove any possible access to that message.

If the pharmaceutical company has its own instant messaging systems, social media or social communication systems on its website or on platforms owned by it (e.g., customer service chats), it must keep a team of administrators responsible for deleting any kind of message or communication which could represent the collection of identifying information relating to a person affected by an adverse event.

Pharmaceutical companies are advised to maintain visible policies for not collecting identifying information relating to persons affected by adverse reactions, legal representatives or third parties reporting adverse events and to appropriately channel possible notifications. The use of closed files preventing the inclusion of identifying information relating to the person affected shall be considered good practice.

2.1.2.3 Through Social Media

Pharmaceutical company personnel must keep strict control of possible incidents and notifications arising from the company's activity in its own private social media:

- If the information is received by way of private communication from the person affected, legal representative or third party reporting the adverse event, he or she must be informed of the pharmaceutical company's guidelines for action in relation to the collection of identifying information, namely, avoiding identifying information relating to the person affected. If the person affected, legal representative or third party reporting the adverse event includes a type of identifying information which allows his or her identification, the personnel of the pharmaceutical company must collect and record those data which are necessary for the notification and follow-up of the adverse event.

- If identifying information are collected because the person affected, legal representative or third party reporting the adverse event places an enquiry in the public part of the social media network, controlled by the pharmaceutical company, the latter shall delete the public comment and, if possible, privately contact the person affected, legal representative or third party reporting the adverse event. The personnel of the pharmaceutical company shall try to contact the person affected, legal representative or third party reporting the adverse event, in order to notify that person of the reasons for deleting the public comment and offering him or her information regarding the pharmaceutical company's data collection policy, pointing out that the collection of identifying information relating to the person affected will be avoided and that only those data necessary to manage the adverse event will be collected.

  If the person affected, legal representative or third party reporting the adverse event should include identifying information again in this private channel, action shall be taken in accordance with the preceding point.

- In the case of public social media, the pharmaceutical company shall instruct its personnel to collect the data necessary to perform pharmacovigilance tasks, mentioning the possibility of contacting the pharmaceutical company.

- If the personnel of the pharmaceutical company are aware of the person affected, legal representative or third party reporting the adverse event having made comments on an adverse event in public profiles of third parties, they shall record the data necessary to perform pharmacovigilance tasks, mentioning the possibility of contacting the pharmaceutical company. If, in the private channel, identifying information relating to the person affected is also communicated, the personnel of the pharmaceutical company shall apply the provisions of section 1.2.3 of this Protocol.

2.1.2.4 Collection by Ordinary Post

Upon receipt of the letter, the personnel of the pharmaceutical company shall delete the identifying information relating to the person affected, legal representative or third party reporting the adverse event, or use any mechanism that renders the original message illegible.

It is also recommended that the envelope containing the message be destroyed if it contains any identifying information relating to the person affected, legal representative or third party reporting the adverse event.

2.1.2.5 Collection of Data in Person

In the event that a person affected, legal representative or third party reports an adverse event in person, the collection of identifying information relating to the person affected should be avoided and personnel should be instructed to record only information that is necessary to perform pharmacovigilance activities.

2.2 COMMON ISSUES

In relation to the coding of identifying information relating to persons affected which may be received from HCPs, the person affected, his or her representatives or third parties, pharmaceutical companies shall create a specialised internal team which continually reviews the procedures established in this Code, adapting its review to the specific circumstances which may arise in its daily activities and correcting any procedural errors which may be discovered.

Pharmaceutical companies must at all times instruct their other employees (i.e., those not responsible for monitoring pharmacovigilance) to re-direct any enquiries from a HCP, person affected, representative and/or third party reporting an adverse event to the pharmacovigilance team. After re-directing the enquiry, they must delete any record or document associated with that enquiry.

As a general rule of communication between pharmaceutical companies and HCPs, persons affected, their representatives or third parties reporting adverse events, in order to be able to locate the initial record of an adverse event, the reporting person shall, if necessary, be assigned a code, which will be associated to the symptoms relating to the adverse event. In this way, if the reporting person needs to communicate further with the pharmaceutical company, reference need only be made to that code, without adding personal data relating to the patient.

2.2.1 LEGAL BASIS FOR THE PROCESSING

As regards the legal basis for processing data relating to HCPs in the context of pharmacovigilance activities with coded data, the provisions of section 1.1 shall apply, the legal basis being compliance with a legal obligation pursuant to Article 6(1)(c) of the GDPR.

2.2.2 RECORD OF PROCESSING ACTIVITIES

Pharmaceutical companies performing pharmacovigilance activities with coded data must maintain a record of processing activities, in physical or electronic format, containing all the information set out in Article 30 of the GDPR. Nevertheless, that record shall only include information relating to the processing of data relating to HCPs in relation to adverse reactions reported to them, and shall specify that health information is coded and that no identifying information relating to patients is included.

2.2.3 RECIPIENTS

2.2.3.1 Access by Third Parties

If a pharmaceutical company subcontracts pharmacovigilance tasks to a CRO, it shall enter into a data processing contract with that CRO which includes at least the following matters:

- All matters specified in Article 28 of the GDPR.

- The obligation to comply with the coding procedure in accordance with this CC.

- Undertakings to comply with personal data protection laws.

- The obligation to undergo periodic audits by the controller or by a third party appointed by the controller.

- The need to have an insurance policy in force for the duration of the contractual relationship covering possible liability in the case of security breaches.

- The liability regime in the event that the processor fails to comply with the provisions of the contract.

Attached as Annex 24 is the minimum content to be included in contracts entered into by pharmaceutical companies carrying out pharmacovigilance activities with coded data with CROs providing them such services.

2.2.3.2 Disclosures

To the extent that pharmaceutical companies perform pharmacovigilance activities with coded data, disclosures

of information relating to adverse reactions which do not include identifying information relating to HCPs may take place without observing any requirements. This is so provided that for the recipient of such information reversing the process of coding would involve a disproportionate effort given that not even the pharmaceutical company which sends the information has identifying information relating to the patients.

If the information disclosed includes identifying information relating to the HCP, the provisions of section 1.4.2 above shall apply.

2.2.4 TRANSFERS TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS OF PERSONAL DATA RELATING TO PERSONS AFFECTED, LEGAL REPRESENTATIVES OR OTHERS

If information relating to adverse reactions is transferred to a third country or international organisation without including identifying information relating to the HCP and the coding procedure described in this CC has been used, it will not be necessary for a pharmaceutical company to adopt the safeguards established in Article 46 of the GDPR provided that it is able to demonstrate that it has performed a procedure for the anonymisation of the data which prevents their re-identification and their connection with identified or identifiable persons in accordance with the provisions of section 3.4 of the Protocol for Clinical Trials and other Clinical Research.

If, however, the information transferred contains identifying information relating to the HCP or in the event that data are incorporated that allow the re-identification of the data subjects, the provisions of section 1.5 of the Protocol for Clinical Trials and other Clinical Research must be observed.

2.2.5 STORAGE LIMITATION PRINCIPLE

Data which has been coded in accordance with the provisions of this Code may be retained for a period of ten years, in accordance with pharmacovigilance legislation.

As regards personal data relating to HCPs, the provisions of section 1.6 shall be observed.

2.2.6 EXERCISE OF RIGHTS

Given in these circumstances neither pharmaceutical companies nor CROs to which they may subcontract pharmacovigilance activities will be able to materially access identifying information relating to persons affected by adverse reactions, they will not be able to deal with requests for the exercise of rights sent by them.

Nevertheless, although pharmaceutical companies cannot deal with such requests, they have an obligation to reply to anyone making a request informing them that they have no data in their records.

Attached as Annex 25 is a form of response which should be used to respond to requests for the exercise of rights.

If the request to exercise rights comes from a HCP, it should be handled in accordance with the provisions of the section on the exercise of pharmacovigilance rights with identifying information.

Annex 1:
Telephone information on data processing for the purpose of notifying the pharmacovigilance department

Your data will be processed by [*] for the purpose of notifying the Pharmacovigilance Department of your call and allowing it to contact you. You may exercise your rights, as well as request additional information relating to the processing of your data.

If additional information is requested, the following message should be provided:

The data will be stored until the Pharmacovigilance Department contacts you to deal with your call and, thereafter, for as long as may be required in order to comply with a legal obligation or deal with any liabilities which may arise as a result of processing.

You may exercise your rights of access, rectification, erasure and restriction of processing by contacting [*] by way of [*], giving your name and surnames and attaching a copy of your National Identity Card (DNI) or equivalent document or by lodging a complaint with the Spanish Data Protection Agency (the Agencia Española de Protección de Datos) on its website **www.aepd.es**.

We hereby inform you that [*] has adhered to the Code of Conduct Regulating the Processing of Personal Data in Clinical Trials and Other Clinical Research and Pharmacovigilance Activities, sponsored by FARMAINDUSTRIA and approved by the Spanish Data Protection Agency (the Agencia Española de Protección de Datos) and that you may lodge a complaint with the Code of Conduct Governance Body addressed to [****].

19 Reference should be made to any international transfers of data, and the safeguards adopted in accordance with the GDPR and this Code of Conduct.

Annex 2:
Telephone information on data processing for the purpose of managing an adverse event reported by a patient or patient's legal representative

We will process your data in order to manage the adverse event. You may exercise your rights, as well as access additional information by [pressing [*]/listening to the information] after the call has ended.

Please provide us with the contact details of the HCP who has information relating to the adverse event.

The following message should be provided with the additional information:

Your data will be processed by [*] for the purpose of managing the adverse event on the basis of compliance with a legal obligation by [*].

[*] will not disclose your data to third parties unless this is necessary for compliance with the legal obligations of [*] and the group to which it belongs in relation to pharmacovigilance. Our provider of pharmacovigilance services will be able to access the data[20].

The data will be stored until the Pharmacovigilance Department contacts you to deal with your call and, thereafter, for as long as may be required in order to comply with a legal obligation or deal with any liabilities which may arise as a result of processing. You may exercise your rights of access, rectification, erasure and restriction of processing by contacting [*] by way of [*], giving your name and surnames and attaching a copy of your National Identity Card (DNI) or equivalent document or by lodging a complaint with the Spanish Data Protection Agency (the Agencia Española de Protección de Datos) on its website **www.aepd.es**.

We hereby inform you that [*] has adhered to the Code of Conduct Regulating the Processing of Personal Data in Clinical Trials and Other Clinical Research and Pharmacovigilance Activities, sponsored by FARMAINDUSTRIA and approved by the Spanish Data Protection Agency (the Agencia Española de Protección de Datos) and that you may lodge a complaint with the Code of Conduct Governance Body addressed to [****].

20 Reference should be made to any international transfers of data, and the safeguards adopted in accordance with the GDPR and this Code of Conduct.

Annex 3:
Telephone information on data processing for the purpose of managing an adverse event reported by a third party

We will process your data and data relating to the patient in order to manage the adverse event. You may exercise your rights, as well as access additional information by [pressing [*]/listening to the information] after the call has ended.

Please provide us with the contact details of the HCP who has information relating to the adverse event.

The following message should be provided with the additional information:

Your data and data relating to the patient will be processed by [*] for the purpose of managing the adverse event on the basis of compliance with a legal obligation by [*].

[*] shall not disclose your data to third parties unless this is necessary for compliance with the legal obligations of [*] and the group to which it belongs in relation to pharmacovigilance. Our provider of pharmacovigilance services will be able to access the data[21].

The data will be stored until the Pharmacovigilance Department contacts you to deal with your call and, thereafter, for as long as may be required in order to comply with a legal obligation or deal with any liabilities which may arise as a result of processing. You may exercise your rights of access, rectification, erasure and restriction of processing by contacting [*] by way of [*], giving your name and surnames and attaching a copy of your National Identity Card (DNI) or equivalent document or by lodging a complaint with the Spanish Data Protection Agency (the Agencia Española de Protección de Datos) on its website **www.aepd.es**.

We hereby inform you that [*] has adhered to the Code of Conduct Regulating the Processing of Personal Data in Clinical Trials and Other Clinical Research and Pharmacovigilance Activities, sponsored by FARMAINDUSTRIA and approved by the Spanish Data Protection Agency (the Agencia Española de Protección de Datos) and that you may lodge a complaint with the Code of Conduct Governance Body addressed to [****].

21 Reference should be made to any international transfers of data, and the safeguards adopted in accordance with the GDPR and this Code of Conduct.

Annex 4:
Telephone information on data processing for the purpose of managing an adverse event reported by a healthcare professional

In order to manage the adverse event, we will need your data and data relating to the patient. You may exercise your rights, as well as access additional information relating to processing by [pressing [*]/listening to the information] after the call has ended.

The following message should be provided with the additional information:

Your data and data relating to the patient will be processed by [*] for the purpose of managing the adverse event on the basis of compliance with a legal obligation by [*].

[*] shall not disclose your data to third parties unless this is necessary for compliance with the legal obligations of [*] and the group to which it belongs in relation to pharmacovigilance. Our provider of pharmacovigilance services will be able to access the data[22].

The data will be stored until the Pharmacovigilance Department contacts you to deal with your call and, thereafter, for as long as may be required in order to comply with a legal obligation or deal with any liabilities which may arise as a result of processing. You may exercise your rights of access, rectification, erasure and restriction of processing by contacting [*] by way of [*], giving your name and surnames and attaching a copy of your National Identity Card (DNI) or equivalent document or by lodging a complaint with the Spanish Data Protection Agency (the Agencia Española de Protección de Datos) on its website **www.aepd.es**.

We hereby inform you that [*] has adhered to the Code of Conduct Regulating the Processing of Personal Data in Clinical Trials and Other Clinical Research and Pharmacovigilance Activities, sponsored by Farmaindustria and approved by the Spanish Data Protection Agency (the Agencia Española de Protección de Datos) and that you may lodge a complaint with the Code of Conduct Governance Body addressed to [****].

22 Reference should be made to any international transfers of data, and the safeguards adopted in accordance with the GDPR and this Code of Conduct.

Annex 5:
Electronic information on data processing for the purpose of managing an adverse event reported by a patient or patient's legal representative

Controller: [*]. Data protection officer: [include contact details of DPO if there is one]. **Purpose and legal basis**: your data will be processed for the purpose of managing the adverse event on the basis of compliance with a legal obligation by [*]. **Recipients:** [*] shall not disclose your data to third parties, [although our provider of pharmacovigilance services will be able to access your data][23]. **Storage:** the data will be stored until the adverse event is managed and, thereafter, for as long as may be required in order to comply with a legal obligation or deal with any liabilities which may arise as a result of processing. **Rights:** you may exercise your rights of access, rectification, erasure and restriction of processing by contacting [*] by way of [*], giving your name and surnames and attaching a copy of your National Identity Card (DNI) or equivalent document or by lodging a complaint with the Spanish Data Protection Agency (the Agencia Española de Protección de Datos) on its website **www.aepd.es**. **Additional information:** [*] has adhered to the Code of Conduct Regulating the Processing of Personal Data in Clinical Trials and Other Clinical Research and Pharmacovigilance Activities, sponsored by Farmaindustria and approved by the Spanish Data Protection Agency (the Agencia Española de Protección de Datos) and you may lodge a complaint with the Code of Conduct Governance Body addressed to [****].

Please provide us with the contact details of the HCP who has information relating to the adverse event.

23 Reference should be made to any international transfers of data, and the safeguards adopted in accordance with the GDPR and this Code of Conduct.

Annex 6:
Electronic information on data processing for the purpose of managing an adverse event reported by a third party

Controller: [*]. Data protection officer: [include contact details of DPO if there is one]. **Purpose and legal basis:** your data and data relating to the patient will be processed for the purpose of managing the adverse event on the basis of compliance with a legal obligation by [*]. **Recipients:** [*] shall not disclose your data to third parties, [although our provider of pharmacovigilance services will be able to access your data][24]. **Storage:** the data will be stored until the adverse event is managed and, thereafter, for as long as may be required in order to comply with a legal obligation or deal with any liabilities which may arise as a result of processing. **Rights:** you may exercise your rights of access, rectification, erasure and restriction of processing by contacting [*] by way of [*], giving your name and surnames and attaching a copy of your National Identity Card (DNI) or equivalent document or by lodging a complaint with the Spanish Data Protection Agency (the Agencia Española de Protección de Datos) on its website **www.aepd.es**. **Additional information:** [*] has adhered to the Code of Conduct Regulating the Processing of Personal Data in Clinical Trials and Other Clinical Research and Pharmacovigilance Activities, sponsored by Farmaindustria and approved by the Spanish Data Protection Agency (the Agencia Española de Protección de Datos) and you may lodge a complaint with the Code of Conduct Governance Body addressed to [****].

Please provide us with the contact details of the HCP who has information relating to the adverse event, as well as those of the patient.

24 Reference should be made to any international transfers of data, and the safeguards adopted in accordance with the GDPR and this Code of Conduct.

Annex 7:
Electronic information on data processing for the purpose of managing an adverse event reported by a healthcare professional

[Controller: [*]. **Data protection officer:** [include contact details of DPO if there is one]. **Purpose and legal basis:** your data and data relating to the patient will be processed for the purpose of managing the adverse event on the basis of compliance with a legal obligation by [*]. **Recipients:** [*] shall not disclose your data to third parties, [although our provider of pharmacovigilance services will be able to access your data][25]. **Storage:** the data will be stored until the adverse event is managed and, thereafter, for as long as may be required in order to comply with a legal obligation or deal with any liabilities which may arise as a result of processing. **Rights:** you may exercise your rights of access, rectification, erasure and restriction of processing by contacting [*] by way of [*], giving your name and surnames and attaching a copy of your National Identity Card (DNI) or equivalent document or by lodging a complaint with the Spanish Data Protection Agency (the Agencia Española de Protección de Datos) on its website **www.aepd.es**. **Additional information:** [*] has adhered to the Code of Conduct Regulating the Processing of Personal Data in Clinical Trials and Other Clinical Research and Pharmacovigilance Activities, sponsored by Farmaindustria and approved by the Spanish Data Protection Agency (the Agencia Española de Protección de Datos) and you may lodge a complaint with the Code of Conduct Governance Body addressed to [****].

25 Reference should be made to any international transfers of data, and the safeguards adopted in accordance with the GDPR and this Code of Conduct.

Annex 8:
Form of response to a data subject requesting the amendment of a request

Dear Sir/Madam,

We acknowledge receipt of your request for [access, rectification, erasure, restriction of processing] pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

However, in accordance with the abovementioned regulation, in order to be able to deal with your request properly, it must contain [specify as relevant]:

- Your name and surnames
- A photocopy of your national identity document or evidence of your identity or the power pursuant to which you act
- Your specific request
- An address for the purpose of notices
- Any documentary evidence supporting your request
- The date and your signature

Please do not hesitate to contact us if you need any clarification regarding the above. We hereby inform you of your right to lodge a complaint with the Spanish Data Protection Agency (Agencia Española de Protección de Datos).

Sincerely,

Signed _____

(Position)

Annex 9:
Form of response to a data subject where necessary to extend the legal deadline for responding to a request to exercise rights

Dear Sir/Madam,

We are aware that you have exercised your [right of access, contained in Article 15 / right to rectification, contained in Article 16 / right to erasure, contained in Article 17 / right to restriction of processing, contained in Article 18] of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

We confirm that we are currently managing your request in accordance with the legislation currently in force. However, we would like to inform you that this will take longer than anticipated due to [include reason for delay], which has caused a delay in processing your request.

We would also like to inform you that we are employing our best efforts to deal with your request as quickly as possible and that, once we have finished, we will be in touch with you as soon as possible, and in any event no later than three months following the date on which we received your request, in order to confirm the result.

If you have any further questions, please contact us at [include email address].

Please do not hesitate to contact us if you need any clarification regarding the above. We hereby inform you of your right to lodge a complaint with the Spanish Data Protection Agency (Agencia Española de Protección de Datos).

Sincerely,

Signed _____

(Position)

Annex 10:
Form of notice from a CRO to a data subject informing them that their request has been forwarded to the pharmaceutical company

Dear Sir/Madam,

We are aware that you have exercised your [right of access, contained in Article 15 / right to rectification, contained in Article 16 / right to erasure, contained in Article 17 / right to restriction of processing, contained in Article 18] of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

We hereby inform you that we cannot satisfy your request given that we process your personal data as data processors for [*], which is your personal data controller. We have, however, forwarded your request to [*] in order to deal with it.

Please do not hesitate to contact us if you need any clarification regarding the above. We hereby inform you of your right to lodge a complaint with the Spanish Data Protection Agency (Agencia Española de Protección de Datos).

Sincerely,

Signed _____

(Position)

Annex 11:
Form of response granting right of access

Dear Sir/Madam,

We are aware that you have exercised your right of access, contained in Article 15 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, by way of [*] (the "[*]").

We hereby inform you that we have considered your request and, in accordance with the abovementioned regulation, we attach as Annex 1 a copy of your personal data in our database of [*].

We hope that the information we have provided is of interest to you and satisfies your request in full.

We remind you that you may exercise your right of rectification, erasure or restriction of processing of your personal data in writing, attaching a copy of your National Identity Card (DNI) or other evidence of your identity, to [*] (include postal address). We also inform you that you may, if you consider it necessary, lodge a complaint with the Spanish Data Protection Agency (the Agencia Española de Protección de Datos).

Sincerely,

Signed _____

(Position)

Annex 1:

1. Processed data:
2. Source: [Whether the data have been collected from the data subject or from other sources. If the latter, specify source]
3. Recipients: [Including any international transfers and safeguards for performing them]
4. Purpose of processing:
5. Category of data processed:
6. Storage period:
7. Existence of individual automated decision-making and profiling, as well as the logic involved:

Annex 12:
Form of notice if large volumes of data are processed

Dear Sir/Madam,

We acknowledge receipt of your request to exercise your right of access pursuant to Article 15 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

We hereby inform you that we are dealing with your request. However, we would be grateful if you could specify the personal data which you would like to access and, in particular, if you would like to access any personal data relating to an adverse event.

Please do not hesitate to contact us if you need any clarification regarding the above. We hereby inform you of your right to lodge a complaint with the Spanish Data Protection Agency (Agencia Española de Protección de Datos).

Sincerely,

Signed _____

(Position)

Annex 13:
Form of response denying right of access

Dear Sir/Madam,

We acknowledge receipt of your request for access pursuant to Article 15 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, by way of [*].

We hereby inform you that we have been unable to satisfy your request, [select relevant option: (a) given that it is an essential requirement that the right be exercised by the data subject and you have not provided proof of your authority to act on his or her behalf / (b) given that you exercised your right of access on *** and less than six months have passed since such request. We refer to the response to that request sent by *** on ***.][26]

[If data relating to the person making the request is not being processed: we hereby inform you that no data relating to you appears in our information systems.]

Please do not hesitate to contact us if you need any clarification regarding the above. We hereby inform you of your right to lodge a complaint with the Spanish Data Protection Agency (Agencia Española de Protección de Datos).

Sincerely,

Signed _____

(Position)

26 If a system of remote, direct, permanent and secure access to personal data is established, this could be notified, denying the request for access.

Annex 14:
Form of response granting right to rectification

Dear Sir/Madam,

We are aware that you have exercised your right to rectification, contained in Article 16 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, by way of [*].

We hereby inform you that we have considered your request and that we have proceeded to rectify your data as requested by you, in accordance with personal data protection laws.

Please do not hesitate to contact us if you need any further information or clarification regarding the above.

Sincerely,

Signed _____

(Position)

Annex 15:
Form of response denying right to rectification

Dear Sir/Madam,

We are aware that you have exercised your right to rectification, contained in Article 16 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, by way of [*].

We hereby inform you that we have been unable to satisfy your request to rectify your personal data given that the data you have requested us to rectify *[are not inaccurate / incomplete*,], given that *[include an explanation, if necessary]*.

Please do not hesitate to contact us if you need any clarification regarding the above. We hereby inform you of your right to lodge a complaint with the Spanish Data Protection Agency (Agencia Española de Protección de Datos).

Sincerely,

Signed _____

(Position)

Annex 16:
Form of response granting right to erasure

Dear Sir/Madam,

We are aware that you have exercised your right to erasure, contained in Article 17 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, by way of [*].

We hereby inform you that we have considered your request and that we have proceeded to erase all personal data relating to you which we held, in accordance with personal data protection laws and the terms of the above mentioned article.

Please do not hesitate to contact us if you need any clarification regarding the above.

Sincerely,

Signed _____

(Position)

Annex 17:
Form of response denying right to erasure

Dear Sir/Madam,

We are aware that you have exercised your right to erasure, contained in Article 17 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, by way of [*].

We hereby inform you that we cannot satisfy your request to physically erase or eliminate your person data given that the data you request to be erased *[are necessary for reasons of public interest / must be stored for compliance with a legal obligation by [*]/ must be stored for the establishment, exercise or defence of legal claims].* We will, however, store such data exclusively for that purpose and, once fulfilled, we will proceed to their erasure.

[If data relating to the person making the request is not being processed: we hereby inform you that no data relating to you appears in our information systems.]

Please do not hesitate to contact us if you need any clarification regarding the above. We hereby inform you of your right to lodge a complaint with the Spanish Data Protection Agency (Agencia Española de Protección de Datos).

Sincerely,

Signed _____

(Position)

Annex 18:
Form of response granting right to restriction of processing

Dear Sir/Madam,

We are aware that you have exercised your right to restriction of processing, contained in Article 18 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, by way of [*].

We hereby inform you that we have considered your request and that we have proceeded to restrict the processing of your data as requested by you, in accordance with personal data protection laws.

[If the processing of data has been restricted due to the accuracy of that data having been contested, include: *"We hereby inform you that the restriction of processing of your data shall remain in place until ***, the period necessary to verify the accuracy of such data."*]

Please do not hesitate to contact us if you need any clarification regarding the above.

Sincerely,

Signed _____

(Position)

Annex 19:
Form of response denying right to restriction of processing

Dear Sir/Madam,

We are aware that you have exercised your right to restriction of processing, contained in Article 18 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, by way of [*].

We regret to inform you that we cannot grant your request to restrict processing of your data, as requested by you, given that the circumstances of your request do not match any of the circumstances required by law to exist for such purposes. In particular, [*the accuracy of the data is not being contested / the processing of the data by [*] continues to be necessary for the management of the Adverse Event]*.

Please do not hesitate to contact us if you need any clarification regarding the above. We hereby inform you of your right to lodge a complaint with the Spanish Data Protection Agency (Agencia Española de Protección de Datos).

Sincerely,

Signed _____

(Position)

Annex 20:
Telephone information on data processing for the purpose of managing an adverse event with coded data for a healthcare professional

In order to manage the adverse event, we will need your data. You may exercise your rights, as well as access additional information relating to processing by [pressing [*]/listening to the information] after the call has ended.

The following message should be provided with the additional information:

Your data will be processed by [*] for the purpose of managing the adverse event on the basis of compliance with a legal obligation by [*].

[*] shall not disclose your data to third parties, [although our provider of pharmacovigilance services will be able to access your data] and will be stored until the adverse event is managed and, thereafter, for as long as may be required in order to comply with a legal obligation or deal with any liabilities which may arise as a result of processing.

You may exercise your rights of access, rectification, erasure and restriction of processing by contacting [*] by way of [*], giving your name and surnames and attaching a copy of your National Identity Card (DNI) or equivalent document or by lodging a complaint with the Spanish Data Protection Agency (the Agencia Española de Protección de Datos) on its website **www.aepd.es.**

Annex 21:
Electronic information on data processing for the purpose of managing an adverse event with coded data for a healthcare professional

Controller: [*]. **Purpose and legal basis:** your data will be processed for the purpose of managing the notification of the adverse event on the basis of compliance with a legal obligation by [*]. **Recipients:** [*] shall not disclose your data to third parties, although our provider of pharmacovigilance services will be able to access your data. **Storage:** your data will be stored until the adverse event is managed and, thereafter, for as long as may be required in order to comply with a legal obligation or deal with any liabilities which may arise as a result of processing. **Rights:** you may exercise your rights of access, rectification, erasure and restriction of processing by contacting [*] by way of [*], giving your name and surnames and attaching a copy of your National Identity Card (DNI) or equivalent document or by lodging a complaint with the Spanish Data Protection Agency (the Agencia Española de Protección de Datos) on its website **www.aepd.es.**

Annex 22:
Information by ordinary post and in person on data processing for the purpose of managing an adverse event with coded data for a healthcare professional

Your data will be processed by [*] for the purpose of managing the notification of the adverse event on the basis of compliance with a legal obligation by [*]. Your data will not be disclosed to third parties, although our provider of pharmacovigilance services will be able to access your data. [*] will store your data until the adverse event is managed and, thereafter, for as long as may be required in order to comply with a legal obligation or deal with any liabilities which may arise as a result of processing. You may exercise your rights of access, rectification, erasure and restriction of processing by contacting [*] by way of [*], giving your name and surnames and attaching a copy of your National Identity Card (DNI) or equivalent document or by lodging a complaint with the Spanish Data Protection Agency (the Agencia Española de Protección de Datos) on its website **www.aepd.es.**

Annex 23:
Form of record of processing activities relating to pharmacovigilance

NAME AND CONTACT DETAILS	
Data Controller	[*] TAXPAYER ID (CIF):
Address	[*]

THE CONTACT DETAILS OF THE DPO

DESCRIPTION OF PROCESSING
[*]

PURPOSE OF PROCESSING
[*]

LEGAL BASIS FOR THE PROCESSING

FORMAT IN WHICH RECORD IS KEPT
[Digital/paper] format

DESCRIPTION OF CATEGORIES	
Of data subjects	[*]
Of personal data	[*]

RECIPIENTS	
Identification	[*]

▶ next page

ENVISAGED TIME LIMITS FOR THE ERASURE OF DIFFERENT CATEGORIES OF DATA
[*]

TRANSFERS OF DATA TO THIRD COUNTRIES	
Name of country or international organisation	[*]

GENERAL DESCRIPTION OF TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

Duty of confidentiality and secrecy

- *[Describe measures which seek to avoid access by unauthorised persons to personal data collected, for example, restrict access to hard drives and servers storing images to authorised personnel.]*

Rights of data holders

- *[Describe procedure employed by the organisation to deal with requests by data subjects to exercise their rights.]*

Security breaches relating to personal data

- *[Describe procedure employed by the organisation to deal with security breaches.]*

Safeguarding duty

- *[Describe technical measures adopted to ensure the safeguarding of personal data, for example, security copies, technical measures to avoid external access to organisation's systems, computer anti-virus updates, data encryption, etc.]*

Identification

- *[Describe organisational measures adopted to ensure that those accessing data are authorised to do so, for example, description of the functions of personnel who may access that data, passwords, etc.]*

Annex 24:
Minimum content for contracts entered into by pharmaceutical companies with CROS performing pharmacovigilance activities with coded data

The Service Provider represents and warrants that it will process all data relating to pharmacovigilance activities, including data relating to both persons affected and HCPs associated with an adverse event (the "**Personal Data**") in accordance with the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and Organic Law 3/2018, of 5 December 2018, on the Protection of Personal Data and Guarantee of Digital Rights.

Access by the Service Provider to Personal Data is necessary in order to be able to provide the Services. The Service Provider will therefore be a processor of such data. Such access will not be considered a disclosure of Personal Data, but access required to provide the services subject to this Contract.

The Personal Data processed will relate to the following categories of data subjects [complete] and the following categories of data [complete].

The Service Provider will process the Personal Data exclusively for the purposes of providing pharmacovigilance activity management services to the pharmaceutical company in accordance with any instructions issued in writing by the latter and shall not under any circumstances use such data for any other purposes. The Service Provider will immediately notify the pharmaceutical company if it considers that any instruction provided by the latter infringes any provision of personal data protection laws and, in particular, if an instruction involves access by the pharmaceutical company to identifying information relating to the persons affected.

The Service Provider shall not disclose the Personal Data to any third party, not even for storage, unless such disclosure has been previously authorised by the pharmaceutical company expressly.

The Service Provider shall keep a written record (including in electronic form) of processing activity carried out on behalf of the pharmaceutical company pursuant to this contract.

If the pharmaceutical company decides to carry out a data protection impact assessment evaluating, in particular, the origin, nature, particularity and severity of processing which could involve a risk for the rights and freedoms of natural persons as envisaged in the legislation, the Service Provider undertakes to actively assist and cooperate with the pharmaceutical company in carrying out such an assessment taking into account the nature of the processing and the information at its disposal.

The Service Provider shall adopt technical and organisational security measures to ensure an adequate level of security, including confidentiality, taking into account the state of the art and the costs of implementation with respect to the risks to which the Personal Data are exposed as a result of their processing by the Service Provider.

When assessing the risk in relation to the security of the Personal Data, the Service Provider shall take into account the risks arising from the processing of the Personal Data, such as accidental or unlawful destruction, loss or alteration of the Personal Data transmitted, stored or otherwise processed, or the unauthorised disclosure of, or access to, the Personal Data which could give rise to physical, material or non-material loss or damage.

In the event of (i) loss or undue use of the Personal Data, (ii) unauthorised or unlawful processing, disclosure, access, alteration, corruption, transfer, sale, rental, destruction or involuntary use of the Personal Data or (iii) any other event which compromise or could compromise the security, confidentiality or integrity of the Personal Data (a "**Security Breach**"), the Service Provider shall notify the pharmaceutical company of such event without undue delay and, in any event, no later than thirty-six (36) hours after becoming aware of the Security Breach. If the pharmaceutical company is not notified within such period, the Service Provider shall provide the pharmaceutical company with a reasoned explanation for the delay.

If, in accordance with personal data protection laws, the Security Breach must be notified to the data subjects, the Service Provider shall provide such notification, expressly indicating that it is being provided on behalf of the pharmaceutical company. Without prejudice to the foregoing, the pharmaceutical company may determine the correction mechanisms to be implemented by the Service Provider with respect to the reasons for the Security Breach.

If the pharmaceutical company authorises the Service Provider to subcontract certain services to a third party, the Service Provider shall enter into a contract with the personal data protection obligations contained in this clause with that third party.

If the Service Provider receives a request from the data subjects in relation to the exercise of their rights of access, rectification, erasure or restriction of processing of the Personal Data, it shall deal with such request in accordance with applicable data protection laws and, in any event, in strict compliance with the deadlines established therein.

The Service Provider shall, after finishing the provision of services, return to the pharmaceutical company or destroy, as requested by the latter, any Personal Data to which it has had access in the form in which it is held at that time. The Service Provider may, however, keep the Personal Data, duly blocked, for as long as necessary to deal with possible liability which may arise from the processing or for compliance with any legal obligations to which the Service Provider may be subject.

The Service Provider shall make available to the pharmaceutical company all information necessary for the latter, whether directly or through a third party, to verify the degree of compliance by the Service Provider with the obligations in this clause and shall cooperate actively to achieve this.

The Service Provider shall not provide the pharmaceutical company with personal data relating to an adverse event unless such data have been subject to a prior coding procedure such that the pharmaceutical company is unable to identify the data subject whose data are provided.

Annex 25:
Form of response to requests for the exercise of rights received by pharmaceutical companies performing pharmacovigilance activities with coded data

Dear Sir/Madam,

We are aware that you have exercised your [right of access, contained in Article 15 / right to rectification, contained in Article 16 / right to erasure, contained in Article 17 / right to restriction of processing, contained in Article 18] of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

We hereby inform you that we have been unable to satisfy your request given that, for the performance of pharmacovigilance activities, we only process coded data, and it is not therefore possible to identify you.

You may contact [*], our provider of pharmacovigilance services, by way of [include means of contact] in order to exercise any of your rights.

Please do not hesitate to contact us if you need any clarification regarding the above. We hereby inform you of your right to lodge a complaint with the Spanish Data Protection Agency (Agencia Española de Protección de Datos).

Sincerely,

Signed _____

(Position)

farmaindustria

Código de Conducta

DATOS PERSONALES

María de Molina, 54, 7ª / 28006 Madrid
T. +34 91 515 93 50
codigoprotecciondatos.farmaindustria.org