PRIVACY POLICY

linea directa

Línea Directa Group Privacy Policy

Important information about this document	
Name of the Policy	Línea Directa Aseguradora Group General Privacy Policy
Business unit or function affected	Línea Directa Group companies
Personnel affected	Línea Directa Group employees
Main area responsible for monitoring	Data Protection Office
Approved on	28 June 2022
Effective from	28 June 2022
Version	Version 3.1
Adjustments	Some references in Section 3.1; 3.5; 3.6; 4.1.2; 4.1.3; 4.1.4
Created by	Data Protection Office
Approved by	Board of Directors

Contents

1. Introduction

1.1. Regulatory framework

The content of this Policy complies with the provisions of Regulation 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 ("**GDPR**"), as well as with the provisions of Organic Law 3/2018 of 27 December 2018 on the Protection of Personal Data and the Guarantee of Digital Rights. In the event of contradiction between the provisions of this Policy and the provisions of the regulations applicable at any given time, the latter will ultimately prevail.

1.2. Basic concepts

For the purposes of this Policy, the following basic concepts will be taken into account:

- Personal data: any information relating to an identified or identifiable natural person. An identifiable natural person is any person whose identity can be established, directly or indirectly, in particular by means of an identifier such as a name, an ID number, location data, an online identifier or one or more elements of that person's physical, physiological, genetic, mental, economic, cultural or social identity.
- Processing: any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automatic means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- Profiling: any form of automated processing of personal data consisting of using personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's professional performance, financial situation, health, personal preferences, interests, reliability, behaviour, location or movements.
- Controller: the natural or legal person, public authority, service or other body which alone or jointly with others determines the purposes and means of processing; if European Union or Member State law determines the purposes and means of processing, the controller or the specific criteria for its nomination may be laid down by European Union or Member State law.
- Processor: the natural or legal person, public authority, service or other body processing personal data on behalf of the controller.
- Consent of the data subject: any freely given, specific, informed and unambiguous indication of the data subject's agreement, either by a statement or by a clear affirmative action, to the processing of personal data relating to them.

- Breach of personal data security: any breach of security leading to the accidental or unlawful destruction, loss or alteration of, or unauthorised disclosure of or access to, personal data transmitted, stored or otherwise processed.
- Health-related data: personal data concerning the physical or mental health of a natural person, including the provision of health care services, revealing information about their health status.

2. Scope

2.1. Data controller

The personal data controller shall be the legal person who determines the purposes and means of the personal data processing.

When two or more controllers jointly determine the purposes and means of the processing, they shall be considered jointly responsible for the processing. If a situation of co-responsibility arises that affects any of the controllers to whom this Policy is applicable, a binding agreement must be formalised for all co-responsible parties in which the responsibilities and obligations of each of them in relation to compliance with the GDPR are clearly determined. In particular, the agreement shall specify:

- The responsibilities of each of the co-responsible parties in relation to the handling of requests for the exercise of rights by data subjects. In any event, data subjects may exercise their rights with respect to, and against, each of the co-responsible parties.
- The obligations of each of the co-responsible parties in relation to the provision of information to data subjects.

The essential aspects of this agreement shall be made available to data subjects.

2.2. Group companies subject to this Policy

This Policy shall apply to the following controllers:

- Línea Directa Asistencia, S.L.U.
- Moto Club LDA S.L.U.
- Advanced Repair Centre CAR, S.L.U.
- LD Activos, S.L.U.
- Ambar Medline, S.L.U.
- LD Reparaciones, S.L.U.

Any new processing activity planned within the Línea Directa Group must precisely identify the legal entity that will be responsible for the processing.

3. General principles

3.1. Lawfulness, loyalty and transparency

1. All Línea Directa Group employees are obliged to ensure that the processing of personal data carried out within the scope of their duties respects the principles of lawfulness, loyalty and transparency in relation to data subjects.
2. The principle of lawfulness implies that any processing carried out by controllers is generally lawful under the applicable legal system. In particular, in order for the processing to be lawful under the GDPR and other data protection legislation, it must be possible to demonstrate that one of the legitimate bases for processing exists and that this legitimate basis is being used in accordance with the applicable requirements. The legal bases and requirements for each case are set out in section 4.2 of this Policy.
3. In order to comply with the principles of lawfulness and transparency, the controller shall provide data subjects with adequate and sufficient information on how the data controllers process their personal data.

   Data controllers subject to this policy shall comply with the information obligations regarding data protection established in the GDPR and in any other applicable regulations, including sectoral regulations. The specific content of the reporting obligations is set out in section 4.3 of this Policy.
4. All Línea Directa Group employees will be obliged to report to the DPO any conduct that, in their opinion, may jeopardise compliance with the principles set out above.

3.2. Purpose limitation

The purpose limitation principle implies that the following issues should be taken into account in relation to the collection and further processing of personal data:

- The data must be collected for specified, explicit and legitimate purposes.
- Data subjects must be clearly informed of these purposes at the time of data collection.
- Data may only be processed for the purposes for which they were originally collected.
- When data are to be processed for purposes other than those for which they were originally collected, the data subjects must be informed and the lawfulness of the processing must be ensured.

3.3. Data minimisation

Only data necessary for the purposes of the processing which have been defined and of which the data subjects have been informed may be collected, stored and processed.

The data currently permitted for use in the Línea Directa Group are those included in the Record of Processing Activities.

Before initiating any new processing or amending an existing processing operation, consideration must be given to what data are necessary for the purpose for which the processing is to be carried out and the opinion of the DPO on this matter must be sought.

3.4. Accuracy

The data processed by the data controllers subject to this Policy shall be accurate and up to date. Without prejudice to the data subjects' rights of erasure and rectification, reasonable steps should be taken to rectify or erase data that may be inaccurate or unsuitable for the purposes for which they are processed.

3.5. Limitation of the retention period

Personal data may not be kept for longer than is necessary for the purposes for which they were collected, without prejudice to the obligation to block these data prior to their definitive erasure. The criteria applicable to the retention of personal data and the obligation to block are set out in section 4.1.6 of this Policy.

3.6. Integrity and confidentiality

Personal data shall be processed in such a way as to ensure an appropriate level of security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, by implementing appropriate technical or organisational measures. Details of the measures implemented to ensure the security of personal data are set out in section 4.3 and 4.4.4 of this Policy.

3.7. Privacy by design and by default.

The GDPR includes the obligation to consider privacy requirements from the early stages of designing products and services. Therefore, from the outset of personal data processing, attention must be given to privacy and data protection principles.

In order to guarantee privacy from the design stage and by default, a specific policy has been designed so that the DPO and its team are involved from the beginning in each and every project in which personal data may be processed.

3.8. Proactive responsibility

In relation to the processing of personal data, all decision-making processes, measures taken and procedures carried out shall be documented in order to be able to demonstrate compliance with the GDPR and other applicable data protection legislation. In particular, the following matters must be clearly documented:

- Designation or appointment of the DPO, position in the organisational chart of data controller, their functions, reporting channels and the resources assigned to them.
- Employee responsibilities with regard to data protection.
- Organisation and content of the Record of Processing Activities.

- Legitimate bases for processing operations, including, inter alia, evidence of obtaining consent and weighting analyses for the application of legitimate interest.
- Risk assessment of each processing.
- Data Protection Impact Assessments, including the methodology and criteria for conducting these assessments, their process and results.
- Technical, organisational or any other type of measures implemented to guarantee the security of the processing.
- Process for detecting, managing and notifying security breaches, as well as the cases detected and the measures taken in each case for their mitigation.
- Criteria and retention periods for personal data.
- Procedure for the exercise of rights by data subjects as well as evidence of the correct handling of each request for exercise of rights.

3.9. Responsibility of employees and collaborators

All employees and collaborators of the data controllers subject to this Policy are obliged to:

- Comply with the principles and obligations set out in the GDPR and in the applicable data protection regulations.
- Comply with the principles and obligations set out in this Policy, its annexes and any other relevant internal regulations and procedures.
- Respect the principle of confidentiality and therefore not disclose personal data processed in the performance of their duties to third parties in an unlawful manner.
- Collaborate with the DPO in the exercise of its functions.
- Consult the DPO whenever any new processing activity is to be carried out or any existing activity is to be modified.
- Inform the DPO whenever a possible breach of the GDPR, data protection regulations, this Policy or any other internal regulations is detected. In particular, employees and collaborators must inform the DPO when they detect a potential security breach or when they receive, through any channel, a request to exercise rights or any other data protection claim.
- Participate in due time and form in all training actions on data protection aimed at their group or department and participate in the awareness-raising actions that are implemented.

Employees and collaborators who fail to comply with the above obligations shall be subject to disciplinary, contractual or any other applicable sanctions.

3.10. General prohibition of processing of specially protected categories of personal data, subject to exceptions

The following are considered special categories of data:

- Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership.
- Genetic data.
- Biometric data aimed at uniquely identifying a natural person.
- Health-related data
- Data concerning the sex life or sexual orientation of a natural person.

The data controllers subject to this Policy may process special categories of data only in those cases in which the GDPR or the applicable sectoral legislation authorises it. Specifically, health-related data may be processed for the purposes of (i) billing of medical services by the provider of the services to an insurer, and (ii) medical diagnosis, provision of health care and management of health care services.

In any case, whenever special categories of data, and in particular health-related data, are to be processed, the DPO must be consulted and the decision-making process must be properly documented before processing starts.

3.11. Prohibition of processing personal data relating to criminal convictions and offences

Controllers subject to this Policy may not process data relating to criminal convictions or offences or related security measures, such as precautionary measures.

An exception to this prohibition is made for the processing of personal data for the purpose of exercising the right of defence in the context of legal proceedings in which the controller is involved, in accordance with the applicable criminal and procedural law; as well as when a special or sectoral rule provides otherwise or provides for an exception.1

4. Commitments and obligations

4.1 Data processing

4.1.1 Record of Processing Activities

The Record of Processing Activities shall contain the details of each processing activity carried out by the controllers subject to this Policy.

Prior to carrying out new data protection processing operations or when modifying an existing processing operation, the information relating thereto must be included in the specific tool designed to keep the Record of Processing Activities up to date. This tool is aimed at carrying out an appropriate management of data protection, adapted to the requirements of current legislation, as well as following the guidelines of the guides published by the Spanish Data Protection Agency ("AEPD"). This

tool shall include the corresponding risk analysis of the processing and shall incorporate the mitigating measures associated with the risks of each personal data processing operation.

The DPO will determine the criteria for the proper completion of the Record of Processing Activities in accordance with its criteria, the GDPR and data protection regulations; and shall advise the employees of Línea Directa Group so that they can complete or modify the aforementioned Record in an appropriate manner.

The legitimate basis for the processing of personal data shall be defined in the Record of Processing Activities prior to the commencement of the activity in question.

4.1.2 Data collection

The general principles set out in section 3 of this Policy must be observed in processing that involves the collection of data, which is necessary and occurs prior to any other processing. In particular, the following matters must be considered:

- In accordance with the purpose limitation principle, data must be collected for one or more specific purposes.
- In accordance with the principle of data minimisation, only data necessary for the purpose(s) for which they are to be processed may be collected.
- In accordance with the principle of transparency, sufficient information must be provided to data subjects at the time of data collection, in accordance with section 4.3 of this Policy.

4.1.3 Uses and purposes

The concept of purpose of processing refers to the specific reason why the data are processed, i.e. the goal or intention of the data processing.

As a preliminary to any personal data processing, the following matters must be taken into account regarding the purpose:

- All processing operations carried out must serve one or more specific purposes and comply with the principles set out in section 3 of this Policy.
- The purpose and the corresponding legitimate basis must be included in the Record of Processing Activities.
- Data subjects must be adequately informed about the purpose of the processing of their personal data before such processing is carried out. When data are to be processed for purposes other than those for which they were originally collected, the data subjects must be informed and the lawfulness of the processing must be ensured.

4.1.4 Transfer to third parties

The transfer of data to third parties constitutes a processing of personal data as such. For this reason, it must always serve a specific and lawful purpose.

A third party shall be any natural or legal person, public authority, service or body other than the data subject, the controller, the processor and the persons authorised to process personal data under the direct authority of the controller or the processor.

A data processor's access to subjects' data shall not be considered a transfer of data to third parties. In any case, it is necessary to comply with the obligations and requirements relating to the relationship between data controller and data processor, which are detailed in section 4.5 of this Policy.

Whenever any of the data controllers subject to this Policy intend to transfer data to a third party, the DPO must be consulted before such transfer takes place. The DPO must assess the appropriateness of the transfer, its lawfulness (including the possible need to obtain the consent of the data subjects) and the measures necessary to comply with the requirements of the GDPR and data protection law.

In cases where any controller subject to this Policy receives a request from an administrative body or authority or a judicial authority to transfer personal data pursuant to a legal obligation, the controller shall act in accordance with the **procedure for handling requests from external bodies**.

4.1.5 International transfers

Transfers of personal data to countries outside the European Economic Area may only take place in the following cases:

- When the European Commission has established that a given country ensures an adequate level of data protection.
- When adequate safeguards are provided and data subjects have their rights and the possibility of effective legal action.
- When the data subject has given their properly informed consent to the international transfer.
- When the international transfer is necessary for the performance of a contract with the data subject.
- When the transfer is necessary for the formulation, exercise or defence of claims.

Whenever an international transfer of data is intended to be carried out by any of the controllers subject to this Policy, the DPO must be consulted before the international transfer takes place. The DPO must assess the relevance of the international transfer, the lawfulness of the transfer and the measures necessary to comply with the requirements of the GDPR and data protection law.

4.1.6 Retention rules

Personal data will be kept for as long as they are necessary for the purpose for which they were collected or for other purposes, provided that there is an adequate legitimate basis and the data subjects have been informed accordingly.

Once the data are no longer necessary, they will be blocked for as long as they may be required by a judicial or administrative authority or for the exercise of defence in the context of claims by the data controller.

The specific time limits for the retention and blocking of personal data will be set out in a separate document.

4.1.7 Cancellation and erasure

When the data are no longer necessary for a specific purpose, they must be deleted, without prejudice to the above mentioned obligation to block them.

Data also be deleted, at the request of the data subject, in cases where a request to exercise the right to erasure is admissible.

4.2 Legitimacy for the processing.

4.2.1 Contractual relationship

Processing operations are lawful if they are necessary for the management or execution of a contract with the data subject, i.e. for the fulfilment of the contract by the controller.

This legitimate basis also applies to preparatory acts for the contract requested by the data subject, even if the contract is not formalised.

The concept of contract will be understood in a broad sense. This includes commercial, labour, administrative contracts and others.

In all cases, in order for a processing operation to have the contractual relationship as a legitimate basis, it must be strictly necessary for the execution of the contract and must not serve purposes other than the contractual relationship.

4.2.2 Consent

When none of the other legitimate grounds for processing can be applied, the consent of the data subject must be obtained for the purpose(s) of the processing which require it.

The data subject's consent is defined as any freely given, specific, informed and unambiguous indication of their agreement, either by a statement or by a clear affirmative action, to the processing of personal data relating to them for a specific purpose.

Data subjects have the right to withdraw consent at any time. Before giving consent, the data subject must be informed of this right.

The controllers subject to this Policy shall take the necessary measures to properly document consent that has been obtained and, where appropriate, withdrawn.

The DPO shall advise the data controller on the manner and means of obtaining the data subject's consent and on the appropriateness of using consent as a legitimate basis.

Consent must be given by the data subject specifically for each of the purposes for which it is necessary, and the execution of the contract may not be made conditional on the data subject's consent to the processing of personal data for purposes unrelated to the maintenance or execution of the contract.

4.2.3 Other legal bases

In addition to cases where the processing is necessary for the execution of a contract or where the data subject's consent has been obtained, the processing of personal data is lawful where one of the following legitimate grounds applies:

- The processing is necessary for **compliance with a legal obligation** applicable to the controller.
- The processing is necessary to protect the **vital interests of the data subject** or of another natural person.
- The processing is necessary for the performance of a **mission carried out in the public interest** or in the exercise of official authority vested in the controller.
- The processing is necessary for the fulfilment of **legitimate interests** pursued by the controller or by a third party, provided that such interests are not overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data, in particular when the data subject is a child.

When the basis for the processing is compliance with a legal obligation, such obligation must be clearly set out in a regulation of EU law or in a Member State regulation with the status of law.

When the basis for processing is the legitimate interest of the controller, an analysis of the balance between this interest and the rights and freedoms of data subjects that are affected must be carried out before processing is started. Any legitimate interest-based processing may only be carried out if the result of such an analysis is favourable.

The DPO shall actively participate in carrying out the required balancing analyses and, on the basis of these analyses, will conclude in which cases it is possible to use legitimate interest as a legal basis for one or more processing operations. The weighting analyses will be carried out in accordance with the DPO criteria, the recommendations of European and national data protection authorities and applicable administrative and judicial precedents.

4.3 Information and data subjects' rights

4.3.1 Information to data subjects

In accordance with the principle of transparency, controllers under this Policy shall provide data subjects with the following information when collecting their personal data:

- Identity and contact details of the data controller.
- DPO contact details.
- Purposes of the processing for which the personal data are collected and the legal basis for the processing.
- When the processing is based on the legitimate interest of the controller or of a third party, details of this legitimate interest.
- Recipients or categories of recipients of personal data, if any.

- Future international transfers of personal data and details of such transfers.
- The period for which the personal data will be retained or, when this is not possible, the criteria used to determine this period.
- Availability of the rights of access, rectification, opposition, cancellation, data portability and restriction of processing; as well as the channels for exercising these rights.
- When the processing is based on the data subject's consent, the right to withdraw that consent.
- The right to lodge a complaint with the Spanish Data Protection Agency.
- Existence of automated decisions, including profiling and significant information on the logic applied and the meaning and expected consequences of such processing for the data subject.
- Consequences of not providing personal data when they are necessary for the execution of a contract.

Additionally, in cases when the personal data are not collected directly from the data subject, the data subject shall be informed, in addition to the matters already described, of the source from which the personal data originate and, if applicable, whether they originate from publicly accessible sources.

The information shall be provided in a concise, transparent, intelligible and easily accessible form, in clear and plain language and, in any case, in writing, either on paper or by electronic means.

When the data subject already has the information, it is not necessary to provide it.

4.3.2 Exercising rights

Any data subject may exercise the following rights against the data controllers subject to this Policy under the terms and conditions established in the GDPR and in the data protection regulations:

- Right of access
- Right of rectification
- Right to data portability
- Right of cancellation/erasure
- Right to object
- Right to restriction of processing

The department responsible for handling requests to exercise these rights is the Data Protection Office. If an employee outside this department receives, through any channel, a request to exercise any of these rights, they must inform the DPO immediately.

Requests for the exercise of rights shall be handled in accordance with a specific procedure.

The channels established for the exercise of data protection rights are as follows:

- ✓ By email: privacidad@lineadirectaaseguradora.es
- ✓ By post: Línea Directa Aseguradora S.A. Compañía de Seguros y Reaseguros S.A. with tax no. A-80871031 and address at Ronda de Europa, 7, Tres Cantos, Madrid, C.P. 28760

- ✓ Via the website (https://www.lineadirecta.com/politica-de-privacidad.html) by filling in the form on the website. You can access via the link included in the Privacy Policy.
- ✓ By means of a check, inserted in each of the commercial communications by email/SMS.
- ✓ Customer area of the website: In the "Contact details and access" tab, under "my details" and in the commercial information section.

Access

Data subjects shall have the right to obtain confirmation from the controller as to whether it is processing personal data concerning them and, if so, to access such data.

Where a data subject exercises their right of access, the controller shall provide them with all information relating to the processing of their personal data.

Rectification

Data subjects shall have the right to have their data rectified or supplemented by the controller if the data are inaccurate.

Portability

Data subjects shall have the right to receive the data they have provided from the controller in a structured, commonly used and machine-readable format, provided that the processing is based on consent or on a contract and is carried out by automated means.

Data subjects exercising the right to data portability may transfer their data to another data controller without being prevented from doing so by the data controller who provided them with this data. They may also, where technically possible, request that the transmission of such data be made directly from controller to controller.

Erasure

Data subjects shall have the right to have personal data relating to them deleted by the controller. The controller shall do so in the following cases:

- When the personal data are no longer necessary for the purposes for which they were collected.
- When the data subject withdraws consent and the data are not required for other purposes with a different legitimate basis.
- When the data subject exercises their right to object.
- When personal data have been processed unlawfully.
- When personal data must be deleted in order to comply with a legal obligation.

However, this obligation to erase personal data shall not apply if the processing is necessary:

- For compliance with a legal obligation requiring the processing of data imposed by European Union or Member State law applicable to the controller.

- For reasons of public interest in the field of public health.
- For archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.
- For the formulation, exercise or defence of claims.

Objection

Data subjects shall have the right to object to processing operations carried out on the basis of legitimate interest. The controller may only continue to carry out the processing operation(s) in question if it proves that the legitimate interest on which the processing is based overrides the interests, rights and freedoms of the data subject or for the purposes of the formulation, exercise or defence of claims.

When personal data are processed for direct marketing purposes, data subjects may object to the processing (including profiling) at any time, in particular through the marketing communication received.

Restriction of processing

Data subjects shall have the right to have the controller restrict the processing of their personal data in the following cases:

- When the data subject contests the accuracy of the personal data, for a period of time allowing the controller to verify the accuracy of the personal data.
- When the processing is unlawful and the data subject objects to the erasure of the personal data and requests instead the restriction of their use.
- When the controller no longer needs the personal data for the purposes of the processing but the data subject needs them for the purposes of making, exercising or defending claims;
- When the data subject has objected to the processing, while verifying whether the legitimate grounds of the controller outweigh those of the data subject.

When, in accordance with the above, the processing has been restricted, the data may only be processed for the purposes of storage, with the data subject's consent or for the formulation, exercise or defence of claims.

4.4 Responsible processing

4.4.1 Protocol for conducting risk analysis.

Risk management is one of the key issues in the field of Personal Data Protection. It must be carried out with a focus on the rights and freedoms of individuals. On this basis, the fundamental rights that could be affected by the data processing analysed will be taken into account.

The analysis of risks derived from the processing of personal data carried out **by** the organisation **shall be performed in compliance** with the requirements established in the GDPR, in the Organic Law on

Protection of Personal Data and Guarantee of Digital Rights, and following the guidelines set out by the Spanish Data Protection Agency ("AEPD"), in the Guide on "Risk Management and Impact Assessment in the Processing of Personal Data".

Risk analyses shall be carried out using a specific tool for this purpose.

The procedure for carrying out risk analyses and, where appropriate, impact assessments of processing shall be set out in a specific document.

4.4.2 Protocol for carrying out the impact assessment

The analysis of the need for an impact assessment is integrated into the risk management process, to protect the rights and freedoms of data subjects. In cases where, as a result of the risk analysis, it is detected that a certain type of processing entails a high risk to the rights and freedoms of data subjects, it will be necessary to carry out the corresponding impact assessment. In order to assess whether or not it is necessary to carry out an impact assessment, the List of processing operations that require an impact assessment, published by the AEPD, shall be taken into account, as well as when the processing corresponds to one of the examples of obligation listed in the WP248 guidelines.

The procedure for carrying out impact assessments will be set out in a specific document.

4.4.3 Technical and organisational measures

Controllers subject to this Policy shall take appropriate technical and organisational measures to ensure that the processing operations carried out are in compliance with the GDPR and data protection law.

The definition of the technical and organisational measures to be taken shall consider the nature, scope, context and purposes of each specific processing operation. In addition, the results of risk assessments and, where appropriate, impact assessments carried out should also be considered.

Should any of the factors taken into account change, the implementation of technical and organisational measures should be reconsidered, and modified if necessary.

The details of the technical and organisational measures to be applied by data controllers are set out in the **Security Document**.

Specifically, controllers subject to this Policy shall implement such measures from the design phase of processing operations to ensure that the principles, guarantees and obligations set out in the GDPR and in data protection law are applied from the moment the means and purposes of the processing operations begin to be defined.

4.4.4 Security measures

Controllers subject to this Policy shall take appropriate measures to ensure a level of security appropriate to the risk of each processing operation. The definition of the appropriate security level shall result from the risk analysis and, where appropriate, from the impact assessments carried out.

When defining the security measures to be applied, not only the risk must be taken into account, but also the current state of the art, the costs of implementation, and the nature, scope, context and purposes of the processing.

The details of the security measures to be applied by data controllers are set out in the **Security Document**.

4.4.5 Security breach protocol

In the event of a security breach, the following actions shall be taken:

- Immediately inform the DPO.
- Identify the extent of the breach and put in place the necessary measures to mitigate it.
- Implement the procedure for notifying the AEPD of the security breach.
- Where appropriate, initiate the procedure for communicating the security breach to the data subjects concerned.

Details of these procedures are set out in a **security breach management document**.

Any employee or collaborator of the controllers subject to this policy who detects a potential security breach must immediately notify the DPO.

4.5. Providers

4.5.1 Basic requirements

Controllers subject to this Policy shall only engage providers with the status of processors where they provide sufficient guarantees to implement appropriate technical and organisational measures, so that the processing is in accordance with the requirements of the GDPR and data protection law and ensures the protection of the data subject's rights.

In this regard, for the selection of any provider that is to have access to and process data on behalf of any of the controllers subject to this Policy, the procedure, guarantees and measures set out in the provider contracting policy must be applied.

4.5.2 Provider procurement policy

The policy for contracting providers having the status of processors shall be described in an "ad hoc" document.

4.6 Awareness-raising and training

4.6.1 Awareness-raising policy

Controllers subject to this Policy shall develop and implement a data protection and privacy awareness plan for all employees regardless of their level of involvement in personal data processing operations.

The awareness-raising plan shall aim to disseminate the data protection obligations contained in the GDPR, in the data protection regulations and in this Policy in order to consolidate a culture of privacy within the organisation.

The DPO shall be responsible for the design and implementation of awareness-raising activities, as well as for their modification or improvement when necessary.

A separate document **shall list the awareness-raising activities planned for each year, as well as those carried out.**

4.6.2 Training policy

Controllers subject to this Policy shall develop and implement a data protection and privacy training plan for employees. The content and scope of the training of each employee will depend on the degree of involvement of each employee in personal data processing operations, and different groups of employees may be defined for this purpose.

The aim of the training plan shall be to ensure that employees involved in personal data processing operations have an adequate level of knowledge of the obligations and responsibilities set out in the GDPR and in data protection law.

The DPO will be responsible for the design and implementation of training activities, as well as for their modification or improvement when necessary.

The department that carries out the training functions within Línea Directa Group companies will monitor the implementation of the various training activities that have been carried out in Línea Directa and will report regularly to the DPO and its team.

The DPO will also report to the directors of the different areas of the company on compliance with the training activities carried out by Group employees.

A separate document **shall detail the training activities planned for each financial year, as well as those carried out.**

5. Governance and monitoring framework

The Línea Directa Group has established an organisational structure that ensures that any initiative undertaken or any processing carried out which may impact the right to privacy and the right to data protection complies with the regulations in force regarding these matters.

This organisational structure is supported by the following bodies:

- Privacy Committee

- Data Protection Officer and their assigned office

5.1 Privacy Committee

The composition, scope, decision-making and reporting of the Privacy Committee shall be regulated in a procedure designed specifically for this Privacy Policy, which shall be approved by the Audit Committee.

5.2 The Data Protection Officer

Taking into account the type of processing carried out by the controllers subject to this Policy, as well as the nature of their activity, a Data Protection Officer ("**DPO**") has been appointed. The DPO shall be a single DPO for all controllers subject to this Policy.

The duties of the DPO will be performed by an employee of Línea Directa Aseguradora S.A. Compañía de Seguros y Reaseguros, appointed for this purpose and with specialised knowledge on data protection.

Any employee or external collaborator of the controllers subject to this Policy should contact the DPO for consultation or information in the following cases:

- When they have any doubts or concerns regarding the processing of personal data by any of the controllers subject to this Policy.
- When a new data processing operation is to be carried out or an existing one is to be modified, before carrying out or modifying this operation.
- When they observe any activity that could imply a breach of the GDPR, national data protection regulations or any other related applicable sectoral regulations.
- When they observe any activity that could imply a breach of this Policy or of any other internal regulation related to data protection which is applicable to the data controllers subject to them.
- When they receive, through any channel, a request for the exercise of rights established in the Data Protection regulations, that is, in the RGPD and in the LOPDGDD or any other type of claim related to the protection of personal data.

The designation and identity of the DPO will be communicated to the Spanish Data Protection Agency, as well as to all employees of the data controllers subject to this Policy.

Employees may contact the DPO at any time through the data protection section of the corporate intranet or the following email address: dpo@lineadirectaaseguradora.com.

5.2.1 Data Protection Office

The DPO and the human and material resources under their charge constitute the Data Protection Office. The DPO shall have sufficient working time and resources to perform their duties. Given the importance of privacy in the Línea Directa Group, it has been decided that the DPO should not have other tasks initially entrusted to them, so that they can carry out each and every one of the functions assigned to them in detail. Consequently, no analysis of potential conflicts of interest will be required.

Specifically, the DPO shall have sufficient human resources at their disposal, both internal on a permanent basis and internal or external on an ad hoc basis, attending to their specific needs at all times. They also have a specific IT tool.

5.2.2 Functions of the DPO and their office

The DPO, through the Data Protection Office, shall exercise the following functions in relation to all controllers to whom this Policy applies:

- Inform the controller(s), and the employees of the controller(s) who process personal data, of their data protection obligations. This shall include regular training and awareness-raising activities which, at the DPO's discretion, shall be mandatory for some or all of the employees.
- Deal with any queries or requests for information from controllers subject to this Policy or their employees in relation to the processing of personal data.
- Supervise compliance with the obligations contained in the GDPR or in any other regulation relating to personal data protection.
- Act as a point of contact with the Spanish Data Protection Agency or with any other data protection authority of any Member State of the European Union, as well as cooperate with these authorities. Specifically, they shall be responsible for carrying out, where appropriate, the prior consultation procedure.
- Act as a point of contact with data subjects in relation to the processing of their personal data by any of the controllers subject to this Policy.
- Advise the controller in relation to the determination of the legal basis for processing operations. In particular, participate in determining the form and means by which the data subject's consent is obtained and collaborate in carrying out the balancing analyses when the legitimate interest of the data controller or of a third party is to be used as a legal basis.
- Advise the controller on the carrying out of data protection impact assessments and supervising the implementation of these assessments. In this regard, the DPO must be consulted on the following issues:
  - Whether or not to carry out an impact assessment in each case.
  - Validation of the methodology used.

- Resources needed to carry out the impact assessment and, if necessary, the advisability of subcontracting external resources.
- Technical and organisational measures or other safeguards to be implemented to mitigate the risks identified in the impact assessment.
- The outcome of the impact assessment, in particular whether its conclusions are in accordance with the GDPR.

The DPO shall perform their duties with due regard to the risks associated with the processing operations, taking into account the nature, scope, context and purposes of the processing.

5.2.3 Functions of the DPO and their office

The DPO and their office are part of the General Secretary's Office, reporting to the highest hierarchical level.

The DPO and their team act with full independence in the exercise of their functions, not receiving instructions from any manager and with full dedication to their role.

The functioning of the DPO shall be regulated by means of an **Internal Operating Regulation**, signed by the Company's Board of Directors and the DPO.

The members of the Office of the DPO shall not be personally liable for the failure of the controller to comply with their data protection obligations.

6. Audits

The Linea Directa Group periodically carries out an audit aimed at verifying, evaluating and assessing the effectiveness of organisational and technical measures to ensure compliance with privacy and data protection obligations.

7. Communication of the Policy

This Policy will be communicated to the members of the Group and will be available to the organisation's stakeholders through the intranet and the corporate website.

This Policy shall be effective from the date of its publication.

This Policy was approved by the Board of Directors of Línea Directa Aseguradora, S.A. on 28 June 2022.

End of document: Privacy Policy Línea Directa Aseguradora.doc