

AJ 23

Dated January 1st 2019

4195

CNP Assurances

and

CNP Partners

SERVICES AGREEMENT for the Back-Office Administration of the product called "Toscane Vie"

INTRAGROUP SERVICES AGREEMENT
Back office - "Toscane Vie" life insurance product

BETWEEN THE UNDERSIGNED:

- 1) **CNP PARTNERS de Seguros y Reaseguros, SA.** (hereinafter referred as "**The Provider**"), a Spanish insurance company, whose head office is at Carrera de San Jerónimo nº 21 – CP 28104 Madrid (SPAIN), represented by **DAVID VINCENT LATTES**, acting as Managing Director of CNP Partners;

AND

- 2) **CNP ASSURANCES** (hereinafter referred as "**The Client**"), a French « société anonyme » company, with share capital of €686,618,477, governed by the French Insurance Code, registered under No 341 737 062 with the Paris Trade Registry, with registered office at 4 place Raoul Dautry - 75015 Paris (FRANCE), represented by **MARTINE VAREILLES**, acting as Director of La Banque Postale Business Unit and duly authorized hereto;

For the purposes of this Agreement, the Client and the Provider may be herein, individually or collectively referred to as the "**Party(ies)**".

WHEREAS:

- A. The Client is an insurance company authorized by the French supervisory authority "Autorité de Contrôle Prudentiel et de Résolution (the "ACPR").
- B. The Provider, which is a 100% direct Affiliate of the Client, is an insurance company authorized by the Spanish supervisory authority, DGSFP, that carries out any incidental back office services related to insurance cover.
- C. Since 2014, the Provider, along the time and through different legal CNP PARTNERS' intragroup vehicles, has been supplying intragroup Back-Office Services to the Client in relation to the Toscane Vie life insurance product (the "**Product**"), enabling the Client to obtain optimized management of the Product whilst focusing on its core business.
- D. Whereas such provision of Back-Office Services has initially been exclusively based on Client's purchase orders and Provider's corresponding fee invoices (all of which being fully paid up at the Effective Date of this Agreement), the Parties hereby intend to formalize their relationship through a more robust set of terms and conditions.
- E. The Client and the Provider have thus engaged negotiations and agreed to enter into this Agreement as set forth herein.

THE PARTIES AGREE AS FOLLOWS:

1. DEFINITIONS

The following terms shall have the meanings set out in this Clause:

"**Affiliate**" means, for any Party, any entity which that Party directly or indirectly controls, or which is directly or indirectly controlled by or under common control with that Party, within the meaning of Article L.233-1 et seq of the French commercial code;

"Agreement" means the body of this intragroup services agreement and the schedule appended hereto, as modified or amended from time to time;

"Application" means the software application developed, run and maintained by the Provider, available under <http://app.cnpvida.es/vida> as a "read-only" access interface to the Management Tool, enabling Users to scroll through data and information inserted by the Provider, and download, save and/or print such content;

"Back-Office Services" means the intragroup services performed by the Provider in connection with Product management, as set out in Clause 3.2;

"Business Day" means any day (other than Saturday, Sunday or bank holiday) between 08:30 am and 06:00 pm on any such day, on which banks are open for normal business in France and in Spain;

"Client Data" is defined in Clause 9.2 below;

"Competent Authority" means a court, arbitrator or arbitral tribunal, securities exchange, regulator, tax or other governmental or other body or authority having jurisdiction over the Party concerned or to whose jurisdiction that Party submits, wherever situated;

"Critical Third Parties" means any Third Party to which the Provider subcontracts the performance of part of the Back-Office services under this Agreement. As of the Effective Date, the Critical Third Parties are (i) **UMANIS**, "Societe Anonime" with registered office at Rue Paul Vaillant Couturier, BP 7. 92301 Levallois Perret CEDEX, with corporate ID number 403 259 534 00028 at NATERRE RCS (IT maintenance) and (ii) **IBM GLOBAL SERVICES ESPAÑA S.A.** with registered Office at C/ Sta. Hortensia, 26-28 28002- Madrid. - and Corporate ID A28392769 (Hosting and Mainframe's Maintenance, Back Up and Restoring of CNP Partners Business Data, and Management of Engine's General Security.)

"Data Protection Laws" includes but it not limited to the General Data Protection Regulation (EU) n°2016/679 of the European Parliament and of the Council of 27 April 2016, effective as from 25 May 2018 (the "GDPR") and potential decrees, laws and regulations enacted to effect the GDPR by any EU Member State; **"Data Controller"**, **"Data Processor"**, **"process/processing"** shall have the meaning ascribed to them by Data Protection Laws and further detailed in Schedule;

"Distributor Partner" means La Banque Postale SA, RCS Paris (France) 421 100 645, an entity with which the Client has signed a distribution agreement in conjunction with the Product;

"Management Tool" means the software management program developed, run and maintained by the Provider, which enables the Provider to supply the Back-Office Services;

"Personal Data" means all data and other information about or pertaining to the Client personnel or customers, and all data and information otherwise controlled by the Client defined as "Personal Data" by the relevant Data Protection Laws, processed by the Provider in connection with the provision of the Back-Office Services. The details of the processed Personal Data are provided in Schedule 1;

"Product" means the life insurance product named "Toscane Vie", issued by the Client and currently commercialized by the Distributor Partner;

"Regulatory Requirement" means any applicable law, regulation or requirement of any Competent Authority related to the Product or the Client (and in particular Data Protection Laws and French laws

and regulations in connection with insurance contracts), with impact to the Back-Office Services and which implies adaptations on Back-Office Services supplied by the Provider, from time to time;

"**Third Party**" means any entity or natural person that is not a Party to this Agreement;

"**User**" means any employee of the Client (including but not limited to ME3 team), with access rights to the Application;

"**User Guide**" means the handbook describing the permitted use of the Application, as available under <http://app.cnpvida.es/vida>.

2. PURPOSE AND TERM

- 2.1. Subject to the terms and conditions of this Agreement, the Provider shall:
 - (i) supply the Back-Office Services defined under this Agreement to the Client;
 - (ii) grant the Client (including all Users) a right of access to the Application, pursuant to the process and limitations described in the User Guide.

- 2.2. The Agreement shall come in force as from the 1st January 2019 (the "Effective Date"), shall remain in full force for twelve (12) months, and will be renewed automatically for successive periods of twelve (12) months if none of the Parties notice in writing to the other Party its opposition to such renewal, at least six (6) months prior to the Expiration Date.

3. OVERALL PROCESS - DESCRIPTION OF BACK-OFFICE SERVICES

3.1. Outline of Client tasks

The Client

- centralizes the receipt of all requests insured individuals, in connection with the Product;
- ensures request dematerialization via NUMEA software application;
- performs compliance and admissibility checks over such requests and sends verified requests to the Provider by secure email (dedicated inbox) for further processing.

3.2. Back-Office services

The Provider

- shall supply all Back-Office Services under an "obligation de résultat" commitment as defined by French law.

a. Relevant activities:

The Back-Office services to be supplied by the Provider to the Client shall cover the following activities:

- Investments / Disinvestments
- Asset / Liability reconciliation
- ASSIN dataflow
- IT Support for related systems
- Second level control of data inputs
- Management OST
- Management support services Arcueil and Angers
- Generation and control of automatic batch
- Recovery and seizure of NAVs
- Financial control orders

b. Operations performed:

- **Data entry**

The Provider receives data transmitted by the Client via secure emails. Upon receipt, the Provider shall perform information capture and data entry into the Management Tool. All data entries (updates in Management Tool) are performed by Provider and confirmed by return email to the Client.

- **Calculation**

Provider's assistance is further required for specific matters, including but not limited to (i) calculation of the amount of the death benefit, taxes and beneficiary clause or (ii) calculation of amounts due in case of insured individuals' redemption (buyback) requests.

- **Data disclosure to Client**

The Provider shall share with the Client, via the Application or specific communications, any information or data of relevance to enable the Client to address the various reporting obligations which the Client is subject to in connection with Regulatory Requirements.

The Provider may also send warning emails to the Client (with attached postal mail correspondence to be sent to insured individuals) under certain circumstances.

- **Maintenance**

The Provider shall ensure full corrective (trouble shooting, helpdesk, support and incident resolution), evolutive (updates, upgrades, evolutions) as well as regulatory maintenance, including but not limited to the implementation of any changes to the Management Tool or Application as required by Regulatory Requirements in connection with insurance contracts, as soon as the following conditions are fully applied:

- Such maintenance is formally requested by the Client, and
- The Client fully assumes the respective development and implementation costs.

The Parties agree that the Back-Office Services are (a) provided to the Client only, unless otherwise agreed in writing by the Parties; and (b) subject to (a) above, the Back-Office Services may be performed in conjunction with any Distributor Partner as specified by the Client.

4. **APPLICATION LICENSE**

The Provider hereby grants to the Client (including all Users) a non-exclusive license to use the Application on a "read-only" mode, so as to check the status of each relevant Product insurance contract in the Management Tool.

Such licence is granted in the French territory and for the full term of this Agreement (including the period of exit assistance). It is unlimited in the number of Users and includes the right to download, save and/or print any part of the Application content.

Without prejudice to Clause 5 below, the Provider confirms that it holds all rights enabling it to grant the abovementioned license to the Client.

DC
AN.

5. INTELLECTUAL PROPERTY RIGHTS

- 5.1. All intellectual property rights belonging to the Provider or its Affiliates prior to the Effective Date under this Agreement (including in the Management Tool or the Application) shall remain vested in the Provider or such Affiliates.
- 5.2. All intellectual property rights belonging to the Client or its Affiliates prior to the Effective Date under this Agreement shall remain vested in the Client or such Affiliates.
- 5.3. Nothing in this Agreement shall transfer the ownership of, or grant any other interest in, any intellectual property rights of any Party or its Affiliates to the other Party or its Affiliates.
- 5.4. In relation to Third Party software licenses, the Provider hereby grants the Client a royalty-free, non-exclusive, non-transferable, irrevocable licence to use, such software licenses to the extent reasonably necessary to receive the benefit of the Back-Office Services and the Application.
- 5.5. The Provider acknowledges that all correspondence, documents, information, statements and other papers and records in the possession of or under the control of the Provider and relating to the Product ("**Product Records**") (whether already existing at the Effective Date or not and whether created by the Client or not) are and will remain the property of the Client.
- 5.6. The Provider shall indemnify the Client against and defend any claim by a Third Party that the Back-Office Services or the Application (including any Third-Party software licenses supplied pursuant to Clause 5.4) infringe that Third Party's intellectual property rights. The Client shall notify the Provider if it becomes aware of such a claim and provide such assistance to the Provider as the Provider may require in the defense or settlement of such claim at the Provider's expense. If condemned by virtue of a judicial decision, the Provider must pay for any damages a court orders the Client to pay, together with any associated legal costs. This applies for each and any subsequent judicial decisions and/or for settlement agreement(s) approved by the Provider.
- 5.7. In any event, where as a result of a signed settlement between the Provider and the Third-Party applicant or legal proceedings resulting in a court ordering that any Back-Office Service or the Application is prohibited from use, the Provider may, at its own cost, and with the Client's approval:
 - obtain the right for the Client to continue accessing and using the affected Back-Office Service or the Application as provided for in the Agreement;
 - or replace the affected Back-Office Service or the Application with another non-infringing version which meets the Client's needs;
 - or amend the affected Back-Office Service or the Application in such a way as to prevent the aforementioned infringement in accordance with the Client's needs.

6. SERVICE FEES

6.1. Price

In order to comply with the transfer pricing regulation, the Parties agree to set the price of the services in accordance with the arm's length principle, by using the cost-plus method, with a 5 % margin.

For 2019, the price resulting from this method is assessed to **€34.000**. All amounts stated in this Agreement are expressed exclusive of value added tax.

This amount will be billed before the 30th of November of each year.

6.2. Payments terms

Invoices should be issued in the Client's name as follow:

CNP ASSURANCES

BU La Banque Postale
4 place Raoul Dautry
75716 Paris cedex 15.

and should be e-mailed to Martine Vareilles at: martine.vareilles@cnp.fr

The time frame for payment of any sums owed by the Client to the Provider is set at sixty (60) days following the date of invoicing, subject to the Provider complying with all legislative and regulatory provisions as well as any provisions set out herein. Any failure to effect payment prior to the deadline shall result in the outstanding sum being subject to late interest, calculated on the basis of three (3) times the French legal interest rate. Any delay in payment shall also result, in addition to the payment of late penalties, in the payment of a lump sum compensation for recovery costs in the amount of forty (40) euros. This indemnity shall be lawfully due and payable, without formalities, by the Client.

7. CRITICAL THIRD PARTY

Without prejudice to the provisions in Schedule 1 relating to the appointment or change of subprocessors, the Provider shall:

- (a) notify the Client in writing of the identity of any new Critical Third Party and the Back-Office Services to be subcontracted to that Critical Third Party;
- (b) inform the Client reasonably in advance of any change of Critical Third Party, in order for the Client to be able to object to such change in due time.

The Provider shall remain fully responsible for the Back-Office Services performed by any Critical Third Party.

8. CONFIDENTIALITY

For the purposes of this Clause:

- "**Confidential Information**" means any data of any kind whatsoever, including technical, IT, organizational, strategic, legal, administrative, financial, customer-related and/or economic data, including Client Data (including Personal Data), and/or, protected or not by intellectual property laws, whether sent directly or indirectly by the Discloser to the Recipient, in any form whatsoever, either orally, or in writing, in paper format, any electronic format whatsoever, or which the Recipient may have access to as a result of completing this Agreement.
- "**Discloser**" or "**Recipient**", means, depending on the circumstances, either one of the Parties who (i) either directly or indirectly sends (as Discloser), or (ii) directly or indirectly receives (as Recipient), the Confidential Information within the context of completing this Agreement, either in writing, orally, electronically or in any other form.

- 8.1. The Recipient agrees to process and keep Confidential Information strictly confidential and only use the Confidential Information in accordance with the terms and conditions of this Agreement within the context of completing the Back-Office Services. The Recipient shall deal with the Confidential Information of the Discloser with at least the same care as the one used when dealing with its own Confidential Information. The Recipient agrees to take all necessary

measures to protect the Confidential Information, to strictly limit its employees' access to the Confidential Information for the purposes of completing the Back-Office Services and warrant that its employees shall not disclose or use the Confidential Information at any time, or for any matter not authorized under this Clause.

8.2. Obligations defined in this Clause shall not apply to Confidential Information.

(a) that the Recipient already possessed the Confidential Information prior to the Discloser sending it; or

(b) which were already known to the public or accessible to the public prior to it being communicated by the Discloser, or

(c) which became known to the public at the time it was sent by the Discloser, other than by way of the Recipient, or

(d) which had been communicated by Third Parties, legitimately and without restriction or violation, who were not bound by a confidentiality agreement, or

(e) which had been independently developed by the Discloser, subject to written evidence.

However, the Recipient may disclose Confidential Information in the event that it is required to do so by law or by a court, on condition that the Recipient immediately notifies the Discloser in writing so that the Discloser may request an interim order or any other form of appropriate protective measures. In the event that no appropriate protective measures are obtained, the Recipient agrees that it shall only disclose that portion of Confidential Information that is legally required of it and shall use its best endeavors to confidentially process the Confidential Information.

8.3. Upon expiry of the Agreement, or at any time the Discloser requests, the Recipient agrees to immediately return to the Discloser (or, upon written request from the Discloser, to destroy) all Confidential Information, associated documents and/or containing Confidential Information, without retaining copies, extracts and/or summaries, regardless of the form and device, excepting one copy that the Recipient may keep in its legal records for the purposes of identifying its obligations under this Agreement. The Recipient must obtain written confirmation from any authorized Third Party to whom Confidential Information had been disclosed, that this Third Party is subject to the same obligation.

8.4. Obligations set out in this Clause must be complied with throughout the term of this Agreement and for a period of ten (10) years following its termination or expiry.

9. DATA AND SECURITY

9.1. Compliance with Data Protection Laws

The Parties agree to comply with the provisions set out in Schedule 1 with respect to the handling of Personal Data pursuant to the Agreement.

9.2. Data ownership

Without prejudice to Clause 5 above, as agreed between the Parties, all data supplied by the Client or generated on behalf of Client as part of the Back-Office Services, including but not limited to Personal Data ("**Client Data**") are the sole and exclusive property of the Client.

The Provider shall preserve and keep safe the Product's data records and must not destroy or permit or suffer to be destroyed any of them except with the prior written consent of the Client. On reasonable prior notice the Provider must permit the Client, or anyone authorized by the Client to inspect and take copies of the Product's data Records.

9.3. Data hosting

The Provider acknowledges and agrees that Client Data (including Personal Data) may exclusively be hosted within the European Union. No transfer of Personal Data outside the European Union is permitted.

J. G. S.

9.4. Security

The Provider acknowledges that security is a critical issue for the Client and that the Provider's compliance with the information security measures and appropriate security policies, as detailed in Schedule 1, is an essential condition of the Client's consent to the Agreement.

Furthermore, the Provider undertakes to strictly conform with the Information Security Assurance Plan, as completed by the Provider and validated by the Client. If necessary, the Provider will take supplementary reasonable measures to ensure the security and confidentiality of hosting data.

10. BUSINESS CONTINUITY PLAN

10.1. The Provider shall:

- provide the Client with evidence of its business continuity and disaster recovery capabilities in case of a major disruption of its activities;
- at its own expense, maintain, update and test a business continuity plan and disaster recovery plan ("**Business Continuity Plan**") covering the Back-Office Services provided under this Agreement.

10.2. The Provider shall ensure at all times throughout the term of the Agreement that such Business Continuity Plan is consistent with the industry good standard practice in relation to the provision of Back-Office Services in the insurance sector.

11. WARRANTIES

11.1. Each Party warrants to the other that:

- It complies with all applicable provisions related to anti-money laundering, set forth by the European Union as well as by the EU Member States;
- It has and shall maintain all necessary registrations, authorizations, consents, licenses or agreements required or that are necessary to enable it fully and effectively to carry out and discharge its obligations under this Agreement.

11.2. The Provider warrants that:

- The Back-Office Services and the Application are and will remain free from any known viruses detected by up-to-date anti-virus tools;
It will not collect, use and disclose quantitative data (including Client Data) derived from the use of the Back-Office Services;
- It will promptly notify the Client if it becomes the subject of any investigation by any Competent Authority.

12. PROVISION OF INFORMATION AND INSPECTION OF RECORDS

12.1. The Provider shall prepare and maintain full and proper accounts, books and records of the Back-Office Services in compliance with Regulatory Requirements.

12.2. The Client, its designated representatives, and/or its auditors and / or the Competent Authority may:

- (a) inspect any documents, books and/or records relevant to the performance of this Agreement;
and
- (b) take any original documents or copies, books and/or records for the purpose of any investigation, dispute, process or proceedings involving any Competent Authority in any jurisdiction.

12.3. The Provider shall take all steps to enable the Client, its designated representative and/or its auditors to perform audit investigations and provide appropriate office space, access to personnel and to Critical Third Parties (it being agreed that the Client shall be entitled to the same

Jc
Q

rights whether the documents, books and/or records are held by the Provider or such Critical Third Parties).

12.4. The Client shall give ten (10) Business Days written notice to the Provider prior to making any inspection pursuant to this Clause. Any inspection shall take place during normal Business Day hours at such times as may be agreed between the Parties and at Provider's premises or at such other premises as may be agreed between the Parties (including Critical Third Parties facilities).

13. LIABILITY

13.1. As provided under Clause 3.2 above, the Provider shall supply all Back-Office Services under an "*obligation de résultat*" commitment as defined by French law. In particular, the Provider shall:

- Perform all data entries into the Management Tool with completeness and error-free;
- Perform all computations and calculations of premiums, for each insurance contract, with accuracy and disclose exact results of such calculations to the Client;

Communicate all necessary information and data to the Client, enabling the Client to ensure full compliance with its obligations under Regulatory Requirements

13.2. Either Party's liability shall be limited to direct and actual damages within the meaning of articles 1231-1 et seq. of the French civil code and shall exclude compensation for indirect damages.

14. TERMINATION

14.1. Without prejudice to its other rights and remedies, each Party may terminate this Agreement as of right with immediate effect by written notice to the other Party (the "**Breaching Party**") on or at any time after the occurrence of any event specified in this Clause in relation to the other Party:

- (a) any material breach of this Agreement to the extent the Breaching Party fails to remedy within thirty (30) Business Days after the occurrence of such breach;
- (b) any material failure to provide Back-Office Services, or any part of them by reason of any Force Majeure Event as defined in Clause 16.1 for a period in excess of thirty (30) Business Days.

14.2. Without prejudice to its other rights and remedies and notwithstanding Clause 14.1(a), in the event of a persistent breach or repeated breach by the Breaching Party of an obligation under the Agreement that cause or may cause a material impact on the conduct of the Client's business (whether or not it is capable of remedy), the Client may terminate the Agreement as of right immediately (after notice of it is given to the Provider).

14.3. Each Party shall be entitled forthwith to terminate this Agreement as of right by written notice to the other Party:

- (a) If the other Party, for whatever reason, ceases to hold the requisite authorisation(s) to provide for the obligations set for in this Agreement;
- (b) if there is at any time a material change in ownership or control of one Party resulting in that one Party becoming owned or controlled by a direct competitor of the other Party; or
- (c) any changes in or introduction of Regulatory Requirements shall occur so that the performance of all or a substantial part of the Agreement would be substantially frustrated or unlawful.

15. CONSEQUENCES OF TERMINATION – EXIT ASSISTANCE

15.1. Client Data

- (a) The Provider hereby guarantees the full portability of all Client Data required to facilitate the exit transition and migration from the Provider to a Third-Party provider (or back to an in-house IT environment), and further smooth operation of services similar to the Back-Office Services.
- (b) Upon Client's request prior to (or at) the effective date of termination or expiry of this Agreement and without prejudice to the Client's right to recover Client Data at any point in time during the term, the Provider shall make available for download files containing all Client Data in the native structure of the information system of the Provider (CSV format). The description of the structure can be provided at the client's request.

15.2. Other information and documentation

Upon termination or expiry of the Agreement, the Provider shall forthwith deliver to the Client all records, documents, books, ledgers and other material of whatever kind (in complete, correct and up-to-date form) and in the current standard format agreed between the Parties which relate to, or contain information concerning, the Product. The Provider will, at the Client's request, effect such delivery in either or both of machine readable and hard copy form, any machine-readable data being on virus-free media.

15.3. Exit assistance

The Provider shall provide for a period of up to six (6) months from termination or expiry of this Agreement, to support the Client with any further query or reasonable assistance request as the Client may reasonably require to ensure the efficient transfer of the provision of any Back-Office Services to the Client or to any other Third Party as appointed by the Client. If there is any cost relating to this assistance, the Parties undertake to discuss in good faith about the financial impact that the Provider will be entitled to invoice to the Client. In any case, there will be no cost supported by the Client for the implementation of the articles 15.1 and 15.2 except for the case in which the Provider is requested by the Client to make available any Client Data in a customized format other than in CSV format or with a different structure of data. Under no circumstances, this potential cost assumed by the Client shall apply in case the termination of the contract is occurred following a material breach by the Provider or on the Provider's initiative in respect of the terms of the contract.

15.4. General

Termination or expiry of this Agreement does not affect accrued rights and obligations of the Parties at the date of termination or expiry. Each Party's further rights and obligations shall cease immediately on termination or expiry except the Clauses the survival of which is necessary for the interpretation or enforcement of this Agreement, shall survive termination or expiry of this Agreement, and shall continue in full force and effect.

16. MISCELLANEOUS

16.1. Force majeure

- (a) If either Party is prevented from fulfilling its obligations under this Agreement in whole or in any material part, by reason of any event as described in article 1218 of the French civil code (the "**Force Majeure Event**"), the Party unable to fulfil its obligations (the "**Affected Party**") shall immediately give notice to the other Party of that fact, explaining the circumstances preventing it from fulfilling its obligations and shall do everything in its power and at its own cost to resume full performance.

- (b) Upon the occurrence, and during the subsistence, of any Force Majeure Event, neither Party shall be deemed to be in breach of its obligations under this Agreement provided that the relevant Party shall use all reasonable endeavours at its own cost to mitigate the interruption and any damage caused to it by such supervening event.
- (c) As soon as reasonably possible after the end of the Force Majeure Event, the Affected Party shall notify the other Party that the Force Majeure Event has ended and resume performance of its obligations under this Agreement. If such Force Majeure Event lasts for more than thirty (30) Business days, either Party may terminate the Agreement pursuant to Clause 14.1(b).

16.2. Assignment – subcontracting

Neither Party shall be entitled to assign, transfer or sub-contract this Agreement nor all or any of their rights and obligations hereunder without the prior written consent of the other. Notwithstanding the foregoing:

- each Party hereby authorizes the other Party to assign, transfer and sub-contract the Agreement or any of its rights and obligations to its parent company or to its affiliates;
- the Client authorizes the Provider to subcontract part of the Back-Office Services to the Critical Third Parties defined in Clause 1, subject to the provisions related to Data Protection Laws in Schedule 1.

16.3. Notice

Any notices or other communications pursuant to the terms of this Agreement must be sent by registered letter with acknowledgement of receipt at the following addresses:

Notice to the Provider:

CNP PARTNERS de Seguros y Reaseguros, SA
Carrera de San Jerónimo, 21.
Madrid 28014, Spain

To the attention of the LOB of Servicing Director of the Company
Tel: +34 91 5243420
Email: carlos.rey@cnppartners.eu

Notice to the Client:

CNP ASSURANCES
4 place Raoul Dautry
75716 PARIS CEDEX 15, FRANCE

To the attention of the Director of BU La Banque Postale, Martine VAREILLES
Tel : +33 01 42 18 79 71
Email : martine.vareilles@cnp.fr

16.4. Severability

If any provision of this Agreement shall be found by any court or administrative body of competent jurisdiction to be invalid or unenforceable the invalidity or unenforceability of such provision shall not affect the other provisions of this Agreement and all provisions not affected by such invalidity or unenforceability shall remain in full force and effect. The Parties hereby agree to attempt to substitute for any invalid or unenforceable provision a valid or enforceable

dc
9/10

provision which achieves to the greatest extent possible the economic legal and commercial objectives of the invalid or unenforceable provision.

16.5. Entire Agreement – amendments – no waiver

This Agreement constitutes the entire agreement and supersedes any previous agreements between the Parties relating to the subject matter of this Agreement.

No variation in this Agreement shall be effective unless evidenced in writing and duly signed on behalf of each Party. Unless otherwise agreed in writing by the Parties, any failure by a Party to exercise or delay a right or remedy provided by this Agreement or by law shall not impair or constitute a waiver of that or any other right or remedy. No single or partial exercise of a right or remedy provided by this Agreement or by law shall prevent any further exercise of that or any other right or remedy.

16.6. No partnership

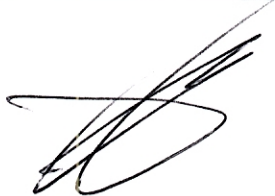

Nothing in this Agreement shall constitute or be deemed to constitute a partnership, agency or joint venture between the Parties or constitute or be deemed to constitute either Party the agent of the other Party for any purpose whatsoever. Neither Party shall have any authority or power to bind the other Party, or to contract in the name of, or create any liability against, the other Party.

17. GOVERNING LAW - JURISDICTION

17.1. This Agreement shall be governed by and construed in accordance with the laws of France.

17.2. **EACH PARTY HEREBY AGREES THAT THE PARIS COURTS SHALL HAVE EXCLUSIVE JURISDICTION TO HEAR AND DETERMINE ANY SUIT, ACTION OR PROCEEDINGS THAT MAY ARISE OUT OF OR IN CONNECTION WITH THIS AGREEMENT, AND FOR SUCH PURPOSES EACH PARTY HEREBY IRREVOCABLY SUBMITS TO THE JURISDICTION OF SUCH COURTS.**

This Agreement has been signed by or on behalf of the Parties on January 1ST, 2019.

Signed for and on behalf of the Provider by Name: DAVID VICENT LATTES	Signed for and on behalf of the Client by Name: MARTINE VAREILLES
Signature: 	Signature: 

SCHEDULE 1 – PROTECTION OF PERSONAL DATA / GDPR

For the purposes of data protection, “**Data Controller**” means the Client and “**Data Processor**” means the “**Provider**”.

For the interpretation of concepts related to the protection of personal data, reference should be made to the definition as stated in article 4 of the European data protection regulation (GDPR 2016/679).

1. PURPOSE AND NATURE OF THE PROCESSING

The Data Processor shall process, on behalf of the Data Controller, any Personal Data required to provide the Back-Office Services included in the Agreement. The processing will consist of:

<input checked="" type="checkbox"/>	Collection	<input type="checkbox"/>	Recording
<input type="checkbox"/>	Structuring	<input checked="" type="checkbox"/>	Alteration
<input checked="" type="checkbox"/>	Store	<input checked="" type="checkbox"/>	Retrieval
<input checked="" type="checkbox"/>	Consultation	<input type="checkbox"/>	Disclosure by transmission
<input type="checkbox"/>	Dissemination	<input type="checkbox"/>	Combination
<input type="checkbox"/>	Alignment	<input type="checkbox"/>	Restriction
<input checked="" type="checkbox"/>	Erasure	<input checked="" type="checkbox"/>	Destruction
<input checked="" type="checkbox"/>	Disclosure		

With respect to this, Destruction Processing should never be executed without the express consent of the Data Controller.

2. CATEGORIES OF DATA SUBJECTS AND TYPES OF PERSONAL DATA

In order to provide the Back-Office Services, the Data Controller provides the Data Processor, Clients Data, including the information described below in relation to the data subjects (i.e. customers (insured individuals) and persons identified in the Product insurance contracts, e.g. relatives, beneficiaries):

PERSONAL INFORMATION

- MAIDEN NAME
- FAMILY NAME
- FIRST NAME
- MARITAL STATUS
- CUSTOMER N°
- E-MAIL
- PHONE

BIRTH AND PROFESSION

- BIRTH DATE
- COUNTRY OF BIRTH

- DEPARTMENT / PROVINCE OF BIRTH
- PLACE OF BIRTH
- NATIONALITY
- PROFESSION
-

IDENTITY DOCUMENT

- TYPE OF DOCUMENT
- IDENTITY DOCUMENT NUMBER
- EXPIRATION DATE
- VALIDITY
- PLACE OF ISSUE
- COUNTRY OF ISSUE
- AUTHORITY OF ISSUE

TAX ADDRESS

- NUMBER AND NAME STREET
- CITY
- CODE POSTAL
- DEPARTMENT
- COUNTRY

MAIL ADDRESS

- NUMBER AND NAME STREET
- CITY
- CODE POSTAL
- DEPARTMENT
- COUNTRY
-

LEGAL CAPACITY

BANK ACCOUNT NUMBER

3.DURATION

The duration of the processing is linked to the term of the Agreement concluded between the Client and the Provider.

When the Agreement ends, the Data Processor will return the Personal Data to the Data Controller or, if so requested by the Data Controller, deliver them to another Data Processor designated by the Data Controller, and will destroy any copy that is in its possession.

4.OBLIGATIONS OF THE DATA PROCESSOR

The Data Processor and all of its staff will:

- a. Use the Personal Data that is subject to processing, or any Personal Data that is collected for inclusion, only for the purpose set forth herein. Under no circumstances may it use the Personal Data for its own purposes.
- b. Process the Personal Data based on the Data Controller's instructions.
If the Data Processor considers that any of the instructions of the Data Controller violate the General Data Protection Regulation or any other data protection provision of the

dc
q.v.

European Union or the Member States involved (ie Spain and France), he will immediately inform the Data Controller and then will wait for clarifications.

- c. Keep a written record of all categories of processing activities carried out on behalf of the Data Controller. This record will contain:
1. The name and contact information of the subprocessors (i.e. the Critical Third Parties as defined in article 1 of the intragroup services agreement); of each Data Controller on whose behalf the processor acts; and if applicable, of the representative of the Data Controller or processor and of the data protection officer (if a data protection officer must be designated pursuant to regulations).
 2. The categories of processing carried out on behalf of each Data Controller.
 3. If applicable, any transfers of Personal Data to a third country or international organization, including the identification of this third country or international organization and, in the case of the transfers described in article 49(1), paragraph two, of the General Data Protection Regulation, documentation of the suitable safeguards. In any event, the Data Processor is expressly prohibited to host, store, use, process or transfer any Client Data (including Personal Data) owned by the Data Controller outside the European Union.
 4. A description of the technical and organizational security measures relating to:
 - i) The pseudonymisation and encryption of Personal Data.
 - ii) The ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services.
 - iii) The ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident.
 - iv) The process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.
- d. Not disclose the Personal Data to Third Parties, unless it has express authorization from the Data Controller, in the cases allowed by law. The Data Processor may disclose the Personal Data to authorized subprocessors (ie the Critical Third Parties) handling data processing for the same Data Controller, based on the Data Controller's instructions and located within the European Union. In this case, the Data Controller will identify, in advance and in writing, the entity to which the data must be disclosed, the data to be disclosed, and the security measures to be applied in order to proceed with the disclosure. If the Data Processor is required to transfer Personal Data to a third country or an international organization under applicable European Union or Member State law, it will notify the Data Controller of that legal requirement in advance, unless prohibited by such law for important reasons of public interest.
- e. Subcontracting.
Not subcontract any of the Back-Up Services, except to the listed authorized Critical Third Parties (subprocessors).
If any additional subcontracting of any processing is necessary, prior written notice will be given to the Data Controller, thirty days in advance, indicating the processing that is intended to be subcontracted and clearly and unambiguously identifying the subcontractor company, its location, and its contact information. The subcontracting may be carried out if the Data Controller does not express its objection.
The subcontractor, which will have the status of subprocessor, is also required to meet the obligations set forth in this document for the Data Processor and any instructions given by the Data Controller. The Data Processor is responsible for regulating the new relationship so that

DC

the subprocessor is subject to the same conditions (instructions, obligations, security measures...) and has the same formal requirements as the Data Processor, with regard to the appropriate processing of the Personal Data and the protection of the rights of the data subjects. In the event of non-compliance by the subprocessor, the iData Processor will remain fully liable to the Data Controller for compliance with the obligations.

- f. Maintain the obligation of secrecy with respect to Personal Data to which it has had access under this order, even after the completion of the Agreement.
- g. Ensure that the persons authorized to process Personal Data provide an express, written commitment to respect confidentiality and to comply with the relevant security measures, of which they must be properly informed.
- h. Make available to the Data Controller any documentation proving compliance with the obligation established in the previous section.
- i. Ensure that the persons authorized to process Personal Data have the necessary Personal Data protection training.
- j. Assist the Data Controller in responding to the exercise of the rights of:
 - 1. Access, correction, deletion, and objection
 - 2. Restriction of processing
 - 3. Data portability
 - 4. To not be subject to automated individual decision-making (including profiling)

When the data subjects go to the Data Processor directly to exercise their rights of access, correction, deletion, and opposition, restriction of processing, data portability, and to not be subject to automated individual decision-making, the Data Processor will first inform the Data Controller of such request immediately. Subject to Data Controller's permission, the Data Processor will then communicate this by email, using the address: gdp.es.petition@cnppartners.eu.

- k. Right of information
It is the responsibility of the Data Controller to fulfil the right to information when the Personal Data is collected from the data subjects.
- l. Notification of Personal Data breaches
The Data Processor will notify the Data Controller immediately, without undue delay, and in any event before the maximum period of 12 hours, of any breaches of the Personal Data under its responsibility that it may become aware of. This notification will be made with all relevant information for documenting and communicating the incident, and will be made using the address dpd.es@cnppartners.eu and send to Data Controller's address urgence.dpog@cnp.fr

At least the following information will be provided:

- a) Description of the nature of the Personal Data breach, including, where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of Personal Data records concerned.
- b) The name and contact details of the data protection officer or other contact point where more information can be obtained.
- c) Description of the possible consequences of the Personal Data breach.

- d) Description of the measures taken or proposed to address the Personal Data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and in so far as, it is not possible to provide the information at the same time, the information will be provided gradually without undue further delay.

If the Data Controller decides to notify the Data Protection Authority of the Personal Data breach, the Data Processor will cooperate in the process whenever requested by the Data Controller. The Data Processor will provide information on the Personal Data breach and in particular on the matters indicated in the notification.

- m. Support the Data Controller in conducting impact assessments regarding the data protection, where appropriate.
- n. Support the Data Controller in conducting prior consultations with the supervisory authority, where appropriate.
- o. Provide the Data Controller with any information required to demonstrate compliance with its obligations, as well as any information required for any audits or inspections carried out by the Data Controller or by another auditor authorized by the Data Controller.
- p. Implement the security measures contained in Appendix 1 to this Schedule. In any event, it will implement mechanisms to:
 - (i) Ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services;
 - (ii) Restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;
 - (iii) Regularly test, assess, and evaluate the effectiveness of technical and organizational measures for ensuring the security of the processing;
 - (iv) Pseudonymise and encrypt the Personal Data, if applicable.
- q. Designate a data protection officer and communicate his/her identity and contact information to the Data Controller (if a data protection officer must be designated do to regulations).
- r. **Data return**
Without prejudice to the provisions of Clause 15.1 of the Agreement, once the Back-Office Services have been completed, the Data Processor, based on the instructions given by the Data Controller and as indicated by the Data Controller, will return to the Data Controller, or to the Third Party provider designated in writing by the Data Controller, the Personal Data and, if applicable, any storage media where they are included. The return of the Personal Data will include the complete erasure of the the Personal Data present on the computer equipment used by the Data Processor. Once destroyed, the Data Processor will certify their destruction in writing and will deliver the certificate to the Data Controller.

DC 9.1.1

Appendix 1 to Schedule 1 – Security Measures

The Security Measures applicable to the provision of the Back-Offices Services will be as follow:

Organisational Measures

- The staff of the Data Processor with access to Personal Data will be aware of their obligations with regard to the Personal Data processing and will be informed of these obligations.
- The functions and obligations of the various users or user profiles will be clearly defined and documented.
- One of the obligations that the entire staff must be aware of is the OBLIGATION OF CONFIDENTIALITY AND SECRECY. More specifically:
 - Access by unauthorised persons to the Personal Data will be avoided. To this end, exposing the Personal Data to Third Parties will be avoided. When any person leaves his or her workstation, the screen will be blocked, or the session will be closed, and any documentation with Personal Data that is accessible will be put away.
 - Paper documents and electronic storage media will be stored in a secure location (closets or rooms with restricted access) 24 hours a day.
 - Documents or electronic storage media (CDs, pen drives, hard drives, etc.) with Personal Data will not be discarded without guaranteeing their destruction (in the case of both documents and electronic storage media) or their secure deletion (in the case of electronic storage media).
 - Personal data or any personal information will not be disclosed to Third Parties.
 - The obligation of secrecy and confidentiality will persist even after the completion of the worker's employment relationship with the company.

Technical Measures

- Identification**
 - When the same computer or device is used for Personal Data processing and for personal use, it will have several different profiles or users for each of the purposes. Professional and personal uses of the computer will be kept separate.
 - There will be user profiles with administrative privileges for installing and configuring the system, and user profiles without administrative privileges for access to Personal Data. In the event of a cyberattack, this measure will prevent access privileges from being obtained and modifications from being made to the operating system.
 - It will be ensured that passwords are in place for access to the Personal Data stored on electronic systems. The password will have at least eight characters and a mix of numbers and letters.
 - Passwords will be stored on the systems in an unintelligible format and will be changed periodically.
 - There will be a limit on the number of attempts for repeated, unauthorised access to the systems. After this limit has been exceeded, access to the system will be blocked and will only be restored, at the request of the user, by an administrator, who will generate a new password to replace the expired password.
 - When several people have access to the Personal Data, there will be a specific user and password (unambiguous identification) for each person with access to the Personal Data.

- The confidentiality of the passwords will be protected, in order to ensure that they are not exposed to Third Parties. The passwords will under no circumstances be shared or recorded in a shared location; people other than the user will not have access to the passwords.

Safeguards.

- The following are the minimum technical measures to ensure the safeguarding of the Personal Data:
 - **UPDATES OF COMPUTERS AND DEVICES:** The devices and computers used for the storage and processing of Personal Data will be kept up-to-date. There will be an inventory of all storage media and devices containing Personal Data.
 - **MALWARE:** The computers and devices where the automated processing of Personal Data is performed will have an antivirus system to safeguard against, to the extent possible, any theft and destruction of the Personal Data and information. The antivirus system will be updated periodically.
 - **FIREWALL:** To avoid improper remote access to the Personal Data, actions will be taken to ensure the activation of a firewall in those computers and devices where the storage and/or processing of Personal Data takes place.
 - **DATA ENCRYPTION:** When it is necessary to remove Personal Data from the site where they are processed, either by physical means or by electronic means, an encryption method will be used to safeguard the confidentiality of the Personal Data in the event of undue access to the information. Each time these Personal Data enter or leave the site where they are processed, this will be recorded, including the following:
 - Document or storage medium.
 - Date.
 - Issuer/recipient.
 - Type of information.
 - Form of delivery.
 - Authorised person for reception/delivery.
 - **BACKUP COPY:** A backup copy will be made periodically on an alternative storage medium, different from the one used for everyday work. The copy will be stored in a secure location, different from the location of the computer with the original files, in order to allow for the recovery of the Personal Data in the event of loss of the information.

General Measures.

Mechanisms will be implemented to:

- Ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services.
- Restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident.
- Regularly test, assess, and evaluate the effectiveness of technical and organisational measures for ensuring the security of the processing.
- Pseudonymise and encrypt the Personal Data, if applicable.

Handwritten initials: N. O. P.



CNP PARTNERS
Micaela Majdalani Tonda
Coordinadora Servicing Iberia
Carrera San Jerónimo,21
28014 MADRID
SPAIN

DEPARTEMENT DROIT DES AFFAIRES – GJ8
LEGAL DEPARTEMENT

Paris, 2nd of October 2019

Object **Service agreement Toscane Vie / Signed**

Dear Micaela,

Please find attached the original contrat duly signed by Mrs. Martine Vareilles.

Thank you for your help.

Your sincerely.

Ayako Dao

A handwritten signature in black ink, appearing to be 'Ayako Dao', written over a horizontal line.

El proceso de negociación a nivel de Senior Management lo han llevado entre David Miseray y Martine VAREILLES - martine.vareilles@cnp.fr, de la Business unit partenariat lbp de CNP Assurances.

Los aspectos informáticos los ha negociado Frédéric Metenier.

La gestión del borrador del contrato la ha llevado a cabo Carlos Rey junto con Ayako DAO - ayako.dao@cnp.fr, Juriste del Département Droit des Affaires - GJ8

Seguidamente pasaremos la hoja de firmas para la validación de Legal y rúbrica de David Lattes.

Personas

Responsable:	Maria Conesa
Informante:	Carlos Rey
Votar (0)	Observando (2)

Fechas

Creada:	12/07/19
Actualizada:	Hoy 9:29 AM



(CIS Spain) Legal Advice CSPLA-807

(TOSCANE VIE) Service agreement CNP Assurances / CNP Partners => 07102019 => REVISIÓN

Detalles

Tipo:	Asistencia	Estado:	Formalizada (Ver Flujo de Trabajo)
Prioridad:	Medium	Resolución:	Sin resolver
Componente(s):	Contracts	Nivel de Seguridad:	CIS Security Level (CIS Security Level)
Etiquetas:	Ninguno		
Perceived Priority:	Medium		
Full Name:	Carlos REY		
Department:	CIS Business Development		
Contact Data:	Ext 420		
Location:	Madrid		

Descripción

En las últimas semanas hemos estado negociando con CNP Assurances la formalización del contrato del TPA de TOSCANE VIE.

El proceso se inició con el modelo propuesto por nosotros a partir del que en su momento nos validasteis para TRÉSOR PREMIUM VIE (CSPLA-782, correo adjunto), y continuó con una versión simplificada propuesta por CNP Assurances.

Al respecto, adjunto os remitimos el texto finalmente consensuado con Paris, para vuestra revisión y validación previa al pase a firma.

Quedamos a la espera de vuestro feedback.

Adjuntos

	2019.07.10 CNP TOSCANE VIE intragroup services agreement-version 20190712_FOR SIGNATURE.docx	98 kB	12/07/19
	CNP-PARTNERS JIRA Carlos Rey compartió CSPLA-782 Trésor Premium Vie - ACTUALIZACIÓN CONTRATO contigo .msg	108 kB	12/07/19
	FINAL Version CLEAN - CNP TOSCANE VIE intragroup services agreement_FOR SIGNATURE_envio LEGAL.docx	97 kB	19/09/19

Actividad

Todo Comentarios Bitácora de Trabajo Histórico de Cambios Actividad Transitions Summary

Araceli Benito Sánchez añadió un comentario - 16/07/19

Necesitamos que nos indiquéis el detalle de los aspectos negociados para poder hacer la revisión.

Carlos Rey añadió un comentario - 17/07/19

Los aspectos negociados han sido los siguientes:

- Simplificación global de la redacción del contrato
- Sometimiento del contrato a los Tribunales franceses para la resolución de conflictos
- Coste del mantenimiento correctivo y/o regulatorio de la herramienta de administración a asumir íntegramente por el cliente
- Plena titularidad del proveedor sobre la herramienta
- Acuerdo anual renovable a partir del 01/01/2019
- Preaviso de 6 meses para manifestar la oposición a la renovación del contrato a su vencimiento
- Precio por los servicios de 34.000 € / año
- Precio de Transferencia por el Método del Coste Incrementado con un margen del 5%



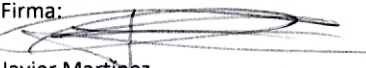

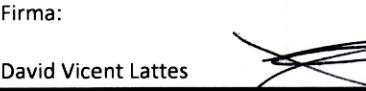
Saludos,

Carlos Rey añadió un comentario - 19/09/19 - editado

El 17/09/2019 se ha llegado a un acuerdo en la redacción final del TPA Agreement a formalizar (WORD adjunto).

Datos a facilitar, imprescindibles, en el caso de proveedores de IT y Desarrollo:	
Definición del perímetro funcional y servicio que se llevará a cabo	
Causas determinación del contrato (incumplimiento de SLA, incumplimiento de cláusulas requeridas, ...)	
KPIs y penalizaciones asociadas a la facturación	
Documentación y entregables. Plazos y condiciones.	
Periodos de garantía del software	

- (1) Indicar la fecha en que se inicia el proceso de revisión y autorización del documento.
- (2) Indicar la fecha de entrada en vigor del contrato, anexo, Change Control Note, etc.
- (3) Indicar la fecha de finalización del contrato, anexo, Change Control Note, etc. si existe. En caso de no existir indicarlo.
- (4) Datos a rellenar por **Contabilidad & Control de Gestión** imprescindibles para la verificación económica del documento. **Es exigible en cualquier documento que implique obligaciones de pago o cobro para la Compañía.**
- (5) La hoja de control siempre deberá ser firmada por la persona que ha negociado y decidió la contratación o elaboración del documento en cuestión.
- (6) Si no se corresponde con un director la hoja de control deberá ser validada por el Director del Departamento del que dependa la partida presupuestaria afectada.
- (7) La validación del **Director de Cuenta** será **imprescindible y obligatoria en las Change Control Notes.**
- (8) **Siempre** deberá disponer de la revisión de **Asesoría Jurídica**, con la excepción de las Change Control Notes si bien **Asesoría Jurídica** conservará copia de todas las Change Control Notes.
- (9) En el caso de contratos deberá contener un resumen del mismo realizado por la persona que lo ha negociado.

OBLIGATORIO (5) – Responsable del Proyecto / Negociación (5) (Persona que ha solicitado y negociado el documento)	Fecha: 19/09/2019	Firma:  Micaela Majdalani
Director del Departamento (6) y /o Validación del Director de Cuenta(6): (si procede)	Fecha: 19/09/2019	Firma:  Carlos Rey
Verificación de Control de Gestión (4): (si procede. Siempre si hay importe económico)	Fecha: 19/09/2019	Firma:  Javier Martínez
Revisión Área Legal (8) (persona del equipo legal que ha revisado el contrato y si cumple con todos los requerimientos solicitados, excepto en el caso de CCN)	Fecha: 19/09/2019	Firma:  maria Conesa <i>*No se hacen comentarios al ser un contrato negociado con / por CNP ASSURANCE</i>
Director General ó Country Manager: (si procede)	Fecha: 19/09/2019	Firma:  David Vicent Lattes

- OBLIGATORIO –

<p>Resumen del contenido del contrato por el Project Manager o responsable de la negociación del documento (9):</p> <ul style="list-style-type: none"> • Principales acuerdos discutidos y aprobados • Entregables del proveedor • Descripción del servicio • Cualquier información relevante en términos económicos o de prestación. 	<p>Este contrato de Servicios de Delegación de Gestión Administrativa de Back-Office para el producto “TOSCANE VIE” tiene como fecha de inicio el 01 de enero del 2019 y contempla la prestación de los siguientes servicios administrativos de Back Office:</p> <ul style="list-style-type: none"> - Inversiones / Desinversiones - Conciliación de Activo/Pasivo - Flujo Datos ASSIN - Soporte informático - Control de segundo nivel de toma de datos - Management OST - Gestión de servicios de soporte - Arcueil y Angers - Generación y Control de Batch automático - Recuperación y Captación de NAV - Control de ordenes financieras <p><u>Duración del contrato:</u> La duración del contrato es de 12 meses, renovable tácitamente por periodos sucesivos de igual duración. No obstante, las Partes podrán rescindir el contrato, mediante notificación escrita y con 6 meses de antelación a la fecha de vencimiento del contrato.</p> <p><u>Coste del servicio:</u> El coste del servicio es de 34 mil €uros anuales (sin IVA) y será pagadero por el Cliente antes del 30 de noviembre de cada periodo.</p>
--	--

Hoja de Control Documentación a Firmar

Fecha ⁽¹⁾:	19 de septiembre del 2019						
Sociedad: <small>(denominación social de la sociedad que suscribirá el documento)</small>	CNP PARTNERS						
Tipo de documento: <small>(identificar si el documento es un contrato, u otro)</small>	Contrato /Anexos <input checked="" type="checkbox"/>	Presupuesto/ Proyecto <input type="checkbox"/>	Doc. Consejo <input type="checkbox"/>	Doc. Hacienda <input type="checkbox"/>	Doc. DGSFP <input type="checkbox"/>	Doc. Planes/EPSV <input type="checkbox"/>	Otro: A:
Solicitado por: <small>(Responsable del área que ha cursado la petición)</small>	DIRECCIÓN DE LOB SERVICING. -						

Contenido/ Objetivo: <small>(Explicación del contenido y características del documento sometido a firma)</small>	CONTRATO DE SERVICIOS DE DELEGACION DE GESTION ADMINISTRATIVA DEL PRODUCTO «TOSCANE VIE». – entre CNP PARTNERS de Seguros y Reaseguros, SA y CNP Assurances
--	--

Rellenar en caso de contrato, presupuestos, proyectos, u obligaciones de pago

Denominación del Documento:	"Services Agreement for the Back-Office Administration of the product called "TOSCANE VIE".		
Apoderado/s:	DAVID VINCENT LATTES		
Contraparte: <small>(denominación del proveedor, o interviniente)</small>	MARTINE VAREILLES (directora de la BU en La Banque Postale y Miembro del Comité Ejecutivo de CNP Assurances).		
Fecha de inicio ⁽²⁾: 01 de enero de 2019	Fecha de finalización de los servicios prestados ⁽³⁾: 31 de diciembre 2019, renovable tácitamente.		
Budget-Partida presupuestaria ⁽⁴⁾: <small>(Incluir información sobre la partida si el contrato o servicio cuenta con un presupuesto específico)</small>			Código PEP⁽⁴⁾:
Importe Económico del Documento ⁽⁴⁾: <small>(se indicará el importe total del contrato)</small>	34.000€ al año (2.833€/mes)		Periodicidad del cobro⁽⁴⁾: Anual (antes del 30 de noviembre de cada período)