PERSONAL DATA PROCTECTION POLICY

REGULATORY FRAMEWORK

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th April 2016 on the protection of individuals with regard to the processing of personal data and the free movement of such data, and repealing Directive 95/46/EC, hereinafter "**GDPR**".
Law No 78-17 of 6 January 1978 on data processing, files and freedoms

WHAT IS PERSONAL DATA?

A personal data is defined as **any information relating to an identified or identifiable natural person** (hereinafter referred to as "**data subject**"). An "identifiable natural person" is deemed to be a natural person who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location data, an online identifier, or one or more specific elements specific to its physical, physiological, genetic, psychic, economic, cultural or social identity.

For example, the last name/first name couple, the social security number, the IP address, the date/place couple are personal data.

BACKGROUND AND SCOPE OF THE PERSONAL DATA PROTECTION POLICY

YOUNITED has implemented a policy on **the protection of personal data of its prospects, customers, investors and employees** in accordance with the principles set out by the GDPR.

The objective of this document is to indicate all the principles or measures put in place by YOUNITED to ensure compliance with the GDPR in terms of:

- implementation of lawful processing;
- respect for the rights of individuals with regard to their personal data (access, rectification, opposition, limitation of processing, portability, erasure);
- possible transfer of personal data to countries outside the European Union;
- transparency on the identity of the recipients of the data collected;
- retention period of the collected data;
- data security measures.

This document is updated as necessary and at least every three years, by or after validation by the Data Protection Officer (hereinafter the "**DPO**"). It is used by YOUNITED employees, customers, prospects, investors and partners.

This document is available on the YOUNITED websites in English and/or French. A fortiori, it is kept at the disposal of the supervisory authority in charge, Commission Nationale de l'Informatique et des Libertés (CNIL).

PERSONAL DATA PROCTECTION POLICY

THE PERSONAL DATA PROTECTION SYSTEM IN YOUNITED

The personal data protection system at YOUNITED is based on three pillars:

- The DPO, whose role is clearly defined below, the privileged point of contact including the CNIL for any problem related to the processing of personal data;
- Specific documentation through processing registers, impact studies or contractual documentation (with prospects, customers, employees, subcontractors and partners);
- technical and organizational security measures.

1. *The Data Protection Officer (DPO) Role*

If you have any questions about this policy or your personal data, you can contact us at

- An email in English or French to our Data Protection Officer at dpo@younited-credit.fr
- a letter to his attention at the address of the head office of YOUNITED located at 21, rue de Chateaudun – 75009 PARIS

YOUNITED's DPO is common to YOUNITED and its branches. The data protection officer is based in France, with relays in Spain and Italy.

The DPO is appointed by the Management Board for an indefinite period. Its designation shall be communicated to the CNIL and, where appropriate, to the national supervisory authorities of the countries where YOUNITED has a branch. The performance of the DPO function may, if necessary, be outsourced.

YOUNITED ensures that its DPO has, at the time of its designation and throughout the exercise of its mission, the professional quality, the specialized knowledge and the freedom to carry out its mission. As such, **the DPO reports directly to the Management Board in the exercise of its mandate.**

The DPO may combine his role with the performance of other duties at YOUNITED, subject to the absence of conflicts of interest. Its missions as a DPO must be clearly defined in a document and appropriate resources (time allocated, human resources) allocated to it.

The DPO may request the support of other support departments and in particular the Risk departments (and in particular the Head of Information Systems Security, HISS) and Compliance & Internal Control, as well as their relays in the countries where YOUNITED has set up a branch.

YOUNITED's DPO monitors compliance with the data protection policies put in place.

The DPO is involved from the conception of new processes, contracts, partnerships or projects giving rise to the use of personal data. DPO analyses treatment projects and treatments in terms of:

- the purpose of the processing;
- the proportionality of the processing with regard to the purpose;
- minimisation of the data collected with regard to the purpose;
- the lawfulness of the processing;
- security of the collected data;
- the retention period of the collected data;

- recipients of the collected data;
- supervision of relations with subcontractors (from the selection procedures via due diligence to the drafting of contractual clauses including, if necessary, audit clauses);
- clear and prior information of the persons concerned;
- conditions for the exercise of the rights of persons;
- and, where appropriate, a framework for data transfers outside the European Union.

The DPO carries out the necessary data protection awareness actions with the employees of YOUNITED.

The DPO shall immediately defer any obstacle or obstacle to the proper exercise of his role to the Management Board. The DPO shall produce an annual report to the Management Board before 30 April of the following financial year summarizing:

- The checks carried out during the year;
- The main findings and areas for improvement;
- The action plans put in place and the recommended implementation dates;
- This report shall be made available to the supervisory authority.

The DPO shall monitor the implementation of the recommendations issued by the DPO on a quarterly basis. It can rely on the Compliance & Internal Control Department for this monitoring.

2. *Documentation in place at YOUNITED*

The register of treatments

YOUNITED maintains **an electronic record of processing**, which includes branch processing. YOUNITED does not subcontract on behalf of other companies and therefore has only a register.

The register is the main documentation tool for the mapping of personal data. Each processing is the subject of a dedicated tab within the register and allows to identify:

- The purpose of the processing;
- The basis or legal basis of the processing: consent of the data subject, processing necessary for the execution of the contract (for example for credit, deposit or investment contracts), legitimate interest of Younited (for example the fight against fraud) or legal obligations;
- The categories of personal data processed with particular distinction between the particular categories of data, said sensitive, and the others;
- The actors (internal or external) who process this data, clearly identifying the subcontracting service providers;
- Flows indicating the origin and destination of the data, in particular to identify any data transfers outside the European Union;
- The retention period of the processed data;
- Technical and organizational security conditions related to the processing.

The processing register is updated as necessary and checked by the DPO at least once a year.

YOUNITED undertakes to make its register available to the CNIL (and any competent equivalent supervisory authority) without delay upon written request from the latter.

Impact analysis on data protection

Based on its analysis of the processing, the DPO may recommend the conduct of an impact analysis on data protection (hereinafter **PIA**, "*Privacy Impact Assessment*") for processing that may pose a high risk to the rights and freedoms of the persons concerned.
The PIA is carried out by the Department at the initiative of the processing ("*Business Owner*"), for example the Product & Brand Department as part of the launch of a new product.
The PIA is formalized thanks to the tool made available by the CNIL on its site:
https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil

The PIA involves several stakeholders, including:

- The preparation and description of the treatment envisaged is the responsibility of the Business Owner;
- The risk assessment and the proposal of any action plans are the responsibility of the Risk Department, and in particular the HISS for the IT security conditions of the proposed processing;
- DPO formally validates the PIA.

At any time, other stakeholders may be consulted and in particular the Compliance Department for the assessment of legal risks related to processing and/or contracting with a partner or subcontractor.

YOUNITED has put in place a guide summarizing the approach and content of a PIA.

Contracts and relations with subcontractors

The YOUNITED subcontractor or partner selection policy includes an assessment of the risks related to personal data and compliance with the obligations reinforced by the GDPR.

Subcontractors are required to comply with specific obligations regarding security, confidentiality and documentation of their activity.

YOUNITED shall ensure, contractually and/or through audits on the part of the parties or on the spot, that its subcontractors comply with these obligations, in particular the maintenance of a register of processing activities carried out on behalf of YOUNITED.

Monitoring data transfers outside the EU

YOUNITED limits as much as possible the choice of subcontractors or partners that process (including hosting even as a back-up) personal data in a country outside the EU or whose level of protection has not been recognized as equivalent to that of the EU. Where applicable, YOUNITED shall require the subcontractor or partner to comply with the obligations set out in the GDPR and, after having carried out an impact analysis of the data transfer, uses the models of personal data transfer agreements adopted by the European Commission (**Standard Contractual Clauses**) available on the CNIL website: https://www.cnil.fr/fr/les-clauses-contractuelles-types-de-la-commision-europeenne or any other mechanism of appropriate safeguards in accordance with Article 46 of the GDPR (binding corporate rules, code of conduct,

certification).

3. *The technical and organizational security measures in place at YOUNITED*

YOUNITED implements security measures, including IT and organizational measures to ensure the protection of personal data, which is based on several pillars: the awareness of employees, internal procedures and a leader, the HISS.

Raising staff awareness

YOUNITED regularly sensitizes its employees to the protection of personal data of customers and prospects, through the dissemination of materials and/or the holding of awareness sessions, and to IT security (including arrangements for the storage, retrieval and external dissemination of information, documents, confidential and/or including personal data of customers or prospects).

This document is sent to all new employees as part of their arrival.

Managing access to personal data

YOUNITED has a policy for managing access to its IT system, which makes it possible to limit access to the personal data of customers and prospects to employees who have the need.

The procedure for managing access provides for the procedures for periodic review of access.

The procedure for storing data and documents

YOUNITED has a data and document retention procedure and complies with it. The retention periods for personal data are based on the regulatory or legal obligations to which YOUNITED is subject.

Personal data are deleted or anonymized at the latest 6 years from the end of the contractual relationship for customers, investors and employees, 3 years from the last active contact for prospects, unless YOUNITED's legitimate interest (such as the fight against fraud) or legal obligation. In case of suspicion of money laundering or terrorist financing, the data relating to this case are kept for 6 years in France, in compliance with legal and regulatory obligations.

Internal procedures in case of data breach

YOUNITED has a procedure for notification of a breach of personal data, which provides for an information period of 3 days after becoming aware of it with the CNIL and as soon as possible with the data subjects.

The procedure provides for close coordination between the HISS and the DPO.

PERSONAL DATA PROCTECTION POLICY

INFORMATION FOR THE PERSONS CONCERNED

1. *Information mentions of the persons concerned*

YOUNITED complies with the information obligations introduced or reinforced by the GDPR through its various communication media: contractual or pre-contractual information, legal notices of its subscription tunnel, or the Legal Notice page of its various sites.

At the time of any collection of personal data from prospects, customers or employees, Younited informs the persons concerned:

- the contact details of YOUNITED and its status as Data Controller;
- the contact e-mail address of the YOUNITED DPO;
- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing (as well as the legitimate interests pursued by YOUNITED, in the event of use of this legal basis);
- whether or not the provision of data is mandatory, the contractual or regulatory origin of that obligation, and the possible consequences of not providing the data;
- possible recipients of personal data, as well as the possibility of transfer outside the EU;
- the duration or criteria for the retention of personal data;
- the existence of automated decision-making, including profiling where appropriate;
- the rights of the persons concerned by the processing and the procedures for exercising those rights.

If the processing of personal data is subject to the prior consent of the data subject, YOUNITED ensures that the evidence of this consent is kept, in particular in its computer systems.

It is also recalled that any data subject has the right to lodge a complaint:

With YOUNITED by the usual procedure available here.

To the CNIL or any competent equivalent supervisory authority, in particular via the **online complaint procedure**: https://www.cnil.fr/fr/plaintes/

2. *Procedures in place for exercising the rights of data subjects*

YOUNITED has put in place procedures to allow any data subject to be able to easily exercise his rights, in particular:

- Access to, rectification or erasure of personal data;
- If the processing is based on consent, exercise of the right to withdraw consent at any time;
- A limitation of the treatment relating to the person concerned;
- The right to object to automated processing or decision-making and;
- The right to data portability.

PERSONAL DATA PROCTECTION POLICY

Any data subject may contact YOUNITED for this purpose:


By registered mail with acknowledgement of receipt
YOUNITED
For the attention of the Personal Data Protection Officer
21 Rue de Chateaudun
75009 PARIS - FRANCE


By e-mail: dpo@younited-credit.fr
Via the contact form by selecting the "Personal Data" category available on the Younited website: https://www.younited-credit.com/contacter-younited-credit

Any customer, investor or prospect may also at any time withdraw their consent to be contacted again in the context of commercial prospecting. To unsubscribe, the person can:

- Use the unsubscribe link in all promotional communication materials sent by Younited;
- Log in to your customer area and click on the "My subscriptions" section;
- Send an e-mail to dpo@younited-credit.fr

Be careful, rights can only be exercised by the person concerned. YOUNITED reserves the right not to proceed with a request if it has not been able to identify the person concerned, in particular in support of a legible and valid identity document.

Access to personal data is limited to the data subject. In case of co-holders of a contract, access is limited to the person making the request. YOUNITED reminds that customers can access part of their personal data via their Customer area.

Any rectification of personal data must be supported by a supporting document (proof of residence of less than 3 months, identity document, etc.) legible and valid.

YOUNITED reserves the right not to act on a request for erasure of data, unless one of the following reasons is completed:

- Personal data are no longer necessary for the purposes for which they were collected or otherwise processed;
- The data subject withdraws the consent on which the processing is based, and there is no other legal basis for the processing;
- The data subject objects to the processing, and there is no compelling legitimate reason for the processing;
- Personal data has been illegally processed;
- Personal data must be deleted in order to comply with a legal obligation laid down by Union law or by the law of the Member State to which the controller is subject.

In case of a request for data portability, the data will be provided in the form of a usable file. YOUNITED is not responsible for the computer equipment used by the data subject.

PERSONAL DATA PROCTECTION POLICY

INFORMATION NOTICE CONCERNING THE DATA PROCESSING OF CUSTOMERS, PROSPECTS AND INVESTORS

The purpose of this notice is to provide you with the information required to enable you to understand how Younited, a public limited company registered in the Trade and Companies Register under the number RCS 517 586 376 Paris, approved by the ACPR under number 16488 and by the ORIAS under number 11 061 269 processes your personal data

1. What data is collected by Younited?

As part of our activity as a credit institution and service provider, we may collect the following categories of data:

- Identification information: surname, first name, date and place of birth, gender, title, copy of passport or identity card, nationality, etc.;
- Private or business contact information: tax, postal and electronic addresses, telephone number, etc;
- Information about your family situation and family life: marital status, surname and first name of the spouse, children or other dependents, dates of birth of the spouse, children or other dependents, composition of the household, etc. ;
- Economic, financial and tax information: income, tax bracket, tax identifier, tax status, country of residence, amount and composition of wealth, origin of wealth, investor profile, information on outstanding loans, knowledge and experience of financial instruments and financial position, including ability to bear losses, investment objectives and risk tolerance, etc. ;
- Education and employment information: occupation, name of employer, remuneration, status…;
- Banking and financial information: bank accounts, etc.;
- Transactional data: data relating to transactions, including transfers, including data relating to beneficiaries including their full names, address and contact details, etc. ;
- Data relating to your habits and preferences: data related to your use of the products and services you have subscribed to us;
- Data collected in the context of our exchanges with you (meeting reports), on our websites, our applications, our pages on social networks (login and tracking data such as cookies, connection to online services, IP address), during meetings, calls, discussions via instant messaging, e-mails, interviews, telephone conversations;
- Geolocation data;
- Information about your device (IP address, technical data and unique identification data);
- Custom login credentials or security devices used to connect to Younited's website and applications.

Younited adheres to the principle of "privacy by design" and ensures that, by default, only the personal data required for each specific purpose of processing is processed.

We never ask you to provide us with other sensitive data such as data relating to your racial or ethnic origin, your political opinions, your religious or philosophical beliefs or your union membership, genetic data or data relating to your life or sexual orientation, unless we are required by law to do so.

All this data is usually obtained during our interactions, whether via our online platform, by

phone, by mail or by email. However, we may sometimes have to process data obtained through third-party organizations, for example in order to meet our regulatory obligations or, with your consent, in connection with the use of services such as banking aggregation. Telephone communications with our Customer Service are recorded to ensure the quality of service, improve the efficiency of our operational teams and continue to offer you a fairer and faster credit. In addition, the retention of such exchanges may be used for evidence purposes or as part of compliance with legal and regulatory obligations. We also collect certain information about your type of browser, your internet service provider and your type of material used to combat fraud, to maintain the quality of our services and to obtain general statistics on their use. We use cookies or similar technologies to offer you the best digital experience. We also use cookies to offer you the most suitable offers for your needs.

We finally collect data about other people indirectly. We collect information about people even if they have no direct connection to us because they have a connection to you, whether you are a customer or a prospect, for example:

- Members of your family;
- Heirs and assigns;
- Co-borrowers/guarantors;
- Legal representatives (mandates/delegations of authority);
- Beneficiaries of payment transactions;
- Beneficiaries of a contract or insurance policy and trust/trust;
- Of the owners;
- Beneficial owners;
- Creditors (for example in case of bankruptcy);
- Shareholders of corporations.

When you send us the personal data of third parties such as those in the list above, be sure to inform the person to whom this data relates that we process his personal data and direct to this Information Notice relating to the protection of personal data. We will also provide them with this information where possible (for example, if we do not have their contact information, we will not be able to contact them).

In order to verify and enrich our databases, we may also collect personal data from:
Of our trading partners;

- Payment initiation service providers and account aggregators (account information service providers);
- Third parties such as data brokers, who must ensure that they legally collect the relevant information;
- Publications/databases made available by authorities or official third parties (for example the Official Journal of the French Republic, databases managed by financial sector supervisory authorities);
- Websites/social media pages of legal entities or professional clients containing information that you have made public (for example, your own website or social media page);
- Public information such as that published in the press.

2. For what purposes and on what legal basis does Younited process your data?

The processing of your personal data is lawful because it is necessary:

a) To comply with our various legal or regulatory obligations:

We use your personal data to comply with applicable regulations, including banking and financial regulations, in order to:

- Manage, prevent and detect fraud;
- Issue and retain electronic certificates related to electronic signatures;
- Monitor and report risks (financial, credit, legal, compliance, reputational, default, etc.) that we may encounter;
- Record, if necessary, telephone calls, chat exchanges, emails, etc., notwithstanding any other use described below;
- Detect situations of financial fragility in order to propose to the clients concerned appropriate accompanying measures;
- Establish your investor profile
- Exchange and report various transactions, transactions or requests or respond to an official request from a duly authorized local or foreign judicial, criminal, administrative, tax or financial authority, arbitrator or mediator, law enforcement authorities, governmental bodies or public bodies;
- Prevent and detect money laundering and terrorist financing and comply with any international sanctions and embargoes regulations as part of our KYC procedure (to identify yourself, verify your identity, verify your information against the sanctions lists and determine your profile);
- Fight against tax fraud and fulfil our obligations in terms of tax declarations or audits;
- Detect and manage suspicious requests and transactions;
- Conduct an assessment of the suitability of each client and the appropriateness of the provision of investment services in accordance with financial instrument market regulations (MiFID II);
- Record transactions for accounting purposes;
- Prevent, detect and report risks related to Corporate Social Responsibility and sustainable development;
- Detect and prevent corruption.

Your data may be used in particular for the transmission of information to the “Fichier central des Chèques” (FCC).
In addition, and as part of the credit granting procedure, we are required to consult the “Fichier des Incidents de remboursement de Crédits aux Particuliers” (FICP), and in case of a typical payment incident, request that information about you be entered in this file. It is important to note that if your request is denied, you can ask us for an interview to present your observations.

b) To perform any contract to which you are a party or to perform pre-contractual measures taken at your request

We use your personal data to enter into and execute our contracts and to manage our relationship with you, in particular in order to:

- Define your credit risk score and repayment capacity;
- Evaluate (for example on the basis of your credit risk score) whether we can offer you

a product or service and under what conditions (including price);
- Assist you, in particular by responding to your requests;
- Manage and process payment incidents, unpaid payments (identification of customers in a situation of unpaid payment and, where applicable, exclusion of them from the benefit of new products or services) and the resulting amicable and legal recovery operations.

c) <u>To serve our legitimate interests to protect our company, provide you with the best service, improve our products and grow our business:</u>

We process your personal data, including data relating to your operations, for the following purposes:

- Risk Management:
  - Establish proof of transactions, including in electronic format;
  - Manage, prevent and detect fraud;
  - Develop individual statistical models to facilitate the definition of your borrowing capacity;
  - Monitor transactions and identify those that are abnormal/unusual (for example when a large amount of money is deposited into your account in a country where you do not live);
  - Recovery;
  - Assert legal rights and defend ourselves in litigation.
- Personalize our offer and:
  - Improve the quality of the products or services we offer,
  - Deduce your preferences and your needs to present you a personalized commercial offer in particular by segmenting our prospects and customers in order to provide them with the most suitable products or services;
  - Promote products and services that match your situation or profile.

  This can be achieved by:
  - Analyzing your habits and preferences through different channels (e.g. emails, communications, visits to our websites);
  - Analyzing character traits or behaviors of existing clients and looking for others who share the same characteristics for prospecting purposes;
  - Offering products or services that correspond to your situation, and products or services that you already own or use;
  - Monitoring operations to identify those that appear unusual.

As a result, you may receive offers electronically for our products or services similar to those you have already subscribed to. However, you may object to it under the conditions set out in section 7 below.

- Research and development (R&D) activities to develop statistics and models for:
  - Optimize and automate our business processes (for example creating a chatbot for FAQs);
  - Offer products and services that allow us to best meet your needs;
  - Adapt the distribution, content and pricing of our products and services based on your profile;
  - Create new offerings;
  - Prevent potential security incidents, improve customer authentication and manage access;
  - Improve safety management;
  - Improve risk and compliance management;
  - Improve fraud management, prevention and detection;

- Improve the fight against money laundering and terrorist financing.
- Security and performance management objectives for IT systems, including:
  - Manage information technology, including infrastructure (for example, shared platforms), business continuity and security (for example, authentication of Internet users);
  - Prevent damage to people and property (for example, video protection).
- More generally:
  - Inform you about our products and services;
  - Perform financial transactions such as sales of debt portfolios, securitizations, financing or refinancing of Younited;
  - Organize contests, lotteries and other promotional operations;
  - Conduct customer opinion and satisfaction surveys;
  - Improve process efficiency (train our staff by recording phone conversations in our call centers and improve our call scenarios);
  - Improve automation of our processes including testing our applications, automatically handling complaints, etc;
  - Perform checks on the quality of our data.

In all cases, our legitimate interest remains proportionate and we ensure, through a balancing test, that your fundamental interests or rights are preserved. If you would like more information about the Weighing Test, please contact our services at the contact details in section 7.

- To respect your choice when we have asked your consent for a specific treatment

In the course of certain personal data processing activities, we will provide you with specific information and invite you to consent to this processing. Please note that you may withdraw this consent at any time.

3. With whom do we share your data?

The personal data that we collect can be processed by Younited's authorized personnel, for example our granting teams as part of your credit application, our accounting, marketing, compliance...

We transmit your personal data to providers of IT services, printing, telecommunications, archiving, IT maintenance, payment services, etc. These service providers need your personal data to carry out and provide the services we entrust to them. They have the status of subcontractor of personal data. Subcontracting and outsourcing of our services are subject to special rules. We choose these providers with the utmost care and our subcontracts with them include the necessary clauses to ensure the security and confidentiality of the data transmitted. We remain fully responsible to you, even if we use these third parties

Finally, we transfer your personal data to third parties acting on their own behalf. They are themselves responsible for the use of your data and are subject to the same obligations as Younited in terms of personal data protection:

- The following organizations or jurisdictions for mandatory reporting:
  - La Banque de France: register and delete accounts in the FICOBA file, register and delete persons in the incident files if necessary (credits, cheques)
  - La Caisse de Dépôts et Consignations: inform and transmit your personal data for accounts and assets in default.

  - The French Tax Administration: providing tax information for non-resident clients (CRS, FATCA)
  - TRACFIN: make suspicious activity reports relating to money laundering operations or as part of an asset freeze
  - L'Autorité des Marchés Financiers: reporting suspected market abuse

- Financial partners, intermediaries and counterparties: As part of the execution of the contract binding us or to comply with our legal obligations, we may transfer your personal data to an external third party, namely the bank of the beneficiary of a transfer, a guarantor organization, payment service initiators and account aggregators acting at your request
- Public authorities: We must transmit your data to public authorities if we are obliged to do so within the framework of an official request from them, such as a request from the tax authorities, the Autorité de Contrôle Prudentiel et de Résolution, the Autorité des Marchés Financiers, the European Central Bank, the Ombudsman, a judicial officer, the judicial police...
- Regulated professions: Your personal data can be shared with lawyers, court assistants and legal officers, administrative or judicial authorities seized of a dispute as appropriate or to enable Neuflize OBC to ensure the defense of its rights and interests, with notaries in the case of gifts and estates, auditors in the context of annual audits or audits
- Other third parties: In the context of a merger or acquisition of all or part of Younited by a third party or in the case of sale, assignment or restructuring, Younited may have to transmit your personal data to the parties involved in the transaction (buyer, partner, consultant, etc.).

4. Are your personal data shared outside the European Union?

We limit as much as possible the choice of subcontractors or partners who process (including hosting even as a backup) personal data in a country outside the EU. However, in order to fulfil the purposes detailed in this policy, we may have to transfer personal data to countries that are not members of the European Economic Area, whose personal data legislation has not been recognized as equivalent to that of the European Union. Where appropriate, we will implement all appropriate technical and organizational measures to ensure the security of your personal data and will inform you beforehand of such transfers. We require the subcontractor or partner to comply with the obligations set out in the Regulations and use the models of contracts for the transfer of personal data adopted by the European Commission or other appropriate guarantee mechanisms, which you can consult by contacting our Data Protection Officer (see Section 7 below).

5. How long do we keep your personal data?

Younited retains your personal data only as long as necessary to achieve the purpose for which the data is collected and processed and to comply with its legal and regulatory obligations. The retention period of the data thus depends on the nature of the data processed and the purposes pursued. When the objective is achieved, the data must nevertheless be retained until the retention periods imposed by laws or regulations have expired. Your data can then only be consulted by persons specifically authorized. At the end of these periods, we delete or anonymize your data.

a) Personal data relating to a prospect

If you are not our customer but have made a request for information or a request for a product or service, your contact details (surname, given names, addresses, telephone number, date and place of birth and e-mails) are kept in order to be able to offer you our offers (if you agree) for 3 years, either after the last contact with you, or after their collection in case of no further contact.
You can request their deletion before this deadline.

b) Personal data collected for pre-contractual purposes

When you have contacted us for a product or service request and your request has not been followed by a subscription (cancellation or refusal), the information you have been able to provide us (personal situation, financial information, etc.) as well as, where applicable, the refusal and the related analyses are kept for 6 months from the date of their collection or the decision.
In case of a request or internet simulation interrupted or abandoned, the data collected via cookies are, if you have accepted them, kept for 30 days.
In the case of proven fraud, the fraudster's identification data and the data relating to the fraud are kept for a maximum of 5 years from the entry in the list of fraudsters found.

c) Personal data of our customers

Information about you and your product or service is kept for as long as necessary for the performance of the contract and until the expiry of the applicable legal deadlines:

- In accordance with the rules relating to civil, commercial and criminal prescription, data relating to the product or service held will be kept for a period of 5 years from the end of our commercial relationship (closure of the account, full repayment of the sums due, termination of the legal proceedings, etc.), with the exception of data showing the absence of participation of Younited or its clients in crimes, which can be kept for a period of 6 years.
- In the event of a dispute related to a situation of unpaid payments, the data may be kept for a period equivalent to the period of validity of the enforceable title obtained against you or a minimum period of 10 years from the issue of it.
- In accordance with the French Commercial Code, accounting documents, supporting documents and related data are kept for a period of 10 years from the close of the accounting year or the close of your contract.
- In accordance with the doctrine of the CNIL, data relating to proven fraud are kept for a maximum period of 5 years from the date of entry in the list of proven fraudsters.
- In accordance with the Monetary and Financial Code relating to the fight against money laundering and the financing of terrorism, the documents and documents

collected in respect of vigilance are kept for 5 years from the end of the relationship.
- In accordance with the amended decree of 26 October 2010, FICP's interrogation evidence is, in the event of refusal or abandonment, deleted after consultation. In case of subscription to the product, they are kept for 5 years after closing of the contract. Registration in the FICP is lifted after a maximum of 5 years or upon repayment of the debt.

Specific deadlines are applied in certain transactions/situations in accordance with the regulations or the recommendations of the CNIL:
- Incivility management data are retained for 1 year from the end of the year in which the incivility occurred.
- The data from the customer area are kept for 5 years from the deletion of the access to this space or 6 months after the termination of the contract
- In case of payment of your monthly payments by Credit Card, the number of this one is kept for 15 months from the date of debit.

d) Telephone conversations

Recordings of telephone conversations for training and quality of service improvement are kept for 6 months unless you object to the recording.
If using the chat, the conversation is kept for 6 months.

6. Automated Decision Making

Younited reserves the right to use, in its lending decision, a technology that performs automated decision making and profiling only when:
- This is necessary for the conclusion or performance of a contract between us; or
- We have obtained your express consent to do so for these purposes

While we have confidence in how our technology works, we understand the concerns about automated decisions. Therefore, in accordance with the applicable regulations, we remind you that you can request human intervention, express your point of view and challenge the decision contacting our Data Protection Officer according to the terms described below.

7. What are your rights and how can you exercise them?

In accordance with the legislation applicable to your situation, you may exercise, where applicable, the following rights:
- Right of access: you may obtain information relating to the processing of your data and a copy thereof;
- Right of rectification: if you consider that your personal data are inaccurate or incomplete, you have the right to have these data modified accordingly;
- Right to erasure: you can request the deletion of your personal data, to the extent permitted by law;
- Right to the limitation of the processing: you can request the limitation of the processing of your personal data;
- Right to object: you can object to the processing of your personal data for reasons related to your particular situation. You have the absolute right to object at any time to your data being used for commercial prospecting, or for profiling purposes if this profiling is related to commercial prospecting. If you do not wish to receive offers

electronically for our products or services similar to those you have already subscribed to, you may object to them in the manner described below.

- Right to set guidelines for the retention, erasure or disclosure of your personal data, applicable after your death.
- Right to withdraw your consent: If you have given your consent to the processing of your personal data, you may withdraw your consent at any time.
- Right to the portability of your data: when the law allows it, you can request the restitution of the personal data you have provided to us, or, where this is technically possible, the transfer of these to a third party

You can exercise your rights by sending your request to the dedicated address dpo@younited-credit.fr or by sending your request by mail to the address Younited Credit – DPO – 21 rue de Châteaudun 75009 PARIS. Younited uses the services of the subcontractor Universign to sign contracts electronically. You can also request the exercise of your rights by contacting Universign – Data Protection Officer - 7 rue du Faubourg Poissonnière 75009 Paris or by email at privacy@universign.com. Finally, you have the right to file a complaint with the Commission Nationale de l'Informatique et des Libertés (CNIL) - 3 Place de Fontenoy - TSA 80715 - 75334 Paris - Cedex 07.