

## Banquup Website Privacy Notice

Last update : December 29th, 2025

### 1. Introduction

We understand that your privacy is important to you and that you care about how your personal data is used. We respect and value the privacy of everyone who uses our website and will only collect and use personal data in ways that are described here, and in a way that is consistent with our obligations and your rights under the General Data Protection Regulation (EU Regulation 2016/679) (the “GDPR”) or any other data protection legislations. Please read this Privacy Notice carefully and ensure that you understand it.

This notice policy applies where we are acting as a data controller with respect to the personal data of our website visitors (namely candidates and prospects) potential customers in other words, where we determine the purposes and means of the processing of that personal data.

Please note that this Privacy Notice does not apply to other websites, applications or platforms offered by Banquup Group SA or its affiliates. We advise you to look at the relevant privacy notices when using such websites, applications or platforms.

Please read this Privacy Notice carefully and ensure that you understand it.

We also recommend that you read our relevant cookie policy when you visit our websites or when you use Banquup digital services. It explains what cookies are, which ones are used by Banquup, how you can change your cookies preferences and how we protect your privacy. The cookie policy can always be found in the websites (link available at the bottom of the webpage).

### 2. Information about us

This website is an initiative of Banquup Group SA a company incorporated and existing under the laws of Belgium with registered address at Avenue Reine Astrid 92, 1310 La Hulpe and with company number BE0886.277.617 (referred to as “Banquup” or “we” or ‘us’). The entity which processes your personal data shall be the controller of your personal data.

You can contact our Data Protection Officer (‘DPO’) in writing at the following address: Banquup, for the attention of the DPO – Avenue Reine Astrid 92 A, 1310 La Hulpe, Belgium or by sending an email to [gdpr@banquup.com](mailto:gdpr@banquup.com).

### 3. What is personal Data?

Personal data is defined as ‘any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier’. Personal data is, in simpler terms, any information about you that enables you to be identified. Personal data covers obvious information such as your name and contact details, but it also covers less obvious information such as identification numbers, electronic location data, and other online identifiers.

The personal data that we use is set out in section 4 of this Privacy Notice.

### 4. What are my rights?

Under Data Protection legislation, you have the following rights, which we will always work to uphold:

- The right to be informed about our collection and use of your personal data. This Privacy Notice should tell you everything you need to know, but you can always contact us to find out more or to ask any questions.
- The right to access the personal data we hold about you. If you want to know what personal data we have about you, you can ask us for details of that personal data and for a copy of it (where any such personal data is held). This is known as a “subject access request”.
- The right to have your personal data rectified if any of your personal data held by us is inaccurate or incomplete.
- The right to be forgotten, i.e. the right to ask us to delete or otherwise dispose of any of your personal data that we have. Please note that this right is not absolute and can only be exercised if (i) we no longer need your personal data for the original purpose, (ii) if you withdraw your consent for processing it, (iii) if you object to us processing your personal data for our legitimate interest, (iv) if we unlawfully process your personal data or (v) if a local law requires us to erase your personal data.
- The right to restrict (i.e. prevent) the processing of your personal data. You have the right to ask us to restrict the use of your personal data if (i) you believe that the personal data which we hold is inaccurate, (ii) if we are processing the personal data unlawfully, (iii) you have objected to us processing your personal data for our legitimate interests or (iv) we no longer need the personal data for the purposes of processing but you want us to keep this for the establishment, exercise or defence of legal claims.
- The right to object to us using your personal data for a particular purpose or purposes. If you make such an objection, we will cease to process the personal information unless we can demonstrate compelling legitimate grounds for the processing which override your interests (for example combating fraud), rights and freedoms, or the processing is for the establishment, exercise or defence of legal claims
- The right to data portability. This means that, if you have provided personal data to us directly, we are using it with your consent or for the performance of a contract, and that data is processed using automated means, you can ask us for a copy of that personal data to re-use with another service or business in a structured, commonly used and machine readable format. However, this right does not apply where it would adversely affect the rights and freedoms of others.
- Rights relating to automated decision-making and profiling. You have the right not to be subject to decisions which may legally or significantly affect you and that were based solely on automated processing using your personal data. We will however not use your personal data in this way.

To the extent that the legal basis for our processing of your personal information is consent, you have the right to withdraw that consent at any time. Withdrawal will not affect the lawfulness of processing before the withdrawal.

For more information about our use of your personal data or exercising your rights as outlined above, we advise you to consult our FAQs (if any) or we advise you to contact us via email ([gdpr@banquup.com](mailto:gdpr@banquup.com)) or in writing to the following address: Banquup, Avenue Reine Astrid 92 A, 1310 La Hulpe, Belgium (for the attention of the DPO).

There is in principle no charge for exercising your right. If, however, your request is ‘manifestly unfounded or excessive’ (for example, if you make repetitive requests) a fee may be charged to cover our administrative costs in responding.

We will respond to your request within one month after receiving it. Normally, we aim to provide a complete  
© Banquup Group S.A. – Website Privacy Notice - 4.0

response, including a copy of your personal data within that time. In some cases, however, particularly if your request is more complex, more time may be required up to a maximum of three months from the date we receive your request. You will be kept fully informed of our progress.

If you consider that our processing of your personal information infringes data protection laws, you have a legal right to lodge a complaint with a supervisory authority responsible for data protection. The contact details of your supervisory authority can be found [here](#). If you are located in the UK, please contact the [ICO](#). You may do so in the country of your habitual residence, your place of work or the place of the alleged infringement. We would welcome the opportunity to resolve your concerns ourselves, however, so please contact us first.

## 5. **What personal data do we process?**

In this section we have set out:

- a) the general categories of personal data that we may process;
- b) the purposes for which we may process personal data; and
- c) the legal bases of the processing.

Depending upon your use of our website, we may collect some or all of the following personal data:

### ***Usage data***

We may process data about your use of our website ("**usage data**"). The usage data may include your IP address, geographical location, browser type and version, operating system, referral source, length of visit, page views and website navigation paths, as well as information about the timing, frequency and pattern of your service use. The source of the usage data is our analytics tracking system. This usage data may be processed for the purposes of analysing the use of the website. The legal basis for this processing is our legitimate interests, namely monitoring and improving our website. However, where we collect usage data through non-essential cookies, we may request your consent. For more information please check our cookies policy.

### ***Job application data***

We may process your information like your contact details, your CV and your cover letter ("**job application data**"). The job application data may include your name, address, telephone number, email address, profile pictures, gender, date of birth, relationship status, interests and hobbies, educational details and employment details.

The application data may be processed for the following purposes: assess your skills, qualifications, and suitability for the role, communicate with you about the recruitment process, and keep records related to our hiring processes.

The legal basis for processing Job application data is the performance of the contract. The processing is necessary for the execution of pre-contractual measures and the establishment of the contractual relationship between Banquup and the candidate.

We may retain personal data from your CV for as long as it is necessary for our recruitment process but not longer than one year. In case we would like to keep it longer, we will request your consent. You may withdraw your consent at any time by sending an email to [gdpr@unfiedpost.com](mailto:gdpr@unfiedpost.com) .

As part of the Banquup Payments regulatory framework, we may also process your job application data if you apply to a job related to our payment services to prevent the use of Banquup Payments' systems and services for money laundering and terrorism financing, sanction circumvention or tax evasion. The legal basis is our legitimate interest, which is to protect the company's infrastructure from infiltration by criminals

and/or terrorists.

Banquup will always ask for your explicit consent to contact your previous and current employers and/or the contacts you have indicated.

### ***Enquiry data***

We may process information contained in any enquiry or registration form you submit to us regarding our company and/or our services ("**enquiry data**"). The enquiry data may be processed for the purposes of offering, marketing and selling relevant services to you. This is also the case if you participate in a contest or if you register for a webinar. The legal basis for this processing is our legitimate interest.

### ***Notification data***

We may process information that you provide to us for the purpose of subscribing to our email notifications and/or newsletters ("**notification data**"). The notification data may be processed for the purposes of sending you the relevant notifications and/or newsletters. The legal basis for this processing is your consent.

### ***Customer relationship data***

We may process information relating to our customer relationships, including customer contact information ("customer relationship data"). The customer relationship data may include your name, your employer, your job title or role, your contact details, and information contained in communications between us and you or your employer. The source of the customer relationship data is you or your employer. The customer relationship data may be processed for the purposes of managing our relationships with customers, communicating with customers, keeping records of those communications and promoting our products and services to customers. The legal basis for this processing is our legitimate interests, namely the proper management of our customer relationships.

### ***Supplier relationship data***

We may process information relating to our supplier relationships, including supplier contact information ("supplier relationship data"). The supplier relationship data may include your name, your employer, your job title or role, your contact details, and information contained in communications between us and you or your employer. The source of the supplier relationship data is you or your employer. The supplier relationship data may be processed for the purposes of managing our relationships with our suppliers/partners, communicating with the suppliers, and keeping records of those communications. The legal basis for this processing is our legitimate interests, namely the proper management of our supplier relationships.

### ***Whistleblowing data***

When submitting a whistleblower report, you may choose to do so anonymously. If you choose to identify yourself, we may collect your first and last name, email address, home address, and phone number. In addition, we may process personal data contained in the whistleblower report, which may, depending on the case, include identity information, information about the misconduct being reported, about the witnesses and third parties which were involved in the whistleblowing case, and information about the persons mentioned in the reports because they are victims of undesirable behaviour committed by the persons reported. We process these data to carry out preliminary investigations regarding the reported whistleblowing. The legal basis for processing these personal data is our legal obligation, namely an applicable national law transposing the EU Directive 2019/1937 on the protection of persons who report breaches of Union law (hereinafter Whistleblowing Directive). When the Directive doesn't apply, you still have the opportunity to submit a whistleblower report since UPG is committed to the highest standards of integrity and accountability. In that case, our legal basis is a legitimate interest to prevent and suppress any unlawful acts within the entities of the UPG.

In principle, we do not request or process any special categories of personal data (also known as sensitive personal data), e.g. information on racial and/or ethnic origin, religious and/or ideological convictions, trade union membership or sexual orientation nor personal data related to criminal convictions. However, such personal data may be contained in a whistleblower report. We will process such personal data when it is necessary for the establishment, exercise or defence of legal claims. To the extent that such legal basis would not exist, we would stop processing such personal data immediately.

#### **AGM Data**

We may process personal data of our shareholders, holders of other securities issued by UPG (if any) and proxy holders received in the context of the annual shareholders meeting that we are obliged to hold as a public listed company pursuant to the Belgian Company and Association Code. The personal data that we may collect in this context may include address, email address, and number of shares the shareholders have. These personal data may be processed for the purpose of management of the participation and voting procedure. The legal basis for this processing is our legal obligation to hold annual shareholders meetings, namely the statutory requirement under the Belgian Company and Association Code.

#### **Other's data**

We may process any of your personal data identified in this Notice where necessary for the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure. The legal basis is our legitimate interests, namely the protection and assertion of our legal rights, your legal rights and the legal rights of others.

We may process any of your personal data identified in this Notice where necessary for the purposes of obtaining or maintaining insurance coverage, managing risks, or obtaining professional advice. The legal basis for this processing is our legitimate interests, namely the proper protection of our business against risks.

In addition to the specific purposes for which we may process your personal data set out in this section, we may also process any of your personal data where such processing is necessary for compliance with a legal obligation to which we are subject, or in order to protect your vital interests or the vital interests of another natural person.

Please do not supply any other person's personal data to us, unless we prompt you to do so.

### **6. Do you share my personal data?**

#### **6.1. Use of processor(s)**

We are free to rely on data processors (which may include any member of the Banquup Group). A processor is the natural or legal person who processes your personal data upon request and on behalf of us, the controller. The processor is required to ensure the security and confidentiality of the personal data. The processor will always act on our instructions. We may rely on processors for hosting purposes, administrative purposes, marketing purposes, analytic purposes, communication purposes, whistleblowing purposes.

With a view to the optimal protection of your personal data, we have made the necessary contractual arrangements with our processors to ensure that they apply the highest privacy standards. In any event, data processors shall be required to ensure the security and confidentiality of the personal data.

#### **6.2. Transfer of personal data to third parties**

In addition to the specific disclosures of personal data set out in this section, we may also disclose your personal data where such disclosure is necessary for the establishment, exercise, or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure. We may also disclose your personal data where such disclosure is necessary for compliance with a legal obligation to

which we are subject, or in order to protect your vital interests or the vital interests of another natural person. We may disclose AGM data for the purpose of providing assistance in the management of participation and voting procedures, and for analysing the composition of the shareholder base of UPG.

## 7. International transfers of your personal data

In certain circumstances, we may store or transfer some or all of your personal data in countries that are not part of the EEA. This might for instance be the case when we are making use of processors who make use of specific sub-processors. These are known as "third countries" and may not have data protection laws that are as strong as those in the EEA. This means that we will take additional steps in order to ensure that your personal data is treated just as safely and securely as it would be within the EEA and under the Data Protection Legislation as follows:

We transfer your personal data to third countries whose levels of data protection are deemed 'adequate' by the European Commission, the UK government or the Swiss Federal Council. More information is available from the [European Commission](#), [ICO](#) and the [FDPIC](#) websites.

We use specific contracts with external third parties that are approved by the European Commission for the transfer of personal data to third countries. These contracts require the same levels of personal data protection that would apply under the GDPR, UK GDPR, Swiss FADP.

If you are located outside the EEA, similar restrictions apply.

Please contact us for further information about the particular data protection mechanisms used by us when transferring your personal data to a third country.

### 7.1. How long will you keep my personal data?

We will not keep your personal data for any longer than is necessary in light of the reason(s) for which it was first collected. Your personal data will therefore be kept until you delete your account or as long as required by mandatory law. Your data personal data will therefore be kept for the following periods:

Type of Data	How long we keep it
Usage data	Please check our cookies policy for the detailed retention periods
Enquiry data	6 months
Job application data	1 year
Customer/Supplier relationship data	10 years after the end of the contractual relationship
Whistleblowing data	6 months when it concerns closed cases
AGM Data	5 years

In some cases, it is not possible for us to specify in advance the periods for which your personal data will be retained.

Notwithstanding the other provisions of this section, we may retain your personal data where such retention is necessary for compliance with a legal obligation to which we are subject, or in order to protect your vital

interests or the vital interests of another natural person.

## **8. How do we protect your personal data?**

The security of your personal data is essential to us. To protect your data, we will take appropriate technical and organisational precautions. This means that we have the necessary policies and procedures and IT security measures in place to ensure the confidentiality and integrity of your personal data. These policies, procedures and measures are periodically updated to keep them in line with regulations and market developments.

Internal access to the personal data is limited on a strict 'need-to-know' basis. Only authorized personnel, whose activity will be monitored to prevent any misuse, will be able to access the personal data.

## **9. Third party websites**

Our website includes hyperlinks to, and details of, third party websites. We have no control over, and are not responsible for, the privacy policies and practices of third parties.

## **10. Personal data of children**

Our website is targeted at persons over the age of 18. If we have reason to believe that we hold personal data of a person under that age in our databases, we will delete that personal data.

## **11. Changes to this Privacy Notice**

We reserve the right to change this Privacy Notice from time to time. This may be necessary, for example, if the law changes, or if we change our website in a way that affects personal data protection and privacy. Every change will be posted on our website. We advise you to consult our Privacy Notice regularly to be kept up to date.

Last update : December 29th, 2025