

## **CANDIDATE PRIVACY POLICY (RECRUITMENT)**

The purpose of this Privacy Policy is to inform candidates about how their personal data is collected, used, stored and shared within the recruitment process.

This Charter applies to all applications submitted:

- via the careers website,
- by email,
- through third-party platforms (LinkedIn, Indeed, etc.),
- through recruitment firms, headhunters or temporary employment agencies mandated by us, or
- from professional social networks or recommendations.

### **1. The Data Controllers of your personal data**

For the processing of your personal data as described below, the data controller is the FDJ United Group company which is the originator of the recruitment need, and which may become your potential employer as identified in the advertisement to which you are applying or during your interview (hereinafter the "Data Controller").

Each Data Controller remains responsible for the processing of personal data from applications it receives for its own recruitment needs and remains responsible for communicating any complementary Privacy Policy corresponding to its activities as well as the needs and specificities of its territory.

Other companies in the Group as well as service providers involved in all or part of the processing of personal data from these applications must be considered as subcontractors, in particular by maintaining a shared application management system.

### **2. Our commitments**

Your privacy is a priority for the Data Controller.

We are committed to building a relationship of trust with our candidates and future employees and we pledge to protect your privacy in accordance with, in particular, the French Data Protection Act of 6 January 1978 as amended and Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 (" **GDPR** ") where applicable.

In this respect, we adhere to the following principles:

- We only collect the personal data we need,
- We process your personal data for explicit, legitimate and specific purposes,
- We retain your personal data for the period necessary to carry out the processing for which it was collected or, if applicable, for the period stipulated by law,
- We only disclose your personal data to legal entities and individuals who need to know it,

- We take care to implement appropriate security measures to ensure a high level of protection for your personal data.

### 3. What categories of personal data do we collect and how do we collect them?

Personal data is defined as any information relating to an identified or identifiable natural person.

We are required to collect the following personal data:

#### Personal data provided by you:

- **Identification data:** Information that allows the employee to be identified directly or indirectly (e.g., identity, contact details),
- **Data usually found in resume (CV) and professional profiles:** academic and university background, professional background, training, skills; cover letter, current or desired salary, availability,
- **Supporting documents for the right to work** (identity card, residence permit, work permit, etc.), when required by applicable regulations.

#### Personal data we collect:

- Public data from public sources and professional forums or networks (such as LinkedIn),
- Data related to individuals providing a reference about you,
- Data related to your browsing on our sites when you consent to the use of cookies,
- Data from diploma verification bodies and public bodies.

#### Personal data generated by the recruitment process:

- Data from interviews and assessments: interview reports, comments from internal or external recruiters.
- Data related to your access to our sites during face-to-face interviews and meetings.

### 4. How do we use and store your personal data?

Your data is used primarily for the following purposes:

Treatment	Purposes	Legal Basis	Retention Period
Application management and initial profile assessment	Evaluation, management and monitoring of applications Evaluation of profiles and suitability for the position	Implementation of pre-contractual measures at the request of the candidate	The data of unsuccessful candidates is kept for 2 years from the last contact with the candidate. The data of successful candidates are integrated

Treatment	Purposes	Legal Basis	Retention Period
			into the employee's administrative file, according to the applicable internal rules
Management of pre-contractual information	Verification of legal capacity to work	Compliance with legal obligations (e.g., verification of the right to work)	The data is retained only for the period necessary for the verification.
Access control to premises	The need to ensure the safety of people and property, for the purposes of site access control	legitimate interest in ensuring the safety of people and premises	For identification data: 12 months after the last site visit
CV database	Creation of an internal CV database	Consent	The data of unsuccessful candidates is kept for 2 years from the last contact with the candidate unless the candidate withdraw its consent.
Internal reporting	Reporting and management of recruitment at group level.	Legitimate Interest	The data of unsuccessful candidates is kept for 2 years from the last contact with the candidate, unless the candidate objects.
Defending our interests in case of disputes	Defending interests in the event of litigation against companies	Legitimate interest	Up to 5 years in intermediate archiving after recruitment is closed

Final candidates may be asked to participate in a background check that includes credit checks and demonstrating potential previous criminal convictions. These records will never be stored. We will never request you to provide sensitive data (data related to religion, health, sexual orientation, political beliefs, ethnicity or trade union memberships) unless we are legally required to do so in the country where you may be hired.

## 5. Who are the recipients of your personal data?

The personal data processed is intended for the Data Controller who initiated the recruitment request and is to benefit from it.

Only persons authorized by virtue of their function may access the personal data of candidates, and this is strictly limited to the performance of their duties and functions.

This could include, for example:

- to the HR teams and managers of the position concerned,
- to the HR teams involved in the recruitment process,
- to the service providers involved in the process (hosting providers, HR software publishers, recruitment agencies, testing providers),
- authorized persons responsible for ensuring the safety of people and property, for the purposes of access control to the premises.

Your personal data may also be shared with subcontractors (hosting providers, recruitment agencies, training organizations, etc.) only to the extent necessary for them to perform the services we entrust to them. We require our subcontractors to adhere to strict personal data protection rules in accordance with applicable laws and regulations.

Furthermore, your personal data may be transmitted to any competent authorities or bodies such as Social Security, pension fund, or Directorate General of Public Finances.

In some cases, your personal data may be transferred outside the European Union. These transfers are always subject to strict legal frameworks to ensure a high level of protection and security for your personal data, as well as compliance. This includes adequacy decisions by the European Union, Standard Contractual Clauses and permitted safeguard measures to protect your privacy and other rights.

The candidate is informed that their personal data may be transferred to other companies in the Group located abroad, solely for recruitment purposes.

## **6. How is your personal data secured?**

We take care to implement appropriate technical, physical and organizational control measures to ensure the security and confidentiality of your personal data, in particular to protect it against loss, accidental destruction, alteration, and unauthorized access.

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

In accordance with applicable legal and regulatory provisions regarding the protection of Personal Data, you have the following rights described below. Please note that these rights may be restricted to comply with legal obligations or legitimate interests, or if your requests are deemed manifestly unfounded or excessive. In other words, the applicability of your rights will vary depending on the circumstances related to the processing of your data.

### **Right to be informed**

You have the right to be provided with clear, transparent and easily understandable information about how we use your information and your rights. This is why we're providing you with the information in this Privacy Notice.

### **Right of access**

You are entitled to a copy of the personal data we hold about you (if we are processing it) and certain details of how we use it.

### **Right to rectification**

You are entitled to have your information corrected if it is inaccurate or incomplete.

### **Right to erasure**

In certain circumstances, you may have the right to ask us to erase your personal information, for example where the personal information we collected is no longer necessary for the original purpose or where you withdraw your consent. However, this will need to be balanced against other factors. For example, we may have legal and regulatory obligations which mean that we cannot comply with your request fully.

#### **Right to restriction of processing**

You have the right to restrict some processing of your personal information, which means that you can ask us to limit what we do with it.

#### **Right to data portability**

Where processing is based on your consent or for the performance of a contract and where the processing is carried out by automated means, you have the right to data portability. Whilst it is unlikely that this right will apply in the context of our processing, we will consider requests where you feel this right applies.

#### **Right to object**

You have the right to object to processing which is based on our legitimate interests. Unless we have a compelling legitimate ground for the processing, we will no longer process the personal data on that basis when you file an objection.

#### **Rights relating to automated decision-making**

You have the right not to be subjected to automated decision-making, including profiling, which produces legal effect for you or has a similar significant effect. Please note that we do not use automated decision-making or profiling in the recruitment process that produces legal or similar significant effects for you.

#### **Right to withdraw consent**

In most cases, we do not base the processing of your personal data on your consent. However, it may happen that we ask for your consent in specific cases (for example the CV database). Where we do this, you have the right to withdraw your consent to further use of your personal information.

#### **Right to file a complaint**

If you believe that your rights described in this policy have not been respected, you have the right to lodge a complaint with the supervisory authority for data protection.

#### **How to exercise your rights etc.**

You can exercise your rights by simply writing to:

- If you are applying for a position in France: [donneespersonnellesRH@fdunited.com](mailto:donneespersonnellesRH@fdunited.com)
- If you are applying for a position outside of France: [DPHR@kindredgroup.com](mailto:DPHR@kindredgroup.com).

Please be as precise as possible, in particular by indicating which job offer concerns you and which right you wish to exercise and the personal data concerned.

In accordance with applicable data protection regulations, the legal deadline for responding is a maximum of one month from the date of receipt of the request. This deadline may be extended by two months in the event of complexity or a large number of requests, in which case you will be informed of this extension and the reasons for the delay within one month of receipt of the request. For example, if you send us a letter that we receive on June 10, we have until July 10 to respond, or until September 10 if the request is complex.

You may have the option to leave specific instructions regarding the management of your personal data after your death.

\*\*\*

It should be noted that this Charter may be amended to take into account legal, organizational or technical developments.

**Last updated:** January 2026