



Applicant Data Protection Notice

Version and Change Control

Date	Effective	Revision	Change reference
May 2026	May 2026	1.0	Initial version

Table of Contents

1. What is the purpose of this document?.....	3
2. Data protection principles.....	3
3. How do we collect your personal data?.....	3
4. Why we collect and process your personal data, legal basis and data retention period.....	4
5. Data recipients and transfers.....	11
6. What security measures do we provide for your data?.....	11
7. Applicants rights & duties.....	11
8. Glossary.....	12

1. What is the purpose of this document?

This privacy notice describes how Pigment (collectively “Pigment”, “we”, “us” and “our”) will collect and use the personal data of people that apply to Pigment positions or send spontaneous applications (the “Applicants”, “you”, “your”), in accordance with all relevant data protection legislations, including the EU and UK General Data Protection Regulation.

This notice applies to the Processing of Personal Data of Applicants that can be:

- People who apply to join an open position at Pigment that they found on our career website, on LinkedIn or on another job applications website;
- People who send a spontaneous application to Pigment;
- People who are approached by recruiters to apply to Pigment.

For the purposes of this document, these individuals are generally referred to as “Applicants”.

This Notice describes how we collect and use your Personal Data during your application process, in accordance with the applicable data protection legislation. If you join Pigment as a Staff Member following your application process, another data protection notice will apply to you for the duration of your working relationship with us and afterwards.

The terms used in this document (the “Pigment Applicants Data Protection Notice”) such as Personal Data or Processing have the meaning given to them by the glossary in Section VI or, failing that, by GDPR or the applicable local data protection legislation, if any.

We may update this notice at any time and if we do so, we will inform you.

2. Data protection principles

Pigment is committed to complying with all the laws and regulations that govern the Processing of Personal Data. Accordingly, Pigment undertakes that the Personal Data we hold about you must be:

- used lawfully, fairly and in a transparent way;
- collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes;
- relevant to the purposes we have told you about and limited only to those purposes;
- accurate and kept up to date;
- kept only as long as necessary for the purposes we have told you about; and
- kept securely.

3. How do we collect your personal data?

At Pigment, we collect and process different categories of Applicants’ Personal Data.

The Personal Data collected may be:

- identity and identification data (e.g. surname, first name, gender, scan of ID/passport);
- contact information (e.g. postal address, e-mail address and telephone number);
- information available in your CV (e.g. degrees, current company, former experiences, academic formation, details of any other relevant skills, such as language capabilities);
- all the information in your application (cover letter, all other relevant document);
- as appropriate, copies of certificates, diplomas or other documentation verifying the information you provide to us;
- all the you give us during the interview process (e.g. details about your professional and academic background, current salary and salary expectations, reasons for leaving your current company, ability to work in hybrid mode, existence of a non-competition clause in your current employment contract);
- location and right to work information (including information required to confirm your right to work in the country in which you will be employed, including as appropriate your nationality, national identity number and passport details);
- if you undergo a case study, all the information you share during this case study;
- notes and feedback on interviews taken by the recruiter (e.g. adequation of your application with the job and the team);
- videorecording and transcript of the interview (only if you consented to it beforehand);
- NDA-related data (e.g. name, surname, email address, NDA information, signature) in case you access our confidential information.

Pigment may also collect personal data about you from third parties:

- references from professional referees, after requesting your consent (e.g. summary of the exchange with them);
- information you made publicly available via LinkedIn or other social media profiles;
- Pigment may, from time to time, use external recruitment agencies which will directly collect information about you and share it with us.

4. Why we collect and process your personal data, legal basis and data retention period

We need to collect and process your personal data for the main purpose of recruitment.

We will only retain your personal data for as long as necessary to fulfil the purposes for which we collected it, including for the purposes of satisfying any legal, accounting or reporting requirements. Details of all the purposes for which we can process your data are available below and are associated with the legal basis, categories of personal data processed and the retention periods (for each country in which we operate). In some circumstances, we may anonymize your personal information so that it can no longer be associated with you, in which case we may use that information without further notice to you.

Why	Legal basis	What	Data retention period
To source potential Applicants	<ul style="list-style-type: none"> • Legitimate interest 	<ul style="list-style-type: none"> • identity and identification data (e.g. surname, first name, gender) • contact information (e.g. e-mail address, telephone number) • LinkedIn profile and all information you made publicly available via LinkedIn or other social media profiles; 	<ul style="list-style-type: none"> • France: <ul style="list-style-type: none"> ○ Successful recruitment: during the recruitment process and until the contract is signed then the necessary data can be kept for the duration of the employment ○ Unsuccessful recruitment: data can be kept for 5 years from the date on which the post was filled for evidential purposes, in the event of any discrimination claims. • Canada (Ontario): Employers must keep job postings, candidate applications, and communications after interviews for at least three years after a job posting closes • USA (federal): 1 year after creation of the document or the hire/no-hire decision, whichever is later. • Germany: <ul style="list-style-type: none"> ○ Successful recruitment: for the duration of your employment contract ○ Unsuccessful recruitment: 6 months (unless consent was obtained to store longer : 3 years maximum)

			<p>starting from end of application process</p> <ul style="list-style-type: none"> ● UK: <ul style="list-style-type: none"> ○ Successful recruitment: 2 years from the end of employment ○ Unsuccessful recruitment: 6 months from the last action
<p>For the application process (selection of candidates, interviews, organisation of interviews)</p>	<ul style="list-style-type: none"> ● Performance of pre-contractual measures 	<ul style="list-style-type: none"> ● identity and identification data (e.g. surname, first name, gender, scan of ID/passport) ● contact information (e.g. postal address, e-mail address and telephone number); ● information available in your CV (e.g. degrees, current company, former experiences, academic formation, details of any other relevant skills, such as language capabilities); ● all the information in your application (cover letter, all other relevant document); ● as appropriate, copies of certificates, diplomas or other documentation verifying the information you provide to us; ● all the information you give us during the interview process (e.g. details about your professional and academic background, current salary and salary expectations, reasons for leaving your current company, ability to work in hybrid mode, existence of a non-competition clause in your current employment contract) 	<ul style="list-style-type: none"> ● France: <ul style="list-style-type: none"> ○ Successful recruitment: during the recruitment process and until the contract is signed then the necessary data can be kept for the duration of the employment ○ Unsuccessful recruitment: data can be kept for 5 years from the date on which the post was filled for evidential purposes, in the event of any discrimination claims. ● Canada (Ontario): Employers must keep job postings, candidate applications, and communications after interviews for at least three years after a job posting closes ● USA (federal): 1 year after creation of the document or the hire/no-hire decision, whichever is later. ● Germany:

		<ul style="list-style-type: none"> • calendar information to find availability for interviews • notes and feedback on interviews taken by the recruiter (e.g. adequation of your application with the job and the team); • videorecording of the interview (only if you consented to it beforehand); 	<ul style="list-style-type: none"> ○ Successful recruitment: for the duration of your employment contract ○ Unsuccessful recruitment: 6 months (unless consent was obtained to store longer : 3 years maximum) starting from end of application process • UK: <ul style="list-style-type: none"> ○ Successful recruitment: 2 years from the end of employment ○ Unsuccessful recruitment: 6 months from the last action
<p>To check that the applicant is fit for the job (reference checks, case study that requires the signature of an NDA)</p>	<ul style="list-style-type: none"> • Performance of pre-contractual measures • Legitimate interest 	<ul style="list-style-type: none"> • references from professional referees, after requesting your consent (e.g. summary of the exchange with them) • NDA-related data (e.g. name, surname, email address, NDA information, signature) in case you access our confidential information. • if you undergo a case study, all the information you share during this case study; • notes and feedback on interviews taken by the recruiter (e.g. adequation of your application with the job and the team); • videorecording of the interview (only if you consented to it beforehand); 	<ul style="list-style-type: none"> • France: <ul style="list-style-type: none"> ○ Successful recruitment: during the recruitment process and until the contract is signed then the necessary data can be kept for the duration of the employment ○ Unsuccessful recruitment: data can be kept for 5 years from the date on which the post was filled for evidential purposes, in the event of any discrimination claims. • Canada (Ontario): Employers must keep job postings, candidate applications, and communications after interviews for at least

			<p>three years after a job posting closes</p> <ul style="list-style-type: none"> ● USA (federal): 1 year after creation of the document or the hire/no-hire decision, whichever is later. ● Germany: <ul style="list-style-type: none"> ○ Successful recruitment: for the duration of your employment contract ○ Unsuccessful recruitment: 6 months (unless consent was obtained to store longer : 3 years maximum) starting from end of application process ● UK: <ul style="list-style-type: none"> ○ Successful recruitment: 2 years from the end of employment ○ Unsuccessful recruitment: 6 months from the last action
<p>For administrative purposes (visa requirements, reporting obligations)</p>	<ul style="list-style-type: none"> ● Legal obligation 	<ul style="list-style-type: none"> ● identity and identification data (e.g. surname, first name, gender, scan of ID/passport) ● contact information (e.g. e-mail address, telephone number) ● location and right to work information (including information required to confirm your right to work in the country in which you will be employed, including as appropriate your nationality, national identity number and passport details); 	<ul style="list-style-type: none"> ● France: <ul style="list-style-type: none"> ○ Successful recruitment: during the recruitment process and until the contract is signed then the necessary data can be kept for the duration of the employment ○ Unsuccessful recruitment: data can be kept for 5 years from the date on which the post was filled for

			<p>evidential purposes, in the event of any discrimination claims.</p> <ul style="list-style-type: none"> ● Canada (Ontario): Employers must keep job postings, candidate applications, and communications after interviews for at least three years after a job posting closes ● USA (federal): 1 year after creation of the document or the hire/no-hire decision, whichever is later. ● Germany: <ul style="list-style-type: none"> ○ Successful recruitment: for the duration of your employment contract ○ Unsuccessful recruitment: 6 months (unless consent was obtained to store longer : 3 years maximum) starting from end of application process ● UK: <ul style="list-style-type: none"> ○ Successful recruitment: 2 years from the end of employment ○ Unsuccessful recruitment: 6 months from the last action
<p>To keep a CV database</p>	<ul style="list-style-type: none"> ● Legitimate interest 	<ul style="list-style-type: none"> ● information available in your CV (e.g. degrees, current company, former experiences, academic formation, details of any other 	<ul style="list-style-type: none"> ● France: <ul style="list-style-type: none"> ○ Unsuccessful recruitment: data can be kept for 5 years from the date on which

	<ul style="list-style-type: none"> • Consent (if we want to keep it longer) 	<p>relevant skills, such as language capabilities);</p> <ul style="list-style-type: none"> • all the information in your application (cover letter, all other relevant document); 	<p>the post was filled for evidential purposes, in the event of any discrimination claims</p> <ul style="list-style-type: none"> • Canada (Ontario): Employers must keep job postings, candidate applications, and communications after interviews for at least three years after a job posting closes • USA (federal): 1 year after creation of the document or the hire/no-hire decision, whichever is later. • Germany: <ul style="list-style-type: none"> ○ Unsuccessful recruitment: 6 months (unless consent was obtained to store longer : 3 years maximum) starting from end of application process • UK: <ul style="list-style-type: none"> ○ Unsuccessful recruitment: 6 months from the last action
<p>To make statistics</p>	<ul style="list-style-type: none"> • Legitimate interest 	<ul style="list-style-type: none"> • Data about applicants (e.g. gender, seniority level) • Number of interviews conducted, conversion rate, time to recruit: number of days between application and acceptance of the offer 	<p>The data is aggregated and can be kept without the need to establish a data retention period.</p>

5. Data recipients and transfers

Who has access to your data within Pigment?

At Pigment, we share Personal Data on a need-to-know basis only. Based on this principle, your Personal Data will be shared, on a granular basis, within the People Team. Your Personal Data will only be shared with other teams (e.g. Legal, Finance, IT) if you accept an offer after the recruitment process and sign a contract with a Pigment Entity.

When do we share your personal data with third parties and with Pigment affiliates?

We may share your Personal Data with other entities that are part of Pigment Group (i.e Pigment Inc. (USA), Pigment Corp. (Canada), Pigment Global Limited (UK) and Pigment GmbH (Germany), if necessary.

In addition, we share your Personal Data with other third-parties such as services providers (e.g. applicant tracking system, visioconference, e-signature, sourcing providers, job application websites), or authorized recipients (e.g professional referees). When we do so, we require third parties to respect the security of your data and to process it in accordance with the law. When your Personal Data is transferred outside of the UK or EEA, we make sure a similar degree of protection is implemented as if your Personal Data was processed within the EEA.

We may also need to share your personal information with a regulator or to otherwise comply with the law.

6. What security measures do we provide for your data?

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

To learn more about security at Pigment, please read our security policies.

7. Applicants rights & duties

Your rights and how to enforce them:

As data subjects, Applicants are entitled to exercise the rights set out in the applicable regulations (such as GDPR) and domestic data protection legislation. Applicants have, subject to certain conditions and limits, a right of access, to rectify and erase their Personal Data collected by a Pigment Entity. Data subjects also have the right to data portability (except where we rely on our legitimate interest to process your data), to request its restriction or to object to the Processing of

their Personal Data. In the limited circumstances where you may have provided your consent to the collection, Processing and transfer of your Personal Data for a specific purpose, you have the right to withdraw your consent for that specific Processing at any time.

These rights can be exercised by sending either:

- An email to dpo@pigment.com, or
- A letter, to Pigment – Data Protection Officer – 8-12 rue Sainte-Cécile, 75009, Paris (France).

To protect the Personal Data of the data subject exercising their rights Pigment will need to identify the data subject before responding to the request. If there are reasonable doubts about their identity, the data subject may be asked to provide a copy of an official identity document, such as an identity card or passport, to support his or her request. The data subjects are entitled to file a complaint with a supervisory authority.

Your duty to inform us of changes:

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your application process.

8. Glossary

Pigment (or Group):	refers to Pigment SAS and its affiliates.
Pigment Entity:	refers to any legal entity of the Pigment Group, i.e. companies controlled directly or indirectly by Pigment SAS.
Data Controller:	the person who, alone or jointly with others, determines the purposes and means of Processing Personal Data.
Personal Data:	any information relating to an identified or identifiable individual. An individual who can be identified, directly or indirectly, including by reference to an identifier, such as a name, identification number, location data, online or to one or more specific elements specific to one's physical, physiological, genetic, psychological, economic, cultural or social identity is deemed to be an identifiable individual.
Processing:	any operation or set of operations performed or not in an automated manner and applied to data or data sets such as collection, recording, organisation, structuring, retention, adaptation or modification, extraction, consultation, use, communication by transmission, circulation or any other form of dissemination, reconciliation or interconnection, limitation, erasure or destruction.

Recipient:	whether a third party or not any individual or legal entity, public authority, department or any other organisation to which Personal Data is disclosed.
Staff Member:	refers to (i) employees and other workers working for Pigment Group, including interns and work-study trainees and (ii) former employees of Pigment Group.
GDPR:	refers to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals in relation to the processing of personal data and the free circulation of this data.