

Candidates Privacy Policy

Last updated in October 2026

BIC Group
BIC Candidates Privacy Policy
Responsible: Legal & Compliance
Date: OCTOBER 2026

TABLE OF CONTENTS

I. PRIVACY STATEMENT 2
II. DATA CONTROLLER 2
III. SOURCES OF PERSONAL DATA 2
IV. WHAT PERSONAL DATA DOES BIC PROCESS AND WHY? 3
V. REFERRAL CANDIDATES 3
VI. USE OF ARTIFICIAL INTELLIGENCE 3
VII. HOW AND WITH WHO WE MAY SHARE PERSONAL DATA 4
VIII. YOUR PRIVACY RIGHTS AND HOW TO EXERCISE THEM 4
IX. INTERNATIONAL DATA TRANSFERS AND DATA STORAGE 6
X. HOW LONG WILL BIC KEEP YOUR PERSONAL DATA? 6
XI. HOW DOES BIC KEEP YOUR PERSONAL DATA SECURE? 6
XII. COOKIES 7
XIII. CHANGES TO THE POLICY 7
APPENDIX 1. GLOSSARY 8
APPENDIX 2. LIST OF PROCESSING ACTIVITIES 9
APPENDIX 3. EXERCISING YOUR PRIVACY RIGHTS 12

I. PRIVACY STATEMENT

BIC is a multinational group which has been engaged for many years in the business of research, development, manufacturing, marketing and sale of Stationery, Lighters, Shavers and Brushes. BIC operates worldwide through its network of affiliated companies and subsidiaries.

In this Candidates Privacy Policy (the "Policy"), references to "BIC", "we", "us" and "our" will mean the hiring BIC entity, as specified in the job description. BIC and subsidiaries will be referred to collectively as BIC.

This Policy applies to Personal Data we collect through our career website and through other websites where candidates can submit applications for job opportunities at BIC.

BIC is committed to protecting your privacy. The purpose of this Policy is to inform you about the types of Personal Data we may gather about you, how we use that data, whether we disclose it to anyone, and the choices you have regarding our use of your Personal Data. This is done in compliance with applicable laws relating to the protection of Personal Data.

If local applicable law provides stricter obligations for BIC than the provisions contained in this Policy, the stricter obligations of local law shall prevail, and shall be deemed incorporated in this Policy. On the contrary, where the provisions of this Policy are more stringent than what is required by local law, the rules of this Policy must be applied.

Words in capital letters have the meaning given by the GDPR unless (i) other Data Protection Laws apply, in which case, they will be interpreted in light of the closest term of the applicable Data Protection Laws or (ii) as otherwise specified under **Appendix 1**.

II. DATA CONTROLLER

The Data Controller is **Société BIC**, having its registered office 12 boulevard Victor Hugo 92611 Clichy, France. BIC determines how and why your Personal Data is processed.

For certain Processing, the Data Controller of your Personal Data is the hiring BIC entity as specified in the job description.

III. SOURCES OF PERSONAL DATA

BIC may collect Personal Data from the following categories of sources:

- **Directly from you**: Most of the Personal Data BIC processes is obtained from you when you file your application with BIC, or in the course of the application process, for example during interviews.
- **From your device**: Our career website, and other electronic interactions (such as emails we send to you) may automatically collect Personal Data about your interaction with our team.
- **From other sources**: Other Personal Data may be collected from third parties, including recruitment agencies or networking platforms, such as LinkedIn, where we may identify and contact potential candidates, or through background checks conducted during the recruitment process.

IV. WHAT PERSONAL DATA DOES BIC PROCESS AND WHY?

The categories of Personal Data that BIC collects, together with the applicable legal basis for the collection and use of such Personal Data, are set out in the table in **Appendix 2**.

For each purpose, we ensure that there is a legal basis for the Processing. In general, we use Personal Data to review candidates' resumes, recruit and hire new team members. We may process certain Personal Data with your consent, for legitimate reasons allowed under Data Protection Laws or in order to comply with a legal obligation.

When we rely on our legitimate interest as the legal basis for Processing your Personal Data, we conduct a balancing test prior to the Processing, to assess whether our legitimate interests are outweighed by your interests and rights, as required under applicable Data Protection Laws.

Certain Personal Data must be collected to enable the recruitment process, while the collection of other data may be optional. Whether providing such information is mandatory or optional is clearly indicated to candidates when they complete their application. In some cases, a third option may also be proposed, allowing candidates to select "*I do not wish to answer*".

BIC does not process Special Categories of Data during the recruitment process.

V. REFERRAL CANDIDATES

If you receive an email from BIC inviting you to apply for a job position, it means that a referrer provided BIC with a recommendation for your consideration as a candidate along with your resume. If you do not wish to apply for the position and would like your information removed, please follow the link provided in the email or contact our Data Protection Officer ("DPO") at privacy@bicworld.com.

VI. USE OF ARTIFICIAL INTELLIGENCE

As of today, BIC does not use artificial intelligence ("AI") systems in its recruitment processes to make final hiring decisions. All final assessments and decisions are made by human recruiters and hiring managers. However, at the initial screening stage, an automated decision tree may be used to assist the initial screening and categorization of CVs based on predefined criteria. Such tools do not make hiring decisions and are used solely to support human review.

Online interviews may be recorded and transcribed using AI-based tools, the candidate will be informed in advance, and such recording or transcription will occur only with the candidate's explicit consent.

Also, some third-party providers we work with (see Section VII below), such as LinkedIn, where we post job offers, may have integrated AI functionalities into their platforms, but we do not exercise control over these third parties' platforms.

If, in the future, BIC begins to use AI for recruitment purposes, candidates will be informed in advance that they are interacting with an AI system, and this Policy will be updated accordingly.

VII. HOW AND WITH WHO WE MAY SHARE PERSONAL DATA

BIC may disclose Personal Data for the purposes described in Section IV.

The categories of recipients with whom BIC may share Personal Data include the following:

- **BIC**: Your Personal Data is shared between BIC and its affiliates in specific circumstances and only where it is lawful to do so, for example, with members of the Talent Acquisition team or the HR and IT departments, who may be working for different BIC entities. Whenever we need to share your Personal Data, we do so on a need-to-know basis and only with selected team members, to the extent necessary, for them to carry out their responsibilities.

- **Third-party service providers:** We use third-party service providers, e.g., SuccessFactors as applicant tracking system, or recruitment agencies, who provide technical and support services in connection with the application and recruitment process. In providing the services, your Personal Data might be processed by the service provider on BIC's behalf. For any service providers we partner with, we have a process in place to ensure they provide guarantees regarding the confidentiality and security of your Personal Data, and that they comply with Data Protection Laws. In any case, service providers are prohibited from using your Personal Data except to provide their services to BIC.

- **Authorized third parties**: In certain circumstances we might share your Personal Data with third parties; as necessary to detect security incidents and fraudulent or illegal actions; to protect the safety, property, or other rights of BIC, you, and other persons and entities; to comply with applicable law, in each case in accordance with applicable Data Protection Laws.

In all cases, BIC implements measures designed to ensure that appropriate safeguards are in place to protect candidates' Personal Data and ensure compliance with applicable Data Protection Laws.

Information for candidates based in California: in the past 12 months since the "Last Updated" date of this Policy, BIC has not "sold" or "shared" (*NB: these terms are defined under the CCPA*) Personal Data of candidates.

VIII. YOUR PRIVACY RIGHTS AND HOW TO EXERCISE THEM

Under the Data Protection Laws, you may have some or all the following rights.

Rights	What does it mean?
Right to be informed	You have the right to be informed about the collection and use of your Personal Data by us.
Right of access	You have the right to access and receive a copy of your Personal Data we hold about you and other information, including if applicable, in a machine-readable format.
Right to rectification	You have the right to have inaccurate Personal Data rectified or completed if it is incomplete.
Right to erasure/delete/to be forgotten	You have the right to ask us to delete or remove Personal Data we collected from or about you.

Rights	What does it mean?
Right to restrict Processing or right to limitation	You have the right to request the restriction of the Processing of your Personal Data, under some circumstances and for certain purposes.
Right to object	You have the right to object to us using your Personal Data in the context of direct marketing, and targeted advertising or where Processing is on the ground of legitimate interest. Objecting does not affect the lawfulness of the collection and Processing of Personal Data performed prior to the objection.
Right to withdraw your consent	At any time, in the context of any consent-based Processing of your Personal Data. Withdrawing your consent does not affect the lawfulness of the collection and Processing of Personal Data performed prior to the withdrawal.
Right to not be subject to an automated decision	You have the right not to be subject to a decision based solely on automated Processing, if this decision has legal effects concerning you or similarly affects you.
Right to data portability	You have the right to obtain and reuse your Personal Data for your own purposes across different services.
France specific: **Right to organize what happens to your Personal Data in the event of your death**	You can give us instructions on how to store, delete and communicate your Personal Data after your death.

To exercise your rights, you may contact our DPO at privacy@bicworld.com at any time.

Requests will be reviewed in accordance with applicable Data Protection Laws, and a response will be provided within one month. In certain cases, if the request is particularly complex or if multiple requests have been made, this period may be extended by an additional 2 months (or by such period as permitted under applicable Data Protection Laws). If an extension is necessary, you will be informed accordingly.

Please note that, as required or permitted under applicable laws, we may take steps to verify your identity before addressing your request related to privacy rights. We may require you to provide your first name, last name, email address, and other necessary information to help verify your identity. We may not be able to respond to your request or provide you with Personal Data if we cannot verify your identity or the authority of the person submitting the request and confirm the Personal Data relates to you.

We also invite you to consult **Appendix 3** below to learn how to contact us based on your location, as well as which local Supervisory Authority you can refer to.

IX. INTERNATIONAL DATA TRANSFERS AND DATA STORAGE

BIC is a global company with operations in many countries and Personal Data is processed globally, with headquarters in France and in the United States of America.

Personal Data is stored at a secured location and on servers located in Germany. We or our service providers may use servers located in the United States of America for back up and emergency storage.

BIC may transfer your Personal Data to countries outside your country of residence for various operational purposes. This may occur because the data is hosted outside your country of residence, or because managers are based abroad in another BIC affiliate.

To the extent BIC transfers Personal Data across borders, BIC relies on legally provided mechanisms to lawfully transfer Personal Data, including Standard Contractual Clauses approved by the European Commission, relevant United Kingdom authorities, by the Brazilian Data Protection Authority and other local legislation as applicable.

X. HOW LONG WILL BIC KEEP YOUR PERSONAL DATA?

If your application for employment is successful and you are hired by BIC, your Personal Data will be transferred to your employee file and will be processed for employment-related purposes.

In the event of an unsuccessful application, BIC will retain your Personal Data for six months in order to inform you of potential future job opportunities. You may object to this use of your Personal Data at any time. At the end of this period, if you wish to submit a new application, you will have to provide all the necessary information and Personal Data again.

BIC establishes and maintains data retention periods in compliance with Data Protection Laws, including any applicable local requirements. Local addendums to this Policy, or local work instructions, may specify the data retention periods that apply in your jurisdiction.

XI. HOW DOES BIC KEEP YOUR PERSONAL DATA SECURE?

BIC takes the security of your Personal Data very seriously and implements technical and organizational measures designed to protect it.

We make efforts to ensure that all Personal Data we hold about you:

- Can only be accessed, altered, disclosed or deleted by those who are authorized to do so, in accordance with the principle of least privilege.
- Is accurate, up to date and contains only information needed for our purposes outlined in this Policy
- Remains accessible and usable only by authorized individuals, ensuring business continuity and the proper functioning of our services.

In addition, BIC regularly reviews its data security practices, provides training to staff, and requires third-party providers to meet equivalent security standards through contractual obligations.

Further, if we are required to provide you with notice of a Data Breach, or do so voluntarily, you agree that we may do so via reasonable electronic notice, including by sending notice to any email address we have on file to you, at our discretion. In any case, where Data Breach occurs and its reporting is required by law, we will follow the local applicable legal provisions.

XII. COOKIES

We may use standard technology called "cookie" to collect information about how our websites are used. You can accept, refuse or set your cookie preferences when you first log on to the website, and change your preferences at any time.

XIII. CHANGES TO THE POLICY

This Policy is subject to change at our discretion.

Revision	Date	Description of Change	Revised By	Approved By
New	09-2020	Established Policy	DPO	
V1	10-2026	Revision, new format, new and updates sections.	DPO	Global Compliance Director

APPENDIX 1. GLOSSARY

Data Controller means a person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

Data Protection Laws means all applicable laws relating to the protection of Personal Data, privacy and electronic communications as amended from time to time. These laws may include the European Union General Data Protection Regulation ("GDPR"), the California Consumer Privacy Act ("CCPA"), the UK Data Protection Laws ("UK GDPR"), the Data Protection Law(s) of Mexico, the Data Protection Law(s) of Switzerland ("LPD"), the Data Protection Law(s) of Brazil ("LGPD"), and the Data Protection Law(s) of any other relevant country.

Personal data (or Personally Identifiable Information) means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly.

Personal Data may include:

- Personal identification & contact details: **name, surname, photo, video, address, telephone number, etc.**
- Professional identification & contact details: **email, address, phone number, team members number/code, etc.**
- Data about personal life: **life habits, family situation, etc.**
- Data about professional life: **department, hierarchy, CV, diploma, etc.**
- Financial and economic data: **income, fiscal situation, etc.**
- Governmental identification: **ID number, passport number, social security number, etc.**
- Individual connection & location data: **IP address, other logs, GPS, GSM data, etc.**
- Legal and compliance data: **background check results, confirmation of eligibility to work in a given country.**

This list is not exhaustive because what is considered Personal Data depends on local legislation, context and how data can be combined or linked to identify a person. Also, new technologies constantly generate new types of data (biometric data, behavioural data, device identifiers, etc.).

Some types of Personal Data are likely to be more sensitive, known as "**Special Categories of Data**".

Processing means any operation performed on Personal Data. It includes collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of Personal Data.

Supervisory Authority is the independent public authority responsible for monitoring the application of the applicable Data Protection Law.

APPENDIX 2. LIST OF PROCESSING ACTIVITIES

Processing activity	Personal Data collected and processed	Legal basis for the use of Personal Data
In the context of recruitment administration and communication		
Recruitment administration: publication of job offers online, setting up candidates' accounts to receive applicants' information and documents.	Candidate's name, contact information, country of residence, recruitment details, qualifications and diplomas, foreign language spoken, CV, disability situation.	This is necessary for the purpose of our legitimate interests to recruit new team members and assess their qualifications and ability to perform the job.
Job updates communications: notifying you about future BIC job opportunities.	Candidate's contact details.	You provided your consent to receive such communications from us.
Referral program: contacting candidates referred by BIC team members as part of the referral program.	Candidate's name, contact details and referrer's contact details.	This is necessary for the purpose of our legitimate interests to recruit new team members and assess their qualifications and ability to perform the job.
In the context of reviewing candidates' profiles		
Resumes and cover letters screening: handling Personal Data for screening, and evaluating applications, based on the criteria of the position, such as the required experience or the expected level of seniority.	Candidate's name and contact details, professional background, any additional information contained in these documents.	This is necessary for the purpose of our legitimate interests to recruit new team members and assess their qualifications and ability to perform the job.
Assessing reports from external recruitment agencies	Candidate's name, contact details of former manager, professional background, professional skills and	This is necessary for the purpose of our legitimate interests to recruit new team members and assess

Processing activity	Personal Data collected and processed	Legal basis for the use of Personal Data
and references management provided by former managers.	any additional information provided by the former manager and recruitment agencies.	their qualifications and ability to perform the job.
Background checks: conducting background checks on candidates in accordance with a legal obligation or for positions above a certain job level.	Candidate's name, employment history, data related to criminal convictions and offenses.	This is necessary to fulfill our statutory and regulatory obligations and for the purpose of our legitimate interests to recruit new team members and assess their qualifications and ability to perform the job.
In the context of conducting interviews		
Candidates' interviews: organization of interviews between the candidates and the relevant stakeholders at BIC.	Candidate's name and contact details, professional background, financial and economic data, communication data, interview details and notes.	This is necessary for the purpose of our legitimate interests to recruit new team members and assess their qualifications and ability to perform the job.
Feedback from interviewers: collecting and analyzing feedback from interviewers regarding candidates.	Candidate's name, interview details and notes, assessment results.	This is necessary for the purpose of our legitimate interests to recruit new team members and assess their qualifications and ability to perform the job.
In the context of securing the premises		
Security of the premises: managing access to premises via badge control and with CCTV.	Candidate's name, photo and video.	This is necessary for the purpose of our legitimate interest to secure BIC's premises from unauthorized external parties.
In the context of judicial enquiry or legal proceedings		
Request from authorities: responding to official requests and	Any information required by the authorities, within the limits of the applicable law.	This is necessary to fulfill our statutory and regulatory obligations.

Processing activity	Personal Data collected and processed	Legal basis for the use of Personal Data
providing any information required by authorities.		
Legal proceedings: handling and responding to legal claims, investigations, or disputes.	Any information relevant or potentially relevant to a dispute or legal proceeding affecting BIC.	This is necessary to fulfill our statutory and regulatory obligations and for the purpose of our legitimate interests to defend BIC's rights and to protect BIC's interests.

For candidates based in California: Personal Data we collect generally includes the following categories of Personal Data recognized under the CCPA:

Categories of Personal Data	Examples
Identifiers	Name, postal address, online identifier(s), IP address, email address(es), login credentials for online accounts; social security number, driver's license number, or similar identifiers,
Personal information described in California Civil Code § 1798.80(e)	Including any additional identifiers, or certain financial information.
Characteristics of protected classifications under California or federal law	Demographic information (such as gender, age, ethnicity, citizenship and national origin, disability status, veteran status, and/or union membership) and certain information in pre-employment screenings, each as voluntarily provided and/or collected as permitted or required by law.
Commercial information	Records of products or services obtained or considered, or other similar histories or tendencies.
Internet or other electronic network activity information	Browsing history, search history, information regarding interaction with a website or application, or similar network activity information.
Audio, visual, or similar information	Recordings of calls (if in connection with job duties and/or as permitted by law), and information captured via CCTV cameras or systems.
Geolocation data	As permitted by law and your permissions, we may collect location data.
Professional or employment-related information	All information relating to candidates' application for employment with BIC, including recruitment details, CV and information contained therein or in job applications, or otherwise obtained in connection with the application process.
Education information	Education history, diplomas and academic qualifications, or similar education information.

Categories of Personal Data	Examples
Inferences	Inferences about candidates based on Personal Data described in this Privacy Policy.
Sensitive personal information	Government identification numbers (such as social security or driver's license number); certain protected classifications outlined above; and login credentials for online accounts. Please note we do not use sensitive personal information for the purpose of inferring characteristics about candidates.

APPENDIX 3. EXERCISING YOUR PRIVACY RIGHTS

If you have any questions or complaints regarding how we use your Personal Data or wish to exercise any of your rights set out in Section VIII of this Policy, please use the following details to contact us.

Please note that further information about your rights can also be obtained from your local data Supervisory Authority.

Location	How to reach us	Supervisory Authority (if applicable)
If you are in the EEA	Send us an email to privacy@bicworld.com, or protection-données@bic.com. Or write to us by post to the following address: BIC, Compliance Team, 12 boulevard Victor Hugo, 92210 Clichy, France.	The Supervisory Authority competent to deal with request concerning us, is the *Commission Nationale de l'Informatique et des Libertés* ("CNIL"), website: https://www.cnil.fr/en. You can always contact any Supervisory Authority, particularly in your country of residence, the country where you work, or the country of which you are a citizen, who will forward your request to the CNIL. The European Data Protection Board ("EDPB") published a list of all Supervisory Authorities within the European Union and European Economic Area: please follow this link to have the contact details of the Supervisory Authority in your respective country. In any event if you do have an issue, we would like to resolve it with you first.
If you are in UK	Send us an email to privacy@bicworld.com. Or write to us by post to the following address: BIC UK LTD, 1 Lyric Square, Hammersmith, London, W60NB, UK.	The Supervisory Authority in the UK is the Information Commissioner's Office ("ICO"). If you have any cause for complaint about our use of your Personal Information, you have the right to lodge a complaint with the ICO.

Location	How to reach us	Supervisory Authority (if applicable)
	To exercise rights with **Tangle Teezer,** send us an email to gdpr@tangleteezer.com.	
If you are in US-Canada	Send us an email to PIIRequest@bicworld.com. Candidates in California may designate an authorized agent to exercise their rights on their behalf, using the above methods to submit the request. Candidates in California may make such a designation by providing the agent with written permission and may also require candidates in California to verify their own identity (even if they choose to use an agent).	
If you are in a country in Latin America or in Mexico	Send us an email to datos.personales@bicworld.com. **If you are in Brazil**, send us an email to protecao.dados@bicworld.com.	The Supervisory Authority in Brazil is the Autoridade Nacional de Proteção de Dados ("ANPD"). In Argentina, the Access to Public Information Agency, is the enforcement authority responsible for handling complaints and claims related to violations of Personal Data protection regulations.
If you are in a country in the Middle East Africa (MEA) region	Send us an email to: privacy@bicworld.com.	The relevant authority in Morocco is the Commission Nationale de Protection des Données Personnelles. The relevant authority in Tunisia is the Instance Nationale de Protection des Données Personnelles (« INPDP »). The relevant authority in Nigeria is the Nigeria Data Protection Commission. The relevant authority in Ivory Coast is the Autorité de Régulation des Télécommunications de Côte d'Ivoire (« ARTCI »).

Location	How to reach us	Supervisory Authority (if applicable)
		The relevant authority in South Africa is the Information Regulator.
If you are in a country in the Asia-Pacific (APAC) region	Send us an email to: privacy@bicworld.com.	The relevant authority in Australia is the Office of the Australian Information Commissioner ("OAIC"). The relevant authority in China is the Cyberspace Administration of China (CAC).