

# Applicant Privacy Notice

---

## Index

To help you find information quickly on any particular section you are interested in, or explore individual sections in more detail, we have set out an index below. We have labelled sections to make it easy for you to navigate to the information that may be most relevant to you. Just click on the section you are interested in and you will be taken to the relevant section:

<b>Introduction</b> .....	<b>1</b>
<b>What categories of personal data does Belkin collect about me and how does it collect the data?</b> .....	<b>2</b>
<b>Why does Belkin need to collect, process and use my personal data and what is the legal basis for doing so?</b> .....	<b>2</b>
<b>Who might Belkin share my personal data with?</b> .....	<b>5</b>
<b>Security of personal data</b> .....	
<b>How long will Belkin keep my personal data for?</b> .....	<b>6</b>
<b>What rights do I have in respect of my personal data?</b> .....	<b>6</b>
<b>Who can I contact about this notice?</b> .....	<b>7</b>

## Introduction

The Belkin Group of companies has prepared this Applicant Privacy Notice ("**Notice**") for individuals who apply for roles with Belkin.

You are being provided with this Notice because you are applying for a role with Belkin. When we say "**Belkin**", "**we**" or "**us**" in this Notice, we mean the Belkin entity with which you are applying for a role, which will be the data controller of your personal data in the course of your application with us. In addition, you will see in this Notice a number of references to the "**Belkin Group**", which includes the Belkin entities globally. (Details of these can be obtained [here](#)).

We think that it is very important that you understand how we use your personal data, and we take our obligations in this regard very seriously. Please read this Notice carefully as it explains how Belkin collects, uses, stores and otherwise processes personal data about you, and your rights in relation to that information, in connection with your application and candidacy.

There are also statutory requirements we must comply with in relation to your application. If we are not able to carry out the processing activities we describe in this Notice, we may not be able to continue with your application.

There may be circumstances (as required, or to the extent permitted, by applicable law) where we ask for your specific consent to process your personal data in a particular way. For example, in some countries we may do this for the purpose of conducting specific background checks prior to you commencing employment with us, and to enable relevant third parties to release information about you as part of those checks. Where we rely on consent, we will make this clear at the time, and ask that you **sign and complete a consent form**

to confirm you consent to us processing your data for the purposes of carrying out the specific background checks listed.

## What categories of personal data does Belkin collect about me and how does it collect the data?

**"Personal data"** means any information describing or relating to an identified or identifiable individual. During your application, Belkin will to the extent permitted by local law, collect, use and otherwise process some or all of the following categories and types of personal data about you, which together will be referred to as **"Applicant Data"**:

- **identification data**, such as your name, citizenship, passport data, photo, drivers' licence information, national insurance number, health insurance and governmental retirement plan information and tax reference;
- **personal information**, such as your date and place of birth, and gender;
- **contact details**, such as your home address, telephone number, email address and emergency contact details;
- **education and work experience**, such as contact details for your current/former employer, information about your educational background, your qualifications, your work experience and other experience;
- **other application data**, such as the information included in your application form/CV;
- **information collected as part of the recruitment and interview process**, such as notes taken from your interview, information provided from recruitment agencies or references, or any other personal data which you choose to disclose to us during the course of the recruitment and interview exercise whether verbally or in written form (for example in emails);
- **background check information**, such as information obtained through reference checks and confirmation about your work/educational background.

In addition to the collection, processing and use of the Applicant Data, Belkin collects, uses and otherwise processes the following special categories of personal information about you which we describe as **"Sensitive Applicant Data"**:

- **health and medical data**, if permissible under local rules and regulations, such as information on disability (for example to accommodate you during the application process);
- **criminal records data** if required under local rules and regulations, information necessary to be provided to a governmental agency for purposes of a criminal background check;
- **race or ethnicity data** where this has been provided voluntarily to Belkin;
- **sexual orientation data** where this has been provided voluntarily to Belkin.

Belkin mainly collects your personal data from you. You will provide this information directly to Belkin personnel managing the recruitment and interview exercise or enter it into our systems (for example, through your participation in recruitment and selection processes, emails and instant messages you send or through verbal information which is recorded electronically or manually).

We also obtain some information from third parties: for example, references from a previous employer, information from recruitment consultants or where we employ a third party to carry out a background check (where required or permitted by applicable law).

In some circumstances, data is collected indirectly from monitoring devices or by other means (for example, building and location access control and monitoring systems, CCTV, telephone logs and recordings), if and to the extent permitted by applicable laws. In these circumstances, the data may be collected by Belkin or a third party provider of the relevant service. This type of data is generally not accessed on a routine basis but access is possible.

Some data may be obtained from publicly accessible sources.

In the event that particular information is required by the contract or statute this will be indicated at the time of collection. We will also let you know where there are consequences of you not providing the information requested. Failure to provide some information will mean that we cannot continue with your application as we will not have the personal data we believe to be necessary for the effective and efficient administration of your application.

## Why does Belkin need to collect, use and otherwise process my personal data and what is the legal basis for doing so?

We collect, use, store and otherwise process, Applicant Data for a variety of reasons linked to processing your application for a role with us (the "**Processing Purposes**"). However, in certain jurisdictions, we can only collect and use this data if we have a valid legal basis for doing so, and we are required to explain the various legal bases that we rely on to you. Please note that any processing of Sensitive Applicant Data requires an additional legal basis in certain jurisdictions, as set out in further detail below.

In the majority of cases, the processing of your personal data will be justified on one of the following legal basis:

- the processing is **necessary for compliance with a legal obligation** to which we are subject; or
- where there is no legal obligation, we will process your personal data where the processing is **necessary for the performance of a contract** to which you are a party or in order to take steps at your request prior to entering into such a contract; or
- where the above two legal bases do not apply, we may process your personal data where the processing is **necessary for the legitimate interests pursued by Belkin**, except where such interests are overridden by your interests or fundamental rights and freedoms which require protection of personal data.

As set out above, one of the legal bases that we rely on to process Applicant Data is "**legitimate interests**". Where we refer to "legitimate interests" of Belkin or third parties in the table below, this can include:

- Assessing your suitability for employment/engagement with Belkin;
- Implementation and operation of a group-wide organisational structure and group-wide information sharing;
- Right to freedom of expression or information, including in the media and the arts;
- Prevention of fraud, misuse of company IT systems, or money laundering;
- Operation of a whistleblowing scheme;
- Physical security, IT and network security;
- Internal Investigations;
- Compliance with our legal obligations;

- Proposed mergers and acquisitions.

Where we are relying upon legitimate interests for processing your personal data, we will balance the legitimate interests pursued by us and any relevant third party with your interests and fundamental rights and freedoms in relation to the protection of your personal data to ensure it is appropriate for us to rely on legitimate interests and to identify any additional steps we need to take to achieve the right balance.

Further, where we rely upon legitimate interest to process your personal data, then you have the right to object to that processing. If you object, we must stop that processing unless we can either demonstrate compelling legitimate grounds for the processing that override your interests, rights and freedoms or where we need to process the data for the establishment, exercise or defence of legal claims. Where we rely upon legitimate interest as a basis for processing we believe that we can demonstrate such compelling legitimate grounds, but we will consider each case on an individual basis.

To give you the full picture, we have set out in the tables below the purposes we may use your personal data for (including Applicant and Sensitive Applicant Data), i.e., the Processing Purposes, and mapped each of these against the different legal bases that we rely on.

Processing Purposes	Legal Bases
<ol style="list-style-type: none"> <li><b>Administering and processing your application (including processing a job offer should you be successful)</b> including identification data, contact details, information about your qualifications and employment history, and information obtained during your interview and information contained in your CV.</li> <li><b>To determine your eligibility for the role you applied for and to provide you with feedback on your application</b>, including identification data, contact details, information about your work and education experience, information obtained during your interview or reference calls and letters and information contained in your CV.</li> <li><b>Conducting background checks as part of your application</b>, including identification data, contact details, information about your qualification and employment history.</li> </ol>	<p><b>Processing Purposes 1 to 3:</b></p> <ul style="list-style-type: none"> <li>• Necessary for performing a contract with you as the data subject;</li> <li>• Legitimate interests of Belkin in fully assessing applicants to ensure that only suitable and appropriate applicants are selected, to compare applicants and make a fair decision on the most appropriate applicant for the role;</li> <li>• Compliance with legal obligations which Belkin is subject to, for example in relation to employment law; and when not covered by this legal basis; and</li> <li>• (where permitted by law), your consent.</li> </ul>
<ol style="list-style-type: none"> <li><b>Complying with applicable laws and employment-related requirements</b> along with the administration of those requirements, such as income tax, national insurance deductions (once an offer has been made), and employment and immigration laws which involves the processing of identification data and contact details.</li> <li><b>Monitoring and ensuring compliance with applicable policies and procedures and laws</b>, which involves the processing of your identification data and contact details, including the operation of a whistleblowing hotline.</li> </ol>	<p><b>Processing Purposes 4 to 5:</b></p> <ul style="list-style-type: none"> <li>• Compliance with legal obligations which Belkin is subject to, particularly in relation to tax law, employment law, social security law and immigration law; and</li> <li>• Legitimate interests of Belkin in ensuring that applicants for employment or engagement do not pose an unacceptable risk to the business or its customers and considers the verification carried out necessary to prevent crime and other unlawful acts and to protect the business and its customers from fraud, dishonesty or incompetence.</li> </ul>

<p>6. <b>Communicating with you, Belkin employees and third parties, including informing you of future opportunities with Belkin</b> (including communicating future employment opportunities, which involves the processing of identification data and your contact details).</p>	<p><b>Processing Purpose 6:</b></p> <ul style="list-style-type: none"> <li>• Necessary for performing a contract with you as the data subject - we need to be able to communicate with you so that we needed to enter into a contract with you;</li> <li>• Legitimate interests of Belkin in maintaining an appropriate pool of talent who have shown an interest in working for Belkin and who are potentially suitable applicants for employment. This will potentially benefit both initially unsuccessful applicants and Belkin continuing to meet its business objectives, maintain its reputation and attract high calibre employees; and</li> <li>• Compliance with a legal obligation to which data controller is subject.</li> </ul>
<p>7. <b>Responding to and complying with requests and legal demands from regulators or other authorities</b> in or outside of your home country which involves the processing of identification data and contact details.</p>	<p><b>Processing Purpose 7:</b></p> <ul style="list-style-type: none"> <li>• Compliance with legal obligations which Belkin is subject to; and</li> <li>• Legitimate interests of Belkin.</li> </ul>
<p>8. <b>Complying with corporate financial responsibilities</b>, including audit requirements (both internal and external) and cost/budgeting analysis and control which involves the processing of identification data, contact details, and information about the role you have applied for, including the role's salary and benefits.</p>	<p><b>Processing Purpose 8:</b></p> <ul style="list-style-type: none"> <li>• Legitimate interests of Belkin, i.e. we need to ensure that we manage our business effectively; and</li> <li>• Compliance with legal obligations which Belkin is subject to.</li> </ul>
<p>9. <b>Applicant Onboarding</b>, including making job offers, providing contracts of employment or engagement and preparing to commence your employment or engagement where you accept an offer from us, which include (amongst others) the processing of identification data, contact details, gender, nationality, date of birth, age, personal contact details, national ID number, immigration and eligibility to work information, driving licence, emergency contact information, details of any disability and any reasonable adjustments required as a result.</p>	<p><b>Processing Purpose 9:</b></p> <ul style="list-style-type: none"> <li>• The processing is necessary for us to administer our contract with you - or take steps to consider entering into an employment contract with you;</li> <li>• Compliance with legal obligations which Belkin is subject to; and</li> <li>• Our legitimate interests in ensuring the effective engagement of staff on appropriate terms and conditions of employment and information supplied in the recruitment process, which is relevant to ongoing employment, is maintained. This will contribute towards us continuing to meet our business objectives, maintain our reputation and attract high calibre employees.</li> </ul>
<p>10. <b>Recruitment feedback and complaints</b>, including dealing with any query, challenge or</p>	<p><b>Processing Purpose 10:</b></p>

<p>request for feedback received in relation to our recruitment process and decisions.</p>	<ul style="list-style-type: none"> <li>• Compliance with legal obligations to which we are subject including for example ensuring that Belkin is able to demonstrate its compliance with data protection laws and anti-discrimination laws; and</li> <li>• Our legitimate interest in being able to provide feedback to job candidates and to be able to defend any challenge or claim made in connection with Belkin's recruitment decision. This will assist us to avoid the risk of financial exposure or costs incurred through challenges to recruitment decisions and to maintain Belkin's reputation.</li> </ul>
<p><b>11. Enforcement, exercise or defence of legal claims and litigation</b>, including information reasonably required in compliance with the listed purpose, including details of the potential and/or actual legal claim and enforcement.</p>	<p><b>Processing Purpose 11:</b></p> <p>Our legitimate interest in protecting Belkin from breaches of legal obligations owed to it and defending Belkin's business against litigation. This is needed to ensure that our legal rights and interests are protected appropriately, to protect Belkin's reputation and to protect Belkin from other damage or loss.</p>

**Additional legal bases we rely on where we process Sensitive Applicant Data**

Where we process Sensitive Applicant Data, it will be justified by a legal basis set out above, and also by one of the following additional legal basis:

Processing Purpose	Legal Bases
<p>1. <b>To accommodate your application and interview and for compliance with legal obligations</b>, we may use health and medical data, such as to adapt the application process and application conditions to the level of disability or incapacity of the data subject.</p> <p>2. <b>Criminal records background checks</b> if required or authorized under applicable law, local rules and regulations may for example involve information necessary to be provided to a governmental agency for purposes of a criminal background check; or where we have a legal or regulatory requirement to report an offence, or where there is an allegation of a criminal offence or conviction arising during your relationship with us.</p>	<ul style="list-style-type: none"> <li>• Your explicit consent as allowed by local data protection law; and</li> <li>• Necessary to comply with legal obligation, for example, carry out the obligations and to exercise specific rights of Belkin or you in the field of employment and social security and social protection law as permitted by local data protection law.</li> </ul> <ul style="list-style-type: none"> <li>• Your explicit consent as allowed by local data protection law;</li> <li>• Necessary to carry out the obligations and to exercise specific rights of Belkin or you in the field of employment and social security and social protection law as permitted by local data protection law; and</li> <li>• Necessary for reasons of substantial public interest as permitted by local data protection law.</li> </ul>

Processing Purpose	Legal Bases
<p>3. <b>Equal opportunities monitoring and diversity monitoring and initiatives</b> may involve us using race or ethnicity data or sexual orientation data in each case where this has been provided voluntarily by you to Belkin.</p>	<ul style="list-style-type: none"> <li>Necessary for reasons of substantial public interest as permitted by local data protection law; and</li> <li>Your explicit consent as allowed by local data protection law.</li> </ul>
<p>4. <b>To assess and review applicants' eligibility to work for Belkin in the jurisdiction in which the applicant would work</b>, information and documentation including work permits, details of residency, proof of citizenship.</p>	<ul style="list-style-type: none"> <li>Necessary to comply with legal obligation, for example, carry out the obligations and to exercise specific rights of Belkin or you in the field of employment and social security and social protection law as permitted by local data protection law; and</li> <li>Legitimate interest of Belkin to ensure that applicants are able to work in the required location for the role applied for.</li> </ul>
<p>5. <b>In the event of a complaint, claim or litigation or potential claim or litigation by, against or involving Belkin</b>, special category personal data of any type.</p>	<ul style="list-style-type: none"> <li>Our legitimate interests to defend our rights and interest.</li> </ul>

If consent is required for the processing in question as set out above, it will be sought from you separately to ensure that it is freely given, informed and explicit. Information regarding such processing will be provided to you at the time that consent is requested, along with the impact of not providing any such consent. You should be aware that it is not a condition or requirement of your recruitment to agree to any request for consent from Belkin.

## Who might Belkin disclose my personal data to?

As you may know, we are part of the global Belkin Group, and several entities in this group are involved in the Processing Purposes. To ensure that the Processing Purposes can be completed, your information may be disclosed to any of the entities within the Belkin Group network. Where we disclose data in this way, however, it is our policy to limit the categories of individual who have access to that personal information.

Belkin may disclose personal data to third parties, including to entities within and outside the Belkin Group located in any jurisdictions where Belkin Group entities or third parties are located, for the Processing Purposes as follows:

- Within the Belkin Group.** As the Belkin entity that you are applying to is part of a wider group headquartered in California, United States with offices located across the globe, which all partially share management, human resources, legal, compliance, finance and audit responsibility. Belkin may transfer the Applicant Data and Sensitive Applicant Data to, or otherwise allow access to such data by other entities within the Belkin Group, which may use, transfer, and otherwise process the data for the following purposes: to maintain and improve effective administration of the workforce; to communicate information about the Belkin Group; to maintain a corporate directory; to maintain IT systems; to monitor and assure compliance with applicable policies and procedures, and applicable laws; and to respond to requests and legal demands from regulators and other authorities.
- Regulators, authorities, and other third parties.** As necessary for the Processing Purposes described above, personal information may be disclosed to regulators, courts, and other authorities (e.g., tax and law enforcement authorities), independent external advisors (e.g., auditors),

insurance providers, pensions and benefits providers, internal compliance and investigation teams (including external advisers appointed to conduct internal investigations).

- **Data processors.** As necessary for the Processing Purposes described above, personal data may be disclosed to one or more third parties, whether affiliated or unaffiliated, to process personal information under appropriate instructions ("**Data Processors**"). The Data Processors may carry out instructions related to recruitment, workforce administration, IT system support and maintenance, payroll and compensation, training, compliance, and other activities, and will be subject to contractual obligations to implement appropriate technical and organisational security measures to safeguard the personal information, and to process the personal information only as instructed.

For a full list of the Belkin Group entities and third parties that we may disclose your data to, please contact us as set out below.

As you may expect, some of the recipients we may disclose Applicant Data and Sensitive Applicant Data to may be located in countries outside of Europe and/or European Economic Area ("**EEA**") whose data protection laws may be less stringent than those in your jurisdiction.

Whenever we make cross-border transfers of your personal data, we implement appropriate safeguards in accordance with applicable data protection laws, e.g.:

- within the Belkin Group, an intra-group agreement gives specific contractual protections and regulates cross border intra group transfers of personal data;
- the EU Standard Contractual Clauses and additional measures to supplement such clauses as may be required in line with transfer impact assessments we carry out, to prevent interference by public authorities of third countries;
- the UK Addendum; and/or
- by checking that an adequacy decision by the European Commission and/or the UK Information Commissioner's Office is in place.

If you are in the EU or UK, you have a right to request a copy of any appropriate safeguards relied upon to transfer your personal data to a country which does not have adequate data protection laws (such as a copy of a data transfer agreement). You can request sight of these by contacting us as set out below ("**Who can I contact about this notice?**").

## SECURITY OF DATA

We are committed to protecting the security of the personal data you share with us. We use technical and organisational methods designed to secure your personal data in accordance with applicable laws. However, please note that no environment or security procedures or protocols are ever guaranteed to be 100% secure or error-free.

## How long will Belkin keep my personal data for?

It is our policy not to keep personal data for longer than is necessary. We may, for example, keep your personal information for a reasonable time after your application process is completed, in case we have future job opportunities that we consider you are suitable for. Where personal information is kept, that period will be determined based on the applicable local law. For further information, please contact us as set out below to request further details on how long Belkin will retain different categories of personal information.

## What rights do I have in respect of my personal data?

Subject to applicable law, you may have certain rights in relation to your personal data. These differ by country, and in certain circumstances these rights might not be absolute, as they depend on our reason for processing your personal data. but can be summarised in broad terms as follows:

**(i) Right of access**

You have the right to confirm with us whether your personal data is processed, and if it is, to request access to that personal data including the categories of personal data processed, the purpose of the processing and the recipients or categories of recipients. We do have to take into account the interests of others though, so this is not an absolute right, and (to the extent permitted by law) if you want to request more than one copy we may charge a fee.

**(ii) Right to rectification**

You have the right to rectify inaccurate or incomplete personal data concerning you. We encourage you to review this information regularly to ensure that it is accurate and up to date.

**(iii) Right to erasure (right to be forgotten)**

You may have the right to ask us to erase personal data concerning you, but only where:

- it is no longer needed for the purposes for which it was collected; or
- you have withdrawn your consent (where the data processing was based on consent); or
- following a successful right to object (see below); or
- it has been processed unlawfully; or
- to comply with a legal obligation to which Belkin is subject.

We are not required to comply with your request to erase your personal data if the processing of your personal data is necessary:

- for compliance with a legal obligation; or
- for the establishment, exercise or defence of legal claims.

There are certain other circumstances in which we are not required to comply with your erasure request, although these two are the most likely circumstances in which we would deny that request.

**(iv) Right to restriction of processing**

You can ask us to restrict (i.e. keep but not use) your personal data, but only where:

- its accuracy is contested (see below), to allow us to verify its accuracy; or
- the processing is unlawful, but you do not want it erased; or
- it is no longer needed for the purposes for which it was collected, but we still need it to establish, exercise or defend legal claims; or
- you have exercised the right to object, and verification of overriding grounds is pending.

We can continue to use your personal data following a request for restriction, where:

- we have your consent; or
- to establish, exercise or defend legal claims; or

- to protect the rights of another natural or legal person.

**(v) Right to data portability**

You may have the right to receive personal data concerning you, which you have provided to us, in a structured, commonly used and machine-readable format and you may have the right to transmit that data to another entity.

**(vi) Right to object and rights relating to automated decision-making**

Under certain circumstances you have the right to object, on grounds relating to your particular situation, at any time to the processing of your personal data, including profiling, by us and we may be required to no longer process your personal data.

Further, as set out above, you can object to any processing of your personal data which has our “legitimate interests” as its legal basis if you believe your fundamental rights and freedoms outweigh our legitimate interests. Once you have objected, we have an opportunity to demonstrate that we have compelling legitimate interests which override your rights and freedoms.

**(vii) Withdrawal of consent**

Where you have given your consent to the processing of your personal data, you can revoke it at any time with effect for the future. The lawfulness of the processing of your data before this remains unaffected.

**(viii) Lodge complaint with Supervisory Authority**

You also have the right to lodge a complaint with the competent data protection supervisory authority, which may vary depending on your location. Please click [here](#) for a list of contact details for the EEA data protection supervisory authorities, and the Information Commissioner is the UK’s supervisory authority for data protection at <https://ico.org.uk>.

To exercise any of these rights, please contact us as stated below (**Who can I contact about this notice?**). You also have a right to lodge a complaint with your national data protection supervisory authority at any time. Please click [here](#) for a list of contact details for the EEA data protection supervisory authorities. The UK Information Commissioner’s Office can be contacted at [Contact us | ICO](#).

## Who can I contact about this notice

We hope this Notice has been helpful in setting out the way we handle your personal data and your rights to control it. If you have any questions that have not been covered, please contact [privacy@belkin.com](mailto:privacy@belkin.com), or your appropriate Belkin People Team contact. If you have a complaint or concern about how we use your personal data, please contact us in the first instance and we will attempt to resolve the issue as soon as possible.

### Additional Information for California Residents

This Section applies, generally, to the personal information, referred to in this section as “Personal Information,” that we collect and otherwise process about Applicants that are California residents (each a “**CA Applicant**”), in the context of reviewing, assessing, considering, managing, storing or processing their applications or otherwise considering them for a position with us.

This section does not address or apply to our collection of Personal Information that is not subject to the California Consumer Protection Act (“**CCPA**”), such as consumer credit reports and background checks, publicly available data, or other information that is exempt under the CCPA. This section also does not apply to the Personal Information we collect from contractors or employees, which is subject to different privacy notices, or to the Personal Information we collect about our customers.

**Categories of Personal Information Collected and Disclosed.** The table below, generally, identifies the categories of as Personal Information, about CA Applicants (that we collect and have collected in the prior twelve (12) months), as well as the categories of third parties to whom we may disclose this information for a business or commercial purpose. In some cases (such as where required by law), we may ask for consent or give you certain choices prior to collecting or using certain Personal Information.

Categories	Description	Third Party Disclosures for Business or Commercial Purposes
<b>Identifiers</b>	Such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, and other government identifiers.	<ul style="list-style-type: none"> <li>• service providers</li> <li>• advisors and agents</li> <li>• recruiters</li> <li>• affiliates and subsidiaries</li> <li>• regulators, government entities and law enforcement</li> <li>• internet service providers, operating systems, and platforms</li> <li>• others with your permission or as required by law</li> </ul>
<b>Categories of Personal Information Described in Cal. Civ. Code § 1798.80.</b>	Records containing Personal Information, such as name, signature, photo, contact information, education and employment history, Social Security number and other government identifiers, financial or payment information, medical information.	<ul style="list-style-type: none"> <li>• service providers</li> <li>• advisors and agents</li> <li>• recruiters</li> <li>• affiliates and subsidiaries</li> <li>• regulators, government entities and law enforcement</li> <li>• internet service providers, operating systems, and platforms</li> <li>• others with your permission or as required by law</li> </ul>
<b>Characteristics of Protected Classifications Under California and Federal Law</b>	Such as race/ethnicity, gender, sex, veteran status, disability, and other characteristics of protected classifications under California or federal law. (Note: generally, this information is collected on a voluntary basis, and is used in support of our equal opportunity and diversity and inclusion efforts and reporting obligations or where otherwise required by law. )	<ul style="list-style-type: none"> <li>• service providers</li> <li>• advisors and agents</li> <li>• affiliates and subsidiaries</li> <li>• regulators, government entities and law enforcement</li> <li>• others with your permission or as required by law</li> </ul>

<b>Audio, Electronic, Visual, Thermal, or Similar Information</b>	Audio, electronic, visual, or similar information, such as CCTV/video footage, photographs, call recordings, and other audio recording (e.g., recorded webinars).	<ul style="list-style-type: none"> <li>• service providers</li> <li>• advisors and agents</li> <li>• affiliates and subsidiaries</li> <li>• regulators, government entities and law enforcement</li> <li>• others with your permission or as required by law</li> </ul>
<b>Professional or Employment-related Information</b>	Such as performance information, professional membership records, references, assessment records, resumes, cover letters and work history, conduct information, and termination data.	<ul style="list-style-type: none"> <li>• service providers</li> <li>• advisors and agents</li> <li>• recruiters</li> <li>• affiliates and subsidiaries</li> <li>• regulators, government entities and law enforcement</li> <li>• others with your permission or as required by law</li> </ul>
<b>Education Information</b>	Such as degrees earned, educational institutions attended, transcripts, training records and other information about your educational history or background that is not publicly available personally identifiable information as defined under the Family Educational Rights and Privacy Act.	<ul style="list-style-type: none"> <li>• service providers</li> <li>• advisors and agents</li> <li>• recruiters</li> <li>• affiliates and subsidiaries</li> <li>• regulators, government entities and law enforcement</li> <li>• others with your permission or as required by law</li> </ul>
<b>Sensitive Personal Information</b>	Such as: (a) Social Security number and other government identifiers; (b) financial account and payment information (e.g., for direct deposit purposes); (c) racial or ethnic origin or sexual orientation (e.g., on a voluntary basis to support of our equal opportunity and diversity and inclusion efforts and reporting obligations, or where otherwise required by law, or union membership); and (e) health information (e.g., as necessary to provide reasonable accommodations during your application process).	<ul style="list-style-type: none"> <li>• service providers</li> <li>• advisors and agents</li> <li>• affiliates and subsidiaries</li> <li>• regulators, government entities and law enforcement</li> <li>• others as required by law</li> </ul>

We do not sell or share (as defined by the CCPA) applicants' Personal Information or sensitive Personal Information related to CA Applicants, including those we know who are under the age of 16.

**Sources of Personal Information.** In general, we may collect CA Applicant Personal Information identified in the table above from the following categories of sources:

- Directly from you;
- Recruiters and recruiting platforms;
- Referrals and references (including former employers);
- Publicly available information;
- Service providers, representatives and agents;
- Affiliates and subsidiaries;

**Retention.** It is our policy not to keep Applicant Personal Information for longer than is necessary. We may, for example, keep your Personal Information for a reasonable time after your application process is completed, in case we have future job opportunities that we consider you are suitable for. Where Personal Information is kept, that period will be determined based on the applicable local law. For further information, please contact us as set out below to request further details on how long Belkin will retain different categories of Personal Information. Where your application is successful, any Personal Information we require for your employment will be transferred to a personnel file.

**Purposes for Collecting, Using, Disclosing and Processing Personal Information.** Subject to applicable legal restrictions, generally we collect, use, disclose and otherwise process CA Applicant Personal Information as reasonably necessary for the following general purposes (as further described in the “Why do we process your Personal Information?” section above):

- Administering and processing your application (including processing a job offer should you be successful);
- To determine your eligibility for the role you applied for and to provide you with feedback on your application, including to assess and review applicants’ eligibility to work for Belkin in the jurisdiction in which the applicant would work;
- As required, conducting background checks as part of your application;
- Complying with applicable laws and employment-related requirements;
- Monitoring and ensuring compliance with applicable policies and procedures and laws;
- Communicating with you, Belkin employees and third parties, including informing you of future opportunities with Belkin;
- Responding to and complying with requests and legal demands from regulators or other authorities;
- Complying with corporate financial responsibilities;
- Applicant Onboarding;
- Solicit and process recruitment feedback and complaints;
- Carrying out business transfers or selling all or part of the business or assets of Belkin;
- Enforcement, exercise or defence of legal claims and litigation, including in the event of a complaint, claim or litigation or potential claim or litigation by, against or involving Belkin; and

- Administering our equal opportunities monitoring and diversity monitoring and initiatives

**Sensitive Personal Information.** Notwithstanding the purposes described above, we do not collect, use or disclose of sensitive Personal Information about CA Applicants beyond the purposes authorized by the CCPA (pursuant to Cal Civ. Code § 1798.121 and § 7027(l) of the CCPA regulations). Accordingly, we only use and disclose sensitive Personal Information about CA Applicants as reasonably necessary and proportionate: (i) to perform our services requested by you; (ii) to help ensure security and integrity, including to prevent, detect, and investigate security incidents; (iii) to detect, prevent and respond to malicious, fraudulent, deceptive, or illegal conduct; (iv) to verify or maintain the quality and safety of our services; (v) for compliance with our legal obligations; (vi) to our service providers who perform services on our behalf; and (vii) for purposes other than inferring characteristics about you.

**CA Applicant CCPA Rights.** CA Applicants have certain rights under the CCPA with respect to their Personal Information, subject to certain limitations and exceptions:

- **Deletion:** the right to request deletion of their Personal Information that we have collected about them.
- **Know/access:** the right to know what Personal Information we have collected about them, including the categories of Personal Information, the categories of sources from which the Personal Information is collected, the business or commercial purpose for collecting, selling, or sharing Personal Information, the categories of third parties to whom we disclose Personal Information, and the specific pieces of Personal Information we have collected about them.
- **Correction:** the right to request correction of inaccurate Personal Information we maintain about them.
- **Opt-out of sales and sharing:** the right to opt out of the sale and sharing of their Personal Information. However, as discussed above we do not sell or share CA Applicant Personal Information.
- **Limit use/disclosure of sensitive Personal Information:** the right to request to limit certain uses and disclosures of sensitive Personal Information. However, as discussed above, we do not use or disclose CA Applicant Personal Information beyond the purpose authorized by the CCPA.
- **Non-discrimination:** not to be subject to discriminatory treatment for exercising their rights under the CCPA.

**Submitting CCPA Requests.** CA Applicants may submit a request to us in order to exercise their CCPA rights to know/access, to delete and to correct their Personal Information held by us by submitting a privacy request to us online [here](#), via email at [privacy@belkin.com](mailto:privacy@belkin.com) or by calling us at +1 877-310-2443 (toll-free).

We will take steps to verify your request by matching the information provided by you with the information we have in our records. Your request must provide sufficient information that allows us to reasonably verify you are the person about whom we collected Personal Information or an authorized representative (i.e., by completing all required fields on our webform if you choose to submit a request in that manner) and describe your request with sufficient details that allows us to properly understand, evaluate, and respond to it. In some cases, we may request additional information in order to verify your request or where necessary to process your request. Authorized agents may initiate a request on behalf of another individual through one of the above methods; authorized agents will be required to provide proof of their authorization and we may also require that the relevant consumer directly verify their identity and the authority of the authorized agent.

**Contact Us.** For additional details, or if you have questions regarding our use of your Personal Information as described in this California section, you may contact your Belkin People Team contact, or reach us at [privacy@belkin.com](mailto:privacy@belkin.com).