PRIVACY NOTICE FOR CANDIDATES

This Candidate Privacy Notice ("Notice") is effective as of January 18, 2021. If a previous version exists, you can find it at the bottom of this page.

Allegro MicroSystems, Inc., a Delaware Corporation, is committed to protecting and respecting your privacy. This "Notice" explains what Personal Data we collect, why we collect this Personal Data and how we use and protect it in relation to our recruitment activities and the rights you have in connection with that information. This Notice refers to all Personal Data we collect and that we could use to personally identify you. Please read this Notice carefully. We are happy to answer any question you may have on this.

In this Notice, "Personal Data" means any information on its own or combined with other information that relates to an identified or identifiable natural person ("Data Subject").

This Notice applies to Allegro Microsystems Inc. as well as its wholly-owned direct and indirect subsidiaries and affiliated companies, including Voxtel, LLC, ("Allegro"), for which Allegro is a "Data Controller". Notwithstanding the foregoing, if any Allegro affiliated companies have published their own privacy notice, such notice will take precedence over this Notice with respect to that entity. If you have any questions about this Notice, please contact Allegro at its registered address: 955 Perimeter Road, Manchester, NH 03103, United States of America or alternatively you may email us at privacy@allegromicro.com. When this Notice refers to "we", "us" or "our", it refers to all Allegro entities which collectively or individually may act as a Controller of your Personal Data, in other words those entities who may be deciding why and how your Personal Data is being processed.

This Notice applies to all Personal Data we collect about you when you interact with us as a job candidate.

The term "Candidate" is used in this Notice to refer to anyone who applies for a job role, or who otherwise seeks to work with or for us, whether on a permanent or non-permanent basis.

The Personal Data We Collect

When you apply for a job role with us or otherwise seek to work with us, we may collect certain information automatically, from you personally, or from third party sources (for example from a recruitment agency acting on your behalf or from references supplied by former employers or agencies and where applicable information from criminal records checks permitted by law).

Personal Data we may collect automatically

You can visit the Careers section of our website ("Website") and search for job roles without providing any Personal Data. However, we do collect certain Personal Data automatically from your device when you visit our Website. For further information, please see our Privacy Notice.

Personal Data we may collect from you

- We need to use your personal information to decide whether to enter into an employment relationship with you. In connection with your application for work with us, we may collect, store, and use the following categories of information from you: Name, title and other personal details such as gender, date and place of birth and nationality;
- Personal contact details such as addresses, telephone numbers and personal email addresses;
- Your curriculum vitae (CV)/résumé, cover letter or any other supplementary document included as part of the application process where requested or not (which may include details of any memberships or interests constituting Sensitive Personal Data (as that term is defined herein));
- Past employment history (including previous employers, job titles or positions) and references in order to evaluate you for potential employment;
- Other academic, professional, training and salary-related information, such as academic degrees and professional qualifications;
- National identifiers such as nationality, national IDs/passport, social security/insurance numbers, immigration information and visa status;

- Information relating to previous applications you have made to us and/or any previous employment history with us;
- Photographs if included on CV's or otherwise on supplementary documents submitted as part of the recruitment process;
- The results of any personality profiling assessment that we may carry out as part of the recruitment process;
- Your bank account details (if these are necessary to reimburse reasonable travel expenses); and
- Any other information you voluntarily provide through the recruitment process, including through interviews and other forms of assessment.

As a general rule we try not to collect or process any "Sensitive Personal Data" during the recruitment process, unless authorised by law or where necessary to comply with applicable laws. Sensitive Personal Data includes the following: information that reveals your racial or ethnic origin religious, political, or philosophical beliefs, or trade union membership; genetic data; biometric data for the purposes of unique identification; or information concerning your health, sex life or sexual orientation.

However, in some circumstances, we may need to collect or request on a voluntary disclosure basis some Sensitive Personal Data for legitimate recruiting-related purposes. For example, information about your racial/ethnic origin, gender and disabilities may be collected for the purposes of equal opportunities monitoring, to comply with anti-discrimination laws and for government reporting obligations. Any reports prepared for this purpose would not contain Personal Data, i.e. the data would be aggregated and anonymized. Furthermore, information about your physical or mental condition may be collected in order to consider what special adjustments/accommodations we need to make for the recruitment process and/or subsequent job role.

You may provide, on a voluntary basis, other Sensitive Personal Data during the recruiting process.

<u>Personal Data we may collect from other sources</u>
We may collect some or all of the following Personal Data from other sources (in each case where permissible and in accordance with applicable law) when you apply for a role with us:

- Information provided by recruiting or executive search agencies;
- Information contained in references from previous employers;
- Copies of right to work documentation and other immigration data, including visa information;
- Other background information provided or confirmed by academic institutions and training or certification providers; and/or
- Other information received from providers of background and reference checks and/or screening providers.

Upon registering your interest via our Careers portal, you may also be asked to provide us with specific information in relation to your application. Where a third-party acts as a representative on your behalf, for example, a recruiter, that third party will be asked to submit your details via the same recruitment portal.

If your application to work for us is successful, we will hold additional information about you as your employer in accordance with our Employee Privacy Notice, which will be provided at the relevant time.

The Way We Use Your Personal Data

Personal Data, whether provided now or in the future will be held and processed by us for the purposes of your registration of interest, the handling of your job application(s) and to make a hiring decision.

Allegro has a legitimate interest in processing Personal Data during the recruitment process and for keeping records of the process and/or it is necessary to enable us to comply with our legal obligations. We also require Personal Data about you in order to take steps to enter into a contract with you and will retain that Personal Data in order to perform that contract (assuming you enter into an employment relationship with Allegro). In some cases, we need to process data to ensure that we are complying with our legal obligations (e.g. right to work).

We will use the Personal Data we collect about you to:

- Assess your skills, qualifications and suitability for a role;
- For speculative applications, to match you to appropriate vacancies;
- Communicate with you and/or your recruiter/representative about the recruitment process;

- Depending on where you are in the interview process, carry out background and reference checks and certain screenings against governmental lists where applicable and to the extent considered necessary;
- Keep records relating to our hiring processes;
- Comply with legal or regulatory requirements.

Where We Process or Store Personal Data

Allegro is headquartered in the United States and stores data on servers located in the United States and in Europe and Asia. When we transfer Personal Data to third party service providers, including our HR platform (Workday), we take steps to ensure and guarantee that adequate safeguards are in place to protect your Personal Data.

Personal Data Sharing

Your Personal Data may be shared among Allegro entities, or with our Parent Company (Sanken Electric Co. Limited) and any of our employees, officers, insurers, agents, professional advisers around the world to administer our recruitment processes and store data. This includes members of the Human Resources team, relevant hiring managers and interviewers involved in the recruitment process, and IT staff if access to the Personal Data is necessary for the performance of their roles.

We may have to share specific and relevant components of your Personal Data with third-parties who provide services relating to the recruitment process to us, including (a) recruiting or executive search agencies involved in your recruiting; (b) background checking or other screening providers; (c) data storage, shared services and recruiting platform providers, IT developers and support providers and providers of hosting services in relation to our careers website; and (d) third parties who provide support and advice including in relation to legal, financial/audit, management consultant, insurance, health and safety, security and whistleblowing/reporting issues. We require third parties to respect the security of your Personal Data and to treat it in accordance with the law.

Allegro will also share or release information, including Personal Data if (i) Allegro has your permission to make the disclosure, (ii) when Allegro believes release is appropriate or is required to comply with the applicable laws and/or to respond to requests from competent public and government authorities including public and government authorities outside your country of residence, (iii) in connection with any ongoing or prospective legal proceedings, (iv) enforce or apply Allegro Terms of Use and other policies or agreements, or (v) protect the rights, property or safety of Allegro and other users (including for fraud protection and credit risk reduction).

How Long We Keep Your Personal Data

We will only keep your Personal Data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. If we delete your Personal Data from our servers, it may be retained on backup media for an additional period of time.

If your application is successful and you become an employee, the Personal Data collected as part of the recruitment process will be transferred to employee records and retained during your employment. The periods for which your Personal Data will be held will be provided to you in an Employee Privacy Notice at the relevant time.

For Applications from Europe (including the United Kingdom and except for Germany): If your application is unsuccessful or you withdraw your application, we retain all your Personal Data for a period of 12 months from the date you were advised that your application was unsuccessful or the date we received your written request to withdraw.

For applications from Germany: If your application is unsuccessful or you withdraw your application, we retain all your Personal Data for a period of 6 months from the date you were advised that your application was unsuccessful or the date we received your written request to withdraw.

All other Applications outside of Europe: If your application is unsuccessful or you withdraw your application, we retain all your Personal Data for a period of 24 months from the date you were advised that your application was unsuccessful or the date we received your written request to withdraw

We retain your Personal Data for these periods so that we can monitor re-applications and to show, in the event of a legal claim, that we have not discriminated against candidates on prohibited grounds and that we

have conducted the recruitment process in a fair and transparent way. During these periods we may also use your Personal Data to consider whether to invite you to apply for future vacancies or to alert you to future vacancies which we believe will be of interest to you. We process your information this way in the legitimate interests of recruiting appropriate personnel into our business. After these periods, we will securely destroy your Personal Data in accordance with our data retention policy.

For employment applications made via our career website/portal, your portal account will be deleted two (2) years after the last time you login unless you become an employee. You can also contact our support team (privacy@allegromicro.com) at any time to get your account deleted earlier.

Your Rights in Relation to Your Personal Data

If you are a resident of the European Union/European Economic Area, you have the following rights with respect to your Personal Data:

- The right to request a copy of your Personal Data that we hold about you.
- The right to request that we correct your Personal Data if inaccurate or out of date.
    - If you have registered to use the Allegro Career Site, you may update your user profile by logging into the Career Site.
- The right to request that your Personal Data is deleted when it is no longer necessary for us to retain such data (please note that we may be able to reject or restrict the request in some circumstances, depending on the Personal Data we hold and our lawful reason for keeping it).
- The right to request that we provide you with your Personal Data and, if possible, to pass on this information directly (in a portable format) to another Data Controller when the processing is based on consent or contract.
- The right to request a restriction on further data processing, in some situations, you have the right to request that we do not use the Personal Data you have provided (e.g. if you believe it to be inaccurate).
- The right to object to the processing of Personal Data unless we have overriding compelling grounds to continue processing.

California Privacy Notice: If you are an employee or potential candidate of Allegro and a resident of California, you have a right to notice of the types of Personal Data we may collect, and how we use it. We may collect the above indicated Personal Data, and use it for compliance with legal obligations, security and maintenance reasons, and employment purposes such as employment screening, identity verification, direct deposit, etc.

Any query or request about your privacy rights should be sent to privacy@allegromicro.com.

To exercise your privacy rights you may submit a Subject Access Request (SAR) by completing a SAR using our online portal or by completing a specific form using the following links as a Microsoft Word or PDF file. If downloading the form, you may submit the completed SAR to privacy@allegromicro.com or print the form and send it to Allegro's attention at the appropriate address as detailed in the "Our Contact Details" section of this policy. For any queries about the content or how to complete the SAR please contact Allegro at privacy@allegromicro.com.

We respond to all requests we receive from individuals wishing to exercise their data protection rights in accordance with applicable data protection laws.

Automated Processing

We do not generally make any recruitment decisions based solely on automated decision-making. In the event that we do ever use automated decision-making that could have a significant impact on you, we will let you know in advance and give you an opportunity to object.

International Transfer of Personal Data

Some recipients of Personal Data will be located or may have relevant operations outside of your country, such as in the United States, where the data protection laws may not provide the level of protection equivalent to the laws in your jurisdiction. By entering into appropriate data transfer agreements based on EU Standard Contractual Clauses or taking other measures to provide an adequate level of data protection, we have established or confirmed that data recipients will be provided an adequate level of protection for Personal Data

and that appropriate technical and organizational security measures are in place to protect Personal Data against accidental or unlawful destruction, accidental loss or alteration, unauthorized disclosure or access, and against all other unlawful forms of Processing. In addition, Allegro's European affiliates have implemented data transfer agreements based on the EU Standard Contractual Clauses to provide adequate protection to transfers of Personal Data transferred to Allegro MicroSystems in the United States as well as other affiliated Allegro entities located outside of the EEA. For more information about these measures, please email privacy@allegromicro.com.

Safeguarding the Personal Data

We recognise our responsibility to protect the Personal Data that we collect. We make sure our measures are in compliance with applicable data protection and data security laws. We have implemented appropriate technical and organizational measures to prevent risks, such as unauthorized disclosure of, or access to Personal Data, loss, alteration, accidental or unlawful destruction of Personal Data. We also ensure our external providers process your Personal Data in a secure and confidential manner. Examples of measures that are in place to protect your Personal Data include:

- Limiting access to Personal Data so that only employees on a need to know basis have access to your Personal Data;
- Limiting physical access to our premises;
- Requiring third-party providers to have acceptable security measures to keep Personal Data secure and putting in place physical, electronic and procedural safeguards in line with industry standards.

It is your responsibility to safeguard any password, user ID and other Personal Data while using Allegro sites.

Should you become aware of any data security incident, you may report it by emailing databreach@allegromicro.com.

Cookies

In order to offer and provide a customized and personal service, we may use cookies to store and help track information about you.

A cookie is a small text file that we or our third-party service providers may transfer to your device when you visit our website that helps the site remember information about you and your preferences. Cookies retain certain information to help websites recognize a user's device as they navigate from page to page or when they later return to a website.

In general cookies perform four functions:

- Strictly Necessary cookies are necessary for the website to function and cannot be switched off in our systems. They are usually only set in response to actions made by you which amount to a request for services, such as setting your privacy preferences, logging in or filling in forms. You can set your browser to block or alert you about these cookies, but some parts of the site will not then work. These cookies do not store any personally identifiable information.
- Performance cookies allow us to count visits and traffic sources so we can measure and improve the performance of our site. They help us to know which pages are the most and least popular and see how visitors move around the site. All information these cookies collect is aggregated and therefore anonymous. If you do not allow these cookies we will not know when you have visited our site and we will not be able to monitor its performance.
- Functional cookies enable the website to provide enhanced functionality and personalization. They may be set by us or by third party providers whose services we have added to our pages. If you do not allow these cookies, then some or all of these services may not function properly.
- Targeting cookies may be set through our site by our advertising partners. They may be used by those companies to build a profile of your interests and show you relevant adverts on other sites. They do not store directly personal information but are based on uniquely identifying your browser and internet device. If you do not allow these cookies, you will experience less targeted advertising.

Please note that the specific types of cookies we use depends on the website you are visiting. For more information about our use of cookies and other similar technologies, including our choices regarding the use of cookies, please see the cookie notice displayed on the website you are visiting.

For information on how Google uses the information obtained from sites or applications that use its services, visit the following link: www.google.com/policies/privacy/partners/.

For general information about cookies, visit www.allaboutcookies.org.

Our Contact Details

For North America	Allegro MicroSystems 955 Perimeter Road Manchester, NH 03103 USA privacy@allegromicro.com
For Europe (excluding European Union countries)	Allegro MicroSystems Europe Ltd Melita House 124 Bridge Road Chertsey KT16 8LA United Kingdom privacy@allegromicro.com
For European Union countries (excluding Germany)	Allegro MicroSystems Europe Ltd Rohanské nábřeží 693/10 Prague 8, 186 00 Czech Republic privacy@allegromicro.com
For Germany only	Dr. Rainer Harwardt ORGATEAM Unternehmensberatung GmbH Im Ettenbach 13a 77767 Appenweier Germany dpo-de@allegromicro.com

Your Right to Complain to a Supervisory Authority

If you are unhappy with the way in which your Personal Data has been processed, you may in the first instance, contact privacy@allegromicro.com.

If you remain dissatisfied, EU residents have the right to apply directly to the relevant competent supervisory authority. The current list of EU data protection supervisory authorities can be accessed here https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612080.