



## RECRUITMENT PRIVACY POLICY

Effective Date: May 19, 2020

This recruitment privacy policy (“Policy”) describes how Ultra Corporation and Ultra Europe (“Ultra” or “We”) handle and protect your personal data to which Ultra is provided access in connection with the recruiting process (“Recruitment data”). Recruitment data may include, without limitation, candidate status, work history, education, compensation, employer feedback, contact information, previous addresses or names, references, and criminal history where permitted by law.

### Collection of the Recruitment data

You may use various electronic and paper methods to submit Recruitment data to Ultra. In addition to collecting Recruitment data directly from you, to the extent permitted by law, Ultra may collect Recruitment data from third parties, for example, from recruiters, in connection with a background or employment check or an employment reference (subject to your consent where required by law), from a recruiting or other web site, or credit check.

### Use of the Recruitment data

Ultra processes Recruitment data for legitimate human resources and business management purposes. These include identifying and evaluating candidates for Ultra positions; record-keeping related to hiring processes; communicating with you the recruitment process; and conducting background checks, where permitted by law.

In addition to using Recruitment data for the position for which you have applied, Ultra may retain and use your Recruitment data to consider you for other positions. If you do not want to be considered for other positions or would like to have your Recruitment data removed, you may contact Ultra at [privacy@ultra.io](mailto:privacy@ultra.io)

Your Recruitment data are stored for a maximum duration of three years, unless otherwise required by applicable law. If we do not reply to your application, you allow us to store your data during this term in order to potentially contact you for another position within Ultra.

If you fail to provide Recruitment data when requested, which is necessary for us to consider your application (such as evidence of qualifications or work history), we may not be able to process your application further.

### Sensitive Recruitment Data

Ultra may perform background and criminal checks where permitted by law, and may process other sensitive Recruitment Data, such as citizenship or nationality information to assess whether a work permit and a visa will be necessary for the role, or health information, in order to evaluate a potential reasonable

accommodation in the recruitment and hiring process where requested. We process personal data for these purposes when we are required to do so by law or if you have given your explicit consent.

### Sharing of the Recruitment data

We may share your Recruitment data internally within Ultra for the purposes described in this Policy.

We may transfer Recruitment data to external third-party service providers performing certain services on behalf of Ultra. We do not allow our third-party service providers to use your Recruitment data for their own purposes. We only permit them to process your Recruitment data for specified purposes and in accordance with our instructions.



Ultra requires the service providers to undertake security measures consistent with the protections specified in this Policy.

We may be required to disclose certain Recruitment data to other third parties as required by law or regulation, or in connection with an investigation of suspected or actual fraud, illegal activity, security or technical issues. In addition, in the event of a re-organization, merger, sale, joint venture, assignment, or other transfer or disposition of all or any portion of Ultra's business, Ultra may transfer Recruitment data to successor entities or parties.

### **Security and confidentiality**

We have put in place technical and organizational measures designed to protect the integrity, confidentiality, security and availability of Recruitment data, and to comply with applicable legal requirements for information security. Ultra limits access to internal systems that hold Recruitment data to individuals who need access for a legitimate business purpose. They will only process your personal data on our specific instructions and they are subject to a duty of confidentiality.

### **Candidate rights**

You may exercise the following rights in relation to your Recruitment data:

- Request access to, correction of, or deletion of your Recruitment data;
- Object to processing of your Recruitment data. You also have the right to object where we are processing your Recruitment data for direct marketing purposes;
- Request the transfer of your Recruitment data to another party.

If you wish to request deletion of your Recruitment data or object to the processing of your Recruitment data, please send an email to [privacy@ultra.io](mailto:privacy@ultra.io)

### **Changes to this Policy**

Ultra reserves the right to modify this Policy by posting changes to relevant Ultra websites. If you submit additional Recruitment data or request to be considered for an Ultra position following the effective date of a modified Policy, your Recruitment data will be handled in accordance with the Policy in effect at that time.