Employee Privacy Notice (English) – Data Privacy Notice for Employees and Candidates

Effective Date: 1-December-2021

Responsible Entity: The responsible entity is the hiring or employer group company subsidiary of Maxeon Solar Technologies, Ltd., who can be contacted at 8 Marina Boulevard, #05-02, Marina Bay Financial Centre, Singapore 018981.

Subsidiary group companies: https://sunpower.maxeon.com/int/maxeon-locations-around-world

This Employee Privacy Notice ("Notice") pertains to your employment (or application for employment) with Maxeon Solar Technologies, Ltd. or one of its subsidiaries, which are generally referred to collectively as "Maxeon," "we," or "us."

This Notice describes:

- Our handling of personal and sensitive personal data in connection with your employment (or application for employment) with Maxeon.
- The measures we take to protect the security of personal data.
- The privacy rights you have relating to personal data.

If you have received a prior policy or notice regarding Maxeon's handling of personal data, the processing described in this Notice is in addition to the processing contemplated in your earlier policy or notice. In the event of any conflict, the terms of this Notice shall prevail.

Contact Maxeon Human Resources at askHR@maxeon.com with any questions.

1. THE INFORMATION WE COLLECT

We collect and maintain different types of personal data about you and third parties you share with us in connection with your employment or application for employment. Personal data is defined as any information relating to a natural person (an identified or identifiable individual), but it may also be defined by your country of residence. What data we collect in the context of your employment also depends on the local applicable rules. Personal data may include the following data as well as any documents that include such data.

- **Your Personal Details**: Full legal name; preferred name; address; phone number; email address; date and location of birth; age; gender; language; marital or partnership status; social security or other government identification information; passport information; photographs and videos (with your consent); height, weight and clothing sizes (if relevant to employment); residence status; citizenship status; work permit type; military status; nationality; and driver's license information.
- **Dependents and Beneficiaries**: The full name, gender, age, contact information and government identification information (where applicable) of any spouse, partner, beneficiary or dependent, including minor children.
- **Emergency Contacts**: The contact information, including name, phone number and email address, for any emergency contact you designate.
- **Position and Organizational Details**: Maxeon contact and organizational information (email address, office location, telephone number, etc.); information relating to relocations in

connection with or during your employment, including information needed for tax equalization; application, hire, transfer, promotion, demotion, resignation and termination information (dates, reasons, references, etc.); offer letters, employment contracts and offer acceptances; records of work absences, leave, entitlement and requests, salary history and expectations, performance appraisals, performance improvement plans, letters of appreciation and commendation; and driving information (driver's license number, vehicle registration, driving history, etc.).

- **Education and Talent Management Details**: Recruitment and application materials (resume, CV, letters, experience, education, transcripts, or other information you provide to us); information you provide during an interview or screening; reference and interview notes; technical skills; professional certifications or registrations; language capabilities; and training records and certifications.
- **Compensation, Benefits and Payroll Details**: Taxpayer or government identification number; payroll and banking information; wage, compensation, tax and benefit information; retirement account information; time-worked, sick days (including any basis therefor) and paid time off; and employee stock or equity information, including black-out related information.
- **Systems and Applications Data**: Voicemails, emails, correspondence, documents, call recordings, information documenting your interactions with IT and communication systems (including download logs, web-browser logs, recordings and screen-shots), information concerning hours worked, badging, and other work product and communications created, stored or transmitted using our networks, applications, devices, computers or communications equipment; information captured on security systems, including Closed Circuit Television ("CCTV"), where permitted by applicable law, and key card entry systems.
- **Software and Product Testing and Case Studies**: Identifiers (e.g., first and last name, contact information), feedback you provide in connection with beta testing or case studies, and electronic network information (e.g., information collected in connection with your use of a new application or product).
- **Compliance-related**: Any information required for us to comply with applicable laws and the requests and directions of law enforcement authorities or court orders (e.g., child support and debt payment information).

Sensitive Personal Data

In some circumstances and **only where permitted or required by applicable law**, Maxeon may collect and use sensitive personal data. This may include the following information.

- Racial or ethnic origin, to monitor hiring practices and diversity.
- Religious beliefs, to understand the holidays and labor days of your religion and to make the necessary accommodations to develop your employment.
- Sexual orientation, age and marital status, to provide you, your spouse, partner, dependents or beneficiaries with appropriate employment benefits.
- Physical or mental conditions or disability status, for us to consider requests for reasonable accommodations or adjustments.
- Absence due to illness.
- Health information, for employment purposes, management of industrial health and to provide health insurance benefits to you and your dependents. Health information includes test results for diseases including but not limited to the SARS-CoV-2 virus (COVID-19).

- Vaccine and contact-tracing information, to comply with local regulation and to mitigate the spread of disease. Vaccine information includes vaccination status for COVID-19 and other diseases.
- Trade union membership.
- Information contained in complaints and disciplinary and grievance procedures, including monitoring compliance with and enforcing our policies.
- With your consent, in connection with your employment or application for employment, information contained in criminal, civil, financial, or driving background searches, or information concerning offenses or alleged offenses in relation to you as well as the disposal or the court sentence in such proceedings.
- If relevant to your employment, your height, weight and clothing sizes.

Sensitive personal data collected by Maxeon is used only for the purposes mentioned above. We prohibit all forms of discrimination within the workplace.

Other Information
In addition to your personal data, we also collect other information from you to the extent permitted by law. This includes your use of our IT systems including, but not limited to, your IP address, browser, timestamp, location, country traffic data, location data, weblogs, and other communication data and the resources that you access. Maxeon uses cookies or other tracking technologies, such as web-beacons, to gather your personal data in your capacity as an employee when you access the internal networking service, internal employee portal and/or website.

How We Obtain Personal Data
Maxeon collects most of this personal data directly from you during your application for employment, onboarding and during employment by email, interviews or forms that you complete. We also collect personal data on your use of our IT systems and premises, and from internal Maxeon sources, such as your managers.

Certain personal data is collected from third parties when we check references, conduct a background check, medical examination, or drug screen when you have explicitly consented to such services in writing.

Whether the Provision of Personal Data is Mandatory
In some cases, the provision of your personal data may be necessary for Maxeon to enter into the employment contract with you or to allow Maxeon to comply with statutory requirements. In such cases, the failure to provide your information will result in Maxeon being unable to enter into or perform the contract with you or to process your application for employment. Whether the provision of your personal data is mandatory or voluntary and the consequences of refusal to provide the personal data will be specified to you at the point of collection.

2. HOW WE USE THE INFORMATION WE COLLECT

Maxeon processes your personal data for the business purposes described in this Notice, including the following.

- **Workforce Management and Planning:** To manage all aspects of the employment relationship, including: determining eligibility for employment, including verifying references, qualifications and status; payroll and benefit administration; managing stock options and restricted stock units;

travel and reimbursable expenses; development and training; absence monitoring; project management; auditing, compliance, and risk management activities; conflict of interest reporting; employee communications; performance evaluations; disciplinary actions; grievance and internal investigation activities; career management; transfers and internal candidate hiring; processing claims such as worker compensation and insurance claims; succession planning; relocation assistance; obtaining and maintaining insurance; the provision of employee related services; the provision of post-termination services; and to maintain emergency contact and beneficiary information.

- **Administrative Management:** Administrative management, including directories of employees and organizational charts and employee engagement programs.
- **IT and Communications Systems:** Operating, managing, securing, improving and monitoring information technology (IT) and communications systems; and maintaining records relating to business activities, budgeting, financial management and reporting, and communications, and preparing related audit trails and reports.
- **Safety and Security**: To protect the safety and security of our workforce, guests, property, and assets, including the confidentiality of our information, and to manage and monitor activities using our facilities, computers, devices, networks, communication systems and other resources.
- **Communication and Emergencies:** To facilitate communications to support business continuity, protect the health and safety of employees and others, safeguard IT infrastructure, office equipment and other property.
- **Investigation, Response to Claims, and Legal Compliance:** To investigate and respond to claims, to comply with legal and other requirements, such as income tax, record-keeping and reporting obligations, to conduct audits and investigations to prevent and/or detect fraud or corruption, to complying with government inspections and other requests from government or other public authorities, to respond to legal processes such as subpoenas, to pursue legal rights and remedies, to defend litigation and to manage internal complaints or claims.
- **Software and Product Testing and Case Studies:** To improve the quality, stability, security, customer experience, and reliability of new software and products for which you review and provide feedback as part of voluntary programs and case studies.
- **Business Operations:** To manage and allocate company assets and human resources; for strategic planning, project management, business continuity, and strategic activities such as mergers, acquisitions, sales, re-organizations and disposals, including bankruptcy, scaling business operations and integration with purchasers.
- **Intellectual Property:** To prepare, file, register and manage our intellectual property assets, including patents, copyrights, trademarks and related filings and applications.

Maxeon does not collect or compile personal data from employees for dissemination or sale to third parties for consumer marketing purposes.

2.1. Information on legal bases for employees located in the European Union (EU) – European Economic Area (EEA)

We collect, use and store your personal data for the purposes outlined in this Notice in reliance on the following legal bases:

- where necessary for us to administer your contract of employment or for services or in connection with services or benefits which you request from us;
- where necessary to comply with a legal obligation;

- where necessary for our legitimate interests and where our interests are not overridden by your data protection rights;
- where necessary for the purposes of carrying out obligations in the field of employment and social security and social protection law under local law; and
- where you have given consent.

Besides the legal bases under the General Data Protection Regulation (GDPR) and depending on where the you are located, other specific local legal bases may apply.

3. WHO HAS ACCESS TO YOUR PERSONAL DATA

Your personal data, to the extent allowable under law, is stored centrally in Maxeon's systems and may be accessed by Maxeon, its affiliates and authorized third parties for the purposes set out in this Notice. We only share your personal data on a need-to-know basis, as further explained below, with our affiliates, trusted third parties, and in other instances where required by law.

- **Within Maxeon:** Your personal data will be shared within Maxeon with members of Human Resources, Accounting, Financial, Audit, IT, managers, Compliance, travel services, and Legal, if access to this information is necessary for them to perform their duties. Some of these individuals may be located in different jurisdictions than you, and as such, your personal data may be shared globally. To the extent you participate in an employee discount program or otherwise purchase a Maxeon system, which may be offered from time to time, a subset of your personal data will be shared with Sales or an independent dealer, and will be subject to Maxeon's Privacy Policy at https://corp.maxeon.com/legal.
- **Third-Parties and Service Providers:** We may also share your personal data with third parties who provide services to Maxeon, including professional advisors (accountants, auditors, lawyers, bankers, insurers and other professionals), and service providers who support IT, HR, payroll, benefits, insurance, expense, travel, rewards, equity, our corporate credit card, or other business activities.
- **Corporate Transactions:** With your consent where required under applicable law, a third party in connection with any proposed or actual reorganization, merger, sale, joint venture, assignment, transfer or other disposition (or transition thereof) of all or any portion of Maxeon's business, assets or stocks (including in connection with any bankruptcy or similar proceedings).
- **As Required by Law:** We will share your personal data to comply with legal obligations, including to respond to a lawful governmental request, order or judicially sanctioned document, e.g., a court order or subpoena or to process governmental requests, such as wage garnishments or levies.
- **Our Legal Interests:** We also may disclose your personal data to protect against fraud or to protect our contractual, property, intellectual property or other rights.

4. TRANSFERS OF YOUR PERSONAL DATA

Maxeon operates worldwide and has centralized aspects of our operations in Finance and HR. Accordingly, Maxeon may transfer certain personal data to personnel throughout Maxeon in order to fulfill the purposes described in this Notice, including to Maxeon affiliates in: the United States of America, Singapore and Philippines. The Maxeon affiliates to which your data is transferred may be subject to data protection rules that provide for a lower standard of protection than your jurisdiction. If so, when information is transferred outside of your country, we will ensure that your information is protected to at least the same standard as that which is required in the originating country. For example, we will always that there is a proper legal agreement that covers the data transfer.

Where your personal data is transferred to third parties, we have engaged service providers that have agreed to provide adequate protection of your personal data in accordance with applicable laws and contractual arrangements. Our service providers are expected to protect the confidentiality and security of your personal data, and only use such personal data for the provision of services to Maxeon in compliance with applicable laws.

If you are situated in the European Union and we transfer of your data outside the EEA, we will take steps to ensure that appropriate security measures are taken to ensure that your privacy rights continue to be protected as outlined in this Notice. These steps include imposing contractual obligations on the recipient of your personal information (such as the EU Standard Contractual Clauses) or ensuring that the recipients have subscribed to international frameworks that aim to ensure adequate protection. You may contact us for more information about the protections that we put in place and to obtain a copy of the relevant documents.

5. HOW LONG WE RETAIN YOUR PERSONAL DATA

We retain your personal data for the period necessary to fulfill the purposes outlined in this Notice. Retention periods vary and are based on a number of factors, including: the time periods of the purposes outlined in this Notice, the term of your employment, the type of data, your role and activities while employed, applicable statutes of limitations and statutory data retention obligations, and any claims, lawsuits, public disclosures, audits or investigations.

6. SECURITY

We will take and will also require third parties with access to your personal data to take appropriate administrative, physical, procedural, organizational and technical security measures to protect your personal data from loss, misuse, unauthorized access, disclosure, or modification. We address data security consistent with applicable data protection laws and regulations.

Although we endeavor to protect the security and integrity of the personal data we collect, we cannot guarantee or warrant that any data, during transmission through the Internet or while stored on or using our systems, or otherwise in our care, is 100% secure from intrusion by others. Please contact askHR@maxeon.com with questions or if you have reason to believe that your interaction with us is no longer secure.

7. APPLICABLE LAW

Your personal data will be handled in accordance with applicable laws and regulations in the jurisdiction in which you reside.

8. CHANGES TO THIS NOTICE

Maxeon, in its sole and absolute discretion, may amend, interpret, modify or withdraw any portion of this Notice and related practices in accordance with applicable law. We will provide you with an updated Notice with its effective date sending you any updates or posting the updated Notice available at your local facility. Any changes in this Notice will apply to all personal data in our possession regardless of whether such personal data was obtained before or after any such Notice change. We will notify you about material changes to this Notice in accordance with and if required by applicable laws. If you need clarification regarding any aspect of this Notice, please contact askHR@maxeon.com.

9. YOUR RIGHTS AND CHOICES

You may be entitled to additional rights relating to your personal data. To the extent required by applicable law, you are entitled to request certain data in your personnel file. Please contact askHR@maxeon.com for more information.

9.1. Australia

In **Australia**, you may access and seek the correction of the personal information we hold about you by contacting askHR@maxeon.com. We may decline a request to access or correct your personal information in certain circumstances in accordance with the law. If we refuse a request, we will provide you a reason for our decision to the extent permitted by law.

If you have contacted us with a complaint about how we have handled your personal data, we will investigate and respond as soon as reasonably practicable, noting that more complex matters may take a longer amount of time. If you are not satisfied with our response to a complaint, you may contact the Office of the Australian Information Commissioner by using the contact details located at www.oaic.gov.au.

9.2. EU/EEA

In the **EU – EEA**, if you are an employee located in the European Union, you have the following rights:

- the right to access your personal data;
- the right to correct, delete or restrict (stop any active) processing of your personal data;
- the right to obtain the personal data you provided to us in relation to a contract or with your consent in a structured, machine readable format, and to ask us to share (port) this data to another controller;
- the right to object to the processing of your personal data in certain circumstances, such as where we do not have to process the data to meet a contractual or other legal requirement, or where we are using the data for direct marketing;
- where we have asked for your consent, the right to withdraw consent at any time. The withdrawal of consent will not affect the lawfulness of processing based on consent before its withdrawal; and
- the right to lodge a complaint with your local data protection authority at your habitual residence, place of work or place of the alleged infringement.

These rights may be limited, for example if fulfilling your request would reveal personal data about another person, or if you ask us to delete information which we are required by law to keep or have compelling legitimate interests in keeping.

To exercise any of the above-mentioned rights, please contact askHR@maxeon.com.

9.3. Malaysia

In **Malaysia**, as a data subject, you have rights under the Personal Data Protection Act 2010, which include:

- the right to access your personal data;
- the right to correct your personal data; and
- the right to limit the processing of your personal data, including personal data relating to other persons.

These rights may be limited, for example if fulfilling your request would reveal personal data about another person or where providing access would disclose confidential commercial information. Relevant exemptions are set out under the Personal Data Protection Act 2010. We will inform you of relevant exemptions we rely upon when responding to any request you make.

To exercise your rights, please contact askHR@maxeon.com. Please note that limiting the processing of your personal data may affect the performance of our contract with you or the processing of your application for employment.

9.4. Mexico

In **Mexico**, depending on your place of residence, you may be entitled to enforce your rights of access, rectification, cancellation, or opposition relating to your personal information ("ARCO Rights"). To the extent required by applicable law, you are entitled to request certain information in your personnel file.

To exercise your ARCO Rights you must issue a request to our Data Protection Officer in Mexico at DPOMX@maxeon.com. The request must include the following information:

- Your name, address and e-mail for delivery of the response to your request;
- The documents that evidence your identity (elector card, Passport or other official identification) or the documents that evidence the legal representation of the relevant employee;
- A clear and succinct description of the personal information in connection with which you desire to exercise the Rights;
- Any document or information that facilitates the location of your personal information; and
- If you have requested the rectification of your personal information, the modifications that are being requested and the documents that support such request.

We will respond to your request, indicating the reasons supporting the response, by e-mail no later than 20 business days from the date on which the ARCO Request is received. In the event that the ARCO Request is granted, the requested changes will be made no later than 15 business days from the date of such grant. In the event of you requesting access to your personal data, we will inform you via the email whereby our response to your request is communicated to you, the means by which you will have access to your personal information if the request is granted. The time periods mentioned in this paragraph may be extended by the Data Controller once for an equal period of time, if necessary.

If you wish to limit the use or disclosure of your personal information, you must submit your request to the above-mentioned address in order for you to be registered in an exclusion list created by Maxeon.

To revoke your consent for the processing of your personal information, you must file your request to the above-mentioned address. If after the revocation you request confirmation of the same, we will respond to you explicitly.

We inform you that we may not be able to attend to your request or conclude the processing of your personal information immediately in every case, since it is possible that due to a legal obligation we require to continue processing your personal data (revoking your consent for the processing of your personal data may result in the impossibility of continuing with our legal relationship).

If you believe that your right to the protection of your Personal Data has been injured by us, you may file a claim or complaint at the National Institute of Transparency, Access to Information and Protection of Personal Information (INAI).

9.5. Philippines

In the **Philippines**, As a data subject, you have rights under the Data Privacy Act, which include:

- the right to be informed of the processing of your personal data;
- the right to object to the processing of your personal data;
- the right to access your personal data;
- the right to rectification or to make corrections to your personal data;
- the right to erasure or blocking of your personal data;
- the right to damages;
- the right to lodge a complaint before the National Privacy Commission; and
- the right to data portability.

To the extent required by applicable law, you are entitled to request certain information in your personnel file. Please consult your local HR representative for more information. You may also reach out to our Data Protection Officer in the Philippines at DPOPH@maxeon.com.

9.6. South Africa

In **South Africa**, you have the right to have your personal information processed in accordance with the conditions for the lawful processing of personal information, including the right:

- to be notified that personal information about you is being collected, or when your personal information has been accessed or acquired by an unauthorized person;
- to establish whether an employer holds personal information relating to you and to request access to such personal information;
- to request, where necessary, the correction, destruction or deletion of your personal information;
- to object, on reasonable grounds, relating to your particular situation to the processing of your personal information where Maxeon processes your information on the basis of your or its legitimate interests;
- to submit a complaint to the Information Regulator regarding the alleged interference with the protection of personal information of any employee; and
- to institute civil proceedings regarding the alleged interference with the protection of your personal information.

To the extent required by applicable law, you are entitled to request access to details of the personal information in your personnel file. Please consult askHR@maxeon.com for more information.

The contact details for the Information Regulator are as follows:

Address: JD House, 27 Stiemens Street, Braamfontein, Johannesburg 2001
Email: complaints.IR@justice.gov.za

9.7. China

In **China**, as a data subject, you have rights under the applicable personal data protection laws in China, which include:

- the right to access your personal data;
- the right to correct your personal data;
- the right to delete your personal data; and
- the right to withdraw your consent to the processing of your personal data in relation to your employment or your application for employment.

These rights may be limited, for example, if fulfilling your request would impact the confidentiality of our management deliberations, where the request would infringe the legitimate rights of a third party or if you ask us to delete information which we are required by law to keep. Relevant exemptions are set out under the applicable data protection laws in China. We will inform you of relevant exemptions we rely upon when responding to any request you make. To the extent permitted by applicable law, Maxeon has the right to charge a reasonable fee for unfounded or manifestly excessive data access requests.

To exercise your rights or for further information about your personal data, please contact askHR@maxeon.com. If you have unresolved concerns, especially where you consider that the processing of your personal data has harmed your legitimate rights and interests, you may also report it to the relevant authorities.

9.8. California

In **California**, beginning in 2023, the California Consumer Privacy Act ("CCPA") will grant employees residing in the State of California certain rights with respect to the personal information collected by their employer:

- Right to Know. You may have a right to request that we disclose to you certain information in your personnel file. You may also have a right to request additional information about our collection, use, or disclosure of personal information. Note that we have provided much of this information in this privacy notice.
- Right to Request Deletion. You may have a right to request that we delete personal information under certain circumstances, subject to a number of exceptions.
- Right to Opt-Out. You will have a right to opt-out from future "sales" of personal information. However, we do not "sell" personal information of employees or candidates as defined by the CCPA and have not done so in the past 12 months.

Once these rights are in effect, you may make a request to access or to delete personal information by consulting your HR representative or by contacting askHR@maxeon.com for more information. You may also designate, in writing or through a power of attorney, an authorized agent to make requests on your behalf to exercise these rights. Before accepting such a request from an agent, we will require the agent to provide proof you have authorized it to act on your behalf and we may need you to verify the request directly with you.

Finally, you will have a right to not be discriminated against for exercising these rights.

10. MONITORING

All material and data stored on Maxeon systems and devices is the property of Maxeon. Maxeon reserves the right to access all material and data to the extent permitted by law, including personal and sensitive

personal data, that is stored on Maxeon systems and devices, including devices connected to the Maxeon network or that are otherwise used for business purposes. Maxeon may also monitor your use of IT systems and premises (including CCTV and door entry systems) in accordance with the law.

Employees should have minimal expectations of privacy in relation to information transmitted or stored in or through Maxeon assets, including personal (i.e., non-business related) communications made using Maxeon facilities and communications originating or terminating on personal devices that are connected to corporate networks and other facilities.

To the extent that Maxeon's monitoring activity results in the collection of personal data about individuals, that personal data is handled in accordance with applicable privacy laws and applicable Maxeon policies and procedures.

11. CONTACT US

If you have any questions or concerns regarding the handling of your personal data or to update your personal data, please contact your local HR representative. Alternatively, you can contact HR at askHR@maxeon.com or at https://corp.maxeon.com/contact-us.

Our Data Privacy Officer in Singapore can be contacted at DPOSG@maxeon.com.

Our Data Privacy Office in Mexico can be contacted at DPOMX@maxeon.com.

Our Data Privacy Officer in Philippines can be contacted at DPOPH@maxeon.com, +63 288412432 or by writing to: Data Protection Officer, 100 East Main Ave., Phase 4 Special Economic Zone, Laguna Technopark, Biñan, Laguna, Philippines 0423.

You may report alleged violations of law or policy using Maxeon's Compliance and Ethics Helpline at https://maxeon.ethicspoint.com. You may also report concerns or complaints to our General Counsel at GeneralCounsel@maxeon.com.

12. CONSENT AND ACKNOWLEDGMENT

By clicking the "Accept" button, I agree to and confirm the following.

I acknowledge that I have read and understand the terms of this Employee Privacy Notice ("Notice"). To the extent applicable, I understand that I am responsible for informing my dependents and beneficiaries whose personal data I provide to Maxeon about the content of the Notice. I further represent and warrant that I am authorized by my dependents and beneficiaries to disclose their personal data to Maxeon for the purposes set forth in the Notice.

I authorize Maxeon to access all material and information, including my personal and sensitive personal data and communications, that are created, stored or transmitted using Maxeon networks, systems, devices, computers or other communication equipment.

I grant my express consent (where required under applicable law) to the collection, storage, use, retention, processing, disclosure (including to third party recipients), and transfer (including for transfers outside of my country), of my personal data and sensitive personal data, consistent with the terms of the Notice.

To the extent applicable, I grant or otherwise have obtained express consent (where required under applicable law) for the collection, storage, use, retention, processing, disclosure (including to third party recipients) and transfer (including for transfers outside of my country), of personal and sensitive personal data of my spouse, partner, beneficiary or dependent, including minor children, consistent with the terms of the Notice.

I understand that I may withdraw my consent (where given in accordance with applicable law) for the processing and transferring of personal data at any time by contacting askHR@maxeon.com.

Where consent is required under applicable local law, I understand and acknowledge that a refusal to or a withdrawal of consent to the processing of personal data, including sensitive personal data, of myself, my spouse, partner, beneficiary or dependent, including minor children, may result in the inability to establish or continue a legal relationship with Maxeon, the data controller, including but not limited to employment and the provision of certain benefits.