

APPLICANT PORTAL PRIVACY POLICY

Thank you for applying at Eaton.

Eaton Corporation plc., its subsidiaries and affiliated companies (“Eaton”) respect Personal Data or Personal Information (hereunder “Personal Data”), and strive to collect, use, store and disclose (collectively “process”) them in accordance with applicable laws and regulations. Eaton is committed to protecting the Personal Data that it gathers concerning its prospective, current and former applicants. This Policy informs you about the use of your Personal Data and your rights.

1. What Personal Data (“Your Personal Data”) is Eaton collecting?

- Data that you (“You”, “Your”) input during the application process, joining the Eaton Talent Network or job alert creation which includes, but is not limited to: your resume, personal ID, gender and personal address if you wish to provide it, personal history, cover letter, contact information, experience, education, certifications, attachments ,any screening questions answers if prompted and an evaluation for you and our recruiters if your application matches the positions.
- Eaton does not collect Sensitive Personal Data unless it is required by law. Sensitive data is for example: race, religious beliefs, sexual or political preferences.
- Globally, we ask for gender on a voluntary basis, at the point of application.
- For applicants located in the US, we may ask for information regarding ethnicity, disability and veteran status, on a voluntary basis, at the point of application.
- Your IP Address is not collected by Eaton at the time of your application.
- Your login information (email address and encrypted password) for your Applicant Portal.
- Cookies are only collected for the duration of the sessions (in order to help the applicant, navigate more easily) and are deleted when the online session ends.
- All other data that you are willing to submit to Eaton in support of your application.
- We use third-party cloud vendors to store and process the data collected through our recruiting software. The data is stored in secure data centers, protected by firewalls, access controls, and other adequate security measures. The vendors comply with data protection and privacy regulations and undergoes regular security audits to ensure the security of their infrastructure.
- Background checks: If a background check is required for your application, Eaton will collect your specific consent for it in countries where required; where a consent is not required, you might expect that Eaton will proceed with a background check on your application.

2. What is the Purpose of Collecting and Processing Your Personal Data?

- Help you manage job opportunities: when You apply, You have access to the Applicant Portal, where You can find Your profile information, application information and any saved job searches.
- Help Eaton assess your application(s) to a or several position(s): when You apply, Eaton’s recruiter and/or hiring team will use the information You provided to consider You for the or several positions.
- Eaton’s recruiters can access Your data from within a given region – but at Your demand or upon Your consent, Your data can be shared with an Eaton recruiter or hiring team outside of your region of origin would You be interested in a position abroad.
- Eaton does not share Your data with external Third Parties other than the ones necessary for the performance of the recruitment, notably, the certified Data Processors,

subcontracted for performing the applicants processing service, the background checks and the performance tests where applicable. Please note that if You ask Eaton not to share your Personal Data with other parties (strictly regarding the hiring process), Eaton might not be able to move forward with Your application.

- If Your application is successful, your Personal Data may be processed for human resources, administration, finance and generally employment management purposes. • Unless you have requested a data deletion by emailing Eaton's Talent Acquisition applicantdata@eaton.com
- Eaton will delete your data in abidance with the legal schedule applicable to your country of residence, when no longer needed as specified in section 3 of this policy.
- You can withdraw your application at any time or request to have all Your data deleted, both on the career site and for Your submitted applications, by emailing Eaton's Talent Acquisition Team applicantdata@eaton.com .

3. How will Your Personal Data be processed / used?

- You can set up a personal account on Eaton's career site ("Applicant Portal") which allows You to manage Your job opportunities and track your (different) application(s).
- Eaton's recruitment team will use Your Personal Data only for the purpose of assessing Your solicitation. Eaton's hiring managers have access to Your submitted applications and the data contained therein and will use them to contact You and assess Your solicitation.
- Eaton abides by, at a minimum, the security requirements as prescribed by applicable law and utilizes adequate physical and procedural security controls to protect Personal Data. This includes, but is not limited to, firewalls, access controls, system level security, data protection and privacy training and other procedures to protect Personal Data from unauthorized access.
- We will process your Personal Data only for as long as necessary in relation to the purposes described under section 2 above. Our general policy is that we erase your Personal Data 6 months after you have been rejected a proposition from Eaton. The reason why we keep your Personal Data after the termination of the recruitment process is to ensure that we have all necessary data to protect our rights should a applicant take legal actions. In some cases, we may also process your data for a longer period of time than stated above. This may be the case if we need to protect our legal rights, for example in a legal dispute, or if necessary to fulfil a legal obligation.
- We will leverage artificial intelligence to match the applications to the job descriptions and to recommend you open positions. No automated decision-making is taking place.
- If you consent to further processing of the Personal Data for the purposes of being a part of our talent database, for potential future job opportunities, we will retain your Personal Data as long as you wish to remain in our talent database.
-

4. Your data protection and privacy rights

- You can access Your profile and any applications by accessing <https://jobs.eaton.com/> which can be found at the bottom of the eaton.com/careers site or at the top of the jobs.eaton.com page. Within the Applicant Portal You will see all data You submitted in Your profile, review any applications You've submitted, see the status of those applications in addition to any saved job searches.
- You can ask for the deletion of your Personal Data.
- You can ask for the correction of your Personal Data.

- You can object to processing of your Personal Data, ask us to restrict processing of your Personal Data or request portability of your Personal Data.
- If we have collected and process Your Personal Data with Your consent, You can withdraw Your consent at any time. Withdrawing Your consent will not affect the lawfulness of any processing we conducted prior to Your withdrawal, nor will it affect processing of Your Personal Data conducted in reliance on lawful processing grounds other than consent.
- You have the right to complain to a data protection authority about our collection and use of Your Personal Data.

To exercise one of the above rights (except the last one) please contact us by sending a request to applicantdata@eaton.com.

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

5. Personal Data Dispute resolution

You can also always submit any claim regarding Your Personal Data or Eaton's practices concerning Personal Data to:

Global Ethics and Compliance
Data Protection and Privacy Office
Eaton Corporation
1000 Eaton Center
Cleveland, Ohio 44122
dataprotection@eaton.com

For all other questions, please contact your Talent Acquisition contact or send an email to applicantdata@eaton.com

6. International data transfers

Your Personal Data may be transferred to and processed in countries other than the country in which you are resident. These countries may have data protection and privacy laws that are different to the laws of your country.

However, we have taken appropriate safeguards to require that Your Personal Data will remain protected in accordance with this Notice. These include implementing the European Commission's Standard Contractual Clauses for transfers of Personal Data between our group companies, which require all group companies to protect Personal Data they process from the European Economic Area (EEA) in accordance with European Union data protection law.

CALIFORNIA INFORMATION ON PROCESSING OF PERSONAL INFORMATION

This section applies to California Residents.

Eaton Corporation, together with its subsidiaries and affiliates (collectively, "us," "we," or "our") is committed to the responsible management, use, and protection of personal information. This document describes our practices in connection with the information that we collect from you in connection with your application at Eaton. Note that some of the data collection and uses described below may not apply to you.

CATEGORIES OF PERSONAL INFORMATION

We process the following categories of your Personal Information:

- **Identifiers and information protected by California Civil Code section 1798.80(e).** Such as real name, alias, postal address, unique personal identifier, online identifier, internet protocol address, email address, account name and password, social security number, driver's license number, passport number, state identification card number, social media handle, or other similar identifiers.
- **Professional or employment-related information.** Such as resumes, employment and education history, professional members, board service, licenses and certifications, training records, interview notes, payroll, position/job title, work location, job description, start date/years of service with the company, recruitment details, termination details, attendance records, accident reports, performance reviews, communications, and other human resources related records.
- **Protected class and demographic information.** Such as physical characteristics or description, marital status, number of children, name, gender, and age of spouse or children, race, gender, age, disability, and national origin.
- **Financial, medical, or health information.** Such as bank account number, credit card number, debit card number, credit history check, household income data, salary, payments made to you, loans, medical record number, medical diagnosis, medical history, information related to medical payments, health insurance name/identification or account number, work related injuries, and other insurance and benefits details.
- **Internet activity.** Electronic network activity information, including, but not limited to, browsing history, search history, IP address, cookies and similar IDs, and information regarding a consumer's interaction with an Internet Website, application, or advertisement.
- **Geolocation data.** Such as general and specific location.
- **Education information.** Information that is not publicly available personally identifiable information as defined in Family Educational Rights and Privacy Act.
- **Inferences.** Inferences drawn from any of the above information to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities and aptitudes.

PURPOSE OF USE FOR PROCESSING INFORMATION

Your Personal Information may be processed for the purpose of:

- **Performing Services.** Performing services on behalf of, or in relation to the administration of, our relationship with you. This will include activities such as human resources administration, such as recruiting and travel or other reimbursable expenses.
- **Legal and Compliance Purposes.** Activities related to legal compliance requirements such as maintaining a record of applications.
- **Debugging.** Debugging to identify and repair errors that impair existing intended functionality of company's systems, networks, and devices.
- **Short-Term, Transient Use.** Short-term, transient use as permitted by law.
- **Quality Assurance.** Undertaking activities to verify or maintain the quality and to improve, upgrade, or enhance, our services and devices, such as certain recordkeeping, document management and other similar services.

As a California resident you have the following rights regarding the collection, use, and sharing of your personal information.

Right to Know. You have the right to request information about the categories of personal information we have collected about you, the categories of sources from which we collected the personal information, the purposes for collecting the personal information, the categories of third parties with whom we have shared your personal information, and the purpose for which we shared your personal information (“Categories Report”). You may also request information about the specific pieces of personal information we have collected about you (“Specific Pieces Report”). Please specify which right you want to execute.

Right to Delete. You have the right to request that we delete personal information that we have collected from you unless we have legal purpose to maintain the data. You can execute your right, at any time by contacting us by sending an email to dataprotection@eaton.com, by calling +1-800-386-1911 or by [using this online form](#). Please note that the right to opt-out in the form does only apply for consumers and not for applicants.

In accordance with applicable law, we will not discriminate against you for exercising these rights.

Verification: In order to exercise your rights, we will need to obtain information to locate you in our records or verify your identity depending on the nature of the request. If you are submitting a request on behalf of a household, we will need to verify each member of the household in the manner set forth in this section. For Specific Pieces Report, we will request your first name, last name, email address and application requisition number to verify your identity, along with a signed declaration, under penalty of perjury, that you are who you say you are. For a Categories Report, we will request your first name, last name, email address and application requisition number to verify your identity. For a Right to Delete request, we will request your first name, last name, email address and application requisition number to verify your identity.

You may use an authorized agent to exercise your rights on your behalf. If you are making any of the requests above through an authorized agent, we will request written authorization from you and will seek to verify as described above or we will accept a legal Power of Attorney under the California Probate Code to the authorized agent. We cannot respond to your request or provide you with personal information if we cannot verify your identity or authority to make the request and confirm the personal information relates to you.

Timing: We will respond to Requests to Delete and Requests to Know within 45 days, unless we need more time in which case we will notify you and may take up to 90 days total to respond to your request.

February 22, 2023