

Lutron EA Limited - Privacy Notice – Recruitment

We describe the type of information we process it, why we are processing it and how that processing may affect you in this Recruitment Privacy Notice. We take our responsibilities to look after your data seriously and we are committed to protecting your privacy. There are steps you can take to control what we do with your data and we have explained those steps in this Privacy Notice.

When we talk about data and personal data in this Privacy Notice, we mean personal data which could identify you or which could be used to identify you such as your name and contact details. It may also include information about how you use our websites.

References in this notice to employment, work (and similar expressions) include any arrangement we may have under which an individual provides us with work or services or applies for such work or services. By way of example, when we mention an “employment contract”, that includes a contract under which you provide us with services; when we refer to ending your potential employment, that includes terminating a contract for services. We use the word “you” to refer to anyone within the scope of the notice.

1. Who is responsible for your data?

Lutron EA Limited is responsible for the processing of your personal data. Our registered address is 4/F, 125 Finsbury Pavement, London EC2A 1NQ. Email address for privacy queries - Candidateprivacy@lutron.com.

2. Personal data we collect about you

Depending on how you use our recruitment websites, we might collect the following kinds of information about you:

Your name and contact details (email address, telephone number), your qualifications and work experience details, information on your immigration status and whether you can lawfully work.	<ul style="list-style-type: none">• When you apply for a job with us• When you fill in application forms on our website
Communication we have with you (emails, letters, telephone calls, messages sent to us through our social media platforms, feedback)	<ul style="list-style-type: none">• When you get in touch with us• When we respond to your request for feedback
Information about you, city you live, information about your what you like and dislike to do	<ul style="list-style-type: none">• When you fill in application forms on our website• When you get in touch with us• When we respond to your request for feedback

Where necessary and in accordance with this privacy notice, we will require references and information to carry out background checks. If you have concerns about this in a particular context, you should speak to your recruiter or our HR department. Please note we may also receive data from third party recruiters, agents and similar organizations as a part of the recruitment process.

3. What are the grounds for processing?

According to data protection law, there are various grounds on which we can rely when processing your personal data. In some contexts, more than one ground applies. We have summarized these grounds as Contract, Legal obligation, Legitimate Interests and Consent and outline what those terms mean in the following table.

<i>Term</i>	<i>Ground for processing</i>	<i>Explanation</i>
Contract	Processing necessary for performance of a contract with you or to take steps at your request to enter a contract	This cover carrying out our contractual duties and exercising our contractual rights.
Legal obligation	Processing necessary to comply with our legal obligations	Ensuring we perform our legal and regulatory obligations. For example, providing a safe place of work and avoiding unlawful discrimination.
Legitimate Interests	Processing necessary for our or a third party's legitimate interest	We or a third party have legitimate interests in carrying on, managing and administering our respective businesses effectively and properly and in connection with those interests processing your data. Your data will not be processed on this basis if our or a third party's interests are overridden by your own interests, rights and freedoms.
Consent	You have given specific consent to processing your data	In general processing of your data in connection with employment is not conditional on your consent. But there may be occasions where we do specific things such as provide a reference and rely on your consent to our doing so.

Countries take a different approach to the use by companies of legitimate interests as a reason for processing personal data. We are aware of those different approaches in the countries in which we operate, and we take that into account and respect those differences when we process your personal data.

4. Sensitive personal data

Certain kinds of personal data, such as data about your racial or ethnic origin, your physical or mental health, your religious beliefs or alleged conviction of criminal offences, are special categories of personal data which by law require additional protection.

If we process sensitive personal data about you (for example but without limitation), storing your health records to assist us in ensuring that we provide you with a healthy and safe work workplace or to make reasonable adjustments for you during the recruitment process or processing personal data relating to diversity monitoring), as well as ensuring that one of the grounds for processing mentioned above applies, we will make sure that one or more of the grounds for processing sensitive personal data applies. In outline, these include:

- Processing being necessary for the purposes of your or our obligations and rights in relation to employment in so far as it is authorized by law or collective agreement;
- Processing relating to data about you that you have made public (e.g. if you tell colleagues that you are ill);
- Processing being necessary for the purpose of establishing, making/defending legal claims;
- Processing being necessary for provision of health care or treatment, medical diagnosis, and assessment of your working capacity;
- Processing for equality and diversity purposes to the extent permitted by law.

5. How we use your personal data

In the table below, we have set out the different ways in which we use your personal data and the reasons we rely on for using that data.

<i>Purpose</i>	<i>Examples of personal data that may be processed</i>	<i>Grounds for processing</i>
Recruitment	Standard data related to your identity (e.g. your name, address, email address, ID information and documents, telephone numbers, place of birth, nationality, contact details, professional experience and education (including academic records, professional licenses, memberships and certifications, awards and achievements, and current and previous employment details), financial information (including current salary information) language skills, and any other personal data that you present us with as part of your application related to the fulfilment of the role. Information concerning your application and our assessment of it, your references, any checks we may make to verify information provided or background checks and any information connected with your right to work. If necessary, we will also process information concerning your health, any disability and in connection with any adjustments to working arrangements.	Contract Legal obligation Legitimate interests
Travel to attend interviews	Standard data related to your identity e.g. your name, address, email address, ID information and documents, you're travelling preferences such as seat and pick up arrangements	Legitimate Interests

<i>Purpose</i>	<i>Examples of personal data that may be processed</i>	<i>Grounds for processing</i>
Administering our recruitment process	Administering our online careers portal. Evaluating your experience and qualifications against the requirements of the position you are applying for. Communicating with you in respect of any offer of employment we choose to make and providing you with information about our onboarding process.	Contract Legal obligation Legitimate interests
Entering into a contract with you (if you are made an offer by us)	Information on your terms of employment from time to time including your hours and working patterns, your pay and benefits, such as your participation in pension arrangements, life and medical insurance; and any bonus schemes.	Contract / Legal obligation/Legitimate interests
Contacting you or others on your behalf	Your address and phone number, emergency contact information and information on your next of kin.	Contract Legitimate interests
Payroll administration	Information on your bank account, pension contributions and on tax, national insurance number or other government issued identifier (e.g. social security number).	Contract/Legal obligation/Legitimate interests
Budgeting & Financial planning	Information such as your proposed salary and (if applicable) envisaged bonus levels.	Legitimate interests
Disputes and legal proceedings	Any information relevant or potentially relevant to a dispute or legal proceeding affecting us.	Legitimate interests Legal obligation
Providing information to third parties in connection with transactions that we contemplate or carry out	Information on any offer made to you and your proposed contract and other employment data that may be required by a party to a transaction such as a prospective purchaser, seller or outsourcer.	Legitimate interests
Monitoring of diversity and equal opportunities	Information on your nationality, racial and ethnic origin, gender, sexual orientation, religion, disability and age as part of diversity monitoring initiatives. Such data will have aggregated and used for equality of opportunity monitoring purposes.	Legitimate interests

Please note that if you accept an offer from us the business will process further information as part of the employment relationship. We will provide you with our full Workplace Privacy Notice as part of the on-boarding process.

6. How long we keep your data

Although there is no specific period for which we keep your personal data, we will not keep your personal data for longer than is necessary for our purposes. If you are unsuccessful in gaining employment with us, we will likely keep your personal data for a short period after informing you that you were unsuccessful. In considering how long to keep your data, we will consider its relevance to our business and your potential employment either as a record or in the event of a legal claim. Your data may be kept on file and considered for other roles. If your data is only useful for a short period (e.g. CCTV footage data) we will delete it. Personal data relating to job applicants (other than the person who is successful) will normally be deleted after 12 months.

7. How do we protect your data?

We take a number of steps to protect your personal data against unauthorized access, unlawful use, accidental loss, corruption or destruction. We use technical measures such as encryption and password protection to protect your data and the systems they are held in. We also use operational measures to protect the data, for example by limiting the number of people who have access to the databases in which your information is held. We keep these security measures under review and keep up to date with current best practice.

8. Sharing your data

We will only disclose your personal data outside the group if disclosure is consistent with a ground for processing on which we rely and doing so is lawful and fair to you. We will disclose your data if it is necessary for our legitimate interests as an organization or the interests of a third party (but we will not do this if these interests are over-ridden by your interests and rights in particular to privacy). Where necessary, we will also disclose your personal data if you consent, where we are required to do so by law and in connection with criminal or regulatory investigations.

- i. Specific circumstances in which your personal data may be disclosed include: Government authorities such as border control authorities and law enforcement authorities: In some cases, we must provide your personal data to government authorities to ensure that you can work legally in the EU countries or attend an interview in the US to meet our legal and regulatory obligations
- ii. Recruitment companies/consultants (including online recruitment portals) and similar businesses as part of the recruitment process: We look for candidates via many different channels. We may share your data with the companies who we use to approach you for vacancies and feedback. We will ensure that the transfer is lawful and that there are appropriate security arrangements.
- iii. With our third-party travel company to book flights or arrange a visa if you are required to attend interview in the US at our headquarters
- iv. Within Lutron, where necessary, your personal data will be disclosed to relevant managers, HR and administrators for the purposes of your application as mentioned in this document.

We will also disclose this to other members of our group where necessary for decision making regarding your application – this will depend on the type of role you are applying for.

9. Sending data outside the EEA area

In connection with our business and for employment, administrative, management and legal purposes, we may transfer your personal data outside the EEA to members of our group processors in our Coopersburg USA headquarters. We will ensure that the transfer is lawful and that there are appropriate security arrangements. We have entered into an agreement ensuring appropriate and suitable safeguards with our group member/processors in USA. This is in standard terms adopted by the Information Commissioner and approved by the Commission. If you wish to see details of these safeguards, please send your request in writing to our DPL at Candidateprivacy@lutron.com

10. Your rights

We try to be as open as we reasonably can about personal data that we process. If you would like specific information, just ask us. You also have a legal right to make a “subject access request”. If you exercise this right and we hold personal data about you, we are required to provide you with information on it, including giving you a description and copy of the personal data and telling you why we are processing it.

If you make a subject access request and there is any question about who you are, we may require you to provide information from which we can satisfy ourselves as to your identity. As well as your subject access right, you may have a legal right to have your personal data rectified or erased, to object to its processing or to have its processing restricted. If you have provided us with data about yourself (for example your address or bank details), you have the right to be given the data in machine readable format for transmitting to another data controller. This only applies if the ground for processing is Consent or Contract.

If you gave us your consent to use your data, e.g. so that we can send you emails, you can withdraw your consent. Please note that even if you withdraw your consent, we can still rely on the consent you gave as the lawful basis for processing your data before you withdrew your consent.

11. Complaints & Contact us

To raise any objections or to exercise any of your rights or have any complaints concerning Lutron 's processing of your personal data please email us at Candidateprivacy@lutron.com or you can write to us at Data Protection, Lutron EA Limited, 4/F, 52 Leadenhall Street London EC3A 2EB.

Please note that you have the right to lodge a complaint with the supervisory authority which is responsible for the protection of personal data in the country where you live or work, or in which you think a breach of data protection laws might have taken place.

Candidates in the UK can contact the Information Commissioner's Office by telephone on 0303 123 1113, or by using the live chat service which is available through the Information Commissioner's website www.ico.org.uk.

Candidates in France can contact the Commission Nationale de l'Informatique et des Libertés by telephone on +33 (0)1.53.73.22.22 or by writing to the Commission at 3 Place de Fontenoy, TSA 80715, 75334 PARIS CEDEX 07, France.

Candidates in Spain can contact the Agencia de Protección de Datos by telephone on +34 91399 6200 or by writing to them at 3 C/Jorge Juan, 6, 28001 Madrid

Candidates in Italy can contact the Garante per la protezione dei dati personali by phone on +39-06-696771 or by writing to them at Piazza di Monte Citorio, 121-00186 Roma

Candidates in Germany can contact the Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit by telephone on +49 228 997799 0 or by writing to them at Husarenstraße 30, 53117 Bonn

12. Status of this notice

This notice does not form part of any contract of employment that you may enter into with us and does not create contractual rights or obligations. It may be amended by us at any time. Nothing in this notice is intended to create an employment relationship between Lutron EA Limited and any non-employee.