

APPLICANT PRIVACY NOTICE
EUROPEAN ECONOMIC AREA

This privacy notice (the “Notice”) describes how United Rentals, Inc. and its direct and indirect subsidiaries (the “Company”, “we” or “our”) collect, use and disclose the personal data of employees (“Personal Data”) in the European Economic Area (the “EEA”).

The controller responsible for your personal data is:

- **If you work in Belgium:**

United Rentals Belgium B.V.
Lange Lozanastraat 142, bus 2
2018 Antwerpen
Belgium

- **If you work in France:**

United Rentals S.A.S.
Z.I. les Alizés 5381 voie des Sarcelles
76430 St Vigor d’Ymonville
France

- **If you work in the Netherlands:**

United Rentals International BV and United Rentals B.V.
Bloemendaalse Zeedijk 10
4765 BP Zevenbergschen Hoek
The Netherlands

- **If you work in the United Kingdom:**

United Rentals U.K. Ltd.
Europa Way
Brigg, South Humberside
DN20 8UN
United Kingdom

- **If you work in Germany:**

United Rentals GmbH
Barbarastraße 62
46282 Dorsten
Germany

Data Protection Officer may be contacted by email at: kinast@kinast.eu or at the following address:

KINAST Rechtsanwaltsgesellschaft mbH
Attorneys at Law (Germany)
External Data Protection Officers | External Compliance Officers
Hohenzollernring 54
D-50672 Cologne
Germany

Information We Collect About You

- Details necessary to consider an individual for employment (a “Prospective Employee”) including, but not limited to: name, address, personal contact information, date of birth, social security numbers, employee driver's license numbers and details (including motor vehicle records), state identification card numbers, immigration status, email address, employment history, personal interests, educational history, gender, nationality, salary & benefit history, contact information (email address, phone number), and personality assessment testing results.
- Background details relating to Prospective Employees’ criminal record checks or credit checks (when permitted by law and related to the position for which the Prospective Employee is being considered).
- **When considering a Prospective Employee, the following Personal Data may be collected in accordance with the standards below:**
 - Only that Personal Data necessary and relevant to assess individuals for the position for which they are applying. In particular, information about criminal convictions and Sensitive Personal Data are requested in accordance with applicable local or national laws and regulations;
 - Information reasonably necessary to evaluate Prospective Employees and verify employment and educational histories, including by contacting credit reference agencies, past or current employers, and educational institutions; Prospective Employees are told in advance how and which aspects of their Personal Data will be verified and if any vetting will take place, are required to sign a waiver acknowledging such (where required), and which, if any, external agencies are used;
 - Information about criminal convictions, only if collection of such information is legally permitted, including where the Prospective Employee has given his or her explicit, informed consent, and the information can be justified for the specific role offered.

- Subject to the applicable Drug and Alcohol Policy, in some cases based on job requirements, pre-employment drug and alcohol tests for Prospective Employees., as permitted by law
- *Please note:* Prospective Employees will be given the opportunity to explain any discrepancies that emerge as a result of any verification or any information uncovered by vetting that might negatively affect their application. Moreover, any vetting : (i) is restricted to roles where reasonably necessary; (ii) will not involve approaches to colleagues or the family of individuals, except in exceptional circumstances; and (iii) is targeted at the collection of specific and not general information.

Sensitive Personal Data

- The Company may process certain Sensitive Personal Data of Prospective Employees. You acknowledge that it may be necessary to Process Sensitive Personal Data. This may be to ensure that the Company's workplace is a safe place for everyone, or to ensure compliance with all applicable laws and regulations. The Company also Processes Sensitive Personal Data as needed for carrying out obligations and exercising the Company's or Prospective Employee's rights in the field of employment, social security or social protection laws, as well as for the establishment, exercise or defense of legal claims. We ask for certain diversity-related data (such as gender), in connection with the maintenance of our internal policies relating to diversity, and where necessary in order to comply with the Company's legal obligations.
- When the Company Processes Sensitive Personal Data, it will only do so when necessary or with your consent, while employing measures that minimize the risks to the Prospective Employee and/or otherwise as further provided for in this Notice. The Company will only Process your Sensitive Personal Data where:
 - The Processing is required or permitted by applicable law;
 - The Processing is necessary for the purposes of carrying out the Company's obligations and exercising specific rights; or
 - The Company has, to the extent permitted by applicable law, obtained your explicit consent to Process such Sensitive Personal Data.

Purpose and Legal Basis for Processing

- The Company processes your Personal Data for the purposes of recruitment and evaluation of candidates for employment, and processes your Personal Data based on your consent, to:
 - Process your job application materials;

- Assess your qualifications for a position;
- Communicate with you;
- Comply with applicable law or regulation.

Transfer and Use of Your Personal Data

- The Personal Data the Company receives will be held on the computers and systems of its offices in the United States, Canada, the United Kingdom, and the EEA and may be accessed by or given to its Employees working outside the EEA. For example, Personal Data collected or entered onto the Company systems in the EEA may be accessed from the United States by the Company's employees and/or transferred to the Company systems in the United States. The Company has adopted an Omnibus Data Transfer Agreement (ODTA) to ensure compliance with European adequacy requirements concerning protection of Personal Data transferred outside the EEA. You can request to see the ODTA by contacting privacy@ur.com.
- By providing Personal Data to the Company you understand and acknowledge that the Company will share certain information within the Company as described above and with third parties as described herein.
- The Company shares Prospective Employee Personal Data – as appropriate – with Company personnel as necessary to evaluate your candidacy.
- In addition, the Company shares Prospective Employee Personal Data with third party service providers in order to administer and manage the Company's recruitment and hiring efforts, and to otherwise perform the activities set forth in this notice. These third parties include:
 - Entities providing talent management and recruiting services;
 - Entities that provide back office services, such as HR information systems suppliers and providers.
- Personal data will also be shared with third parties in the following limited circumstances:
 - With credit reference agencies, past or current employers, and educational institutions as reasonably necessary in connection with the evaluation of Prospective Employees.
 - As reasonably necessary to any subsidiary, ultimate parent company, and/or its subsidiaries with such group companies following procedures and policies that are consistent with this Notice.

- In the event that the Company sells or buys any business or assets, in which case the Company may disclose your Personal Data to the prospective seller or buyer of such business or assets.
 - If the Company is under a duty to disclose or share your Personal Data in order to comply with any legal obligation.
- The Company may also share information with its legal and regulatory authorities and the Company's accountants, auditors, lawyers and other outside professional advisors.
- Personal Data will only be transferred to a third-party data processor if it agrees to comply with procedures and policies which are compliant with this notice and the Company's procedures regarding data protection, or if that third party data processor puts in place adequate measures which are compliant with all applicable laws and regulations.

Security

- The Company will strive to protect your Personal Data via the following:
 - The Company has security procedures in place so that any Personal Data the Company holds is kept secure and in accordance with this Policy. This includes, without limitation, conducting periodic testing and monitoring of the Company's systems and security, maintaining an information security policy, training employees, and monitoring compliance with this Policy.
- The Company maintains security measures and technology to prevent Personal Data being inadvertently disclosed to any unauthorized third party either orally, in writing, via the internet, or by other means, accidentally or otherwise. This includes, without limitation, monitoring the Company's systems for unauthorized access; employing firewall protection and system security patches; and employing virus and malware protection.
 - The Company requires laptops, backup tapes, and other portable devices containing Personal Data to be password protected and all Personal Data is encrypted as appropriate.
 - The Company uses physical, administrative, and technical procedures to limit access to Personal Data as described in this Policy.
 - The Company has the ability to remotely destroy Personal Data on certain mobile devices that are lost or stolen; lost or stolen laptops are rendered inaccessible using whole drive encryption.

Data Retention and Destruction

- The Company will only retain your Personal Data for as long as is necessary to achieve the purposes outlined in this Notice and for any period thereafter as required by law or pursuant to your consent.

- After the expiration of the retention period described above, the Company will destroy or delete your Personal Data in a secure manner.

Data Subject Rights

- Subject to certain exceptions, Prospective Employees have the right to:
 - Receive information about the Personal Data that the Company holds about them;
 - Request that any inaccurate or incomplete Personal Data be corrected or supplemented;
 - Have their Personal Data erased, unless the Company has a legitimate reason to retain the Personal Data;
 - Obtain restriction of Processing pending their objections and challenges to the Company's Processing activities, for the time necessary to answer such objections and challenges;
 - Object to their Personal Data being used for a particular purpose;
 - Exercise their right of portability to transmit their Personal Data to another Data Controller, unless the Company has a legitimate reason to retain certain Personal Data; and
 - Withdraw any consent that given to the Company in connection with the processing of their Personal Data.
- All of these rights are subject to certain conditions and exemptions. For example, a Prospective Employee may not have a right to receive a copy of their Personal Data if it is legally privileged, or if disclosing it would harm someone else's privacy rights. The Company will not be obligated to erase a Prospective Employee's Personal Data where the Company needs to retain the data to protect itself in the event of a legal claim or where other applicable laws require the retention of the data.
- To check that any information you have provided to the Company is accurate and up to date, to inform the Company of any changes, to learn what information the Company holds about you, or to otherwise exercise any of the above rights, please submit a written request to privacy@ur.com. You also have a right to lodge a complaint with the Supervisory Authority in your country if you feel that your Personal Data has been mishandled.

Privacy Notice Changes

- This Notice is effective as of March 25, 2021. The Company shall review this Notice and the particular security measures whenever there is a material change in business practices that may reasonably impact on the security or integrity of records containing Personal Data.