Recruitment privacy notice

1. Introduction

Keller values applicants for recruitment and respects and protects their privacy. This recruitment privacy notice sets out the basis on which we process the personal data which you provide to use in the course of your application for employment.

Please note that all entities within Keller may process their own copies of your personal data if they are involved in the recruitment.

This notice applies to applicants for recruitment, as well as any third parties whose information you provide to us in connection with your application (for example, referees or emergency contacts). This notice is not an offer of employment, nor does it put any contractual right on you, or place any contractual obligation on us.

2. Collection of personal data

We collect and use personal details which you provide as part of the recruitment process.
The personal data we collect is used primarily for recruitment and selection. The data may be stored in systems based around the world, and may be processed by third party service providers acting on our behalf.

3. Types of personal data

'Personal data' is a concept defined by data protection law, and refers to information which relates to an identified or identifiable individual.

The types of personal data which we process will vary depending on the role applied for, your location and the conditions attached to the role. Typically the types of personal data will include:

- **Your personal details** - for example your name, date of birth, gender, nationality, second nationality, personal contact details (e.g. home address, telephone number, e-mail), current role and salary;
- **Qualifications** - qualifications, professional memberships or charterships, languages spoken, competencies and skills (ability to drive, first aid etc.)
- **Immigration and right to work data -** including national ID number, social security or national insurance number, visa or work permit;
- **Equality and diversity data** - where permitted under local law and provided voluntarily, data regarding race and ethnic origin (stored anonymously for equal opportunities monitoring purposes;
- **Data about your application** - for example interview notes, assessment results;
- **Vetting and verification information -** including references, birth certificate, drivers licence, background checks (including of publically available information and public social media profiles); criminal record disclosure (where authorised by law).
- **Any other personal data** - which you choose to disclose to us during the application or interview

process, whether verbally or in written form, including in particular any other information which you disclose on a CV / résumé; and

- **Informal data -** including opinion data generated during the application or interview process.

4. Use of personal data

Whenever we process your personal data, we do so on the basis of there being a lawful 'condition' for processing.

In the majority of cases, the processing of your personal data will be justified on one of the following bases:

- it is necessary for us to comply with a legal obligation to which we are subject (for example, conducting immigration and right to work checks);
- it is in our legitimate interests as a business and our interests are not overridden by your interests, fundamental rights or freedoms (for example, grading candidates performance in interviews, carrying out background checks to verify your identity and qualifications / experience);
- subject to your consent (for example, our consideration of a voluntarily submitted CV);
- it is necessary to take steps at your request before entering into an employment contract with you (this applies at the post-offer stage, where we need to collect further information, or process information already collected, in order to enter into and then perform the contract of employment).

The processing of special categories of data will normally be justified by one of the following special conditions:

- it is necessary for the purposes of carrying out obligations under employment law (for example, processing of ethnicity data contained in immigration or right to work documents);
- it is necessary for reasons of substantial public interest authorised under local law (for example, carrying out equal opportunity monitoring exercises); or
- it is necessary for the establishment, exercise or defence of legal claims.

We will only process data revealing criminal convictions (ie in the context of vetting) where there is a legal authorisation to do so under either EU or local law.

Generally, the purposes for which we process your personal data are to assess your suitability for employment with us. If you do not provide some or all of this data it may affect our ability to process your application. In some cases, it may mean that we are unable to continue with your application as we do not have the personal data necessary for effective and efficient recruitment.

We may use your personal data in the evaluation and selection of applications including, for example, setting up and doing interviews and tests, evaluating and assessing as required, including the final recruitment, reviewing your eligibility to work, where authorised by law and required for your role, seeking criminal record disclosure, conducting an equal opportunities monitoring programme and other purposes relevant to the recruitment process.

5. Retention of personal data

Generally, we only keep applicants' personal data for as long as required to satisfy the purpose for which it was collected by us or provided by you.

In certain cases, legal or regulatory obligations require us to keep specific records for a set period of time, including following the end of the recruitment process.

In other cases, we deliberately keep records to resolve queries or disputes which we think may arise from time to time.

6. Sources of personal data

Primarily the personal data we process about you will have been provided by you during your application for employment by using one of our careers websites or by writing to us directly by post or email.

During the recruitment process, we may request references from third parties, for example, references from a previous employer, and we also carry out screening and vetting processes using third party sources.

7. Disclosures of personal data

We may share your personal data with other members of the Keller Group where required to, for example, take decisions about your recruitment. Within Keller, your personal data can be accessed, or may be disclosed internally on a need-to-know basis, by the hiring manager and any other relevant business colleagues responsible for managing or making decisions in connection with your potential employment.

We may use third party suppliers to help us provide recruitment services. These third parties may have access to, or merely host, your personal data, support and maintain the framework of our recruitment system, but will always do so under our instruction and be subject to a contractual relationship.

Your personal data may be shared with certain interconnecting systems (such as HR information, payroll and benefits systems) if your application for employment with us is successful. Data contained in such systems may be accessible by providers of those systems, their associated companies and sub-contractors.

We may be required to disclose your personal data to third parties:

- including tax authorities, IT administrators, lawyers, auditors, investors, consultants and other professional advisors;
- in response to orders or requests from court, regulators, government agencies, parties to a legal proceeding or public authorities; or
- to comply with regulatory requirements or as part of a dialogue with a regulator.

We expect third parties to process any data disclosed to them in accordance with applicable law, including with respect to data confidentiality and security.

8. Cross-border transfers

The global nature of our business means that your personal data may be disclosed to members of the Keller Group, or to third party suppliers or partners, located outside of the European Economic Area ('EEA').

In respect of internal transfers within the Keller Group, we have entered into an Intra-Group Data Transfer Agreement to ensure your data receives an adequate level of protection.

Where third parties transfer your personal data outside of the EEA, we will take steps to ensure that your personal data receives an adequate level of protection, including by, for example, entering into data transfer agreements or by ensuring that third parties are certified under appropriate data protection schemes.

You have a right to request a copy of any data transfer agreement under which your personal data is transferred, or to otherwise have access to the safeguards which we use. Any data transfer agreement made available to you may be redacted for reasons of commercial sensitivity.

9. Security of your personal data

We implement reasonable physical, technical and administrative security standards designed to protect your personal data from loss, misuse, alteration, destruction or damage and to ensure a level of security appropriate to the risk.

We take steps to limit access to your personal data to those staff who need to have access to it for one of the purposes listed in 'Uses of personal data'.

10. Rights in respect of your personal data

You have the following rights in respect of your personal data, where applicable to the processing we carry out:

- to get a copy of your personal data together with information about how and on what basis that personal data is processed;
- to rectify inaccurate personal data (including the right to have incomplete personal data completed);
- to erase your personal data in limited circumstances where it is no longer necessary in relation to the purposes for which it was collected or processed;
- to restrict processing of your personal data where:
  - the accuracy of the personal data is contested;
  - the processing is unlawful but you object to the erasure of the personal data;
  - we no longer require the personal data for the purposes for which it was collected, but it is required for the establishment, exercise or defense of a legal claim;
- to challenge processing which we have justified on the basis of a legitimate interest;
- to object to any decisions which are based solely on automated processing;
- to get a portable copy of your personal data, or to have a copy transferred to a third party controller; or
- to get a copy of or access to safeguards under which your personal data is transferred outside of the EEA.

In addition to the above, you have the right to lodge a complaint with the supervisory authority.

11. Contact information

If you have any questions about the way we use your personal data, or you wish to investigate exercising any rights in respect of your personal data, please contact your local HR team or for Germany, Robert Graf (datenschutzbeauftragter@kellerholding.com)

12. Document change history

Status:	Final
Issue date:	February 2018
Version last reviewed and updated:	October 2020
Next review date:	October 2021
Policy owner:	Company Secretariat