HOMERUN

Privacy whitepaper

This document describes the personal data processing by the Homerun software. It is intended for privacy and data protection professionals at Homerun customers and prospects. This document focuses on personal data as defined in the EU General Data Protection Regulation:

> Personal data means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Overview

Homerun offers recruitment software in the form of Software as a Service (SaaS) that enables you to create a career site and personalised job openings, for which candidates can apply. The software allows your recruiters to manage the recruitment process from start to finish, including communications with candidates and appointment scheduling.

Collection of Personal Data: Customer Control and Responsibility

The personal data processed by the software typically belong to one of two categories of data subjects:

- Candidates: Persons who apply for employment with your company, or persons your company would like to consider or approach for employment.
- Users: Persons who have a user account in the software, typically your employees or consultants, in their capacity as members of a hire team for a certain job.

For Candidates, the personal data can consist of: general identification, the job he/she wants to apply for, education, work experience, photo, personal interests, links to social media accounts or profiles, any other answers to questions you have defined during the application process, appointments or events relating to the recruitment process, comments or assessments by the hire team about the candidate's suitability for the role, communication between the hire team and the candidate, and status of the application. This is highly configurable.

For Users, the personal data typically consists of: general identification, authentication and authorisation data, configuration of the user profile, comments or assessments about candidates' suitability for a certain role, as well as communication between the user (member of one or more hire teams) and candidates or other users.

It is your responsibility as a customer to correctly configure the software through the customer portal in terms of what information you want to collect. It is also your exclusive responsibility to ensure that this customisation is lawful with regards to the relevant legislation. We recommend that you only collect personal data that is absolutely required in order to support the recruitment process.

Purposes and Activities of Personal Data Processing

Personal data is processed solely for the purpose of providing, managing and further developing the software on your behalf, and for supporting you in the use of the software. This is a detailed list of data processing activities:

- Providing the services as agreed under the User Agreement

Legal Framework

All personal data is processed by Homerun BV, based at Singel 542, 1017 AZ Amsterdam, the Netherlands. We are subject to Dutch data protection law, which is based on the EU Data Protection Directive 95/46/EC. On 25 May 2018 this Directive and all EU countries' data protection laws will be replaced with the EU General Data Protection Regulation (GDPR), which sets even stricter requirements for data protection. We have studied the new Regulation and are in the process of updating our practices where necessary to comply with the new requirements before the implementation deadline.

Controller-Processor and Data Processing Agreement

In the sense of the EU Data Protection Directive 95/46/EC and the future EU General Data Protection Regulation, Homerun will act as a processor of personal data on behalf of you, the controller. Together we ensure that your users' personal data is protected. To define our mutual rights and obligations, you must enter into a Data Processing Agreement (DPA) with us.

Homerun has developed a standard DPA. It accurately describes the privacy and data protection characteristics of the software, including the confidentiality requirements, the use of sub-processors, data breach notification details, the right to audit, transfer of personal data, data subject requests, law enforcement requests, indemnity, and data retention, return and destruction. It also includes a description of the roles and responsibilities, contact details for security and privacy communication, the categories of personal data processed, categories of data subjects, the purposes of personal data processing and the technical and organisational security measures taken by Homerun.

Since our service offering is standardised for all customers, we require our customers to make use of our standard agreement, to ensure that all relevant matters have been accurately described. Considering the very competitive pricing of our product as well as the large number of customers we are supporting, we unfortunately do not have the means to evaluate alternative Data Processing Agreements proposed by our customers. Our own DPA has been carefully drafted by an expert and fully complies with the GDPR.

Data Retention

As the controller, you are responsible for deciding how long you want to keep the personal data. For inspiration, you may want to have a look at section 5.3 of the Recruitment Code of the Dutch Association for Personnel Management and Organizational Development (NVP) which can be found at https://nvp-plaza.nl/sollicitatiecode. You can enforce your retention policy by regularly deleting data through the customer portal using date filters and our automated retention period features this process further in future versions of the software.

Delivery and Responsibilities

The software is delivered as a standardised platform in the form of Software as a Service (SaaS). The following table provides an overview of the responsibilities of both parties involved:

Customer	Homerun
Configure the software to your needs Manage job applications Interact with candidates Manage users	Decide on the features of the software Decide on technical implementation (code, systems) Develop and maintain the software Host the software Provide support

Sub-Processors

As a processor to you, the controller, we also make use of two sub-processors in order to provide the software: Amazon Web Services and SendGrid.

All Homerun systems are hosted by Amazon Web Services, Inc (AWS), a company located at 410 Terry Avenue North, Seattle, WA 98109-5210, USA. Homerun has entered into a Data Processing Agreement with AWS. Amazon AWS complies with the EU Data Privacy Directive and with the GDPR. The data itself is stored in the AWS datacenter in Ireland, within the European Union, so no specific legal mechanism is required for this transfer.

Emails to users and candidates are sent through SendGrid, Inc., a company located at 1801 California Street, Suite 500, Denver, CO 80202, USA. Homerun has entered into a Data Processing Agreement with Sendgrid, which complies with the EU-U.S. Privacy Shield and therefore provides an adequate level of protection for personal data.

Although unlikely, Homerun may choose to employ other sub-processors to process personal data. We will ensure that all sub-processors provide an adequate level of protection and that all legal requirements for such a relationship are met, by entering into a Data Processing Agreement and, where applicable, verifying registration with the EU-U.S. Privacy Shield or any other approved transfer mechanism. If we choose to employ another sub-processor, we will inform you, after which you will have 30 days to object to the use of this new sub-processor.

Privacy by Design and Privacy by Default

Homerun endeavours to develop its services using the Privacy by Design and Privacy by Default philosophies. This means we consider privacy and personal data protection throughout all parts of our product development lifecycle. Our services are designed to limit personal data collection by default, requiring you as a customer to explicitly enable features that collect more information. Our default settings reflect this philosophy, and our development team is committed to continuously implement the principles of the General Data Protection Regulation (GDPR) in their efforts to advance our software even further.

Data Protection

Homerun takes adequate technical and organisational measures to protect personal data against loss or unlawful processing. For more information about Homerun's security, see our Information Security Policy.

Location

All personal data is stored and processed in AWS Region EU (Ireland), meaning in the European Union. In the future, we may operate the systems out of different locations within the European Union.

Access to Data

Through our customer portal, you have access to the personal data collected on your behalf. Authorised staff of Homerun also have access to your data for support, development and debugging purposes, on a strict need-to-know basis. All Homerun staff are bound to confidentiality using a non-disclosure agreement that is part of their employment contract. We also have an internal code of conduct for dealing with customer data that is widely communicated throughout the company, and data privacy and confidentiality are key topics in our security and privacy awareness programme.

Termination and Portability

Upon termination of the contract, Homerun will, on your written request, return all collected (personal) data in CSV or JSON format to you and/or remove it from our systems.

Breach Notification

In the event that we become aware of a personal data breach, we will inform affected Homerun customers without undue delay, so that you can fulfil your data breach notification requirements. For this purpose, please ensure to provide us with accurate contact information. Since as a processor, Homerun is not required by Dutch law to report relevant data breaches to the Dutch Data Protection Authority (Autoriteit Persoonsgegevens) or to affected data subjects, we will not report any breaches to authorities without your prior, explicit authorisation and instruction. Homerun has internal policies and procedures to ensure that employees recognise and report possible data leaks to management. These policies and procedures are highlighted during security and privacy awareness trainings.

Subject Data Access

Since Homerun acts as a processor on your behalf, and therefore cannot interact directly with your data subjects, we will redirect all user requests regarding personal data (e.g. access, viewing, updating, removing) to you. If you require our help retrieving, updating or removing data in the context of subject data access, we will provide support.

Law Enforcement Requests

Homerun will cooperate with all legal requests from competent authorities, provided that cooperation is mandatory. Where legally allowed, we will inform you without undue delay of such requests if you are the controller of the requested data.

Cooperation with Data Protection Authorities

Homerun will cooperate with all legal requests from competent Data Protection Authorities, provided that cooperation is mandatory.

Privacy Statement

The privacy statement at https://www.homerun.co/privacy-statement governs the use of the public Homerun website. It does not address the privacy aspects of the Homerun software.

For the usage of this product, Homerun also collects personal data as a controller, mostly in order to maintain the relationship between you and us. This processing is governed by the privacy statement at https://www.homerun.co/portal-privacy-statement.

Note: If you use Homerun's software, it is your responsibility as a data controller to inform the data subjects (users and candidates), for example through your own privacy statement. Homerun is not in a position to advise you on what this privacy statement should contain, as that is your responsibility as data controller.

Should you have any further questions about the privacy aspects of our services, please email privacy@homerun.co.