

DATA MANAGEMENT NOTICE REGARDING THE USAGE OF THE [WWW.RECRUIT.HU](http://www.recruit.hu) WEBSITE AND MANPOWER AGENCY SERVICES

2018. 04. 16.

The provider of the www.recruit.hu webpage (hereafter referred to as **Website**), which is **Recruit Személyzeti és Tanácsadó Llc.** (company reg. no. 01-09-962866; seat: 1055 Budapest, Falk Miksa utca 28.; hereinafter as: **Service Provider**) informs the users of the data management regarding the engagement of the Website and the manpower agency services of Service Provider as follows, in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council, the General Data Protection Regulation (hereafter referred to as **GDPR**).

1. Terms

Service Provider	Recruit Személyzeti és Tanácsadó Llc. (company reg. no.. 01-09-962866; seat: 1055 Budapest, Falk Miksa utca 28.), the provider of the Webpage and the manpower agency services.
Webpage	The entirety of the content and the services that are available via the www.recruit.hu web address.
Manpower agency services	The entirety of services undertaken by Service Provider, which aim to assist the creation of a connection between job seekers and potential employers for the purposes of concluding and employment agreement, including the conveying of Hungarian job seekers abroad, and the conveying of foreign applicants to Hungary, including but not limited to the displaying of offerings of employers who have registered with Service Provider on their Website, the seeking out of job applicants therefore, to the collection of their CV's be it via the database of Service Provider or by recruiting, to the evaluation of applicants, the pre-selection of applicants, the selection of applicants, the introduction of applicants to the Employer and the verification of references.
Employer	The employer in contract with the Service Provider, who seeks job applicants for an open position, in order for which they engage the services of the Service Provider.
Job offer	A job offering displayed on the Website of the Service Provider, the contents of which are determined by the Employer, with which they seek applicants to the advertised position.
Applicant	Natural persons applying to one of the Job offers displayed on the Website.
Visitor	Natural persons who do not apply for Job offers, but are merely browsing the Website.

User Joint denomination of Applicant and Visitor

Website GTC The General terms and conditions of the Website, which are made available on the Website, and which regulate in detail how the Users may use the Webpage and the services available there, such as the Manpower agency services..

2. What is the purpose of the present notice?

The website's terms of use are governed by the Website GTC, which shall apply to all questions not addressed herein. By using the Website and the services, Service Provider and the user enter into an agreement per the provisions of the Website GTC. The present notice serves to provide adequate information to the Users on the management of personal information by Service Provider, relating to the Website and the Manpower agency services, as is required by applicable law.

Regarding the data processing taking place on the Website and the Manpower agency services, Service provider shall be viewed as a data controller. They shall also be deemed as data controller regarding the Applicants' personal data managed relating to the Manpower agency services and those forwarded to Employers, as do all contracted Employers to whom Applicants' personal data and CV's are forwarded . Service Provider and Employers are separate data controllers of their own; all of which conduct their data processing activities per their own data management notices.

Employers, as independent data controllers, and as independent addressees of the Service Provider's data forwarding are compelled to conduct their own data processing in compliance with the applicable legislation, and shall inform the Applicants of this in their own data management notices. Service Provider holds no liability for the occurrence, validity and legality of these, Service Provider shall only be liable for the legality of their own data processing conduct.

Employers are liable for the contents, legality, validity and availability of the Job offers published by Service Provider per their request, Service Provider shall hold no liability for these.

3. What is the purpose of the Website?

On the Website, the Users may browse the Job offers of the Employers, as displayed by Service Provider without registration, they may search among these by various criteria, and may apply for them by filling out the provided application form with their data and by sending their CV to Service Provider, or by sending their CV to the Service Provider by email.

The service on the Website, and the Manpower agency services may only be engaged by persons over the age of 18. The Manpower agency services may only be engaged by the Users for themselves, in case of a User sending another person's CV, or applying for a Job offer on another persons behalf, they guarantee that they are in possession of proper authorization from that person, regarding the processing and forwarding of their data.

Users are liable for the data and the contents uploaded by them, for which Service Provider excludes liability.

4. How does the present notice apply to the Users?

By entering the Website, by utilising the services thereon, and by using any of the Website functions, they automatically acknowledge the contents of the present notice without any separate statements.

5. How and by whom may this notice be amended, and how and where is it published by Service Provider?

Service provider may unilaterally amend this notice at any time, publishing it in a joint, amended version on the Website, under a separate menu item. We request that all Users carefully read the present notice on every Website visit.

The present notice is continuously available on the Website. The Users may open, view, print, save the notice, but may not amend them, only Service Provide may do so.

6. What personal data do we manage, for how long, for what purposes and by what authorization?

The legal bases for our data processing are the following:

- a) GDPR Article 6 (1) a) where the processing is based on the informed consent of the data subject (hereafter referred to as **Consent**)
- b) GDPR Article 6 (1) b), on where processing is necessary for the performance of a contract to which the data subject is party (hereafter referred to as **Conclusion of Contract**)
- c) GDPR Article 6 (1) c) where data processing is necessary for the fulfilment of or compliance with a legal obligation of the data controller (e.g. obligations with tax statues – hereafter referred to as **Compliance**)
- d) GDPR Article 6 (1) f) where data processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, (hereafter referred to as **Lawful interest**)
- e) the data processing authorization afforded by Article 13/A of Act CVIII of 2001 on Electronic Commerce and on Information Society Services, where data controllers are authorized to process the natural identification data and home address of the recipients without the need for consent, as required for contracts for information society services, for defining their contents, for subsequent amendments and for monitoring performance of these

contracts, for invoicing the relevant fees, and for enforcing the claims arising out of or in connection with such contracts., moreover, where data controllers are authorized to process natural identification data and home address for the purposes of invoicing for the fees payable under the contracts for the provision of information society services to the extent related to the use of information society services, and information relating to the date, the duration and the place of using the service. (hereafter referred to as **E-Commerce**)

6.1. Data processing within the Manpower agency service

6.1.1. The present data management notice applies to all of the following Manpower agency service instances:

- a) if the Applicant applies for a Job offer on the Website via filling out the form and by sending in their CV
- b) if the Applicant applies via an email sent to the address specified on the Website, by sending in their CV
- c) if the Service Provider approaches an Applicant within Service Provider's own database with a specific Job offer
- d) if the Applicant is approached by Service Provider through another manpower agent's database or via social media with a specific Job offer
- e) if the Applicant is represented in Service provider's database not for the purposes of applying for a specific Job offer, but for future offers (Database storage)

6.1.2. The Service Provider gains the Applicant's data from several sources:

- a) The Applicant provides their data for a Job offer on the Website via filling out the form and by sending in their CV, in which case the data comes from the Applicant
- b) Service Provider lawfully gains the Applicant's data from other agencies' or portals' databases pursuant to agreements made with the following: CVOnline.hu (Russmedia Digital Llc.), Profession.hu (Profession.hu Llc.) and Jobline.hu (HVG Kiadó Ltd.).
- c) Service Provider gains the CV data of the Applicant from social media, such as the Applicant's LinkedIn profile and Facebook profile
- d) Service Provider collects certain instances of Applicant data themselves from prior employers, such as reference data
- e) Personal data accumulated during the recruiting process, interviews, tests and tasks conducted by Service Provider, which are also governed by the Service Provider, where Service Provider is the data source.

6.1.3. Governed data types, sources, purpose of data processing, legal basis, timeframe

The above source categories, which differ from the data subjects, are nominated below separately, per data categories, in order for the subject to be able to know where instances of their data are sourced from. The table below also holds the purposes and legal bases per data types.

Subject category	Data category (* = mandatory data category)	Data source	Purpose of data processing	Legal basis of data processing	Timeframe of data storage, deletion time
Applicant applying for Job offer of contracted Employer	name*	Applicant Other agencies' databases (CV Online, Profession.hu and Jobline.hu)	Manpower agency services (sending of Job offers, recommendation of Applicant to Employer) Profiling Contact keeping Identification	GDPR Article 6 (1) a – data subject's consent to the processing of their data	If only having consented to data processing related to a specific Job offer: 1 year If having consented to database storage as well: 3 years
	address	Applicant Other agencies' databases (CV Online, Profession.hu and Jobline.hu)	Manpower agency services (sending of Job offers, recommendation of Applicant to Employer) Profiling Contact keeping Identification	GDPR Article 6 (1) a – data subject's consent to the processing of their data	If only having consented to data processing related to a specific Job offer: 1 year If having consented to database storage as well: 3 years
	date and place of birth*	Applicant Other agencies' databases (CV Online, Profession.hu and Jobline.hu)	Manpower agency services (sending of Job offers, recommendation of Applicant to Employer) Profiling Contact keeping Identification	GDPR Article 6 (1) a – data subject's consent to the processing of their data	If only having consented to data processing related to a specific Job offer: 1 year If having consented to database storage as well: 3 years
	telephone number	Applicant Other agencies' databases (CV Online, Profession.hu and Jobline.hu)	Manpower agency services (sending of Job offers, recommendation of Applicant to Employer) Contact keeping	GDPR Article 6 (1) a – data subject's consent to the processing of their data	If only having consented to data processing related to a specific Job offer: 1 year If having consented to database storage as well: 3 years
	e-mail address*	Applicant Other agencies' databases (CV Online,	Manpower agency services (sending of Job offers, recommendation of	GDPR Article 6 (1) a – data subject's consent to the processing of their data	If only having consented to data processing related to a specific Job offer: 1 year

		Profession.hu and Jobline.hu)	Contact keeping		If having consented to database storage as well: 3 years
	Skype username	Applicant Other agencies' databases (CV Online, Profession.hu and Jobline.hu)	Manpower agency services (sending of Job offers, recommendation of Contact keeping	GDPR Article 6 (1) a – data subject's consent to the processing of their data	If only having consented to data processing related to a specific Job offer: 1 year If having consented to database storage as well: 3 years
	nationality	Applicant Other agencies' databases (CV Online, Profession.hu and Jobline.hu)	Manpower agency services (sending of Job offers, recommendation of Applicant to Employer) Profiling Contact keeping Anonymised statistics Anonymised market research	GDPR Article 6 (1) a – data subject's consent to the processing of their data	If only having consented to data processing related to a specific Job offer: 1 year If having consented to database storage as well: 3 years
	gender	Applicant Other agencies' databases (CV Online, Profession.hu and Jobline.hu)	Manpower agency services (sending of Job offers, recommendation of Applicant to Employer) Profiling Contact keeping Anonymised statistics Anonymised market research	GDPR Article 6 (1) a – data subject's consent to the processing of their data	If only having consented to data processing related to a specific Job offer: 1 year If having consented to database storage as well: 3 years
	photo	Applicant Other agencies' databases (CV Online, Profession.hu and Jobline.hu)	Manpower agency services (sending of Job offers, recommendation of Applicant to Employer) Profiling Identification	GDPR Article 6 (1) a – data subject's consent to the processing of their data	If only having consented to data processing related to a specific Job offer: 1 year If having consented to database storage as well: 3 years

	current employment and occupation	Applicant Other agencies' databases (CV Online, Profession.hu and Jobline.hu)	Manpower agency services (sending of Job offers, recommendation of Applicant to Employer) Profiling	GDPR Article 6 (1) a – data subject's consent to the processing of their data	If only having consented to data processing related to a specific Job offer: 1 year If having consented to database storage as well: 3 years
	prior employment and occupation	Applicant Other agencies' databases (CV Online, Profession.hu and Jobline.hu)	Manpower agency services (sending of Job offers, recommendation of Applicant to Employer) Profiling	GDPR Article 6 (1) a – data subject's consent to the processing of their data	If only having consented to data processing related to a specific Job offer: 1 year If having consented to database storage as well: 3 years
	education, alma mater	Applicant Other agencies' databases (CV Online, Profession.hu and Jobline.hu)	Manpower agency services (sending of Job offers, recommendation of Applicant to Employer) Profiling Anonymised statistics Anonymised market research	GDPR Article 6 (1) a – data subject's consent to the processing of their data	If only having consented to data processing related to a specific Job offer: 1 year If having consented to database storage as well: 3 years
	language proficiency	Applicant Other agencies' databases (CV Online, Profession.hu and Jobline.hu)	Manpower agency services (sending of Job offers, recommendation of Applicant to Employer) Profiling Anonymised statistics Anonymised market research	GDPR Article 6 (1) a – data subject's consent to the processing of their data	If only having consented to data processing related to a specific Job offer: 1 year If having consented to database storage as well: 3 years
	driver's license and type thereof	Applicant Other agencies' databases (CV Online, Profession.hu and Jobline.hu)	Manpower agency services (sending of Job offers, recommendation of Applicant to Employer) Profiling	GDPR Article 6 (1) a – data subject's consent to the processing of their data	If only having consented to data processing related to a specific Job offer: 1 year If having consented to database storage as well: 3

					years
	publications	Applicant Other agencies' databases (CV Online, Profession.hu and Jobline.hu)	Manpower agency services (sending of Job offers, recommendation of Applicant to Employer) Profiling	GDPR Article 6 (1) a – data subject's consent to the processing of their data	If only having consented to data processing related to a specific Job offer: 1 year If having consented to database storage as well: 3 years
	presentations	Applicant Other agencies' databases (CV Online, Profession.hu and Jobline.hu)	Manpower agency services (sending of Job offers, recommendation of Applicant to Employer) Profiling	GDPR Article 6 (1) a – data subject's consent to the processing of their data	If only having consented to data processing related to a specific Job offer: 1 year If having consented to database storage as well: 3 years
	projects	Applicant Other agencies' databases (CV Online, Profession.hu and Jobline.hu)	Manpower agency services (sending of Job offers, recommendation of Applicant to Employer) Profiling	GDPR Article 6 (1) a – data subject's consent to the processing of their data	If only having consented to data processing related to a specific Job offer: 1 year If having consented to database storage as well: 3 years
	trainings	Applicant Other agencies' databases (CV Online, Profession.hu and Jobline.hu)	Manpower agency services (sending of Job offers, recommendation of Applicant to Employer) Profiling	GDPR Article 6 (1) a – data subject's consent to the processing of their data	If only having consented to data processing related to a specific Job offer: 1 year If having consented to database storage as well: 3 years
	awards and merits	Applicant Other agencies' databases (CV Online, Profession.hu and Jobline.hu)	Manpower agency services (sending of Job offers, recommendation of Applicant to Employer) Profiling	GDPR Article 6 (1) a – data subject's consent to the processing of their data	If only having consented to data processing related to a specific Job offer: 1 year If having consented to database storage as well: 3 years
	memberships	Applicant Other agencies'	Manpower agency services (sending of Job offers,	GDPR Article 6 (1) a – data subject's consent to the	If only having consented to data processing related to a

		databases (CV Online, Profession.hu and Jobline.hu)	recommendation of Applicant to Employer) Profiling	processing of their data	specific Job offer: 1 year If having consented to database storage as well: 3 years
	references	Applicant Other agencies' databases (CV Online, Profession.hu and Jobline.hu) Recruit Llc.'s own research	Manpower agency services (sending of Job offers, recommendation of Applicant to Employer) Profiling	GDPR Article 6 (1) a – data subject's consent to the processing of their data	If only having consented to data processing related to a specific Job offer: 1 year If having consented to database storage as well: 3 years
	certificates	Applicant Other agencies' databases (CV Online, Profession.hu and Jobline.hu)	Manpower agency services (sending of Job offers, recommendation of Applicant to Employer) Profiling Anonymised statistics Anonymised market research	GDPR Article 6 (1) a – data subject's consent to the processing of their data	If only having consented to data processing related to a specific Job offer: 1 year If having consented to database storage as well: 3 years
	hobbies	Applicant Other agencies' databases (CV Online, Profession.hu and Jobline.hu)	Manpower agency services (sending of Job offers, recommendation of Applicant to Employer) Profiling	GDPR Article 6 (1) a – data subject's consent to the processing of their data	If only having consented to data processing related to a specific Job offer: 1 year If having consented to database storage as well: 3 years
	public social media information of the Applicant	Recruit Llc.'s own research	Manpower agency services (sending of Job offers, recommendation of Applicant to Employer) Profiling	GDPR Article 6 (1) a – data subject's consent to the processing of their data	If only having consented to data processing related to a specific Job offer: 1 year If having consented to database storage as well: 3 years
	analyses	Recruit Llc.'s own research	Manpower agency services (sending of Job offers,	GDPR Article 6 (1) a – data subject's consent to the	If only having consented to data processing related to a

			recommendation of Applicant to Employer) Profiling	processing of their data	specific Job offer: 1 year If having consented to database storage as well: 3 years
	personal and behavioural attributes relevant for aptitude, observed during interviews	Recruit Llc.'s own research	Manpower agency services (sending of Job offers, recommendation of Applicant to Employer) Profiling	GDPR Article 6 (1) a – data subject's consent to the processing of their data	If only having consented to data processing related to a specific Job offer: 1 year If having consented to database storage as well: 3 years
	result of professional tests	Given by data subject	Manpower agency services (sending of Job offers, recommendation of Applicant to Employer) Profiling	GDPR Article 6 (1) a – data subject's consent to the processing of their data	If only having consented to data processing related to a specific Job offer: 1 year If having consented to database storage as well: 3 years

6.1.4. What data are mandatory to provide, and what happens if the Applicant refuses to provide them?

When applying for a Job offer, the Applicant must provide their name, date of birth and e-mail address for the purposes of identification and keeping contact. When applying via the Website application form, if this data is not provided, the application and the CV cannot be submitted, the form will not allow submission. When applying by other means, e.g. via email, the application may be submitted without said data, but Service Provider will not be able to accept the application, nor to forward it to the respective Employer, or if the forwarding does take place, Service Provider cannot guarantee with the data missing, that they will contact the Applicant. In cases of missing data, Service Provider is not obligated to seek out the Applicant to request the missing data. When applying and sending the CV, the Applicant recognises having been informed, and accepts these circumstances.

6.1.5. How do we use the public data available on social media?

Service Provider may view the profile, activity, posts, and comments of the Applicant on social media such as Facebook and LinkedIn, in order to ascertain aptitude for an offer. Service Provider only views publicly available information, and does not seek out information in closed groups or materials of

restricted access. Service Provider does not save or store the social media profile of the Applicant, but may make notes of their observations thereof, which may be stored on paper and electronically.

Service Provider does not store sensitive data about the Applicant, nor do they do so regarding the social media profiles. Service Provider only views material data on social media that are relevant to the fulfilling of a Job offer regarding the Applicants.

6.1.6. Why do we profile Applicants, and what effect does this bear on them?

The data given by the Applicant, the data in their CV, and the data collected by Service Provider, e.g. notes made on the public information on social media such as Facebook and LinkedIn, the notes made regarding their personal and behavioural attributes, the results of the professional tests are linked by the Service Provider, and attributed to the given Applicant. The resulting data compilation is used by Service Provider for the following purposes:

- a) personalised sending of Job offers to the Applicant
- b) recommendation of the Applicant to contracted Employers
- c) making of anonymised statistics both for own use and for clients
- d) ordering, categorising of Applicants in Service Provider's electronic database

For these profiling activities, Service Provider does not use any automated means, which would rate or classify the data of the Applicants without human interaction, and does not make decisions based on automated means by the analysis of the Applicant's data, nor by predictions made of the data. Thus, this profiling does not require separate and express consent from the Applicants.

6.1.7. Processing of the results of professional tests and aptitude tests

In cases of certain Job offers where the given contracted Employer requests this, Service Provider conducts professional tests or aptitude tests with the Applicants. Service Provider notifies the Applicants of the results thereof. Service Provider informs the Applicants on what skill or aptitude is being tested per the instructions of the Employer, on what means are used to measure results, and on whether this is done pursuant to any legislation, and if its, then by what law.

The results and the documentation of the professional and the aptitude tests are only available to the professionals conducting the tests and the Applicants themselves, Service Provider does not forward these to the Employers, Employers only get the information from the Service Provider that the given Applicant is eligible for the given offer, or is not.

6.1.8. Notification of the Applicant on the success of their application

The Applicant receives notices on the success of their application from the Employer, Service Provider is not liable for the provision or the absence of the notice.

6.1.9. Consent and revocation

Applicants give their voluntary consent to the processing of their above data for the above purposes by actively submitting their application for the Job offer, either via the Website submission form or by email. Applicants may freely revoke their given consent at any time via an email sent to info@recruit.hu, where their name, date of birth and email address are mandatory to provide, so the Service Provider can know what Applicant's data must be deleted.

Upon revocation, Service Provider deletes all of the data they govern on the given Applicant, encompassing the data provided by the data subject, those collected by Service Provider and those stemming from other sources as well. This obligation to delete covers data stored both on paper and in electronic form, and extends to the notes and deductions made by Service Provider.

6.1.10. Timeframe of data processing, data processing for the purposes of projects and databases

If an Applicant applies for a specific Job offer, Service Provider processes their data for the time of the recruitment process regarding the given Job offer, and deletes all data with the conclusion of the recruitment process. Should the recruitment process go on for an extended period of time, and extends over a year's time, Service Provider shall process Applicant data for a year, after which they shall inquire whether the Applicant wishes to extend their consent for the entire recruitment process, extending over a year. If the Applicant does not reply to said inquiry within 30 days, or if the Applicant does not wish this extension to be made, Service Provider shall then delete the data of the Applicant.

Service Provider may forward the Applicant's data and CV to other Employers, and may process this data in their own data base for the purposes of sending future Job offers only if the Applicant has expressly consented thereto. Service Provider requests the separate consent of the Applicant thereto. If the Applicant consents thereto, then Service Provider shall be entitled to process their data within their own database for a period of 3 years. The reason behind the 3 year interval is that Service Provider has to ensure validity and actuality of the collected data, which may not be guaranteed after 3 years having passed, as these data would expire and become obsolete. Before the 3 years' time expiring, Service Provider may seek out the Applicants in order to request consent for another 3 years, and to recommend that the Applicants review and actualise their data. If the Applicant does not reply to said inquiry within 30 days, or if the Applicant does not wish this extension to be made, Service Provider shall then delete the data of the Applicant.

6.1.11. Data processing regarding anonymous Job offers

Per the request of Employers, Service Provider may also publish Job offers, in which Employers do not reveal their identity, thus, Applicants shall not know, what Employer’s position they apply for (anonymous Job offer).

In cases of such anonymous Job offers, in order to protect the rights and lawful interests of the Applicants, Service Provider conducts themselves in such a way that when having sent in their application, Applicant is informed of the identity of the Employer after having passed pre-selection and having been sought out by Service Provider, before the Applicant’s data is forwarded to the Employer – in order for the Applicant to be able to decide whether they wish their data to be forwarded or not. If the Applicant expressly objects to their data being forwarded after Service Provider having revealed the identity of the Employer, the Service Provider shall not forward their data then. If the Applicant does not declare their intent within 15 days’ time, Service Provider shall deem Applicant as not having objected to the forwarding, and forwards their data to the Employer.

In order for the trade secrets of Employers’ to be protected, Applicants must keep confidential the identity of the Employer, they may not reveal this without prior consent of the Employer, and may not publish this neither directly nor indirectly.

6.2.Processing the data of persons contacting customer services

Data subject category	Data category	Data source	Purpose of data processing	Legal basis of data processing	Timeframe of data processing, deletion time
Person contacting customer services	Name	Given by data subject	User identification Communication with User during customer service and complaint handling Complaint addressing Exercising of rights and claims	GDPR Article 6 (1) f) on Lawful interest	5 years
	Telephone no.	Given by data subject	User identification Communication with User during customer service and complaint handling Complaint addressing Exercising of rights and claims	GDPR Article 6 (1) f) on Lawful interest	5 years
	E-mail	Given by data	User identification	GDPR Article 6 (1) f) on Lawful	5 years

	address	subject	Communication with User during customer service and complaint handling Complaint addressing Exercising of rights and claims	interest	
	Inquiry or complaint filed	Given by data subject	User identification Communication with User during customer service and complaint handling Complaint addressing Exercising of rights and claims	GDPR Article 6 (1) f) on Lawful interest	5 years

In case of persons contacting customer services, for the purposes of identification and complaint management, name, in case of e-mail contact, e-mail address, and in case of telephone inquiries, the telephone number is mandatory to provide, in absence of which Service Provider cannot accept and handle any complaints, and may not address the issue brought before them. The providing of personal data relating to identification, complaint management and exercising of rights and claims is small-scale and is the joint interest of Applicant and the Service Provider, which does not infringe upon their rights and lawful interests.

The processing and storage time of the customer service data necessary for the exercising of rights and claims is in accordance with the general expiry time in civil law, that is 5 years.

6.3.Regarding the sending of newsletters

Subject category	Data category	Data source	Purpose of data processing	Legal basis of data processing	Timeframe of data processing, deletion time
Addressees of direct marketing messages	name	Given subject	Sending of newsletters and electronic direct marketing messages	GDPR Article 6 (1) a) – data subject’s consent to the processing of their data	Revocation of consent
	e-mail address	Given subject	Sending of newsletters and electronic direct marketing messages	GDPR Article 6 (1) a) – data subject’s consent to the processing of their data	Revocation of consent

By newsletters we mean any and all electronic direct marketing messages sent to the provided e-mails in which we notify addressees of our new offers, developments and other, various news regarding Service Provider or the Employers.

Customer may unsubscribe from said media freely, at any point by sending an email to info@recruit.hu stating said intent, or by selecting the “unsubscribe” option within any newsletter. In such cases, upon receipt of the notification thereof, Simple immediately deletes the email address from their database and ensures that no further messages or other direct marketing media are sent to the Customer.

After having unsubscribed, Users may re-subscribe freely at any time. Subscription is not a pre-requisite of any of our services. The provision of an e-mail address and a name is mandatory, without which a subscription may not be made.

6.4. Regarding the contact personnel of contracted Employers

Service Provider manages the data of the contact personnel of the contracted Employers for the conclusion of their contracts and to keep contacts with them as per the following:

Data subject category	Data category	Data source	Purposes of data processing	Legal basis of data processing	Timeframe of data processing, deletion time
Contact personnel of contracted Employers	name	Contracted Employer	Conclusion of contract Contact keeping	GDPR Article 6 (1) f) on Lawful interest	8 years after contract termination
	telephone no.	Contracted Employer	Conclusion of contract Contact keeping	GDPR Article 6 (1) f) on Lawful interest	8 years after contract termination
	e-mail address	Contracted Employer	Conclusion of contract Contact keeping	GDPR Article 6 (1) f) on Lawful interest	8 years after contract termination
	position	Contracted Employer	Conclusion of contract Contact keeping	GDPR Article 6 (1) f) on Lawful interest	8 years after contract termination

It is the joint lawful interest of both Service Provider and Employer to be able to reach one another via their contact personnel. The data management is small-scale hereunder, and only holds material information for the purposes of contact keeping, the given telephone numbers and email addresses are usually company owned, and as such, the contact persons’ rights and lawful interests are not infringed upon.

6.5. Processing of data collected automatically via the Webpage

We use cookies and other various programs on the website in order to understand the Website Visitors preferences and behaviour relating to the Website, to develop the Webpage based on those, and to generate anonymous statistics on Website traffic. Certain small programs aid the Users in not having to input their data on repeat visits, and to make their identification easier and quicker, while other programs serve to identify the Users. We elaborate on this data collection below:

Data subject category	Data category	Data source	Purposes of data processing	Legal basis of data processing	Timeframe of data processing, deletion time
recruit.hu website Users	IP address, browser used, type of device and operating system, language settings, date of visit	Automatically collected by Recruit Llc.	Statistics Website development User identification and recognition	GDPR Article 6 (1) f) on Lawful interest	2 years from time of visit
	Website visit data (opened pages, time spent, clicks, openings)	Automatically collected by Recruit Llc.	Statistics Website development User identification and recognition	GDPR Article 6 (1) f) on Lawful interest	2 years from time of visit
	PHPSESSID code	Automatically collected by Recruit Llc.	Statistics Website development User identification and recognition	GDPR Article 6 (1) f) on Lawful interest	2 years from time of visit

The above data processing is the lawful business interest of the Service Provider, as it serves to develop the Website and to make it safer. The scope of collected data is insubstantial, these are merely used for anonymous statistics and analyses, it is not used to identify behaviours or preferences, and no automated decisions are made based thereon, no personalised offers are made by the Service Provider based thereon. Concordantly, the fundamental rights and freedoms of the Users are not affected adversely or disproportionately.

Upon visiting the Webpage and utilising the Services, Service Provider places cookies within User's browser and in HTML-based emails as per the regulations herein.

In general the cookie is a small file consisting of letters and numbers which is sent to the device of the User from the web server of the Service Provider. It enables for example the Service Provider to recognize the final appliance of the User when the connection is created between the web server of the Service Provider and the device. The main purpose of the cookie is to enable the Service Provider to make available individualized offers, publicity and advertisements for the User which may personalize the User's experience during the use of the Simple System and may reflect more to the personal needs of the User.

Purpose of cookies utilised by Service Provider:

- a) Security: aiding and ensuring safety, moreover enabling and aiding Service Provider to detect unlawful conduct.
- b) Preferences, attributes and services: cookies let Service Provider know, what language is preferred by the User, what are their communications preferences, aid the User in completing forms on the Website, making them easier to fill out.
- c) Performance, analytics and research: cookies aid the Service Provider in understanding how the Website performs in various areas. Service Provider may use cookies, which rate, improve and search the Website, the products, functions, services, including when User enters the Website from other websites, and the devices, such as User's computer or mobile device.

Types of cookies utilised by Service Provider:

- a) analytics, tracking cookies;
- b) session cookies, which only operate during the active session (usually the webpage visit itself);
- c) permanent cookies: which help in identifying the Customer as an existing user, making it easier for them to return without having to log in again. After the Customer logs in, the permanent cookie remains in their browser, with the webpage being able to read it.

Adobe Flash is another technology equal in function to cookies. Adobe Flash is able to store data on the User's device. Not every browser allows the removal of Adobe Flash cookies however. The Customer may restrict or block Adobe Flash cookies via the website of Adobe. If Customer restricts or blocks them, certain elements of the Website may become inaccessible.

Third party cookies:

Reputable partners aid Service Provider in analysing Webpage statistics, and analytics companies such as Google Analytics, Quantcast, Nielsen and ComScore may also place cookies on the Customer's device.

Users may disallow Google cookies on the page used for the disabling of Google ads.

On <http://www.networkadvertising.org/choices/> there are further means to deny other, third party cookies from being used.

Control of cookies:

Most cookies enable Customers to control cookie usage via their settings. However, if Customer restricts the usage of cookies, this may hinder user experience, since it will no longer be customised. Customer may also stop the saving of personal settings, such as the saving of login information.

If Customer does not wish for Service Provider to use cookies when User visits the webpage, they may refuse usage under their settings page. In order to let Service Provider know that the Customer has refused usage of cookies, a denial cookie is placed on the Customer's device, thus, Service Provider will know that no cookies may be placed on the device upon the next visit of the webpage. If the Customer does not wish to receive cookies, they may change their browser settings accordingly. If no such change has been made, Service Provider will view Customer as having given consent to the sending of any kinds of cookies. The Website shall not function completely without cookies.

For further information of cookies, including types, management and removal, visit Wikipedia.org or www.allaboutcookies.org or www.aboutcookies.org.

7. Who manages your personal data, and who has access to them?

7.1.The data controller

The controller of the personal data specified under point 6. hereto is Service Provider, meaning Recruit Llc., the company data of which are as follows:

Recruit Személyzeti és Tanácsadó Llc.

Seat: 1055 Budapest, Falk Miksa utca 28.
Mail address: 1055 Budapest, Falk Miksa utca 28.
Company reg.: 01-09-962866
Tax reg. no.: 23379743-2-41
Represented by: Vaslaki Tímea, CEO
Telephone: +36-20-402-8301
E-mail address: info@recruit.hu
Website: www.recruit.hu

On behalf of Service Provider, the data is accessible to the employees of Service Provider whose access is essential to the performance of their duties. Access authorizations are specified in a strict internal code.

7.2.Data processors

For the processing of the personal data of representative and contact persons, we engage the following companies, with whom we have entered into data processor agreements. The following data processors conduct the processing of personal data:

Name and address of data processor	Purposes of data processing	Data processed
HRSzoftver Llc. (2045 Törökbálint, Kossuth L. u. 40.; Cg. 13-09-190859; adószám: 14433070-2-13)	IT maintenance services under engagement of the Service Provider	Personal data under point 6 hereto.
Tibor Gulyán sole trader (2310 Szigetszentmiklós, Jegenye u. 9/b.; tax no.: 67477414-1-33)	IT administrator services under engagement of the Service Provider	Personal data under point 6 hereto.
Next Generation Solution Ltd. (2040 Budaörs, Ébner György köz 4.; Cg.: 01-09-922414; adószám: 14839225-2-41)	Website hosting and maintenance	Data collected automatically from the website, such as IP address, browser used, type of device and operating system, language settings, date of visit, website traffic data, viewed pages, time spent, clicks, openings, PHP session ID codes.

8. Who is the data protection officer of the Service Provider and what are their contact details?

Service Provider is not required to appoint a data protection officer.

9. To whom do we forward your personal data?

Regarding Applicant personal data, we forward the following data types to the following entities that we are in contract with:

Type of data forwarding addressee	Categories of forwarded personal data
Employees contracted with Service Provider	Applicant data under point 6.1. hereto

The purpose of the above data forwarding is to send the Applicant's CV and collected miscellaneous data to the Employers who have contracted with Service Provider for their Manpower agency services, so they may seek out the Applicant – should they deem them qualified – for a Job offer, and to

enter into an employment agreement with them. Employers qualify as individual data controllers, and shall conduct themselves per their own data management regulations and notices.

10. What rights do you have regarding the processing of your data, and how can you exercise them?

- a) **Right of access:** they may inquire as to what employee data is managed, for what purposes, for how long, to whom do we forward them, and where the data originates from.
- b) **Right of correction:** should their data change or be recorded wrong, they may request that this be rectified or corrected.
- c) **Right of deletion:** in instances specified by law, they may request that we delete their stored personal data.
- d) **Right of restriction:** in instances specified by law, they may request that data management be restricted regarding their personal data.
- e) **Right to objection:** in instances specified by law, they may object to their personal data being managed, in which case we do not manage their personal data any further.
- f) **Right to data portability:** the subject may request the porting of their personal data, in which case we hand over their stored data either to them, or directly to a data controller of their choosing, if such is technically safe.

We wish to note that data portability requests may only be issued regarding data managed per your consent, or regarding data that is managed automatically, and that we may only conclude data portability requests aimed towards other providers if such is possible from a technical and security viewpoint.

In cases of such requests, we conduct ourselves pursuant to applicable law, and will provide information on the rendered measures in one month.

- g) **Right to revoke consent:** in cases where personal data is managed by the consent of the subject, they have the right to revoke such consent at any time, which does not affect the legality of data management conducted prior to the revocation
- h) **Right of complaint:** should you have any complaints or grievances regarding our data management, you have the right to lodge a complaint by the supervisory authority:

National Authority for Data Protection and Freedom of Information

Website: <http://naih.hu>
Postal address: 1530 Budapest, Pf.: 5.
E-mail: ugyfelszolgalat@naih.hu
Telephone: +36 (1) 391-1400

Moreover, you may file a suit against Service Provider before the Municipal Court of Budapest if your personal data has been infringed upon.

11. How do we ensure the safety of your data?

Service Provider has enacted the following information security procedures for the purposes of data protection:

We follow a detailed information security code regarding the safety of the data and the information that is under our control, with which compliance is mandatory for all our personnel, and which is both known and utilised by our staff.

We regularly coach and train our employees regarding data and information security requirements.

11.1. Data security in IT infrastructure

We store personal data on a rented cloud, provided by HRSzoftver Kft., on a rented server in the server park located at 1132 Budapest, Victor Hugo u. 18-22., and on the hard drives of company computers, access to which is strictly controlled and only granted to a very restricted circle of personnel. We regularly test our IT systems in order to ensure and maintain data- and IT security.

Office workstations are password-protected, third-party storage devices are restricted and may only be used following approval.

Protection against malicious software is provided regarding all of the systems and system elements of the Service Provider.

During the planning and operation of programs, applications and tools, we address security functions separately and with emphasis.

When allocating authorisations to our IT systems, we pay close attention to the protection of data (e.g. passwords, authorisations) affecting these systems.

We generate backups daily, and store these for 7 days, these are incremental saves. The backups may only be accessed by a select circle.

11.2. Data security in communication

Regarding electronically forwarded messages and files, we secure the integrity of data on both the controller's and the user's data, in order to comply with the principle of

Our implemented security measures detect unauthorized modifications, embedding and repetitive broadcasting. We prevent data loss and damage by fault detecting and correcting procedures, and we ensure the prevention of deniability.

Regarding the network used for data transmission, we provide defense against illegal connection and eavesdropping per an adequate security level.

11.3. Data security in document management

We comply with data security requirements in document management as well, which we stipulate in document management by-laws. We manage documents by pre-set access and authorization levels, based on the level of confidentiality regarding the documents. We follow strict and detailed rules regarding the destruction of documents, their storage and handling at all times.

11.4. Physical data security

In order to provide physical data security, we ensure our physical barriers are properly closed and locked, and we keep strict access control regarding our visitors at all times.

Our paper documents containing persona data are stored in a closed locker that is fire- and theft-proof, to which only a select few have authorised access.

The rooms where storage devices are placed in have been made to provide adequate protection against unauthorised access and breaking and entering, as well as fire and environmental damage. Data transit, as well as the storage of backups and archives are done in these confined locations.

12. What procedure do we follow upon an incident?

Pursuant to applicable law, we report incidents to the supervisory authority within 72 hours of having gained knowledge thereof, and we also keep records of them. In cases regulated by applicable law, we also inform subjects of the incidents, where necessary.

13. When and how do we amend this notice?

Should the scope of data, or the circumstances of data management be subject to change, this notice shall be amended and published on www.recruit.hu within 30 days, as is required by GDPR. Please pay attention to the amendments of this notice, as they contain important information regarding the management of your personal data.