Processor Agreement
Adver-Online B.V.

Herenweg 55
2105 MC Heemstede The Netherlands
+31 (0)23 55 30 359

Processor Agreement

The undersigned:

1. **[Company name]** with its registered office and principal place of business in [Postcode] [Town] at [Address], duly represented in this matter by [Authorised Signatory], hereinafter referred to as "Data Controller"

   And

2. **Adver Online B.V.**, with its registered office and principal place of business in (2105 MC) Heemstede, at Herenweg 55, duly represented in this matter by H.O.M. van Rijnswoud, hereinafter referred to as "**Adver-Online**",

Whereas:

A. Adver-Online, in the context of an agreement concluded with the Data Controller (hereinafter: the "**Agreement**"), will gain access to (personal) data from the Data Controller and from other data subjects to whom the data relates (hereinafter: the "**Data**");
B. The parties want to conclude this Processor Agreement for this purpose (hereinafter: the "**Processor Agreement**").

Declare that they have agreed the following:

Article 1. General

1.1 In so far as the Data concerns personal data within the meaning of the Dutch Data Protection Act (hereinafter: the "**Wbp**") (hereinafter: "**Personal data**"), [Company name] is "Data Controller" and Adver-Online is "Data Processor" of this Personal data within the meaning of the Wbp, or Processing Data Controller and Processor within the meaning of the General Data Protection Regulation (AVG).

1.2 The Data Controller has exclusive control over the Data. Adver-Online does not have any autonomous control over the Data and will process the Data solely on behalf of and in accordance with the instructions of the Data Controller.

1.3 This Processor Agreement constitutes an annex to and is part of the Agreement.

Article 2. General obligations of Adver-Online

2.1 The Data will only be used by Adver-Online for performance of the Agreement.

2.2 Adver-Online will process the Data in a proper and careful manner, in accordance with objectives and means defined by the Data Controller and also in observance of what is provided for in the Agreement.

2.3 Adver-Online does not have any autonomous control over the Data and will process the Data solely on behalf of the Data Controller. Unless expressly agreed otherwise, Adver-Online will, therefore, not process the data for its own use, nor provide it to third parties.

2.4 If Adver-Online directly collates Personal Data from data subjects (within the meaning of the Personal Data Protection Act), it must ensure that no more Personal Data is processed than is necessary for the performance of the Agreement.

2.5 Adver-Online must in relation to the processing of the Data adhere to the instructions from the Data Controller and is not entitled to undertake any actions in relation to the Data to which no written authority to do so has been given by the Data Controller. If Adver-Online doubts whether a specific processing is in accordance with the Agreement, it must contact the Data Controller.

2.6 Adver-Online will never pass on to a third party the Data, or grant a third party access to the Data, without Adver-Online's having obtained the express written permission from the Data Controller.

2.7 Adver-Online will, during the performance of this Agreement, comply with the applicable legislation and regulations with regard to the protection of personal data, including but not limited to the Personal Data Protection Act, the General Data Protection Regulation, the Telecommunications Act and all other applicable (European) (privacy) regulations, including but not limited to the codes of conduct of the DDMA and the FEDMA.

2.8 Appendix (1) enclosed with this Processor Agreement stipulates which Personal Data (Data) Adver-Online processes in its role as Processor. It concerns here in all cases applicants (candidate data) from the Data Controller as being the subject of the processing.

Article 3. Third Parties

3.1 Adver-Online is entitled to call in a third party in the execution of its activities. Adver-Online guarantees that for the third party concerned the same terms and conditions apply as described in this Processor Agreement. By signing this Processor Agreement, the Data Controller grants Adver-Online permission to engage sub-processors.

3.2 Irrespective of what is provided for in the previous paragraph, Adver-Online remains responsible at all times towards the Data Controller and liable for compliance with the provisions contained in this Processor Agreement.

3.3 Without permission from the Data Controller Adver-Online will not pass on or process personal data outside the European Economic Area.

3.4 If Adver-Online processes personal data outside the European Economic Area, it will take supplementary measures, if required. These measures are set out in the agreement drafted by the European Commission, directorate C (2010)593 article 26(2) clause 95/46/EC for the purpose of the transfer of Personal Data to Processors in third countries, or the subsequent transferee. If applicable, these measures are available for inspection.

Article 4. Security and duty to report Data breaches

4.1 Adver-Online will ensure all appropriate technical and organisational measures to secure the Data against loss or any form of unlawful processing. The measures currently adopted by Adver-Online in that regard are set out in full in Appendix (2). The Data Controller agrees with the aforementioned measures. Unless agreed otherwise, Adver-Online is not obliged to take supplementary measures.

4.2 Adver-Online will inform the Data Controller at the latter's request of the exact measures taken by Adver-Online as referred to above.

4.3 If Adver-Online knows, or could reasonably presume, that unauthorised access has been obtained to the Data, it will immediately notify the Data Controller thereof. In that case, Adver-Online will endeavour to do its utmost, in close consultation with the Data Controller, to take appropriate measures to minimise as much as possible any damage and consequences of the data breach

concerned. Any communication about the data breach can only take place after consultation with and express permission of the Data Controller.

4.4 The Processor will immediately - but no later than within 36 hours after discovery inform the Data Controller in writing of any (possible) Data breach such as within the organisation of the Processor or Sub-processor or concerning the resources under management of the Processor or Sub-processor. This notification must be given to the Data Protection Officer of the Data Controller, whose contact details are contained in Appendix (3).

4.5 The Processor ensures an internal policy is in place in the event of a security incident so that an adequate response can be provided.

4.6 If there is a potential Data breach the Processor will at any rate provide the Data Protection Officer of the Data Controller with a written response to the following questions contained in Appendix (4).

4.7 The Processor is entitled to provide phased answers to the questions as stated in Appendix (4) in Article 4.6 to the Data Protection Officer of the Data Controller as long as all questions have been answered no later than 36 hours following the infringement.

4.8 The Processor also undertakes to inform the Data Protection Office of the Data Controller immediately in writing about any new developments.

4.9 If the security incident has to be flagged as a Data breach, the Data Controller is obliged to report this to the Personal Data Authority and if necessary also to the data subjects, unless the Data Controller for reasons of its own indicates that the notification - in accordance with the statement of the Data Controller and only if the situation as referred to under Article 4.3 arises - must be made by the Processor or (any) Sub-processor.

4.10 The Data Controller also determines when and how the security incident will be communicated to third parties (including in any case: personnel, Sub-processors, media, insurance firm, trade organisation and/or chain partners.) The Data Controller can in consultation with the the Processor and (any) Sub-processor(s) also decide that another party will communicate to third parties instead of the Data Controller.

4.11 The Processor documents all security incidents, including the facts surrounding the incident, their effects and remedial action taken. The Processor will present these records to the Data Controller at the first [written] request to do so from the Data Controller.

Article 5. Retention period, erasure and destruction

5.1 Adver-Online will not keep the Data for longer than is reasonably necessary for the purpose for which it is being processed. In terms of the Personal Data, Adver-Online will as far as possible adhere to the suggested retention periods by the Personal Data Authority, unless the Data Controller has stipulated a different retention period. In case of doubt, Adver-Online will contact the Data Controller.

5.2 Adver-Online will at the end of the Agreement or, if the applicable retention period ends earlier, at the end of the retention period, provide the Data or a copy thereof - at the discretion of the Data Controller - to the Data Controller.

5.3 Adver-Online will at the end of the Agreement or at the end of the applicable retention period, after it has complied with the obligation as stated in paragraph 5.2, immediately erase all Data from its (automated or otherwise) systems and/or from data carriers (such as documents, CD-ROMs and computer disks) and destroy this Data. The above stipulations do not apply provided in relation to certain Data a statutory retention obligation applies and for counting values. Counting values are maintained and can be used in reports for the Data Controller or Adver-Online itself.

5.4 Adver-Online has no retention right to the Data, unless otherwise agreed.

Article 6. Confidentiality, requests by the Data Subject

6.1 Adver-Online is obliged to maintain confidentiality about the Data and not to make this available to third parties in any way, unless with express prior permission of the Data Controller or the Data has to be disclosed by law or based on other government regulations or based on a judicial decision. In that case, Adver-Online will inform the Data Controller immediately for performance of the mandatory processing.

6.2 Adver-Online will not furnish the "Data Controller" with any information about mandatory processing if the furnishing of this information is prohibited by law.

6.3 Adver-Online obliges the persons it employs or otherwise do work for it to maintain secrecy about all Data which they might become aware of in the context of the performance of the Agreement.

6.4 If a Data Subject submits a request to Adver-Online, Adver-Online will communicate this request to the Data Controller for dealing with, unless the Data Controller instructs Adver-Online to deal with the request. Adver-Online will provide all reasonably necessary assistance for dealing with the request.

6.5 Adver-Online will immediately notify the Data Controller in the unlikely event that a request from a Data Subject has been dealt with by Adver-Online.

Article 7. Information, investigation

7.1 In order to enable the Data Controller to check if Adver-Online fulfils all obligations arising from this Processor Agreement correctly, fully and promptly, Adver-Online will provide the Data Controller with the necessary information.

7.2 The Data Controller is at all times entitled to investigate the fulfilment by Adver-Online of its obligations based on this Processor Agreement or to arrange for this by an independent expert. This right is limited to requesting a copy of a certificate from an auditor. Only in case of reasonable doubt about the veracity thereof or the performance of the agreement may a check then take place. In that case the Data Controller is entitled after prior notice to investigate the office(s) and/or systems of Adver-Online or to arrange for such. The scope of the investigation is not more than is necessary for the purpose as stated in the above paragraph.

7.3 Adver-Online will cooperate fully with the investigation as referred to in section 2 of this article and will provide all reasonably required assistance and information in a timely manner.

7.4 The Data Controller will bear the costs associated with the investigation as referred to in section 2 of this article. Notwithstanding the previous, Adver-Online will bear the costs of such an investigation if it turns out to be necessary from the investigation that Adver-Online has failed to meet its obligations from this Processor Agreement correctly, promptly or in full.

7.5 If, in any way whatsoever, it is apparent that Adver-Online has failed to meet its obligations from this Processor Agreement correctly, promptly or in full and Adver-Online subsequently alleges it has rectified this failure, the Data Controller has the right to check whether the failure actually has been rectified and done so properly by Adver-Onbline, or to arrange for this.

7.6 Adver-Online will assist the Data Controller as far as possible to fulfil the obligations of the Data Controller in order to secure the Personal Data it holds. This concerns, amongst other things, complying with a Privacy Impact Assessment (PIA).

Article 8. Liability, penalty

8.1 Adver-Online is not liable for damage as a result of incorrect information on the websites provided by Adver-Online, or incorrect operation of the system. In all other cases, the liability of Adver-Online under this agreement or otherwise is limited to the amount of damage suffered by the Data Controller, to a maximum of €1,000 (one thousand euros) and shall never exceed the amount of the Agreement to which the unlawful act or attributable breach relates.

Article 9. Term

9.1 This Processor Agreement is concluded for the term of the Agreement and, therefore, ends automatically at the time the Agreement ends. A breach in the fulfilment of this Processor Agreement is regarded as a breach in the performance of the Agreement.

9.2 Provisions in this Processor Agreement which by their nature are intended for this purpose, including although not limited to what is provided for in Article 6, also continue after the end of this Processor Agreement.

Article 10. Final provisions

10.1 Amendments and additions to this Processor Agreement are only valid if they have been agreed in writing by both parties.

10.2 Neither party is entitled to transfer its rights and obligations from this Processor Agreement to a third party without prior approval from the other party.

10.3 Dutch law applies to this Processor Agreement. Disputes arising from this Processor Agreement will be brought before the competent court in Haarlem.

Drawn up in duplicate and signed,

On: [Date]	On: [Date]
At:	On: Heemstede, the Netherlands
[Company name] [Authorised Signatory]	Adver-Online B.V. H.O.M. van Rijnswoud

Appendix 1: Personal information

Salutation	Mr / Ms
First name	*
Surname	*
E-mail address	*
Address	*
Postcode	*
Town/city	*
Country / Province	*
Telephone	*
Mobile	*
CV (.pdf, .doc & .docx)	*
Driving licence	Yes / No
Willing to relocate	Yes/ No
Available from	*
BIG registration number	*
BSN number	*
Civil status	Married / Unmarried / Divorced / Widow
Degree	Yes / No
Photo	*
Date of birth	*
Country of birth	*
Place of birth	*
Nationality	*
Desired contract	Full time / Full time and Part time / Training / On-call service / Part time / Internship / Other
Desired employment	Secondment / Interim / Franchise / Freelance / Apprenticeship contract / Internship / Work from home / Temporary / Trainee / Temporary staffing / Holiday work / Permanent / Voluntary
Desired territory	Drenthe / Flevoland / Friesland / Gelderland / Groningen / Limburg / Noord-Brabant / Noord-Holland / Overijssel / Utrecht / Zeeland / Zuid-Holland / whole of the Netherlands
Desired sector	Automation / IT / ICT / Bio-building / Installation / Communication / Media / Advertising / Services / E-commerce / Online / Financial / Health care / Medical / Welfare / Trade / Commercial catering / Industry / Technology / Art / Culture /

Desired job category	Recreation / Tourism / Education / Research / Local government / Other / Transport / Logistics / Storage Accountancy / Administrative / Secretarial / Agri & Food / Bio (Life sciences) / Chemistry / Food & Pharma / Construction / Craft / Design / Architecture / Financial / Economics / Health care / Medical / Social / Catering / Tourism / Recreation / Installation / Maintenance / Repairs IT / ICT / Automation / Legal / Law / Customer service / Art / Culture / Quality / Management / Executive board / Marketing / Communication & PR / Media / Journalism / Nature / Environment / Education / Training / Research / Science / Local government / Other / Personnel and Organisation / Production, construction & crafts / Project management / Sales / Retailing / Commercial / Technology / Industry / Transport / Purchasing / Logistics / Safety / Security
Hobbies	*
Do you own a car?	Yes / No
Maximum commuting distance	*
Additional functions	*
Education level	HAVO / HBO / HBO/WO / License, IEP, BAC +3 / MAVO / MBO / MBO/HBO / VMBO / VWO / other
Are you doing a course?	Yes / No
Expected course end date	*
Notice period (number of months)	*
Hours available per week	*
Already planned a holiday?	Yes / No
Holiday end date	*
Holiday start date	*
Salary (on full-time basis)	*
Linguistic skills:	
Dutch	Linguistic skills - Moderate / Linguistic skills - good / Linguistic skills - fluent
English	Linguistic skills - Moderate / Linguistic skills - good / Linguistic skills - fluent
Other languages	Arabic / Bengali / Bulgarian / Chinese / Danish / German / French / Greek / Hindi / Hungarian / Irish / Icelandic / Italian / Japanese / Javanese / Cantonese / Korean / Croatian / Mandarin / Norwegian / Ukrainian / Polish / Portuguese / Romanian / Russian / Serbian / Slovenian / Slovakian / Spanish / Czech / Turkish / Simplified Chinese / Vietnamese / Belarusian / Swedish Linguistic skills - Moderate / Linguistic skills - good / Linguistic skills - fluent

Cover letter stating motivation	*
Facebook account name	*
LinkedIn account name	*
Twitter account name	*
Xing account name	*
Privacy report	*

Privacy Statement

I agree that my data will be stored in the applicant database of {..} We will keep this data for a maximum of 1 year, after which we will ask you for permission again. You can have your data changed or removed at any time. You can use the contact form for this. If we reject your application, do not invite you for a job interview or do not hire you, your data will automatically be deleted after 4 weeks. Your data will not be made available to third parties, unless otherwise indicated and used exclusively for your application. Data in the database are used anonymously for statistical purposes. Your data is stored on secure servers in the Netherlands.

Appendix 2: HROffice safeguards concerning storage and distribution of data

OWASP

The current measures comprise at least (but are not limited to) the measures referred to in the OWASP top 10. (https://www.owasp.org/index.php/Category:OWASP Top_Ten_Project). SSL is used for Data encryption and it is not possible to reproduce an End User password. These requirements are tested in accordance with the Certified Secure check lists. (https://www.certifiedsecure.com/checklists)

Storage

Hashing

We never store users' passwords. All passwords are stored as a "salted and peppered hash". This means that a unique key is generated which by definition cannot be traced back to the original password. When a user enters his or her password, the entry is "hashed" and the result is compared with the value in the database. When these values are alike, the password is the same as the original entry.

In order to prevent attackers from being able to compare the hashes with previously generated hashes of frequently occurring passwords (rainbow tables) all passwords have a "salt" (a random series of

characters which is generated per record) and a pepper (a random series of characters which is outside the database).

Encryption

Sensitive data is stored in encrypted form using the AES256 encryption algorithm. Unlike the passwords, this encryption has to be reversible. Or: it must be possible to identify the original value. In order to prevent tracing the original value by recognising patterns (in particular a problem for data with a low variation, such as gender) the data is encrypted in a non-deterministic way. In other words, the same value leads to a different encrypted value for each record.

The private key that is used for encryption and decryption is in a different location than the database server. This so that someone with access to the database or the database server cannot encrypt any data.

Anonymisation

If a backup is reset to an environment different to the production environment all personal data is automatically anonymised. By doing so we prevent any sensitive data from being outside the production servers.

Auditing

All authentication attempts, successful or otherwise, are audited.

Transport

HTTPS

All our applications use HTTPS connections for all parts of the application. Requests to non-HTTPS URLs are automatically rerouted to the HTTPS URL.

HSTS

An HTTPS re-routing is good but not in itself sufficient. If the user personally enters an unsecured HTTP URL, the first request to the server is sent via an unsecured connection. To avoid this, we provide all requests with an “HSTS header”. This header tells the browser that requests to the particular domain must go via HTTPS *at all times*. After receipt of this header, the browser will send all requests via HTTPS, also if the user personally enters an HTTP URL.

Secure cookies

All our cookies are marked ‘Secure”. This means that they are not sent via the browser over non-secured connections.

HTTP-only cookies

All our authentication cookies are marked as ‘HTTP only”. This means that the cookies are not accessible for client-side code (such as Java script).

Hosting

VPN

Our production environment is solely to be accessed via a VPN connection.

Automated deployments

All our deployments are via an automated system. This prevents manual adjustments having to be done on the servers, which reduces substantially the chance of human error.

Our Hosting Partner: Previder

Our hosting partner has the following certifications:

NEN 7510

ISO 9001 | ISO 14001 | ISO 27001

BREEAM Excellent

DigiD Assurance

DHPA Code of Conduct

Financial Soundness Certificate

Appendix 3: Contact details Data Protection Officer of the Data Controller

Appendix 4: Questionnaire for reporting Data breach

Type of report:
1.Is this a follow-up to an earlier report? Choose one of the following options.
a) Yes
b) No

2. What is the number of the original report? (Answer this question if you have answered question 1 with yes)

3. What is the scope of the follow-up report? (Answer this question if you have answered question 1 with yes), choose one of the following options.
a) Addition or modification of information concerning the earlier report
b) Retraction of earlier report

4. What is the reason for the retraction? (Answer this question if you have chosen option b for question 3)

5. On which legal provision are you basing this report?
a) Article 34a, paragraph 1, of the Personal Data Protection Act
b) Article 11.3a, paragraph 1 of the Telecommunications Act

6. Which company or which organisation does it concern? (Enter the following information).
a) Name of the company or the organisation
b) (Visiting) address
c) Postcode
d) Town/city
e) Chamber of Commerce no.:

7. Who is reporting the data breach? (Enter the following information.)
a) Name of the person who reports it
b) Position of the person who reports it
c) E-mail address of the person who reports it
d) Phone number of the person who reports it
e) Alternative telephone number of the person who reports it

8. With whom can the Personal Data Authority get in contact for further information about the report? (Enter the following information if this is someone else than the person who reported the data breach.)
a) Contact's name
b) Contact's position
c) Contact's e-mail address
d) Contact's telephone number
e) Contact's alternative telephone number

9. In which sector is the company or the organisation active?

10.Give a summary of the incident involving the breach of the security of personal data.

11. The personal data of how many people is involved in the breach? (Enter the figures.)
a) Minimum: (enter)
b) Maximum: (enter)

12. Describe the group of people whose personal data is involved in the breach
.
13. When did the breach take place? (Choose one of the following options and provide additional information if necessary).
a) On (date)
b) Between (period start date) and (period end date)
c) Not yet known

14. What is the nature of the breach? (You can tick several options.)
a) Reading (confidentiality)
b) Copying
c) Changing (integrity)
d) Erasure or destruction (availability)
e) Theft
f) Not yet known

15. What type of personal data does it concern? (You can tick several options.)
a) Name, address and place of residence
b) Phone numbers
c) E-mail addresses or other addresses for electronic communication
d) Access or identification data (for example, log-in name/ password or customer number)
e) Financial data (for example, account number, credit card number)
f) Citizen service number (BSN) or social security number
g) Copies of passport of copies of other identity documents
h) Gender, date of birth and/or age
i) Particular personal data (for example, race, ethnicity, criminal records, political convictions, union membership, religion, sexuality, medical details)
j) Other data, namely (enter)

16. What effects can the breach have for the privacy of the data subjects? (You can tick several options.)
a) Stigmatisation or exclusion

b) Damage to health
c) Exposure to (ID) fraud
d) Exposure to spam or phishing
e) Other, namely (enter)

Follow-up actions in response to a data breach

17. Which technical and organisational measures has Adver-Online implemented in order to tackle the breach and in order to prevent further breaches?

18. Have you reported the data breach to the data subjects or are you intending to do so? (Choose one of the following options.)
a) Yes
b) No
c) Not yet known

19. When did you report the data breach to the data subjects, or when are you going to do this? (Answer this question if you have answered question 20 with yes. Choose one of the following options and provide additional information if necessary.)
a) I have reported the data breach to the data subjects on (date)
b) I am going to report the data breach to the data subjects on (date)
c) Not yet known

20) What is the content of the report to the data subjects? (Literal rendering, answer this question if you have answered question 18 with yes.)

21. How many data subjects have you notified or are you going to notify? (Answer this question if you have answered question 18 with yes.)

22. Which means of communication or which communication methods do you use or do you intend to use to notify the data subjects? (Answer this question if you have answered question 18 with yes.)
23. Why do you refrain from reporting the data breach to the data subjects? (Answer this question if you have answered question 18 with no. Choose one of the following options and provide additional information if necessary.)
a) The technical protective measures I have implemented provide adequate protection to be able to omit the report to the data subject.
b) It is unlikely that the data breach will have adverse consequences for the privacy of the data subject because: (enter)
c) I have compelling reasons to omit reporting to the data subject, namely: (enter)
d) Other, namely: (enter)

Technical Protective Measures

24. Is the personal data encrypted, hashed or in some other way made incomprehensible or inaccessible for unauthorised parties? (Choose one of the following options and provide additional information if necessary.)
a) Yes
b) No
c) Partly, namely: (enter)

25. If the personal data is entirely or partially incomprehensible or inaccessible, how has this happened? (Answer this question if you have chosen option a or option c for question 24. If you used encryption, therefore explain the encryption method.)

International aspects

26. Does the breach concern persons in other EU countries? (Choose one of the following options.)
a) Yes
b) No
c) Not yet known

27. Did your company or organisation report the data breach to supervisory bodies in one or more other EU countries?
a) Yes, namely: (enter)
b) No

Follow-up report

28. Is this report complete in your opinion? (Select one of the following options.)
a) Yes, the requisite information has been provided and no follow-up report is required.
b) No, a follow-up report containing additional information about this breach will come later