IP CAMP
PRIVACY STATEMENT

Effective as of: 2018.05.25.

The operator of the WWW.IP-CAMP.COM website (hereinafter: Website), the IP-CAMP Kft. (hereinafter "Data Controller") hereby informs Users about the processing of data on the Website and the activities performed by the Data Controller in accordance with Regulation 2016/679 of the European Parliament and of the Council on the General Data Protection Regulation (hereinafter referred to as "GDPR").

1. Data Controller and access to the Data Controller

IP CAMP Kft.
Registered seat: 1113 Budapest, Bocskai út 134-146.
Registration number: 01-09-299379
Representative: Ferenczi László, general manager
Address: 1113 Budapest, Bocskai út 134-146.
Tax number: 25972665-2-43
Phone: +36 20 930 9866
E-mai: laszlo.ferenczi@ip-camp.com
Website: www.ip-camp.com

The Data Controller does not employ a Data Protection Officer.

2. Definitions

Website: the set of content and services available under the domain www.ip-camp.com.

User: A person visiting and browsing the Website.

Service: IT services provided by the Data Controller: software development, support, training, etc.

Customer: a person contracted with the Data Controller to use the Service, who uses the Service from the Data Controller as a service provider.

Contact Persons: Customer's contractors, employees, subcontractors with whom the Data Controller is obliged to cooperate in order to perform the contract.

3. What is the purpose of this privacy notice?

By using the Website and the Services, a contract is concluded between the Data Controller and the User or the Customer. In this privacy policy, the Data Controller provides detailed information to Users and Customers on the processing of personal data on the Website and in the provision of the Services in accordance with the law. The service provider shall be deemed to be the data controller for the processing of data on the Website. The service provider shall also be deemed to be the data controller for the provision of the Services.

4. What is the purpose of the Website?
The Website allows Users and Customers to obtain information about the Services provided by the Data Controller without registration. Users and Clients are responsible for the data provided by Users and Clients and for the content uploaded by them, for which the Data Controller excludes any liability.

5. How does the privacy notice apply to the User and other data subjects?
By accessing the Website, using the services available on the Website and using the functions of the Website, the User automatically accepts the provisions of this privacy policy without making any further legal declaration. By concluding a contract for the Service or ordering the Service, the Customer automatically accepts the terms of this privacy policy without any further legal declaration.
Information on the processing of cookies placed by the website is included in a separate privacy notice.

6. Who and how can amend the privacy notice and where and how will the Data Controller publish it?
The Data Controller may unilaterally amend this privacy notice at any time. The Data Controller shall publish the amendment to the privacy notice by publishing the consolidated privacy notice with the amendments on the Website under a separate menu item. Users and Customers are kindly requested to read the privacy notice carefully each time they visit the Website. This privacy notice is always available on the Website. Users and Clients may access, view, print and save this Privacy Notice on the Website, but may not modify it, only the Data Controller may do so.

7. What personal data do we process, for how long, what we use it for and under what authority?

The legal bases for our processing are:
(a) the user's voluntary informed consent to the processing of personal data pursuant to Article 6 (1) (a) of the GDPR (hereinafter "Consent");
b) pursuant to Article 6 (1) (b) of the GDPR, processing is necessary for the performance of a contract to which the User, as data subject, is a party (hereinafter referred to as "performance of the contract")
(c) processing is necessary for compliance with a legal obligation to which the controller is subject pursuant to Article 6 (1) (c) of the GDPR (hereinafter referred to as "compliance with a legal obligation")
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or a third party pursuant to Article 6 (1) (f) of the GDPR (hereinafter referred to as 'Legitimate Interest')

7.1. Processing of data of persons requesting an offer

The Data Controller processes the following data of persons who contact it for the purpose of requesting an offer for the following purposes:

Category of data subject	Category of data	Source of data	Purpose of data processing	Legal basis of data processing	Duration of data storage, date of deletion
Person requesting the offer	Name, telephone number, e-mail address	Provided by the data subject	Submission of the offer	Legitimate interest	5 years from the date of receipt of the offer (general limitation period)

The processing and storage period of the data relating to the submission of the offer is the same as the general limitation period of 5 years in civil law; for the purposes of any legal action or claim, the data must be kept within this limitation period.

7.2. Processing of Contracted Customer Contact Details

The Data Controller uses the contact details of the Customer's contracted Customers for the purpose of fulfilling the contract with the Customer and for the purpose of contacting the Customer as follows:

Category of data subject	Category of data	Source of data	Purpose of data processing	Legal basis of data processing	Duration of data storage, date of deletion
Contact persons, authorised representatives of Contracting Parties	Name	Contracting Parties	a) Contractual relations b) Contract performance c) Claims and enforcement	Performance of the contract Legitimate interest	5 years from the termination of the contract
	telephone number / mobile phone number	Contracting Parties	a) Contractual relations b) Contract performance c) Claims and enforcement	Performance of the contract Legitimate interest	5 years from the termination of the contract
	e-mail address	Contracting Parties	a) Contractual relations b) Contract performance c) Claims and enforcement	Performance of the contract Legitimate interest	5 years from the termination of the contract

	position	Contracting Parties	a) Contractual relations b) Contract performance c) Claims and enforcement	Performance of the contract Legitimate interest	5 years from the termination of the contract

It is in the legitimate interest of both the Data Controller and the Customer to be able to reach the Customer through its contact persons on a continuous basis. The contact details are limited in scope, containing only data relevant for the purpose of sending the notification, and the telephone number and e-mail address provided are usually specifically for business communications, so that the fundamental rights and freedoms of the data subject concerned are not disproportionately affected. The retention period is the general civil law limitation period of 5 years, i.e. the data will be deleted at the end of the 5th year after the termination of the contract.

7.3. Processing of job applicants' data

The CVs and other data uploaded by job applicants to the Data Controller on the career site (https://ip-camp.com/career) or submitted to the Data Controller on other electronic or paper basis are processed by the Data Controller as follows:

Please be informed that by submitting your CV or job application to us, you consent to the processing and storage of your personal data for recruitment, job offer, contact and identification purposes and to the sending of messages and notifications to the contact details provided for such purposes.

The personal data you provide in the recruitment process when applying for a specific position, as indicated below, as well as other personal data we collect about you, will be processed for the duration of the recruitment process and will be deleted at the end of the recruitment process.

If the recruitment process is protracted and lasts for more than one year, we will keep your data for a maximum of one year from the date of submission, at the end of which we may ask you again if you wish to extend the processing of your data for the full duration of the recruitment process, which may be longer than one year. If you do not reply to this question within 30 days or if you do not wish to extend the data processing period, your data will be deleted.

However, you also have the right to have this data stored and processed in our database for future recruitment and job posting purposes, irrespective of the position you apply for. We will ask for your specific consent to do so. If you have given your consent, we are entitled to process your data for a further 2 years in our own database for this purpose. The reason for the 2-year period is that we need to ensure that the data you have provided and that we collect and process about you is accurate and up-to-date, and after three years this can no longer be ensured, and the data may become outdated and out of date. Before the three years have elapsed, we may contact you to obtain your consent for a further 2 years and suggest that you update your data to keep it accurate and up to date. If you do not consent to further processing or do not provide

your consent within 30 days of the date of the request, your data will be deleted from the database.
If we enter into an employment relationship with you, the processing of this data will be subject to the data processing period set out in our employee information notice, which we will inform you of at the time you enter into the employment contract.

The legal basis for the processing is set out below, broken down by category of data and by purpose of processing:

Category of data	**Source of data**	**Purpose of data processing**	**Legal basis of data processing**	**Data storage period, date of deletion**
CV details: name, place of residence, mother's name, contact details (email address, phone number), xing.com and linkedIn.com public information, photo, education, schools, qualifications, jobs, work experience, hobbies, etc.)	candidate concerned	Recruitment Bidding Contacts Identification	Consent	At the end of the recruitment process, but for a maximum of 1 year
Personality and behavioural characteristics observed during the interview to assess suitability	Data Controller	Recruitment Bidding	Consent	At the end of the recruitment process, but for a maximum of 1 year
results of professional tests	Data Controller	Recruitment Bidding	Consent	After test evaluation

We can also arrange for you to take professional tests and aptitude tests when you apply for a job. We will administer these tests and aptitude tests and, once the tests have been evaluated, we will immediately destroy the tests and the answers and inform you of the results. Before each such vocational test or aptitude test, we will inform you of the skills or abilities to be assessed and the instrument or method to be used. The Employer will destroy the details and documentation of the vocational tests and aptitude tests after evaluation and will only retain information on your suitability for the job advertised. Notification of the success of your application You will be informed by e-mail after the recruitment process has been completed whether we intend to enter into an employment relationship with you.

Giving and withdrawing consent

You give your voluntary consent to the processing of your data for the above purposes by actively submitting your application to the job advertisement. You can withdraw your consent to the processing of your data at any time by sending an e-mail to info@ip-camp.com, where you will be asked to provide your name, date of birth and e-mail address, so that we can identify whose data we need to delete. In case of withdrawal of consent, all your data processed by us will be deleted. The obligation to erasure covers both electronic and paper data and also applies to the records we have kept and the conclusions we have drawn about you.

8. Who has access to your personal data?

8.1
Employees of the Controller have access to your personal data to the extent strictly necessary for the performance of their work.

8.2 Data Processors

For the processing and storage of your data, we use various companies with whom we have contracted to process your data. The following data processors process your data:

Data processor	**Purpose of data processing**	**Scope of data processed**
IDDQD Kft. (1136 Budapest, Hollán Ernő utca 3. 3. em. 3.a.	Operation, maintenance and supervision of IT systems	All personal data
Onlyfy.com	Recruitment	Name, email address, CV details, xing.com and linkedin.com public information
Microsoft (Microsoft Corporation One Microsoft Way Redmond, WA 98052 United States)	Cloud services	Data indicated in points 7.1.,7.2.,7.3.

The privacy policy of onlyfy.com, the data processor that processes the data uploaded on the careers site (https://ip-camp.com/career), is available at the following link: https://help.onlyfy.com/hc/en-us/articles/8698364896913-Data-processing-in-onlyfy-one-Application-Manager

The transfer of data from this website to third countries is based on the legitimate interest of the Data Controller or on the consent of the User/Customer, but only if the Data Controller has received adequate assurances from the third country data processors that the User/Customer has effective rights and remedies with respect to the User/Customer's data.

The Controller does not transfer Users' personal data to an international organisation.

9. What rights have you got in relation to the processing of your personal data and how do we ensure that you exercise them?
a) Right of access: you can request information about what data we process, for what purpose, for how long, to whom we disclose it, and where it comes from.

b) Right of rectification: if your data changes or we have recorded it incorrectly, you can ask us to correct, rectify or clarify it. Please check your data regularly and notify us of any changes to your data within 15 days at the latest, so that our database is always up to date and accurate about you.

c) Right of erasure: you may request the erasure of your data processed by us in the cases specified by law.

d) Right to restriction of processing: you may request that we restrict the processing of your personal data in the cases specified by law.

e) Right to object: if you have a legitimate interest in the processing of your data, you may object to the processing of your data, in which case we will no longer process your data and will delete it.

f) Right to data portability: by exercising this right, you may request that we disclose your data to you, or transfer it directly to another service provider designated by you, on the basis of your specific request and authorisation. Please note that a request for data portability can only be made for data that you have provided, that we have consented to process and that we process automatically, and that we can only comply with a request for data portability for transfer to another service provider if it is technically and securely feasible. If you make such a request, we will act in accordance with the law and will inform you within one month of the action we have taken in response to your request.

(g) Right to withdraw consent: where we process your data on the basis of your consent, you have the right to withdraw your consent at any time, without prejudice to the lawfulness of our processing of your data prior to the withdrawal of your consent.

h) Right to file a complaint: if you have suffered a breach of rights in relation to our processing, you have the right to file a complaint with the competent supervisory authority:
National Authority for Data Protection and Freedom of Information
Website: http://naih.hu
Postal address: 1530 Budapest, PO Box 5.
E-mail: ugyfelszolgalat@naih.hu
Telephone: +36 (1) 391-1400

In addition to the above, you may also bring an action against the Data Controller in the event of a breach of the protection of personal data. You may exercise the above rights by sending an e-mail to info@ip-camp.com or by registered mail to the head office of the Data Controller, and

if you do so, we will act in accordance with the law and inform you within one month of the action we have taken on your request.

When requesting information in the context of the right of access, we inform you that we are not able to provide you with a copy of data processed on paper only, if they include personal data of other persons, pursuant to Article 15 (3) and (4) of the GDPR, because the disclosure of such data to third parties would violate the data protection and privacy rights of such persons.

10. How do we ensure the security of your data?

The Data Controller has implemented the following information security measures to protect your data:

Personal data is stored on servers rented by us and on the hard disks of the Data Controller's computers, to which only a limited number of personnel and employees have access, based on strict access control rules.
Access to data and documents stored in the cloud document management system is only possible with a password and appropriate authorisation.

Access to our local machines is password protected. Our servers are housed in secure server rooms, where water, fire and intrusion protection is ensured. Our IT systems are periodically, recurrently and regularly tested and audited to establish and maintain data and IT security.

Regular and continuous protection against malicious software is provided for all systems and components of the Data Controller. Security functions are prioritised and segregated in the design and operation of programs, applications and tools. Data affecting the security of the information system (e.g. passwords, privileges, logs) is protected when access rights are assigned.

Data is backed up daily. Only a limited set of authorised persons has access to the backups. To meet the requirement of secure data exchange for electronically transmitted messages and files, data integrity is ensured for both (communication) control and user data. We also comply with the requirements of data security in document management, which are defined in our document management rules. To ensure physical security of data, we ensure that our doors and windows are adequately protected, and we have strict visitor and access control procedures for visitors. Our premises are sufficiently secure against unauthorised or forced entry, fire or natural disasters. And storage of data media used for data transmission, backup and archiving must be in a secure, locked location.

11. What do we do if we have a data breach?
We will notify the supervisory authority of the data breach within 72 hours of becoming aware of it, in accordance with the law, and we will keep records of data breaches. We also inform the affected users in cases specified by law and act in accordance with our incident handling policy.

12. When and how do we change this privacy notice? If the scope of the data processed or the other circumstances of the processing change, we will amend this privacy notice in accordance with the GDPR within 30 days and publish it on the website.