PRIVACY POLICY

INTRODUCTION

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of natural persons with regard to the processing of personal data and on the free flow of such data, as well as on the repeal of Regulation 95/46/EC (hereinafter: the Regulation) stipulates, that the Data Controller takes appropriate measures in order to provide the data subject with all information regarding the processing of personal data in a concise, transparent, understandable and easily accessible form, clearly and comprehensibly formulated, and that the Data Controller facilitates the exercise of the rights of the data subject.

The obligation of the data subject to be informed in advance about the right to self-determination of information and the freedom of information CXII of 2011 is also required by law.

We comply with this legal obligation by providing the information below.

The information must be published on the company's website or sent to the person concerned upon request.

A copy of these regulations in force at all times must be posted on the employee notice board at the Company's headquarters. These regulations also form an appendix to the employment contracts, acceptance of which is confirmed by the signature of the Company's employees.

I. CHAPTER
NAME OF DATA PROCESSOR

The publisher of this information, also the Data Controller:
Company name: First Tech Kft.
Location: 6771 Szeged Palackozó 25.
Company registration number:06 09 011503
VAT number:14020630-2-06
Fax: +36 62 406 406
E-mail address: office@first-tech.hu
Homepage: http://www.first-tech.hu/

(hereinafter: Company)

II. CHAPTER
NAME OF DATA PROCESSORS

Data processor: the natural or legal person, public authority, agency or any other body that processes personal data on behalf of the data controller; (Article 4, 8 of the Regulation)

The use of the data processor does not require the prior consent of the data subject, but information is required. Accordingly, we provide the following information:

1. Our company's IT service provider

For the maintenance and management of its website, our company uses a data processor who provides IT services (hosting services) and within this framework - for the duration of our contract with him - manages the personal data provided on the website, the operation performed by him is the storage of personal data on the server.

Company name: GBaRT Design Stúdió Kft.
Location: 1029 Budapest, Zsíroshegyi út 16.
Company registration number: 01 09 917297
VAT number: 14733655241
E-mail address: info@gb-art.hu
Homepage: http://www.gbart.hu/

III. CHAPTER
DATA MANAGEMENT RELATED TO EMPLOYMENT

1. Labor and personnel records

(1) Only such data may be requested and kept on record from employees, as well as occupational medical suitability examinations, which are necessary for the establishment, maintenance and termination of employment, as well as for the provision of social welfare benefits and which do not infringe the employee's personal rights.

(2) The Company processes the following data of the employee for the purpose of establishing, fulfilling or terminating an employment relationship under the legal title of asserting its legitimate interests as an employer (Article 6 (1, paragraph f) of the Regulation):

1. name
2. birth name,
3. date of birth,
4. his mother's name,
5. residential address,
6. his nationality,
7. tax identification number,
8. “TAJ” insuraance number,
9. pensioner identification number (in the case of a retired employee),
10. telephone number,
11. e-mail address,
12. identity card number,
13. the number of the official ID card confirming the residential address,
14. your bank account number,
15. online ID (if any)
16. starting and ending date of starting work,

17. job title,
18. a copy of a document certifying your education and professional qualifications,
19. photo
20. resume,
21. the amount of your salary, data related to salary payment and other benefits,
22. the debt to be deducted from the employee's salary based on a legally binding decision or legislation, or his written consent, or the entitlement thereof,
23. evaluation of the employee's work,
24. the manner and reasons for the termination of the employment relationship,
25. depending on the job, his moral certificate
26. summary of job suitability tests,
27. in the case of private pension fund and voluntary mutual insurance fund membership, the name of the fund, its identification number and the employee's membership number,
28. in the case of a foreign employee, passport number; the name and number of the document certifying the right to work,
29. data recorded in the records of accidents involving employees;
30. data required for the use of welfare services and commercial accommodation;
31. data recorded by the camera and access control system used by the Company for security and property protection purposes, as well as the location determination systems.

(3) The employer only handles data relating to illness and trade union membership for the purpose of fulfilling the right or obligation specified in the Labor Code.

(4) Recipients of personal data: the manager of the employer, the exercise of employer authority, the employees and data processors of the Company performing labor tasks.

(5) Only the personal data of senior employees may be forwarded to the owners of the Company.

(6) Period of storage of personal data: 3 years after termination of employment.

(7) Before data processing begins, the data subject must be informed that data processing is based on the Labor Code and the enforcement of the legitimate interests of the employer

2. Data management related to aptitude tests

(1) The employee can only be subject to a suitability test that is prescribed by a rule relating to an employment relationship, or which is necessary in order to exercise a right or fulfill an obligation specified in a rule relating to an employment relationship. Before the examination, the employees must be informed in detail about, among other things, what kind of skills and abilities the aptitude test is aimed at assessing, and what means and methods are used for the examination. If a law requires the examination to be carried out, the employees must be informed of the title of the law and the exact location of the law.

(2) The employer can fill out the test forms for work suitability and preparedness both before the establishment of the employment relationship and during the existence of the employment relationship.

(3) In order to provide and organize the work processes more efficiently, the questionnaire, which is clearly related to the employment relationship, can only be completed with a larger

group of employees, suitable for researching psychological or personality traits, if the data revealed during the analysis cannot be linked to individual specific employees, i.e., the test is done anonymously data processing.

(4) Scope of personal data that can be processed: the fact of job suitability and the necessary conditions for this.

(5) Legal basis for data management: legitimate interest of the employer.

(6) The purpose of processing personal data is: establishing and maintaining an employment relationship, filling a position.

(7) Recipients of personal data and categories of recipients: The results of the examination can be seen by the examined employees and the specialist conducting the examination. The employer can only receive information on whether the examined person is suitable for the job or not, and what conditions must be provided for this. However, the employer may not know the details of the investigation or its complete documentation.

(8) Duration of processing personal data: 3 years after termination of employment.

3. Management of the data of employees applying for recruitment, applications, resumes

(1) The range of personal data that can be processed: the natural person's name, date of birth, place, mother's name, residential address, qualification data, photo, telephone number, e-mail address, employer's record of the applicant (if any).

(2) The purpose of processing personal data: application, evaluation of applications, conclusion of an employment contract with the selected candidate. The person concerned must be informed if the employer did not choose him for the given position.

(3) Legal basis for data management: consent of the data subject.

(4) Recipients of personal data and categories of recipients: managers and employees who are entitled to exercise employer rights at the Company and perform labor duties.

(5) Period of storage of personal data: Until the application or tender is evaluated. The personal data of applicants who are not selected must be deleted. The data of the person who withdrew their application or application must also be deleted.

(6) The employer may only retain applications based on the express, clear and voluntary consent of the person concerned, provided that their retention is necessary to achieve the purpose of data management in accordance with the legislation. This consent must be requested from the applicants after the end of the admission procedure.

4. Data management related to workplace camera surveillance

(1) Our company uses an electronic surveillance system at its headquarters, premises, and premises open to customers for the purpose of protecting human life, physical integrity,

personal freedom, business secrets and asset protection, which also enables image, sound, or image and sound recording. does, based on this, the behavior of the person concerned, which is recorded by the camera, can also be considered personal data.

(2) The legal basis for this data management is the enforcement of the legitimate interests of the employer and the consent of the data subject.

(3) Notices and information about the fact of the application of the electronic monitoring system in a given area must be placed in a clearly visible place, clearly legible, in a way that facilitates the orientation of third parties who wish to appear in the area. The information must be provided for each camera. This information contains information on the fact of the surveillance carried out by the electronic asset protection system, as well as the purpose of making and storing images and audio recordings recorded by the system containing personal data, the legal basis for data management, the place where the recording is stored, the duration of storage, the user (operator) of the system also information about his person, the range of persons entitled to access the data, as well as the provisions regarding the rights of the data subjects and the procedure for their enforcement.

(4) Pictures and audio recordings of third parties entering the monitored area (customers, visitors, guests) may be taken and managed with their consent. Consent can also be given by suggestive behavior. Suggestive behavior, in particular, if the natural person staying there enters the monitored area despite the notice or explanation about the use of the electronic monitoring system posted there.

(5) Recordings can be kept for a maximum of 3 (three) working days if they are not used. Use is considered if the recorded image, sound, or image and sound recording, as well as other personal data, is intended to be used as evidence in court or other official proceedings.

(6) The person whose right or legitimate interest is affected by the recording of image, sound, or image and sound recording data may, within three working days from the recording of the image, sound, and image and sound recording, request by proving his right or legitimate interest , so that the data is not destroyed or deleted by its manager.

(7) It is not possible to use an electronic monitoring system in a room in which the monitoring may violate human dignity, so in particular in changing rooms, showers, toilets or, for example, a medical room, or in the corresponding waiting room, and also in a room that is used for employees' breaks between work was designated for the purpose of completion.

(8) If no one is legally allowed to be in the workplace - especially outside of working hours or on holidays - then the entire area of the workplace (such as changing rooms, toilets, rooms designated for breaks between work) can be monitored.

(9) In addition to those authorized to do so by law, the management staff, the manager and deputy of the employer, and the workplace manager of the monitored area are entitled to view the data recorded by the electronic monitoring system for the purpose of revealing violations and checking the operation of the system.

IV. CHAPTER
DATA MANAGEMENT RELATED TO CONTRACT

1. Management of the data of contractual partners - registration of customers and suppliers

(1) The Company processes the name, birth name, time of birth, mother's name, address, tax identification number, tax number, entrepreneur, primary producer of the natural person contracted with it as a buyer or supplier for the purpose of concluding, fulfilling, terminating the contract, and providing contractual benefits. identity card number, identity card number, residential address, address of headquarters, location, telephone number, e-mail address, website address, bank account number, customer number (customer number, order number), online identifier (list of customers, suppliers, main purchase lists). This data management is considered legal even if the data management is necessary to take steps at the request of the data subject prior to the conclusion of the contract. Recipients of personal data: the Company's employees performing tasks related to customer service, employees performing accounting and taxation tasks, and data processors. Duration of processing personal data: 5 years after the termination of the contract.

(2) The data subject must be informed before the start of data management that the data management is based on the legal title of the performance of the contract, this information can also be provided in the contract.

(3) The data subject must be informed about the transfer of his personal data to the data processor.

2. Contact details of natural person representatives of legal entity clients, buyers, suppliers

(1) Scope of personal data that can be processed: name, address, telephone number, e-mail address, online identifier of the natural person.

(2) The purpose of processing personal data: fulfillment of the contract concluded with the Company's legal entity partner, business relationship, legal basis: the consent of the person concerned.

(3) Recipients of personal data and categories of recipients: employees of the Company performing tasks related to customer service.

(4) Duration of storage of personal data: up to 5 years after the existence of the business relationship or the quality of representative of the person concerned.

V. CHAPTER
DATA PROCESSING BASED ON LEGAL OBLIGATION

1. Data management for the purpose of fulfilling tax and accounting obligations

(1) The Company handles the legally defined data of natural persons entering into a business relationship with it as a customer or supplier for the purpose of fulfilling legal obligations, tax and accounting obligations prescribed by law (bookkeeping, taxation). The processed data is

in accordance with CXXVII of 2017 on general sales tax. based on §169 and §202 of the Act, in particular: tax number, name, address, tax status, based on §167 of Act C of 2000 on accounting: name, address, the person ordering the economic operation or designation of the organization, the voucher issuer and the person certifying the implementation of the provision, and, depending on the organization, the signature of the inspector; the signature of the receiver on the stock movement receipts and money management receipts, and the payer's signature on the receipts, CXVII of 1995 on personal income tax. based on the law: entrepreneur ID number, primary producer ID number, tax identification number.

(2) The period of storage of personal data is 8 years after the termination of the legal relationship giving the legal basis.

(3) Recipients of personal data: the Company's employees and data processors performing tax, accounting, payroll, and social security tasks.

2. Payer data management

(1) The Company processes the personal data of those concerned - employees, their family members, employees, recipients of other benefits - as required by tax laws for the purpose of fulfilling legal obligations, for the purpose of fulfilling tax and contribution obligations prescribed by law (tax, advance tax, assessment of contributions, payroll, social security administration), with whom its payers (2017: CL. Act on the Taxation System (Art.) 7.§ 31.) are in contact. The scope of the processed data is determined by Art. § 50, highlighting separately: the natural person's natural personal identification data (including the previous name and title), gender, citizenship, the natural person's tax identification number, social security identification number (Social security number). If the tax laws attach legal consequences to this, the Company may process the employees' health (Szja tv.§ 40.) and trade union (Szja tv. § 47.(2) b./) data for the purpose of fulfilling tax and contribution obligations (payroll, social security administration).

(2) The period of storage of personal data is 8 years after the termination of the legal relationship giving the legal basis.

(3) Recipients of personal data: the Company's employees and data processors performing tax, payroll, social security (paying) duties.

VI. CHAPTER
SUMMARY OF YOUR RIGHTS

In this chapter, for the sake of clarity and transparency, we briefly summarize the rights of the data subject, the detailed information on the exercise of which is provided in the next chapter.

Right to prior information
The data subject has the right to receive information about the facts and information related to data management before the start of data management.
(Articles 13-14 of the Regulation)
We provide information on the detailed rules in the next chapter.

The data subject's right of access

The data subject is entitled to receive feedback from the Data Controller as to whether his personal data is being processed, and if such data processing is ongoing, he is entitled to access the personal data and related information specified in the Regulation.
(Regulation Article 15).
We provide information on the detailed rules in the next chapter.

Right to rectification
The data subject is entitled to have the Data Controller correct inaccurate personal data concerning him without undue delay upon request. Taking into account the purpose of the data management, the data subject is entitled to request the completion of incomplete personal data, including by means of a supplementary statement.
(Regulation Article 16).

The right to erasure ("the right to be forgotten")
1. The data subject has the right to request that the Data Controller delete the personal data concerning him without undue delay, and the Data Controller is obliged to delete the personal data concerning the data subject without undue delay if one of the reasons specified in the Order exists.
(Regulation Article 17)
We provide information on the detailed rules in the next chapter.

The right to restrict data processing
The data subject is entitled to request that the Data Controller restricts data processing if the conditions specified in the order are met.
(Regulation Article 18)
We provide information on the detailed rules in the next chapter.

Notification obligation related to the correction or deletion of personal data or the limitation of data management
The Data Controller informs all recipients of all corrections, deletions or data management restrictions to whom or to whom the personal data was communicated, unless this proves to be impossible or requires a disproportionately large effort. At the request of the data subject, the Data Controller informs about these recipients.
(Regulation Article 19)

The right to data portability
Under the conditions set out in the Regulation, the data subject is entitled to receive the personal data relating to him/her provided to a Data Controller in a segmented, widely used, machine-readable format, and is also entitled to forward this data to another Data Controller without being hindered by the the Data Controller to whom the personal data was made available.
(Regulation Article 20)
We provide information on the detailed rules in the next chapter.

The right to protest
The data subject has the right to object to his personal data at any time for reasons related to his own situation under point e) of Article 6 (1) of the Regulation (the data processing is in the public interest or necessary for the performance of a task carried out within the framework of the exercise of public authority vested in the Data Controller) or point f) (the data

management is necessary to enforce the legitimate interests of the Data Controller or a third party.
(Regulation Article 21)
We provide information on the detailed rules in the next chapter

Automated decision-making in individual cases, including profiling
The data subject has the right not to be covered by the scope of a decision based solely on automated data management, including profiling, which would have legal effects on him or affect him to a similar extent.
(Regulation Article 22)
We provide information on the detailed rules in the next chapter.

Restrictions
The EU or Member State law applicable to the Data Controller or data processor may limit the provisions of Articles 12-22 through legislative measures. Article and Article 34, as well as Articles 12–22. in accordance with the rights and obligations defined in Article
(Regulation Article 23)
We provide information on the detailed rules in the next chapter.

Informing the data subject about the data protection incident
If the data protection incident is likely to involve a high risk for the rights and freedoms of natural persons, the Data Controller shall inform the data subject of the data protection incident without undue delay.
(Regulation Article 34)
We provide information on the detailed rules in the next chapter.

The right to lodge a complaint with the supervisory authority (right to an official remedy)

The data subject has the right to file a complaint with a supervisory authority - in particular in the Member State of his or her usual place of residence, workplace or the place of the suspected infringement - if, in the opinion of the data subject, the processing of personal data concerning him/her violates the Regulation.
(Regulation Article 77)
We provide information on the detailed rules in the next chapter.

The right to an effective judicial remedy against the supervisory authority

All natural and legal persons are entitled to an effective judicial remedy against the legally binding decision of the supervisory authority concerning them, or if the supervisory authority does not deal with the complaint or does not inform the person concerned about the procedural developments related to the submitted complaint or its result within three months.
(Regulation Article 78)
We provide information on the detailed rules in the next chapter.

The right to an effective judicial remedy against the controller or processor

All affected persons are entitled to an effective judicial remedy if, in their judgment, their rights according to this regulation have been violated as a result of improper handling of their personal data and this regulation.

(Regulation Article 79)
We provide information on the detailed rules in the next chapter.

VII. CHAPTER
DETAILED INFORMATION ABOUT YOUR RIGHTS

Right to prior information

The data subject has the right to receive information about the facts and information related to data management before the start of data management

A) Information to be made available if personal data is collected from the data subject

1. If the personal data concerning the data subject is collected from the data subject, the data controller shall provide the data subject with all of the following information at the time of obtaining the personal data:
a) the identity and contact details of the data controller and, if any, the representative of the data controller;
b) contact details of the data protection officer, if any;
c) the purpose of the planned processing of personal data and the legal basis of data processing;
d) in the case of data management based on point f) of Article 6, paragraph (1) of the Regulation (validation of legitimate interests), the legitimate interests of the data controller or a third party;
e) where appropriate, recipients of personal data, or categories of recipients, if any;
f) where appropriate, the fact that the data controller wishes to transfer the personal data to a third country or an international organization, as well as the existence or absence of the Commission's compliance decision, or Article 46, Article 47 or Article 49 of the Regulation (1) in the case of data transfer referred to in the second subparagraph of paragraph 1, indicating the appropriate and suitable guarantees, as well as a reference to the methods for obtaining a copy of them or their availability.
2. In addition to the information mentioned in point 1, the data controller informs the data subject of the following additional information at the time of obtaining the personal data, in order to ensure fair and transparent data management:
a) on the period of storage of personal data, or if this is not possible, on the criteria for determining this period;
b) the data subject's right to request from the data controller access to personal data relating to him, their correction, deletion or restriction of processing, and to object to the processing of such personal data, as well as the data subject's right to data portability;
c) in the case of data processing based on point a) of Article 6 (1) (consent of the data subject) or point a) of Article 9 (2) (consent of the data subject) of the Regulation, the right to withdraw consent at any time, which is not affects the legality of data processing carried out on the basis of consent before withdrawal;
d) on the right to submit a complaint to the supervisory authority;
e) whether the provision of personal data is based on legislation or a contractual obligation or is a prerequisite for concluding a contract, as well as whether the data subject is obliged to provide the personal data, as well as the possible consequences of failure to provide data;
f) the fact of automated decision-making referred to in paragraphs (1) and (4) of Article 22 of the Regulation, including profiling, as well as, at least in these cases, comprehensible

information about the logic used and the significance of such data management for the data subject what are the expected consequences.
3. If the data controller wishes to carry out further data processing of personal data for a purpose other than the purpose of their collection, he must inform the data subject about this different purpose and all relevant additional information mentioned in paragraph (2) before further data processing.
4. The 1-3. points do not apply if and to the extent that the data subject already has the information.
(Regulation Article 13)

B) Information to be made available if the personal data was not obtained from the data subject

1. If the personal data was not obtained from the data subject, the data controller provides the data subject with the following information:
a) the identity and contact details of the data controller and, if any, the representative of the data controller;
b) contact details of the data protection officer, if any;
c) the purpose of the planned processing of personal data and the legal basis of data processing;
d) categories of personal data concerned;
e) recipients of personal data, or categories of recipients, if any;
f) where appropriate, the fact that the data controller wishes to forward the personal data to a recipient in a third country or to an international organization, and the existence or absence of the Commission's compliance decision, or in Article 46, Article 47 or Article 49 of the Regulation. in the case of data transmission referred to in the second subparagraph of paragraph (1) of Article 2, the indication of appropriate and suitable guarantees, as well as a reference to the methods for obtaining a copy of them or their availability.
2. In addition to the information mentioned in point 1, the data controller provides the data subject with the following additional information necessary to ensure fair and transparent data management for the data subject:
a) the period of storage of personal data, or if this is not possible, the criteria for determining this period;
b) if the data management is based on point f) of Article 6 (1) of the Regulation (legitimate interest), on the legitimate interests of the data controller or a third party;
c) the data subject's right to request from the data controller access to personal data relating to him, their correction, deletion or restriction of processing, and to object to the processing of personal data, as well as the data subject's right to data portability;
d) in the case of data processing based on point a) of Article 6 (1) (consent of the data subject) or point a) of Article 9 (2) (consent of the data subject) of the Regulation, the right to withdraw consent at any time, which is not affects the legality of data processing carried out on the basis of consent before withdrawal;
e) the right to submit a complaint addressed to a supervisory authority;
f) the source of the personal data and, where appropriate, whether the data comes from publicly available sources; and
g) the fact of automated decision-making referred to in paragraphs (1) and (4) of Article 22 of the Regulation, including profiling, as well as, at least in these cases, comprehensible information regarding the logic used and the significance of such data management for the data subject what are the expected consequences.
3. The data controller provides the information according to points 1 and 2 as follows:

a) taking into account the specific circumstances of the handling of personal data, within a reasonable time from the acquisition of the personal data, but within one month at the latest;
b) if the personal data is used for the purpose of contacting the data subject, at least during the first contact with the data subject; obsession
c) if it is expected that the data will be communicated to another recipient, at the latest when the personal data is communicated for the first time.
4. If the data controller wishes to carry out further data processing on personal data for a purpose other than the purpose of their acquisition, the data subject must be informed of this different purpose and all relevant additional information mentioned in point 2 before further data processing.
5. The 1-5. point does not have to be applied if and to the extent that:
a) the data subject already has the information;
b) the provision of the information in question proves to be impossible or would require a disproportionately large effort, especially in the case of data processing for the purpose of archiving in the public interest, for scientific and historical research purposes or for statistical purposes, taking into account the conditions and guarantees contained in Article 89 (1) of the Regulation, or if the obligation referred to in paragraph (1) of this article would likely make it impossible or seriously jeopardize the achievement of the goals of this data management. In such cases, the data controller must take appropriate measures - including making the information publicly available - in order to protect the rights, freedoms and legitimate interests of the data subject;
c) the acquisition or disclosure of the data is expressly required by the EU or Member State law applicable to the data controller, which provides for appropriate measures to protect the legitimate interests of the data subject; obsession
d) personal data must remain confidential on the basis of the obligation of professional confidentiality prescribed by an EU or member state law, including the obligation of confidentiality based on legislation.
(Regulation Article 14)

The data subject's right of access

1. The data subject has the right to receive feedback from the Data Controller as to whether his personal data is being processed, and if such data processing is underway, he is entitled to receive access to the personal data and the following information:
a) the purposes of data management;
b) categories of personal data concerned;
c) recipients or categories of recipients to whom or to whom the personal data has been or will be communicated, including in particular recipients in third countries and international organizations;
d) where applicable, the planned period of storage of personal data, or if this is not possible, the criteria for determining this period;
e) the right of the data subject to request from the Data Controller the correction, deletion or restriction of processing of personal data concerning him and to object to the processing of such personal data;
f) the right to submit a complaint addressed to a supervisory authority;
g) if the data were not collected from the data subject, all available information about their source;
h) the fact of automated decision-making referred to in paragraphs (1) and (4) of Article 22 of the Regulation, including profiling, as well as, at least in these cases, comprehensible

information regarding the applied logic and the significance of such data management and the data subject looking at the expected consequences.

2. If personal data is transferred to a third country or to an international organization, the data subject is entitled to receive information about the appropriate guarantees regarding the transfer according to Article 46 of the Regulation.

3. The Data Controller provides a copy of the personal data that is the subject of data management to the data subject. For additional copies requested by the data subject, the Data Controller may charge a reasonable fee based on administrative costs. If the data subject submitted the request electronically, the information must be provided in a widely used electronic format, unless the data subject requests otherwise. The right to request a copy must not adversely affect the rights and freedoms of others.
(Regulation Article 15)

The right to erasure ("the right to be forgotten")

1. The data subject has the right to request that the Data Controller delete the personal data concerning him without undue delay, and the Data Controller is obliged to delete the personal data concerning the data subject without undue delay if one of the following reasons exists:
a) the personal data are no longer needed for the purpose for which they were collected or otherwise processed;
b) the data subject withdraws his/her consent, which is the basis of the data processing pursuant to point a) of Article 6(1) or point a) of Article 9(2) of the Regulation, and there is no other legal basis for the data processing;
c) the data subject objects to the data processing based on Article 21 (1) of the Regulation and there is no overriding legitimate reason for the data processing, or the data subject objects to the data processing based on Article 21 (2);
d) personal data were handled unlawfully;
e) personal data must be deleted in order to fulfill the legal obligation prescribed by EU or member state law applicable to the Data Controller;
f) the collection of personal data took place in connection with the offering of information society-related services referred to in Article 8 (1) of the Regulation.

2. If the Data Controller has disclosed the personal data and is obliged to delete it pursuant to point 1 above, it will take reasonable steps, including technical measures, taking into account the available technology and implementation costs, in order to inform the Data Controllers handling the data, that the data subject requested from them the deletion of the links to the personal data in question or the copy or duplicate of this personal data.

3. Points 1 and 2 do not apply if data management is necessary:
a) for the purpose of exercising the right to freedom of expression and information;
b) for the purpose of fulfilling the obligation under EU or member state law applicable to the Data Controller, which prescribes the processing of personal data, or for the execution of a task carried out in the public interest or in the context of the exercise of public authority vested in the Data Controller;
c) in accordance with points h) and i) of Article 9 (2) and Article 9 (3) of the Regulation on the basis of public interest affecting the field of public health;
d) in accordance with Article 89 (1) of the Regulation, for the purpose of archiving in the public interest, for scientific and historical research purposes or for statistical purposes, if the

right mentioned in point 1 would likely make this data management impossible or seriously endanger it; obsession
e) to present, enforce and defend legal claims.
(Regulation Article 17)

The right to restrict data processing

1. The data subject has the right to request that the Data Controller restrict data processing if one of the following is met:
a) the data subject disputes the accuracy of the personal data, in which case the restriction applies to the period that allows the Data Controller to check the accuracy of the personal data;
b) the data management is illegal and the data subject opposes the deletion of the data and instead requests the restriction of their use;
c) the Data Controller no longer needs the personal data for the purpose of data management, but the data subject requires them to present, enforce or defend legal claims; obsession
d) the data subject has objected to data processing in accordance with Article 21 (1) of the Regulation; in this case, the restriction applies to the period until it is established whether the Data Controller's legitimate reasons take precedence over the data subject's legitimate reasons.

2. If data management is subject to restrictions based on point 1, such personal data, with the exception of storage, will only be processed with the consent of the data subject, or for the presentation, enforcement or defense of legal claims, or for the protection of the rights of other natural or legal persons, or the Union, or can be handled in the important public interest of a member state.

3. The Data Controller informs the data subject, at whose request the data processing was restricted based on point 1, of the lifting of the data processing restriction in advance.
(Regulation Article 18)

The right to data portability

1. The data subject has the right to receive the personal data concerning him/her provided to a Data Controller in a segmented, widely used, machine-readable format, and is also entitled to transmit this data to another Data Controller without being hindered by that Data Controller , to which you provided the personal data, if:
a) the data management is based on consent according to point a) of Article 6 (1) or point a) of Article 9 (2) of the Regulation, or on a contract according to point b) of Article 6 (1) of the Regulation; and
b) data management takes place in an automated manner.

2. When exercising the right to data portability in accordance with point 1, the data subject is entitled to - if this is technically possible - request the direct transmission of personal data between Data Controllers.

3. The exercise of this right may not violate Article 17 of the Regulation. The aforementioned right does not apply in the event that the data processing is in the public interest or is necessary for the execution of a task carried out in the context of the exercise of the public authorities granted to the Data Controller.

4. The right mentioned in point 1 may not adversely affect the rights and freedoms of others.
(Regulation Article 20)

The right to protest

1. The data subject has the right to object to his personal data at any time for reasons related to his own situation under point e) of Article 6 (1) of the Regulation (the data processing is in the public interest or is necessary for the performance of a task carried out in the context of the exercise of public authority vested in the Data Controller) or point f) (data processing is necessary to assert the legitimate interests of the Data Controller or a third party), including profiling based on the aforementioned provisions. In this case, the Data Controller may no longer process the personal data, unless the Data Controller proves that the data processing is justified by compelling legitimate reasons that take precedence over the interests, rights and freedoms of the data subject, or that are necessary for the presentation, enforcement or defense of legal claims are connected.

2. If personal data is processed for direct business acquisition, the data subject is entitled to object at any time to the processing of his/her personal data for this purpose, including profiling, if it is related to direct business acquisition.

3. If the data subject objects to the processing of personal data for the purpose of direct business acquisition, then the personal data may no longer be processed for this purpose.
4. The right mentioned in points 1 and 2 must be specifically brought to the attention of the data subject during the first contact at the latest, and the relevant information must be displayed clearly and separately from all other information.

5. In connection with the use of services related to the information society and deviating from Directive 2002/58/EC, the data subject may also exercise the right to object using automated means based on technical specifications.

6. If personal data is processed for scientific and historical research purposes or for statistical purposes in accordance with Article 89 (1) of the Regulation, the data subject has the right to object to the processing of personal data concerning him for reasons related to his own situation, except if the data management is necessary for the execution of a task carried out for reasons of public interest.
(Regulation Article 21)

Automated decision-making in individual cases, including profiling

1. The data subject has the right not to be covered by the scope of a decision based solely on automated data management, including profiling, which would have legal effects on him or affect him to a similar extent.

2. Point 1 does not apply if the decision:
a) necessary for the conclusion or fulfillment of the contract between the data subject and the Data Controller;
b) it is made possible by EU or member state law applicable to the Data Controller, which also establishes appropriate measures to protect the rights and freedoms and legitimate interests of the data subject; obsession
c) is based on the express consent of the data subject.

3. In the cases mentioned in points a) and c) of point 2, the Data Controller is obliged to take appropriate measures to protect the rights, freedoms and legitimate interests of the data subject, including at least the right of the data subject to request human intervention on the part of the Data Controller, to express his point of view, and file an objection against the decision.

4. The decisions referred to in point 2 cannot be based on the special categories of personal data referred to in Article 9 (1) of the Regulation, unless points a) or g) of Article 9 (2) apply and the rights of the data subject, appropriate measures were taken to protect his freedoms and legitimate interests.
(Regulation Article 22)

Restrictions

1. The EU or Member State law applicable to the Data Controller or data processor may limit the provisions of Articles 12-22 of the Regulation by means of legislative measures. Article and Article 34, as well as Articles 12–22. with regard to its provisions in accordance with the rights and obligations set out in Article 5, the scope of the rights and obligations contained in Article 5, if the restriction respects the essential content of fundamental rights and freedoms, as well as a necessary and proportionate measure for the protection of the following in a democratic society:
a) national security;
b) national defense;
c) public safety;
d) prevention, investigation, detection or prosecution of crimes, as well as the implementation of criminal sanctions, including protection against threats to public safety and the prevention of these threats;
e) other important general public interest objectives of the Union or a Member State, in particular an important economic or financial interest of the Union or a Member State, including monetary, budgetary and tax issues, public health and social security;
f) protection of judicial independence and judicial proceedings;
g) in the case of regulated occupations, the prevention, investigation and detection of ethical violations and the conduct of related procedures;
h) in the cases mentioned in points a)–e) and g) – even occasionally – control, investigation or regulatory activities related to the performance of public authority tasks;
i) the protection of the data subject or the protection of the rights and freedoms of others;
j) enforcement of civil law claims.

2. The legislative measures referred to in point 1 contain, where appropriate, detailed provisions at least:
a) for the purposes of data management or categories of data management,
b) categories of personal data,
c) the scope of the restrictions introduced,
d) guarantees aimed at preventing misuse, unauthorized access or transmission,
e) to define the Data Controller or to define the categories of Data Controllers,
f) for the duration of data storage, as well as applicable guarantees, taking into account the nature, scope and purposes of data management or categories of data management,
g) risks affecting the rights and freedoms of the data subjects, and

h) the right of the data subjects to receive information about the restriction, unless this may adversely affect the purpose of the restriction.
(Regulation Article 23)

Informing the data subject about the data protection incident

1. If the data protection incident likely involves a high risk for the rights and freedoms of natural persons, the Data Controller shall inform the data subject of the data protection incident without undue delay.

2. In the information given to the data subject mentioned in point 1, the nature of the data protection incident must be clearly and comprehensibly described, and at least the information and measures mentioned in points b), c) and d) of Article 33, paragraph (3) of the Regulation must be communicated.

3. The data subject does not need to be informed as mentioned in point 1, if any of the following conditions are met:
a) the Data Controller has implemented appropriate technical and organizational protection measures, and these measures have been applied to the data affected by the data protection incident, in particular those measures - such as the use of encryption - that would be incomprehensible to persons not authorized to access personal data they make the data;
b) after the data protection incident, the Data Controller has taken additional measures to ensure that the high risk to the rights and freedoms of the data subject referred to in point 1 is unlikely to materialize in the future;
c) providing information would require a disproportionate effort. In such cases, the data subjects must be informed through publicly published information, or a similar measure must be taken that ensures similarly effective information to the data subjects.

4. If the Data Controller has not yet notified the data subject of the data protection incident, the supervisory authority, after considering whether the data protection incident is likely to involve a high risk, may order the data subject to be informed or establish that one of the conditions mentioned in point 3 has been met.
(Regulation Article 34)

The right to complain to the supervisory authority

1. Without prejudice to other administrative or judicial remedies, all data subjects have the right to complain to a supervisory authority - in particular in the Member State of their usual place of residence, place of work or suspected infringement - if, in the judgment of the data subject, the personal data relating to them handling violates this regulation.
2. The supervisory authority to which the complaint was submitted is obliged to inform the customer about the procedural developments related to the complaint and its result, including that the customer is entitled to a judicial remedy based on Article 78 of the Decree.
(Regulation Article 77)

The right to an effective judicial remedy against the supervisory authority

1. Without prejudice to other administrative or non-judicial remedies, all natural and legal persons are entitled to an effective judicial remedy against the legally binding decision of the supervisory authority.

2. Without prejudice to other administrative or non-judicial legal remedies, all data subjects are entitled to effective judicial remedies if the competent supervisory authority based on Article 55 or 56 of the Regulation does not deal with the complaint, or does not inform the data subject within three months of the 77 on procedural developments or the result of a complaint submitted pursuant to Article .
3. Proceedings against the supervisory authority must be initiated before the court of the Member State where the supervisory authority is headquartered.

4. If proceedings are initiated against a decision of the supervisory authority in relation to which the Board previously issued an opinion or made a decision within the framework of the uniformity mechanism, the supervisory authority is obliged to send this opinion or decision to the court.
(Regulation Article 78)

The right to an effective judicial remedy against the controller or processor

1. Without prejudice to the available administrative or non-judicial legal remedies, including the right to complain to the supervisory authority according to Article 77 of the Regulation, all data subjects are entitled to an effective judicial remedy if, in their judgment, their personal data has been handled in a way that does not comply with this Regulation your rights under this regulation have been violated.
2. Proceedings against the data manager or data processor must be initiated before the court of the Member State where the data manager or data processor operates. Such a procedure can also be initiated before the court of the Member State of the habitual residence of the person concerned, unless the data controller or the data processor is a public authority of a Member State acting in the capacity of public authority.
(Regulation Article 79)

VIII. CHAPTER
SUBMISSION OF THE APPLICATION OF THE CONCERNED, PROCEDURES OF THE DATA CONTROLLER

1. The Data Controller shall inform the data subject without undue delay, but in any case within one month of the receipt of the request, of the measures taken as a result of his request to exercise his rights.

2. If necessary, taking into account the complexity of the application and the number of applications, this deadline can be extended by another two months. The Data Controller shall inform the data subject of the extension of the deadline, indicating the reasons for the delay, within one month of receiving the request.

3. If the data subject submitted the application electronically, the information must be provided electronically, if possible, unless the data subject requests otherwise.

4. If the Data Controller does not take measures following the data subject's request, it shall inform the data subject without delay, but at the latest within one month of the receipt of the request, of the reasons for the failure to take action, and of the fact that the data subject may file a complaint with a supervisory authority and seek legal remedies with his right.

5. The Data Controller provides information according to Articles 13 and 14 of the Regulation and information about the rights of the data subject (Articles 15-22 and 34 of the Regulation) and measures free of charge. If the data subject's request is clearly unfounded or - especially due to its repeated nature - excessive, the Data Controller, taking into account the administrative costs associated with providing the requested information or information or taking the requested measure:
a) You can charge a fee of HUF 6,350, or
b) may refuse to take action based on the request.
It is the responsibility of the Data Controller to prove that the request is clearly unfounded or exaggerated.

6.If the Data Controller has reasonable doubts about the identity of the natural person submitting the request, it may request the provision of additional information necessary to confirm the identity of the person concerned.

First-Tech Kft. 2018.05.25.