

AGREEMENT ON THE JOINT MANAGEMENT OF PERSONAL DATA

concluded by and between:
WHC d.o.o.
Verovškova ulica 55
SI-1000 Ljubljana
hereinafter referred to as "WHC"

and
Heads Adriatic d.o.o.
Verovškova ulica 55
SI-1000 Ljubljana
hereinafter referred to as "Heads Adriatic"

and
Qonnexa d.o.o.
Verovškova ulica 55
SI-1000 Ljubljana
hereinafter referred to as "Qonnexa"

and
WHC Outsourcing d.o.o.
Verovškova ulica 55
SI-1000 Ljubljana
hereinafter referred to as "WHC Outsourcing"

hereinafter collectively also referred to as "Contracting Parties" or "Contracting Party"

1. Preliminary provisions

WHC is a company that acts as a mediator in the employment of workers, providing both mediation services in the employment of workers and the provision of student work. WHC provides services in cooperation with Heads Adriatic, Qonnexa and WHC Outsourcing.

All four companies are closely interlinked, since they cooperate in the field of personnel recruitment. Due to their close business relationship, the exchange of personal data between companies occurs in the following databases: database of job candidates (hereinafter referred to as the **Candidates database**), database of internal and posted employees (hereinafter referred to as the **Personnel database**) and the database of Data Subjects who perform student work (hereinafter referred to as the **Students database**).

The Contracting Parties process the same (aforementioned) personal databases, jointly determining the purpose and means of processing. Pursuant to Article 26 of the REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC (hereinafter referred to as the "GDPR"), the Contracting Parties shall be considered as joint controllers of personal data in respect of the aforementioned databases.

The Contracting Parties conclude this Agreement on the basis of Article 26 of the GDPR, pursuant to which joint controllers must conclude an agreement to define mutual obligations, in particular when it comes to the exercise of the rights of Data Subjects whose personal data are processed and to the

provision of information to said Data Subjects. The subject of this Agreement is also the establishment of protocols in the event of security incidents, as well as the regulation of contractual processing, the implementation of audits, and the division of responsibilities between the Contracting Parties.

2. Definitions

The Data Subject (hereinafter referred to as the "Data Subject" or "Data Subjects") is any natural person who is identified or identifiable on the basis of personal data processed by the Contracting Parties. In this case, such personal data might mean the Data Subject's name, ID for VAT or any other indicator, e.g. economic, physiological, cultural etc.

Personal information is any information relating to an identified or identifiable individual (hereinafter referred to as the "Data Subject"); an identifiable individual is one who can be identified directly or indirectly, in particular by indicating an identifier such as name, identification number, location data, web identifier, or by indicating one or more factors specific to the physical, physiological, genetic, the mental, economic, cultural or social identity of that individual.

Jointly managed personal data are the personal data processed by the Contracting Parties that are the subject of this Agreement.

Processing means any action or set of actions carried out in connection with personal data or sets of personal data, either with or without the use of automated means, such as collection, recording, editing, structuring, storage, adaptation or alteration, retrieval, viewing, use, disclosure by transmission, dissemination or any other form of access, alignment or combination, restriction, erasure or destruction.

Controller means a natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of processing; where the purposes and means of processing are determined by Union law or the law of a Member State, the Controller or the specific criteria for its designation may be determined by Union law or the law of a Member State.

Joint Controllers are the Parties to this Agreement.

Processor is a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the Controller.

The person responsible for the protection of personal data is a natural person who is employed by an individual Contracting Party (or performs regular work on another contractual basis) and is authorised by the Contracting Party to supervise the protection of personal data with the Contracting Party and communicate with the other Contracting Parties regarding the areas governed by this Agreement.

3. Ensuring compliance with Slovenian and European legislation

Throughout the duration of this Agreement, each Contracting Party must ensure that its operation is in accordance with the applicable Slovenian and European legislation in the field of personal data protection.

Each Contracting Party is obliged to appoint a person responsible for the protection of personal data within its company. The key functions performed by the person responsible for the protection of personal data are: exercising control over the processing of personal data in the company, exercising control over the implementation of the provisions of this Agreement, and resolving individual requests for the protection of personal data in accordance with this Agreement. Said person is appointed by the CEO of each of the Contracting Parties. These persons are responsible for the communication between the Contracting Parties in connection with the execution of this Agreement.

The Contracting Parties agree that the person responsible for the protection of personal data within each Contracting Party is:

- For WHC: Anita Brovč, Personal Data Protection Officer, data-protection-officer@whc-slovenia.com
- For Heads Adriatic: Anita Brovč, Personal Data Protection Officer,

- data-protection-officer@whc-slovenia.com
- For Qonnexa: Anita Brovč, Personal Data Protection Officer, data-protection-officer@whc-slovenia.com
- For WHC Outsourcing: Anita Brovč, Personal Data Protection Officer, data-protection-officer@whc-slovenia.com.

Purposes of personal data processing

This point of the Agreement sets out the purposes for which the processing of personal data that is the subject of this Agreement is permitted.

The joint processing of personal data subject to this Agreement is necessary to ensure the fulfillment of the personal data processing purposes.

The personal data processing purposes are set out in the list below:

- Personalised communication with Data Subjects regarding the provision of our services through SMS messages, phone calls and e-mail messages.
- Marketing communications.
- Customised marketing communications.
- Provision of employee placement services to other contracting entities and related activities (provision of labor and posting of employees).
- Search and selection of personnel.
- Performing recruitment services.
- Enabling the possibility of sending an application into a database of job seekers.
- Enabling the possibility of applying for a job vacancy and performing appropriate activities for the requirements of each individual job vacancy (including sending information to the employer and carrying out the potential employment process).
- Issuing referrals and informing by e-mail about income, income tax and other work-related data of each Data Subject.
- Enabling electronic registration and enrollment.
- Enabling personal registration in Mjob branches.
- Communication related to questions, complaints or other general objections.
- Concluding the contract and complying with the obligations arising from the concluded contract.
- Performing statistical analysis for the use of the website.
- Sending personal data to third parties.
- Enforcing legal claims, protecting our own rights, and resolving disputes.
- Legal obligations.

The Contracting Parties agree that the aforementioned list of processing purposes constitutes a complete list of processing purposes for which jointly managed personal data may be processed. Any processing of jointly managed personal data for any purposes other than those specified in the list above constitutes overprocessing.

In the event that any of the Contracting Parties would like to process jointly managed personal data for purposes other than those defined in this Agreement, said Contracting Party must propose an amendment to this Agreement. An amendment to the Agreement is possible if all Contracting Parties agree to the amendment.

In the event that an additional purpose of processing is included within the scope of this Agreement, each Contracting Party is obliged to inform Data Subjects of said additional purpose of processing. Data Subjects are considered to have been duly informed if the Contracting Parties define an additional purpose within the existing Privacy Policy in force within each of the Contracting Parties. For the avoidance of doubt, the Contracting Parties further clarify that said Privacy Policy is any document containing all prescribed information regarding the processing and protection of personal data of Data Subjects which is published and accessible to Data Subjects.

The collection and/or processing of personal data for an additional purpose must be carried out in accordance with the legislation and meet all legal requirements (e.g. provision of the appropriate legal basis, relaying of all information to the Data Subjects, etc.). The details of the conditions for lawful processing are set out in point 6 of this Agreement. Each Contracting Party is obliged to ensure that all legal prerequisites for the lawful processing of personal data for an additional purpose are met, and bears full responsibility in any event of non-fulfillment of these obligations.

Jointly managed personal data

This point of the Agreement defines the categories of personal data that are the subject of this Agreement and represent the jointly managed personal data, as well as the storage and processing of this data.

Categories of jointly managed personal data

The Contracting Parties agree to process personal data from three databases (**the Personnel database, the Candidates database and the Students database**) as joint controllers.

Within the Personnel database, the Contracting Parties process the following categories of personal data:

- **Identification data** (first name, last name, date of birth, PIN, gender, ID for VAT, current account number)
- **Contact data** (address, phone number, e-mail address)
- **Sensitive personal data** (information on national origin, union membership, data from criminal and other records, data obtained through psychological tests, data from the CV sent by the Data Subject)
- **Communication data** (date, time and content of each correspondence)
- **Employment-related data** (company, place of employment, job position, previous experience)
- **Education-related data** (degree of education, field of education)
- **Data obtained from the Health Insurance Institute of Slovenia and the Pension and Disability Insurance Institute of Slovenia**

Within the Candidates database, the following categories of personal data are processed:

- **Identification data** (first name, last name, date of birth, PIN, gender, ID for VAT, current account number)
- **Contact data** (address, phone number, e-mail address)
- **Sensitive personal data** (information on national origin, union membership, data from criminal and other records, data obtained through psychological tests etc.)
- **Communication data** (date, time and content of each correspondence)
- **Employment-related data** (company, place of employment, job position, previous experience)
- **Education-related data** (degree of education, field of education)

Within the Students database, the following categories of personal data are processed:

- **Identification data** (first name, last name, date of birth, PIN, gender, ID for VAT, current account number)
- **Contact data** (address, phone number, e-mail address)
- **Schooling-relation data** (school and year of schooling)
- **Education-related data** (degree of education, field of education)
- **Certificate confirming the status of a high school/university student**
- **Information from the Data Subject's profile** (work area, work field, foreign language knowledge, mobility, knowledge in the field of IT, information about any additional skills and qualifications)

Storage and processing of jointly managed personal data

The jointly managed personal data are located in the following locations:

- on the servers of each of the Contracting Parties, and
- at the business premises of all Contracting Parties, in physical form.

The Contracting Parties shall establish the following regime of access to jointly managed personal data:

- a) WHC has access to all jointly managed personal data. WHC has the right to process personal data located on Workforce servers, as well as personal data located on the servers of the remaining Contracting Parties. The Contracting Parties must provide Workforce with access to such personal data upon request by Workforce. Workforce has unlimited access to personal data stored in physical form by WHC at its business premises. WHC shall also have unrestricted access to personal data held in physical form by the Contracting Parties who shall, at the request of the WHC, be obliged to provide copies or originals of such personal data.
- b) The Contracting Parties have limited access to the personal data held on their servers and/or in physical form at the business premises of WHC. The Contracting Parties have the right to inspect personal databases, but can only perform changes, deletions and other interventions in the databases for the personal data that they have entered into the database themselves. Exceptionally, the right to those interventions may be granted to an individual Contracting Party of WHC.
- c) The contracting parties have the right to send personal data to each other, as well as to WHC.

6 Lawful and fair processing of personal data

Contracting Parties agree that, as joint controllers, they have the obligation to ensure the lawful, fair, and transparent processing of personal data, which is specified in further details in the sections below.

5.1. Lawfulness of processing

The Contracting Parties must ensure that the processing of jointly managed personal data is in accordance with the provisions of this Agreement and the applicable legislation in the field of personal data protection and information security.

Each Contracting Party is obliged to ensure that the jointly managed personal data are obtained in a lawful manner, which means that each Contracting Party must establish an appropriate legal basis and the purposes for the processing of personal data, and guarantee that the personal data collected by it are not excessive or irrelevant for the achievement of said purposes (i.e. that no excessive processing of personal data has occurred through the collection of data).

The Contracting Party that has collected jointly managed personal data bears full responsibility for the legality of the personal data it has collected. In the event of a procedure before a supervisory authority, the Contracting Party that has collected jointly managed personal data must defend the processing of personal data. In the event that the supervisory authority finds, during the inspection procedure, that unlawful processing of personal data has occurred, the Contracting Party that collected such personal data must delete the unlawful personal data immediately.

If any of the Contracting Parties would process jointly managed personal data for purposes other than those defined in this Agreement, the Contracting Party conducting such processing shall be solely responsible for any consequences of such processing (including compensation for any damage and payment of fines).

If any of the Contracting Parties finds that another Contracting Party has committed irregularities in the implementation of the Agreement, the Contracting Party is obliged to immediately notify the other Contracting Party of such irregularities. The notification referred to in this paragraph must be made in writing. The Contracting Party that received the notification of irregularity must examine and explain the described situation. The explanation and the intended steps to eliminate the irregularity shall be forwarded by the Contracting Party at fault to all other Contracting Parties.

If the Contracting Party fails to remedy the violation within 14 working days, WHC has the right to restrict its access to jointly managed personal data until the violation is remedied.

5.2. The provision of information to Data Subjects

The Contracting Parties undertake to prepare a Privacy Policy defining all the necessary information for Data Subjects required by the applicable legislation. The Privacy Policy must be written in clear, understandable, and concise language. The Contracting Parties undertake to make the Privacy Policy available to the public, and thus enable Data Subjects to become acquainted with the information on the processing of personal data. The Contracting Parties agree that the appropriate method of notification is the publication of the Privacy Policy on the website of each of the Contracting Parties. Each Contracting Party shall bear full responsibility to ensure that, during personal data collection, Data Subjects are provided all necessary information as defined by applicable law (at the time of entering into this Agreement, this is mainly represented by Articles 12, 13 and 14 of the GDPR). When collecting personal data, each Contracting Party must inform Data Subjects of the existence of joint management of personal data, and provide them with relevant information on the course of joint management as defined in this Agreement. Each Contracting Party must inform Data Subjects at the time of personal data collection.

5.3. The provision of the content of the Agreement to Data Subjects

The Contracting Parties undertake to make the content of the Agreement available to Data Subjects processed in the framework of this Agreement.

For this purpose, WHC will prepare an Abstract of this Agreement, which will summarize the key provisions of the Agreement. Each Contracting Party must ensure that such an Abstract is published on its website. For the avoidance of doubt, the Contracting Parties hereby clarify that the websites in question are as follows:

- For WHC: <https://www.whc-slovenia.com/>
- For Heads Adriatic: <https://www.headsadriatic.com/>
- For Qonnexa: <https://www.qonnexa.com/>
- For WHC Outsourcing:

If any of the Contracting Parties changes the website specified in this Agreement, this Contracting Party must notify all other Contracting Parties of its new website within three working days from the date of such change of website.

6. Rights of Data Subjects

Data Subjects have certain rights regarding the processing of their personal data, which are further defined in the Privacy Policy of each of the Contracting Parties. Data Subjects exercise their rights through requests they make to the Contracting Parties (hereinafter referred to as "Data Subject's Request").

6.1. Enforcing Data Subject's Requests

The Contracting Parties agree that Requests shall be received through the single point of contact defined in point 7.2. below. Requests thus submitted are received by the WHC and sent to each of the Contracting Parties for resolution. If the Contracting Party receives the Data Subject's Request separately from the single point of contact, this Contracting Party is also responsible for the execution of the request and appropriate communication with the Data Subject. The Contracting Party must notify the remaining Contracting Parties of any such request received through contacts defined in point 3.1. of this Agreement.

The Contracting Parties agree to assist each other in the execution of the Data Subject's Requests, especially when an individual Data Subject's Request is extensive. Each Contracting Party shall provide assistance to the other Contracting Party in the manner and to the extent most appropriate in each individual case.

After receiving the Data Subject's Request for deletion or transfer of personal data, WHC must examine the request and, in the event that the Data Subject's Request must be complied with, ensure the

deletion or transfer of personal data. WHC shall notify the Contracting Party concerned of the fulfillment of the Request, while also providing appropriate instructions on how to proceed. All assistance provided by the Contracting Parties in fulfilling Data Subject's Requests shall be provided free of charge.

6.2. Points of contact for enforcing Data Subject's Requests

WHC must establish a single point of contact through which Data Subjects can exercise their rights and submit Requests; said single point of contact must be used by all Contracting Parties.

The Contracting Parties agree to designate the e-mail address data-protection-officer@whc-slovenia.com, as the single point of contact.

WHC, which has access to the single point of contact, redirects the received Requests and questions to Contracting Parties concerned by the Request.

Each Contracting Party must publish the aforementioned contacts on its website, as well as in a document providing information on the processing of personal data to Data Subjects (hereinafter referred to as the Privacy Policy). The Contracting Parties must clearly define that the contacts are intended for the exercise of rights of Data Subjects. The Contracting Parties must also ensure that the contacts are easily accessible.

7. Retention period

The Contracting Parties undertake to keep the jointly managed personal data for the period necessary to fulfill the purposes of processing, as set out for each purpose of processing in the Privacy Policy of each Contracting Party (hereinafter referred to as the "retention period"). For greater transparency, the Contracting Parties set out the retention periods in Annex 2 of this Agreement.

After the expiry of the retention period, the Contracting Parties must ensure the effective deletion of jointly managed personal data or the anonymisation of such personal data. Deletion or anonymisation must be carried out in such a way that the reconstruction of personal data is impossible.

WHC must ensure the deletion or anonymisation of jointly managed personal data stored on its servers, as well as of any jointly managed personal data stored in physical form at the business premises of WHC.

Each of the Partners must ensure the deletion or anonymisation of jointly managed personal data stored on its servers, as well as of any jointly managed personal data stored in physical form at the business premises of each individual Partner, taking into account the procedure defined below.

Before deleting jointly managed personal data, each of the Partners must inform WHC, which has the possibility to object to such deletion if it is of the opinion that deletion or anonymisation is not necessary. In the event of a veto objection, the Partner may not proceed with deletion or anonymisation.

In the event of the termination of any of the Partners, such Partner shall be obliged to provide WHC with all jointly managed personal data located on its servers or at its business premises, and ensure the effective and permanent destruction of any copies of jointly managed personal data. The Partner must delete or anonymise all jointly managed personal data related to the deleted company, unless the retention of such personal data is required by law.

8. Transfer of jointly managed personal data

The Contracting Parties agree that transfers and disclosures of jointly managed personal data between the Contracting Parties will be carried out using appropriate technological methods and procedures, so that jointly managed personal data will be protected against any loss, unauthorized disclosure, or interference and destruction. The Contracting Parties agree that the transfer and protection of Personal Data shall be carried out in accordance with the provisions of the Rules on the Protection of Personal Data applicable to WHC. Each Contracting Party shall be fully responsible for any of its

transfers and/or disclosures of jointly managed personal data, which includes the responsibility for the payment of any fines set by penal authorities.

Contracting Parties agree that the processing of jointly managed personal data will result in the disclosure of such data to third parties or in the processing of such data by third parties. For greater clarity, the Contracting Parties agree that contractual processors engaged by any of the Contracting Parties, as well as State authorities that could request jointly managed personal data from the Contracting Parties based on their powers, shall be considered as third parties.

Each Contracting Party is free to decide whether to hire a contractual processor for the processing of jointly managed personal data. The Contracting Parties agree that they must disclose their contractual processors to the remaining Contracting Parties. Each Contracting Party must disclose its contractual processors before signing this Agreement and at any time during the validity of the Agreement, at the request of any Contracting Party. A list of the contractual processors that are currently engaged by any of the Contracting Parties can be found in Annex 1 below. Each Contracting Party undertakes to notify any change of its contractual processors within 14 working days.

Each Contracting Party is obliged to ensure that the contractual processors engaged by said Contracting Party comply with the applicable legislation in the field of personal data protection, and to ensure that the relations with the contractual processors are contractually regulated in an adequate manner. The Contracting Party that hired the contractual processor bears full responsibility for its activities (including any omissions). In the event that other Contracting Parties suffer damage as a result of a breach caused by the Contracting Party, the Contracting Party in breach shall be obliged to fully compensate for this damage, including any loss of profit suffered by the Contracting Parties.

In the event of any doubts regarding the individual transfer or disclosure of jointly managed personal data, the Contracting Party wishing to perform the transfer or disclosure must consult with the person responsible for the protection of personal data acting in the framework of each Contracting Party.

9. Security incidents

The Contracting Parties agree that the following events shall be considered as security incidents for the purposes of this Agreement:

- a) loss or imminent loss,
- b) unauthorised treatment,
- c) unauthorised disclosure or transfer,
- d) any other unlawful interference with jointly managed personal data.

In the event of a security incident, each Partner must notify WHC of the incident. The notification must contain a description of the security incident and the identification of any consequences caused by the security incident.

In the event of a security incident, each Contracting Party is obliged to comply with the law and notify the Information Commissioner within 72 hours of the security incident and, where necessary, inform the Data Subjects where the security incident occurred.

Final provisions

Guarantee. Each Contracting Party must compensate the other Contracting Party against any liability, loss, or costs (including any direct or indirect damage, loss of profit or damage to goodwill, taking into account all costs of any fines, legal advice, and interest rates, as well as any other reasonable business damage or costs) suffered by the other Contracting Party due to or in connection with claims regarding any breach of this Agreement by the Contracting Party.

Period of validity. This Agreement is concluded for an unlimited period. The Agreement shall be terminated in the event of termination of the existence of any of the Contracting Parties. This Agreement shall enter into force when it is signed by all Contracting Parties.

Withdrawal from the Agreement. The Contracting Parties conclude this Agreement on the basis of the legislation, which is why it is not possible to withdraw from this Agreement. Withdrawal from the

Agreement is only possible in the event of the termination of the existence of any of the Contracting Parties.

Force majeure. Contracting Parties shall not be liable for any damage arising from the delay or non-fulfillment of a certain obligation of the Contracting Parties arising from this Agreement, if the delay or non-fulfillment occurred due to force majeure. Events of force majeure are events that are outside of the influence of the Contracting Parties, such as natural disasters, wars, strikes, etc. Each Contracting Party must notify the other Contracting Parties of the occurrence of force majeure immediately or as soon as possible, and determine whether there may be any delay or non-fulfillment of certain obligations due to the occurrence of force majeure.

Severability of provisions. In the event that any provision (or part of a provision) of this Agreement is declared illegal, void, or invalid, that provision (or part of a provision) shall be deemed not to be an integral part of this Agreement, and its invalidity shall not affect the validity and enforceability of the remaining provisions of this Agreement.

Notices. The Contracting Parties agree to send all notices related to this Agreement using the following contact details:

WHC: data-protection-officer@whc-slovenia.com

Heads Adriatic: data-protection-officer@whc-slovenia.com

Qonnexa: data-protection-officer@whc-slovenia.com

WHC Outsourcing: data-protection-officer@whc-slovenia.com

Jurisdiction. The Contracting Parties agree to settle all disputes arising out of this Agreement in an amicable manner. If an amicable settlement of the dispute is not possible, the court in Ljubljana shall have the necessary jurisdiction to settle the dispute.

Amendments to the Agreement. Amendments to this Agreement may be made in writing, as an annex to the Agreement. An amendment to the Agreement is valid when it is signed by all Contracting Parties. Partners agree that WHC has the right to restrict access to jointly managed personal data to each of the Partners until said Partner has accepted an individual amendment to the Agreement.

Copies. This Agreement shall be drawn up in triplicate, one copy of which shall be given to each of the Contracting Parties.

Za WHC:

- FIRA, Bled, d.o.o.
- Tone Skok s.p.
- Ilab d.o.o.
- Manca Uršič Rosas s.p.
- Jan Štovičej s.p.
- Sonrisa Informatikai Kft.
- Codeup d.o.o.

Za Heads Adriatic:

- n.a.

Za Qonnexa:

- H&P Solutions, Rok Švajger s.p.

Za WHC Outsourcing:

- n.a.

Annex 2: Retention periods

Purpose for which the personal data is collected	Retention period
Personalised communication regarding the provision of our services through SMS messages, phone calls and e-mail messages.	Until consent is revoked
Marketing communications	Until consent is revoked
Customised marketing communications	Until consent is revoked
Search and selection of personnel	For the entire duration of the Agreement and for 5 years after its termination.
Performing recruitment services.	For the entire duration of the Agreement and for 5 years after its termination.
Provision of employee placement services to other contracting entities and related activities	For the entire duration of the Agreement and for 5 years after its termination. The data required by law is retained permanently.
Enabling the possibility of registering into a database of job seekers	Until consent is revoked
Enabling the possibility of applying for a job vacancy	Until the end of the job vacancy and for 2 years after the job vacancy
Enabling electronic registration and enrollment	Until consent is revoked
Issuing of referrals	For the entire duration of the Agreement and in accordance with the deadlines stipulated by the applicable legislation.
Enabling personal registration in Mjob branches.	Until consent is revoked
Communication related to questions, complaints or other general objections	6 months from the first communication
Concluding the contract and complying with the obligations arising from the concluded contract	For the entire duration of the Agreement and for 5 years after its termination.
Informing by e-mail and through other communication channels about income, income tax and other work-related data of each Data Subject	Until consent is revoked
Performing statistical analysis for the use of the website	Within the deadlines set out in point 10 of this Agreement in which individual cookies are defined
Enforcing legal claims, protecting rights, and resolving disputes	In accordance with the deadlines stipulated by the applicable legislation
Legal obligations	In accordance with the deadlines stipulated by the applicable legislation