IMPORTANT NOTES TO PROCESS MANAGERS AND PROCESSING PERFORMERS REGARDING THE APPLICATION OF THE GENERAL DATA PROTECTION REGULATION NO. 2016/679

Who is the head of personal data processing?

Natural or legal person, public authority, agency or other body which alone or together with others determines the purposes and means of personal data processing.

Examples of processing managers: companies or trades that process the data of their employees; financial institutions that process the personal data of their clients / clients; associations that process the data of their members; schools or colleges that process the personal data of pupils, students or teachers / their employees; hospitals that process the personal data of their patients; state bodies or bodies of local / regional self-government units that process personal data of citizens.

Who is the executor of the processing?

Natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller. The processing carried out by the executor of processing is regulated by a contract or other legal act.

Examples of processing executors: bookkeeping service that processes data on employee salaries for the employer; companies authorized to provide private protection; receivables collection agencies based on a concluded business cooperation agreement.

IMPORTANT!

the processing manager is NOT OBLIGED to have a processing executor

The General Regulation allows the controller to entrust the controller with the performance of only certain precisely contracted tasks in the name and on behalf of the controller

a contract or other legal act requires detailed regulation of mutual rights and obligations between the controller and the processor

the processor must guarantee the protection and confidentiality of the processing of personal data

the processor is obliged to implement appropriate protection measures in order to ensure and be able to prove that the processing is carried out in accordance with the General Regulation

With regard to the application of the General Data Protection Regulation no. 2016/679 (hereinafter: the General Regulation) we draw attention to the following basic obligations of the processing manager and the processing executor:

What steps must be met in order for processors and processors to comply with the General Data Protection Regulation?

PROVISION OF INFORMATION TO RESPONDENTS FOR THE PURPOSE OF EXERCISING THEIR RIGHTS (Articles 12-21 of the General Regulation)

IMPLEMENTATION OF APPROPRIATE TECHNICAL AND ORGANIZATIONAL MEASURES FOR THE PROTECTION OF PERSONAL DATA (Articles 25 and 32 of the General Regulation)

KEEPING RECORDS OF PROCESSING ACTIVITIES (Article 30 of the General Regulation)

APPOINTMENT OF DATA PROTECTION OFFICERS (Article 37 of the General Regulation)

DATA PROTECTION IMPACT ASSESSMENT (Article 35 of the General Regulation)

PROVISION OF INFORMATION FOR THE PURPOSE OF EXERCISING THE RIGHTS OF RESPONDENTS

What information and in what way is the processing manager obliged to give to the respondent?

Respecting the principle of transparency, the controller is obliged to provide the respondent with all information on the processing of his personal data in a concise, understandable and easily accessible form, using clear and simple language and to acquaint him with his rights under the General Regulation. (right to information, right of access, right to rectification and erasure, right to limit processing, right to portability, right to object and automated decision making).

At the time of collecting personal data, the processing manager is obliged to provide the respondent with information:

- about your identity (contact details of the processing manager)
- about the data protection officer (contact details of the officer)
- be acquainted with the purpose and legal basis for the processing of personal data
- on recipients or categories of recipients of personal data (for example: HZZO, HZMO)
- on the transfer of personal data to a third country or international organization (non-EU)
- on legitimate interest (for example: sending newsletters to service users, monitoring the work of employees via GPS system if the work is performed outside the employer's business premises)
- on the time limit for storing personal data and the criteria for determining the period of storage (for example: records of employees are kept permanently by the employer, while the organizer of the prize game is obliged to delete / destroy participants' personal data after its completion -
- the existence of the right to request access to personal data from the controller, correction, deletion of personal data or

restriction of processing relating to him, the right to object to the processing of such data and the transferability of his data to another controller

- the right to withdraw consent at any time, without prejudice to the lawfulness of processing based on consent before it is withdrawn

- on the right to file a complaint to the supervisory body (Agency for Personal Data Protection)

- whether the provision of personal data is a legal or contractual obligation or condition necessary for concluding a contract and whether the respondent has an obligation to provide personal data and what are the possible consequences if such data are not provided (for example: concluding an employment contract)

- the existence of automated decision-making, which includes the development of profiles and meaningful information on the logic involved, as well as the importance and anticipated consequences of such processing for respondents (for example: client profile development by credit institutions to determine their creditworthiness or the habit of customers and creating profiles for the purpose of marketing offers)

If personal data have not been obtained from the respondent, the controller is obliged to provide the respondent with information on the source of personal data in addition to the above.

IMPORTANT!

Creating privacy policies

In order to achieve legality and transparency of personal data processing and provide information related to personal data processing and thus exercise the rights of respondents: the right to access data, the right to correct inaccurate data, the right to delete data, the right to limit data processing, the right to data portability and the right to object to the processing of personal data, the controller must explain in detail which types of personal data are collected, for what purpose and on what legal basis, how personal data are used, ie who uses personal data and which personal data protection measures are undertake.

It is necessary to harmonize internal acts related to labor relations with the provisions of the General Regulation on Data Protection

It is necessary to harmonize internal acts related to labor relations, ie harmonize / provisions of internal acts related to personal data protection which will include in a comprehensive and clear way the information that the controller is obliged to provide to the respondent at the time of personal data collection (standards referred to in Articles 13 and 14 of the General Regulation).

IMPLEMENTATION OF APPROPRIATE TECHNICAL AND ORGANIZATIONAL PROTECTION MEASURES

Undertaking and implementing appropriate technical and organizational protection measures aims to ensure the security and confidentiality of personal data processing, ie to prevent unauthorized access or unauthorized disposal of personal data and technical equipment used by controllers and executors. Appropriate protection measures ensure that personal data are not automatically available to an unlimited number of persons who are not authorized to process them. Depending on the nature / scope, scope and purpose of the processing of personal data, it is the responsibility of each controller to determine the protection measures that guarantee safe, fair and lawful processing of personal data and the effective application of data protection principles. take into account the necessity of data processing for each specific purpose, reducing the amount of data collected as well as the scope of data during processing, determining data retention periods, their availability, etc.).

IMPORTANT (Agency recommendation)!

the paper document containing the personal data of the processing manager is obliged to store it, for example in lockers or locked drawers which will be under the supervision of authorized persons of the processing manager

access to personal data stored in electronic form should be enabled using a username and password

making backups by authorized persons

signing confidentiality statements of persons who are processing personal data

pseudonymization or encryption of personal data, especially in the case of special categories (eg health data)

recording access to data

KEEPING RECORDS OF PROCESSING ACTIVITIES

Who is obliged to keep records of processing activities?

Each controller or processor, if applicable, shall keep a record of the processing activities for which he is responsible in order to demonstrate the compliance of the processing with the General Regulation.

IMPORTANT!

However, regardless of the number of employees, each processing manager / executor is OBLIGED to keep records of processing if one of the following conditions is met:

if the processing is likely to pose a high risk to the rights and freedoms of respondents (for example: introduction of new technologies such as biometric readers, face recognition, IT services that process personal data)

if the processing is not occasional, or if the processing is permanent (for example: processing of personal data of employees for the purpose of payment of wages by the employer)

if the processing includes special categories of data (for example: health data processed by the hospital, biometric data, genetic data)

if the processing includes personal data relating to criminal convictions and criminal offenses

The stated obligation does not apply to the controller / processor if it has less than 250 employees and if none of the above conditions is applicable.

What is the record of processing activities, what does it have to look like and what does it have to contain?

Records of processing activities are a form that serves as proof that the processing of personal data is lawful. It must contain the information referred to in Article 30 of the General Regulation and must be in writing, including in electronic form. The data contained in the processing records should be adequately protected (for example: centralized database, introduction of authorization and access control measures).

Content of records of processing activities (detailed content):

- name and contact details of the processing manager (for example: name of the legal entity and contact)
- purpose of processing (explained in detail)
- description of the category of respondents (for example: data on workers, data on patients) and the category of personal data (for example: name, surname, residential address, etc.)
- categories of recipients (including those in third countries or international organizations)
- transfer of personal data to third countries or international organizations - deadlines for deleting various categories of data (deadlines for keeping personal data, and the name and provisions of the law if it is determined by a special law)
- description of technical and organizational measures for personal data protection

SPECIAL NOTE!

According to the General Regulation on Data Protection, data controllers are not obliged to submit the records of personal data processing to the Personal Data Protection Agency (formerly the Central Register of Records on Personal Data Collections), but records of water processing activities in writing, including electronic made available at the request of the supervisory body (Agency for Personal Data Protection).

APPOINTMENT OF DATA PROTECTION OFFICER

Who is obliged to appoint a personal data protection officer?

The head of processing and the executor of processing are obliged to appoint a data protection officer in the following cases if:

Processing is carried out by a public authority or a public body, except for courts operating within their jurisdiction

The main activities of the processing manager or the processing executor consist of processing procedures which, due to their nature, scope or purpose, require regular and systematic monitoring of the respondents to a large extent.

The main activities of the controller or processor consist of extensive processing of special categories of data (Article 9 of the Regulation) and personal data related to criminal convictions and criminal offenses (Article 10 of the Regulation).

IMPORTANT!

may be an employee of the organization (processing manager or processor) in which he was appointed, but a person who is not an employee of the organization on the basis of an employment contract (external employee) may also be appointed an official

the controller may appoint one data protection officer provided that it is readily available from each establishment

when appointing an official, take into account that there is no conflict of interest (take into account that such a person does not participate in decision-making determining the purpose and manner of processing personal data)

the controller / processor is obliged to make a Decision on the appointment of officials in accordance with the General Regulation, taking into account professional qualifications (professional knowledge and practice in the field of personal data protection)

the controller / processor is obliged to publish the contact details of the data protection officer and communicate them to the supervisory body (Personal Data Protection Agency).

More detailed information about the Personal Data Protection Officer can be found at

http://azop.hr/info-servis/detaljnije/smjernice.

DATA PROTECTION IMPACT ASSESSMENT

What is an impact assessment?

Data protection impact assessment is one of the procedures for establishing and proving compliance with the General Regulation, ie it is designed to describe processing, assess its necessity and proportionality and provide assistance in

managing risks to the rights and freedoms of individuals arising from personal data processing.

In which cases is a data protection impact assessment necessary?

If it is likely that some type of processing, in particular the use of new technologies, taking into account the nature, scope, context and purposes of processing, will pose a high risk to the rights and freedoms of individuals, the processing manager protection of personal data.

Data protection impact assessment is mandatory in particular in the case of:

Systematic and comprehensive assessments of personal aspects of individuals based on automated processing, including profiling and on the basis of which decisions are made that produce legal effects relating to the individual or similarly significantly affecting the individual

Extensive processing of special categories of personal data (Article 9 (1) of the Regulation) or data relating to criminal convictions and criminal offenses (Article 10 of the Regulation)

Systematic monitoring of the publicly accessible area to a large extent

EXAMPLES OF TREATMENT WHEN IMPACT ASSESSMENT IS NECESSARY:

A hospital that processes the genetic and health data of its patients (hospital information system).

EXAMPLES OF PROCESSING WHEN IMPACT ASSESSMENT IS NOT NECESSARY:

Processing of personal data of patients of individual physicians and healthcare professionals.

IMPORTANT!

The list of types of processing procedures that are subject to the request for data protection impact assessment can be found on the website https://azop.hr/aktualno/detaljnije/odluka-o-uspostavi-i-javnoj-objavi-popisa-vrsta-postupaka-obrade -which-vile.

At what point is a data protection impact assessment needed to be conducted?

A data protection impact assessment should be carried out before the processing of personal data in order to respect the principles of technical and integrated data protection. However, if the processing process is dynamic and subject to constant change, the data protection impact assessment is carried out continuously, not once.