4/16/2021

The Agency for Personal Data Protection has received a submission related to the collection of data on the number of employees interested in vaccination, employed in legal entities within the activities of your department, by priority, and requested by the Croatian Institute of Public Health. Namely, from the presentation of the attached letter from your institution sent to the administrative departments responsible for activities from your department in the counties, it is clear that the delivery of data of employees (all institutions of activities from your department) interested in vaccination is requested by filling in the submitted Excel a table containing the following range of employee personal information: name, surname, date of birth, OIB, MBO, cell phone number, email address. It was also stated that the completed Excel spreadsheets should be forwarded to your institution by e-mail.

Accordingly, the Personal Data Protection Agency as an independent state supervisory body in the field of personal data protection in the Republic of Croatia in accordance with Article 57 (1) (d) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on protection individuals with regard to the processing of personal data and on the free movement of such data and the repeal of Directive 95/46 / EC (General Data Protection Regulation) OJ L119, makes the following recommendation regarding the processing of personal data in this case.

Article 5 of the General Data Protection Regulation prescribes the basic principles applicable to the processing of personal data (principle of lawfulness of processing, principle of accuracy of data, principle of limiting the purpose of processing, principle of reducing the amount of data, principle of data retention and integrity and confidentiality).

Article 6 of the General Data Protection Regulation stipulates that the processing of personal data is lawful only if and to the extent that at least one of the following is met: the respondent has consented to the processing of his personal data for one or more special purposes; processing is necessary for the performance of the contract to which the respondent is a party or in order to take action at the request of the respondent prior to the conclusion of the contract; processing is necessary to comply with the legal obligations of the processing manager; processing is necessary to protect the vital interests of the respondent or other natural person; processing is necessary for the performance of a task of public interest or in the performance of the official authority of the controller; processing is necessary for the legitimate interests of the processing manager or a third party.

We emphasize that in any case for the processing of personal data, and in this particular case for the collection and further

processing of personal data of employees, there must be a legitimate purpose and legal basis under Articles 5 and 6 of the General Data Protection Regulation.

Furthermore, in the present case, it follows that the processing of personal data of employees is based on consent as a legal basis under Article 6 of the General Data Protection Regulation.

In this regard, we emphasize that it is necessary to take into account the conditions of consent, especially that it is a voluntary, special, informed and unambiguous expression of the wishes of the respondent by which he gives a statement or clear affirmative action consent to the processing of personal data. paragraph 1 (11) of the General Data Protection Regulation).

Pursuant to Article 7 of the General Data Protection Regulation, when processing is based on consent, the controller must be able to prove that the respondent has given consent to the processing of his personal data and the respondent has the right to withdraw his consent at any time.

Furthermore, respecting the principles of fair and transparent processing, we emphasize that the duty of the controller is to provide respondents (in this case employees) in accordance with Article 13 of the General Data Protection Regulation, if personal data are collected from respondents, provide all information about the processing of their personal data. for example: on one's identity, on the Data Protection Officer, on the purpose and legal basis for the processing of personal data, on the recipients or categories of recipients of personal data) in a concise, understandable and easily accessible form, using clear and simple language with their rights under the General Data Protection Regulation.

Furthermore, by looking at the official website of the Ministry of Health, more precisely the platform for applying for vaccination against COVID-19 (https://cijepise.zdravlje.hr), it is clear that when applying for vaccination the following range of personal data is collected: OIB or MBO, date of birth, municipality of residence and e-mail address, while information on telephone number and mobile phone number are optional.

In this regard, we emphasize that the processing of personal data must adequately apply the principles of personal data processing referred to in Article 5 of the General Data Protection Regulation, in particular the principle of reducing the amount of data.

Therefore, in this particular case, we consider it appropriate to collect personal data to the extent and in the same way as on the official website of the Ministry of Health, namely the COVID-19 vaccination application platform as mentioned above, especially regarding mandatory and optional data. as well as information about it (markings).

Also, in accordance with Articles 24 and 32 of the General Data Protection Regulation, the controller is required to implement appropriate technical and organizational protection measures to ensure the effective application of data protection principles, such as data reduction and the application of appropriate personal data protection measures. could prove that the rights of the respondents are protected, ie that the processing of personal data is carried out in accordance with the General Data Protection Regulation.

In this regard, we would like to point out that the exchange of personal data by e-mail (without additional protection measures) from the aspect of personal data protection is a very insecure way of communication and data exchange because e-mail travels from sender to recipient in easy-to-read form. a series of points in an e-mail communication channel over which neither the sender nor the recipient has control. Therefore, for the submission of personal data (in this case Excel spreadsheets containing personal data of employees) by e-mail, the Agency also makes recommendations regarding the aspect of security and protection of personal data, as follows:

all attachments / files, ie accompanying documentation to be sent by e-mail must first be "packaged", ie compressed by one of the compression programs, which has the ability to encrypt its contents with a password of high complexity and algorithm for encryption of high complexity encryption and just "packed" and encrypted files are attached as e-mail;

It is recommended to use the following recommendations when creating a password:

A secure password should contain uppercase and lowercase letters (az, AZ).

A secure password should contain digits (0-9).

A secure password should contain special characters (@ # $% ^ * () _ + | ~ - = `{} []:”; ‘, / ?.).

A secure password must be at least 10 characters long. The more, the better.

A secure password should not contain words - regardless of language, dialect, jargon or the like.

A secure password should not contain personal information such as personal names of family members, pet names, addresses, dates of birth, and the like.

it is recommended to deliver the password encrypted by the e-mail attachment to the recipient by a different channel from the channel by which the e-mail is delivered, ie. it is not recommended to deliver the password for decrypting the content of the attachment to the recipient via e-mail, because then the meaning of encryption is lost (possible unwanted / unauthorized recipient of the message potentially has access to the content of the encrypted attachment without any obstacles). SMS

messages, dictate by phone, etc.

it is necessary to take into account when naming attachments / files that will be submitted within the encrypted attachment (as well as the naming of the encrypted attachment itself) by e-mail so that personal data is not disclosed from the name itself (eg contract for something for Ivo Ivić).

In conclusion, we emphasize that this recommendation is given in order to improve the protection of personal data and to reduce the possible risks of unauthorized access or prevent possible misuse of personal data of employees of legal entities within the activities of your department in processing such as in this case. with actions regarding activities conditioned by the circumstances of the COVID-19 epidemic / pandemic.