**Information on the processing of personal data**

**related to the data processing activity carried out by the company INA d.d., or**

**the processing activity carried out jointly by the company INA d.d. and the relevant affiliated INA Group company as indicated in this Information (hereinafter: Affiliated Company) in relation to the collection and processing of personal data by means of video surveillance**

This Information on the processing of personal data refers to the data processing activity carried out independently by INA-INDUSTRIJA NAFTE, d.d. in the Republic of Croatia, or the processing activity carried out jointly by INA-INDUSTRIJA NAFTE, d.d. (hereinafter: Company) and the following Affiliated Companies of INA Group as Controllers (information on Controllers is provided in Appendix I to this Information):

* CROSCO, naftni servisi, d.o.o.
* STSI, Integrirani tehnički servisi d.o.o.
* INA MAZIVA d.o.o.
* Top Računovodstvo Servisi d.o.o.

The Company and the relevant Affiliated Company are considered joint data controllers since they jointly determine the purpose and are jointly and severally liable for data processing. As part of the joint data controlling activity, the Company decides on the means and manner of processing personal data by means of video surveillance and is authorized to select the processors who are able to provide the necessary service. Data controllers share this joint information on data processing that includes their role and relationship with relevant data subjects. Furthermore, data subjects may submit requests for exercising their rights under the GDPR to the Company or the relevant Affiliated Company, as well as to both of them.

General contact information for data subjects: INA Group Data Protection Officer - [szop@ina.hr](mailto:szop@ina.hr), or

Data Protection Officer of the relevant Controller (as stated in Appendix I to this Information)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Name and purpose of personal data processing activity | Legal basis for data processing | Scope and source of personal data | Duration of processing | Categories of data recipients | Processing activity entrusted to the Processor |
| 1. Video surveillance of locations that are legally considered monetary institutions (service stations that are also monetary institutions)   The activity includes control of access and movement of persons and vehicles in protected facilities, reactions to possible  security incidents and system maintenance for the purpose of protecting persons and assets.  The purpose of processing is: (i) meeting the legal obligation of video surveillance of locations that are considered monetary institutions according to the Act on Protection of Monetary Institutions. In practice, these are most often INA d.d. service stations that offer, for example, exchange office services, and (ii) protection of persons and assets. | 1. Article 6 paragraph 1 (c) of GDPR - processing is necessary for compliance with a legal obligation to which the controller is subject, i.e. regulation governing financial operations (Act on Protection of Monetary Institutions) 2. Article 6 paragraph 1 (f) of GDPR - processing is necessary for the purposes of the legitimate interest of the Company.   The legitimate interest of the Company consists in the protection of the Company's assets and the protection of persons who may be found at the Company locations.  A balancing test of legitimate interests was conducted. More information on the performed balancing test can be obtained upon individual request. | The video recording contains personal data of persons (appearance of the person) and vehicles (license plate number, description of the vehicle) moving through the Company's premises, as well as the date, time and location of the recording.  The video surveillance system does not record sound.  Source: data subject | Video recordings will be stored in accordance with the legally prescribed period, i.e. at least 168 hours and at most 30 days from the date of recording (depending on the technical capacities of each location). | INA d.d. is an independent data controller. | 1. Maintenance of the software part of the video surveillance system  2. Video surveillance system management  3. Maintenance of the hardware part of the video surveillance system 4. Provision of IT services closely related to server maintenance and data processing  5. Services of managing the INA d.d. service station |
| 1. Video surveillance of locations that are not considered monetary institutions in accordance with the legal provisions (business premises and services stations that are not monetary institutions)   The activity includes control of access and movement of persons and vehicles in protected facilities, reactions to possible  security incidents and system maintenance for the purpose of protecting persons and assets. | Article 6 paragraph 1 (f) of GDPR - processing is necessary for the purposes of the legitimate interest of the Company, or the relevant Affiliated Company.  The legitimate interest of the Company, or the relevant Association Company, consists in the protection of persons who may be found at the Company locations, or locations of the relevant Affiliated Company.  A balancing test of legitimate interests was conducted. More information on the performed balancing test can be obtained upon individual request. | The video recording contains personal data of persons (appearance of the person) and vehicles (license plate number, description of the vehicle) moving through the Company's premises, or premises of the relevant Affiliated Company, as well as the date, time and location of the recording.  The video surveillance system does not record sound.  Source: data subject | Video recordings will be stored in accordance with the legally prescribed period, at most 30 days from the date of recording (depending on the technical capacities of each location). | INA d.d. and the relevant Affiliated Company are joint controllers. No other data transfer is performed for the controller.  The list of relevant INA Group companies is available below in this Information. | 1. Maintenance of the software part of the video surveillance system  2. Video surveillance system management  3. Maintenance of the hardware part of the video surveillance system  4. Provision of IT services closely related to server maintenance and data processing |
| 1. Processing of personal data collected by means of video surveillance related to internal reports   Prevention, detection and investigation of fraud and abuse, as well as investigation of conduct in violation of the INA Group Code of Ethics.  Prevention and investigation of fraud and abuse are regulated by the INA Group Code of Ethics available at the following link:  <https://www.ina.hr/wp-content/uploads/2020/01/eticki-kodeks-ina-grupe-web.pdf>.  For the purpose of this processing activity, only recordings made on the basis of the processing activities listed under 1 and 2 are used (for the purpose of complying with legal obligations and the legitimate interest of protecting persons and assets). | Article 6 paragraph 1 (f) of GDPR - processing is necessary for the purposes of the legitimate interest of the Company, or the relevant Affiliated Company.  Legitimate interest: preventing, detecting and holding accountable those responsible for irregularities that endanger the assets, trade secrets, intellectual property or business reputation of the Company, as well as creating an appropriate work environment based on respect and free from fear and retaliation.  A balancing test of legitimate interests was conducted. More information on the performed balancing test can be obtained upon individual request. | All personal data listed under the aforementioned data processing purposes.  Source: Electronic database of video recordings (Video recordings of persons and vehicles moving through the Company's premises, or the premises of the relevant Affiliated Company, collected from the activities described under items 1 and 2 of this Information) | 1. If an ethical procedure is initiated involving not only customers or third parties, but also employees, all data relating to the Ethical Procedure and/or the Ethical Report shall be kept during the employee’s employment, as well as for a period of five years thereafter, starting from the end of the year in which employment has ended. 2. In relation to the ethical procedure not involving employees, all data relating to the ethical procedure and/or the ethical report shall be kept for a period of five years, starting from the end of the year in which the subject procedure has ended or was suspended. 3. Notwithstanding the aforementioned, the minutes of the Ethics Committee are kept for a period of five years, starting from the end of the year in which the minutes were made. | INA d.d. and the relevant Affiliated Company are joint controllers. No other data transfer is performed for the controller.  The list of relevant INA Group companies is available below in this Information.  In addition to the aforementioned, employees of local Security, Group Security, Internal Audit, as well as Legal Affairs and Compliance may have access to the data necessary to investigate and establish or defend legal claims. | Provision of IT services closely related to server maintenance and data processing |
| 1. Establishing and defending legal claims of the Company, or the relevant Affiliated Company   For the purpose of exercising or defending legal claims, whether in judicial, administrative, non-litigious or any other similar proceedings. | Article 6 paragraph 1 (f) of GDPR - processing is necessary for the purposes of the legitimate interest of the Company, or the relevant Affiliated Company.  Legitimate interest: establishing claims in relation to the data subject and successful defence in any civil proceedings initiated by the data subject, or in administrative and other similar proceedings.  A balancing test of legitimate interests was conducted. More information on the performed balancing test can be obtained upon individual request. | All personal data collected under the aforementioned data processing purposes. | In the event that the processing of personal data is necessary for establishing, defending or realizing the legitimate interest of the Company, or the relevant Affiliated Company in court proceedings or in administrative or non-litigious proceedings initiated by the data subject based on their own legitimate interest, the Company shall process data until final closure of such proceedings or realization of the legitimate interest in another manner (e.g. by making an out-of-court settlement). | INA d.d. and the relevant Affiliated Company are joint controllers. No other data transfer is performed for the controller.  The list of relevant INA Group companies is available below in this Information.  In addition to the aforementioned, employees of local Security, Group Security, Internal Audit, as well as Legal Affairs and Compliance may have access to the data necessary to investigate and establish or defend legal claims. | Provision of IT services closely related to server maintenance and data processing |

Personal data collected by means of video surveillance will be used in internal investigations conducted in the Company, or the relevant Affiliated Company in order to protect persons and assets of the Company, or the relevant Affiliated Company by Corporate Security, which is organizationally in charge of such activities. The processing of personal data by means of video surveillance is carried out in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, the Act on the Implementation of the General Data Protection Regulation and other applicable regulations, as well as INA, d.d. internal documents. All video recordings are the property of the Company and therefore are considered a business secret. The Company shall not in any manner and in any form submit videos or make them available to unauthorized persons.

Each video surveillance system is designed and installed in accordance with the provisions of the Privacy Protection Act, the Occupational Health and Safety Act and the Regulation on the Conditions and Methods of Implementing Technical Security Measures.

Furthermore, your personal data may be transferred to recipients or third parties, for example legal representatives (lawyers), auditors, insurance companies, Processors in case they are authorized to process personal data on behalf of the Controller (e.g. to the provider of video surveillance system management services), public authorities on the basis of their legal powers, as well as other authorized persons in accordance with the applicable legal regulations.

Information on the processing of personal data is available via the link <https://www.ina.hr/home/zastita-osobnih-podataka/>, and can also be obtained upon individual request.

More information on the performed legitimate interest balancing test can be obtained upon request of the data subject.

**Persons authorized to access data within the Controller’s organization:**

The video recordings are accessed, i.e. processing activities are carried out, by 6 user levels:

1. **Corporate Security employees with administrator powers** - the employee is responsible for the operation of the system and maintaining the established level of protection. They give access permissions and authorizes activities that include modifying data, which is not otherwise permitted (e.g. deletion, exclusion, etc.).
2. **Corporate Security employees who do not have administrator powers** - permitted to view the live feed remotely, as well as to retrieve and extract the recordings.
3. **Regional managers of INA service stations** - only access to watch live camera feed and view videos locally, as well as to retrieve recordings for the purpose of performing work tasks is permitted. They do not have permission to change settings or extract recordings.
4. **Employees of business partners who manage individual INA service stations** - only access to watch live feed and view videos locally, as well as to retrieve recordings for the purpose of performing work tasks is permitted. They do not have permission to change settings or extract recordings.
5. **Maintenance technician - external contractor** - performs the necessary tasks at a physical location in the event of a system failure or change. They have no right to change the data, i.e. to delete the recordings, to stop or start a new recording. They can perform tasks that include modifying data after obtaining special authorization from the administrator. After completing the task, the administrator checks the system and withdraws the authorization, i.e. locks the system again. At the request of the Company, the maintenance technician, as the processor, has the right to extract the recordings locally.
6. **Employees of the property protection service provider**, who are employees of the company engaged by the Company for the purpose of providing property protection services, have the right to view live feed remotely, as well as to retrieve and extract recordings.

In case of initiating an ethical procedure, the members of the Ethics Committee have access to the data they need to conduct the procedure.

**Processors:**

The Company hereby declares that it has concluded data processing contracts with the Processors, which ensure an appropriate level of personal data protection.

At the request of the data subjects, the Company will provide information on the Processors involved in a particular data processing procedure, details of their processing activities and their contact information.

**Processing of special categories of personal data for the purposes stated in this Information:** There is no processing of special data categories.

**Transfer of personal data to third countries:** None.

**Existence of automated decision-making, including profiling (meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject):** No automated decision-making, including profiling is conducted.

**Security measures for data protection:**

The Company stores personal data exclusively on data carriers and hosting sites that allow access only to authorized personnel and in databases that are encrypted and/or password protected to ensure the confidentiality, integrity and availability of data subjects’ personal data in accordance with information security codes and standards. Within the protection proportional to risk and categorization of personal and business data (classification), the Company ensures data protection at the network, infrastructure and application level (using firewalls, antivirus software, encryption mechanisms for storage and communication, content filtering and other technical and process solutions). Data security incidents are constantly monitored and addressed.

In case of paper documents and all personal data processed on paper, the Company ensures the security of data by storing the data in places inaccessible to unauthorized persons. After the expiration of the data processing period, professionally trained employees of the Company destroy the documents by burning them or using a paper shredder.

**Your rights regarding data processing:**

The General Data Protection Regulation (GDPR) contains detailed information about your data processing rights, possible judicial remedies and their limitations (especially Articles 15, 16, 17, 18, 19, 21, 22, 77, 78, 79 and 82). At any moment, you may request information about the processing of your personal data, you may request access to your data, rectification and erasure of your personal data or restriction of their processing, as well as object to the processing of data on the basis of legitimate interest. Below is a summary of the most important provisions regarding your data protection rights and your ability to seek judicial remedy.

You may at any time, on grounds relating to your particular situation, object to the processing of your personal data by the Company or the relevant Affiliated Company under Article 6 paragraph 1 (f) of the GDPR, including profiling based on those provisions. In that case, the Company/relevant Affiliated Company shall no longer process the personal data unless they demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims. In relation to personal data processed for the legitimate interest of the Company/relevant Affiliated Company or a third party, you have the right, pursuant to Article 6 paragraph 1 (f) of the GDPR, to request an explanation of the legitimate interest test, which contains reasons why the interests of the Company/relevant Affiliated Company and third party have priority in the data processing activity in question over your interests, rights and freedoms, and how and to what extent they restrict them.

**Right to information:**

If the Company or the relevant Affiliated Company processes your personal data, they must provide you with information about the data relating to you - even without your specific request - including the most important characteristics of the data processing, as well as the purpose, legal basis and duration of the processing, name of the Company/relevant Affiliated Company and contact information of their representatives, contact information of the Data Protection Officer, recipient of personal data (in case of data transfer to third countries, including information on the existence of a European Commission decision), legitimate interest of the Company/relevant Affiliated Company and/or third parties in case of data processing based on a legitimate interest; furthermore, your data protection rights and your ability to seek judicial remedy (including the right to lodge a complaint with the supervisory authority) and, if your personal data have not been collected directly from you, information about the source of personal data and categories of personal data collected, in case you have not received such information beforehand. The Company or the relevant Affiliated Company shall provide you with the above information by making such information available to you.

**Access right:**

You have the right to obtain confirmation from the Company or the relevant Affiliated Company as to whether personal data relating to you are being processed or not, and if such data are being processed, you have the right to access personal data and certain information related to data processing, such as the purpose of data processing, categories of personal data being processed, recipients of personal data, planned duration of personal data processing, rights of data subject to data protection and ability to seek judicial remedy (including the right to lodge a complaint with the supervisory authority) and, if personal data are not collected directly from you, information about the source from which your data were collected.

At your request, the Company or the relevant Affiliated Company shall provide you with a copy of your personal data being processed. For each additional copy you request, the Company or the relevant Affiliated Company may charge you a reasonable fee for administrative costs. If the data subject submits the request electronically and unless they request otherwise, the information shall be provided in the usual electronic form. The right to obtain a copy shall not prejudice the rights and freedoms of others.

The Company or the relevant Affiliated Company shall, at your request, inform you of the possibility, procedure, potential costs and other details of obtaining the copy in question.

**Right to rectification:**

You have the right to obtain from the Company/relevant Affiliated Company without undue delay the rectification of inaccurate personal data concerning you. Taking into account the purposes of the processing, you have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

**Right to erasure:**

You have the right to obtain from the Company/relevant Affiliated Company erasure of personal data relating to you without undue delay and the Company/relevant Affiliated Company shall have the obligation to erase the personal data without undue delay if there are specific reasons therefor and where certain grounds apply. Among other grounds, the Company/relevant Affiliated Company shall erase your personal data at your request, for example, if the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; if you have withdrawn the consent on which the processing is based and where there is no other legal basis for the processing; if the personal data have been unlawfully processed; if you have objected to the processing and there is no other legal ground for the processing; if the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the Company/relevant Affiliated Company is subject.

The above shall not apply to the extent that processing is necessary:

1. for exercising the right of freedom of expression and information;
2. for compliance with a legal obligation which requires processing in Union or Member State law to which the Company/relevant Affiliated Company is subject;
3. for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in so far it is likely that the right to erasure renders impossible or seriously hinders the achievement of the objectives of that processing;
4. for the establishment, exercise or defence of legal claims.

**Right to restriction of processing:**

You have the right to obtain from the Company/relevant Affiliated Company restriction of processing where one of the following applies:

1. you have contested the accuracy of personal data for a period enabling the Company/relevant Affiliated Company to verify the accuracy of the personal data;
2. the processing is unlawful and you oppose the erasure of the personal data and request the restriction of their use instead;
3. the Company/relevant Affiliated Company no longer needs the personal data for the purposes of the processing, but they are required by you for the establishment, exercise or defence of legal claims;
4. you have objected to processing pending the verification whether the legitimate grounds of the controller override your legitimate grounds.

Where the processing has been restricted for the reasons stated above, such personal data shall, with the exception of storage, only be processed with your consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

If you have obtained restriction of processing, the Company/relevant Affiliated Company shall inform you before the restriction of processing is lifted.

**Right to object:**

At any time, you have the right to object, on grounds of your particular situation, to processing of personal data concerning you, which is based on the legitimate interest of the Company/relevant Affiliated Company. The Company/relevant Affiliated Company shall no longer process the personal data unless they demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms or for the establishment, exercise or defence of legal claims.

**Manner of exercising the rights:**

The Company or the relevant Affiliated Company shall provide information on the measures taken at your request without undue delay, and in any case **within one month** of receiving your request. The deadline may be extended by an additional two months if necessary, taking into account the complexity and number of requests received. The Company or the relevant Affiliated Company shall inform you on such extension of the deadline within one month of receiving your request, as well as the grounds for delay. If the data subject submits the request electronically, the information on the request shall be provided in electronic form whenever possible, unless the data subject requests otherwise in their request.

Information relating to the subject matter of the request shall be provided in writing or otherwise, including electronically where appropriate. If you so request, the information may also be provided to you verbally, provided that your identity has been established by other means.

In case the Company/relevant Affiliated Company fails to proceed according to your request, the Company/relevant Affiliated Company shall inform you without delay, and at the latest within one month about the reasons for failing to take measures and on the possibility to lodge a complaint with the competent supervisory authority in charge of personal data protection, as well as the possibility of seeking judicial remedy.

Read more about how to contact the competent supervisory authorities in the European Union here: <https://edpb.europa.eu/about-edpb/board/members_hr>.

**Contact information of the competent authority for personal data protection in Croatia:**

Croatian Personal Data Protection Agency, Selska cesta 136, HR - 10 000 Zagreb

phone: +385 (0)1 4609-000, e-mail: [azop@azop.hr](mailto:azop@azop.hr), website: <http://www.azop.hr>

# **Appendix I**

# **List and contact information of the Data Controllers**

**Name, registered office, phone number, website (where the Privacy Statement is located) and e-mail address and other contact information of the Controllers:**

|  |  |
| --- | --- |
| **INA-Industrija nafte, d.d.** | Avenija Većeslava Holjevca 10, p.p. 555, 10 020 Zagreb, PIN: 27759560625  phone: +385 0800 1112, website: <https://www.ina.hr/>, e-mail: [ina-besplatni.telefon@ina.hr](mailto:ina-besplatni.telefon@ina.hr) |
| **CROSCO, naftni servisi, d.o.o.** | Grada Vukovara 18, 10000 Zagreb, PIN: 15538072333  website: <https://crosco.com/hr/>, e-mail address: [info@crosco.hr](mailto:info@crosco.hr) |
| **STSI, Integrirani tehnički servisi d.o.o.** | Lovinčićeva 4, 10000 Zagreb, PIN: 99172175603  website: <https://stsi.hr/> |
| **INA MAZIVA d.o.o.** | Radnička cesta 175, 10000 Zagreb, PIN: 63988426425  website: <http://www.ina-maziva.hr/hr> |
| **Top Računovodstvo Servisi d.o.o.** | Savska cesta 41, 10000 Zagreb, PIN: 64603058187  phone: +385 [01 6451 300](file:///C:\Users\TDoresic\AppData\Roaming\Microsoft\Word\01%206451%20300), website: <https://trs.hr/>, e-mail address: [Info-trs@trs.ina.hr](mailto:Info-trs@trs.ina.hr) |

In addition, in accordance with Article 6 paragraph 1 (f) of the GDPR (based on the legitimate interest of the Company/relevant Affiliated Company), the Company/relevant Affiliated Company uses the services of its legal partners to manage and successfully execute their legal claims and transfers necessary personal data to lawyers for this purpose (including details of requests). Such lawyers act as independent Controllers in accordance with the provisions of their own Information on the Processing of Personal Data. At the request of the data subject, the Company/relevant Affiliated Company shall provide data on the legal partner involved in particular data processing, their contact information and processing activities performed, as well as data processed with regard to the data subject.

# **Contact information of the Data Protection Officer of the Controllers:**

|  |  |  |
| --- | --- | --- |
| **INA-Industrija nafte, d.d.** | E-mail address: | [szop@ina.hr](mailto:szop@ina.hr) |
| Address: | Avenija Većeslava Holjevca 10, 10000 Zagreb, attn. Data Protection Officer |
| **CROSCO, naftni servisi, d.o.o.** | E-mail address: | [crosco.zop@crosco.hr](mailto:crosco.zop@crosco.hr) |
| Address: | Grada Vukovara 18, 10000 Zagreb, attn. Data Protection Officer |
| **STSI, Integrirani tehnički servisi d.o.o.** | E-mail address: | [szop@stsi.hr](mailto:szop@stsi.hr) |
| Address: | Lovinčićeva 4, Zagreb, attn. Data Protection Officer |
| **INA MAZIVA d.o.o.** | E-mail address: | [maziva.zop@ina.hr](mailto:maziva.zop@ina.hr) |
| Address: | Radnička cesta 175, 10000 Zagreb, attn. Data Protection Officer |
| **Top Računovodstvo Servisi d.o.o.** | E-mail address: | [TRS.Zop@trs.ina.hr](mailto:TRS.Zop@trs.ina.hr) |
| Address: | Savska cesta 41, 10000 Zagreb, attn. Data Protection Officer |