

## Privacy Notice and Regulation on operation of electronic camera surveillance system (CCTV) and access control system by Syngenta Magyarország Kft.

### CCTV Regulation

**Syngenta Magyarország Kft.** as data controller and as an operator (hereinafter: Data Controller or Operator) hereby informs You that it is operating an electronic camera surveillance system (hereinafter: CCTV) and an electronic access control system (hereinafter: access control system) on its registered office site at 2 Alíz utca, Budapest 1117 (hereinafter: Headquarter) and company seats at, „Industrial park – Syngenta Telephely, Mezőtúr 5400” and Üllői út külterület– Syngenta Telephely, Ócsa 2364 (hereinafter: Company seat) in order to ensure the security of persons and property,.

During the data processing operations Syngenta Magyarország Kft. shall act on the basis of and in accordance with its Internal data protection Regulation, this Regulation, other internal data protection rules and the relevant legislation.

#### I. PURPOSE OF THIS REGULATION

1. In addition to the Internal data protection Regulation this Regulation determines the rules of processing the data recorded by CCTV and/or the access control system.

#### II. DEFINITIONS OF TERMS

- User or Guest or Client (hereinafter: data subject): any natural person who has been identified or is (directly or indirectly) identifiable by reference to any personal data, for the purpose of this Regulation the person identifiable by the data recorded by CCTV;
- Staff member: any natural person being in employment-, mandate or other relationship with the Data Controller to carry out the services on behalf of the Data Controller and during his/her processing activity will or might get contact to personal data and for whose activity the Data Controller undertakes full responsibility toward the data subjects or third parties.
- Personal data: any information relating to a data subject – including but not limited to facial image, sound, identification number of the data subject, one or more physical, physiological, mental, economical, cultural or social characteristics and the conclusion of the data subject that may be drawn from that information, in case of a Staff member the name, time of entry and leave through the access control system.
- Headquarter: the registered office site located at „1117 Budapest, Alíz utca 2.” and operated by the Data Controller;
- Company seat: site of the company seats located at „Industrial park – Syngenta Telephely, Mezőtúr 5400” and „2364 Ócsa, Üllői út külterület– Syngenta Telephely” and operated by the Data Controller;
- Consent: any freely given, specific, informed and unambiguous indication of the data subject's wishes by which the data subject, by a statement or by a clear affirmative action, signifies agreement to the- overall or particular - processing of personal data relating to him or her;
- Data controller: the natural or legal person, or unincorporated body which alone or jointly with others determines the purposes of the processing of data, makes decisions regarding data processing (including the means) and implements such decisions itself or engages a data processor to execute them;
- Procession of data: any operation or set of operations that is performed upon data, whether or not by automatic means, such as in particular collection, recording, organization, storage, adaptation or alteration, use, retrieval, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction, and blocking them from further use, photographing, sound and video recording, and the recording of physical attributes for identification purposes. Procession of data occurs by each Data controller separately..;
- Disclosure by transmission: making data available to a specific third party;
- Data processing: performing any technical operation or set of operations connected to Procession of data;

- Data processor: a natural or legal person or unincorporated organization, public authority, agency or other body that is engaged in processing operations regarding data and acting on the Data controller's behalf or following the Data controller's instructions. and decisions;

### III. SCOPE OF THIS REGULATION

1. The personal scope of this regulation in relation to the CCTV covers every natural person (data subject and Staff member) who enters into or stays in the area observed by the CCTV.
2. The personal scope of this regulation in relation to the access control system covers every employee, Staff member who enters to the sites of the Data Controller.
3. This regulation may confer particular rights or impose obligations in connection with the operation of the CCTV to the Staff member being the person that processes operation regarding data on behalf of the Data controller.
4. This regulation shall be applied to every photo and other personal data recorded by the CCTV and the personal data registered by the access control system. Entry and leave data registered by the access control system are not basis of the work time registry, in justified cases the persons staying inside the site may be checked due to safety reasons.
5. This regulation shall enter into force on 2 October, 2023 and shall exist until its revocation.

### IV. DEFINITION OF THE LEGAL PERSON OPERATING THE CCTV AND THE ACCESS CONTROL SYSTEM

1. CCTV is operated by the Data controller. In this regulation Data controller shall mean:
  - a) **Syngenta Magyarország Korlátolt felelősségű társaság** (short name: Syngenta Magyarország Kft.)
    - a. registered seat: 1117 Budapest, Alíz utca 2.
    - b. address of actual data processing: 1117 Budapest, Alíz utca 2. and 2364 Ócsa, Üllői út külterület – Syngenta Telephely
    - c. company seat: 2364 Ócsa, Üllői út külterület – Syngenta Telephely
    - d. web link:
      - i. <https://www.syngenta.hu/>
    - e. company registration No: 01-09-072997
    - f. tax number: 10537433-2-44
    - g. phone number: + 36 01 4882200
    - h. e-mail: [info.hungary@syngenta.com](mailto:info.hungary@syngenta.com)
    - i. represented by: Kalmár Ferenc managing director with independent right to sign
  - b) On behalf of the Data Controller CCTV and the access control system are operated by the managing director of the Data Controller or the Staff member(s) designated to this task by him/her. These persons have access right that implies right to retrieve and view the recordings..
  - c) On behalf of the Data Controller the technical tasks connected to Data processing are performed by a Data processor according to an agreement concluded with the Data Controller. Operation of CCTV and access control system, and the processing of recordings are performed by external Data processors being: CBRE Global Workplace Solutions Kft. (registered seat: 1097 Budapest, Gubacsi út 6B/1) and Safetrend Kft. (székhely: 8000 Székesfehérvár, Kertalja utca 21). Data Controller and Data processor entered into a separate agreement on data processing in which agreement the Data processor undertakes to perform data processing in accordance with the relevant legal provisions.

### V. DECLARATIONS OF THE DATA CONTROLLER

1. In accordance with the law and data protection directives Data Controller hereby gives full and comprehensive information on the operation of the CCTV and the access control system to the Staff members and persons entering the area observed by CCTV (together: data subjects).
2. This regulation shall be interpreted on the basis of and together with the Internal data protection Regulation of the Data Controller (as amended from time to time), that regulation interpretes, explains and supplements the provisions of this regulation. Effective version of the Internal data protection Regulation and the data protection records are available at weblink: <https://www.syngenta.hu/adatvedelem>.
3. Data Controller hereby informs You that for the recording, use and storage activity the provisions of Act CXXXIII of 2005 on the rules of protection of persons and property and private investigation (Szvvtv.), the Act CXII of 2011 on the right of informational self-determination and on freedom of information (Info tv.) and the 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 movement of such data (GDPR) shall be applied in line with the provisions of this regulation.

## VI. ENFORCEMENT OF RIGHT TO BE INFORMED

1. In order to satisfy the right to be informed the Data Controller hereby informs the data subjects on the operation of CCTV, the rights of data subjects and other conditions.
2. Informing data subjects:
  - a. Data Controller draws the attention of the Staff members to
    - i. the definition of the person operating the CCTV and the access control system, and the persons having the right of access (Chapter IV),
    - ii. legal basis of data processing (Chapter VII.),
    - iii. purpose of data processing and the data that are stored (Chapter VIII.),
    - iv. data recording method, place and duration of storage (Chapter IX.),
    - v. data security arrangements regarding the storage of records (Chapter X.),
    - vi. conditions of retrieval of the recordings, specification of purposes for which the recordings may be used by the Data Controller (Chapter X.),
    - vii. rights of the data subjects in connection with the CCTV and the access control system, and rules of how the data subjects may exercise these rights (Chapter XI. and XII.),
    - viii. rights and means of the data subject in case of a breach of their right of informational self-determination (Chapter XIII.),
    - ix. placement of the cameras, their purpose, the objects and areas observed by these cameras in connection with Üllői út külterület– Syngenta Telephely, Ócsa 2364 (Annex I.),
    - x. site plan of the area observed by CCTV and the range of vision of particular cameras in connection with Üllői út külterület– Syngenta Telephely, Ócsa 2364 (Annex II.)
    - xi. ix. placement of the cameras, their purpose, the objects and areas observed by these cameras in connection with Industrial park – Syngenta Telephely, Mezőtúr 5400 (Annex III.)
    - xii. x. site plan of the area observed by CCTV and the range of vision of particular cameras in connection with Industrial park – Syngenta Telephely, Mezőtúr 5400 (Annex IV.)
    - xiii. form of exercising the rights by data subjects (Annex V.)
    - xiv. information statement on CCTV (Annex VI.)
    - xv. interest consideration test (Annex VII.)
    - xvi. ix. placement of the cameras, their purpose, the objects and areas observed by these cameras in connection with 5th floor of Alíz utca 2., Budapest 1117 (Annex VIII.).
    - xvii. site plan of the area observed by CCTV and the range of vision of particular cameras in connection with 5th floor of Alíz utca 2., Budapest 1117 (Annex IX.)

3. Information to the data subjects others than Staff members (such as visitors, clients):
  - a. In addition to the list detailed in VI./2. above the Data Controller draws the attention of data subjects thereto that each area observed by CCTV are labelled by standard stickers in clearly visible manner.

## **VII. LEGAL BASIS OF DATA PROCESSING**

1. The legal basis of the procession of data for the above purpose is the expressly indicated and voluntary consent given by the data subject after being informed by the Data Controller and the Data Controller's legitimate interest.
2. Entering and staying by the Staff members and the data subjects in the area observed by CCTV after being informed by this privacy notice shall be considered their express consent to procession of data. Data Controller's legitimate interest regarding CCTV is the interest to protect persons and property as of GDPR Art. 6 (1) f.
3. The legal basis of the procession of data in connection with the access control system is the Data Controller's legitimate interest of which interest the Data Controller shall inform the employees. Data Controller's legitimate interest regarding the access control system is the interest to protect persons and property as of GDPR Art. 6 (1) f.

## **VIII. PURPOSE OF PROCESSION OF DATA, SCOPE OF STORED DATA**

1. CCTV and access control system are operated for the following purpose
  - a) based on express consent as of Section 25 (1) of Szvtv. in order to protect persons and property and prevention and proof of infringements detailed hereunder, and
  - b) based on consent as of Section 5 (1) of Info tv. in order to perform the agreement concluded in writing with the Data Controller. (the above hereinafter together: purpose of procession of data)
  - c) The protection of life and bodily integrity of the data subjects and Staff members, detecting potential sources of risks, furthermore monitoring and coordinating workflow belong to purposes as well.
2. Based on the above the purpose of surveillance is particularly:
  - a) property protection of assets, devices, equipments located on the observed area which particularly justifies the surveillance of the area – except where it prejudices the respect of human dignity;
  - b) detecting circumstances of the accident which there occurred;
  - c) follow up of complaint made by the data subject.
3. In accordance with the law, the purposes mentioned above, and in line with the statements and resolutions of the National Authority for Data Protection and Freedom of Information, the placement, focus and accordingly the purpose of procession of data of the particular cameras are detailed in Annex I.-IX. to this regulation.
4. Records and entry and leave data may be processed by the Data Controller only in order to achieve the purpose of procession of data. Use of data shall mean especially but not limited to clarification, detecting and proving the circumstances of an event occurred in the area. Place, time, reason and purpose of use shall be recorded in the minutes.
5. Scope of processed data: data subject's facial image visible on photos, his/her other personal data, employee's name, entry and leave data being personal data.

## **IX. DATA RECORDING METHOD, PLACE AND DURATION OF STORAGE**

1. Data Controller hereby informs the data subjects and the Staff members that CCTV records images and data registered by the access control system directly.
2. CCTV is operating 24/7.
3. Place of storage of data: digital data recording servers operated by the Data Controller and located on the registered seat at 1117 Budapest, Alíz utca 2. and the company seats at Industrial park – Syngenta Telephely, Mezőtúr 5400 and 2364 Ócsa, Üllői út külterület – Syngenta Telephely.
4. Recordings are stored by the Data Controller for 3 days as a general rule, but 30 days in priority cases (in particular in cases where 3 days are not sufficient to detect the incident, e.g.: a request to the authorities). In Annexes I, III and IX. of the Camera Regulations, the duration of the data management of the cameras is specified separately for each camera. Period of storage has been determined on the basis of principles of processing of the data such as data minimisation and storage limitation. At the end of the storage period the recordings are deleted automatically, except for the ones which are requested not to be deleted until the time of automatic deletion by a natural or legal person with reference to his or her legitimate interest.

## **X. DATA SECURITY AND DATA ACCESS RIGHT**

1. In order to ensure safe processing of data the Data Controller implement the following measures regarding the security of stored data:
  - a. data are stored by the Data Controller in a closed system protected by identifier and password which establishes and maintains connections between devices having own individual network identifier address (IP address) or other individual identifier (SIM, IMEI, etc.) and are owned or leased by the Data Controller; and
  - b. access to the data are differentiated by levels as follows:
    - i. Managing director has unlimited access right which means that he or she has access to any image or sound recorded by any part of the CCTV operating on any site, and the data registered by the access control system.
    - ii. Staff member(s) delegated and authorized by the Managing director to this task has/have limited access right.
    - iii. Recordings, entry and leave data may be viewed by the authorized person at any time within the period of data storage.
2. Processing of data is confidential by nature therefore the managing director and/or the Staff member shall be obliged to use the data being in his or her possession exclusively in order to achieve the purpose of processing of the data and to the extent necessary to achieve its purpose, always ensuring that persons who are employed, mandated, ordered by or being in other relationship with the Data Controller without authorization, or any third party may not have access to the data.
3. Person who processes the data shall not be entitled to make copy or record data to use it for a different purpose.
4. Data Controller does not forward any data connected to the recordings, except for the cases when the fulfillment of a request from an authority requires disclosure of data or in case of procedural proof of an authority or court. In each of the above cases those data and recordings with relevant information will be forwarded which have been recorded or registered by the CCTV and the access control system.

## XI. RIGHTS OF THE DATA SUBJECT

1. **Right to be informed or right of access of the data subject:** in accordance with the Act CXII of 2011 and Article 15 of the 2016/679 EU Regulation Data Controller provides the data subject upon his or her request with the following information
  - a. the categories of data and personal data processed by the Data,
  - b. the purpose of the processing,
  - c. legal basis of the processing,
  - d. duration of the processing,
  - e. where possible, the envisaged period for which the data will be stored, or, if not possible, the criteria used to determine that period,
  - f. data of the Data processor, if any,
  - g. the circumstances of any data breach (if any), their impact, and the measures taken to remedy the situation, and
  - h. in the case of transfer of personal data of the data subject, the legal basis, the purpose and the recipients of the transfer.
2. **The right to erasure (to be forgotten):** The data subject is entitled to ask his or her personal data to be erased without delay by the Data Controller (taking into consideration the limits of the relevant Hungarian law, if any), and the Data Controller shall delete the data subject's personal data without delay if
  - a. the personal data is no longer necessary in relation to the purpose for which it was collected or processed;
  - b. the data subject withdraws his or her consent and no other legitimate basis applies;
  - c. the data subject objects to the processing and there is no overriding legitimate grounds to continue processing;
  - d. personal data was unlawfully processed;
  - e. the personal data should be erased to comply with a legal obligation of the Data Controller specified by the relevant law;
  - f. personal data was collected in relation to the offer of information society services mentioned in Article 8 of 2016/679 EU Regulation.
3. Where the Data Controller has made the personal data public and is obliged pursuant to the above to erase the personal data, the Data Controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform other data controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any copy or replication of those personal data.
4. Data Controller draws the attention of the data subject to the limits of the right to erase (to be forgotten) in accordance with the EU Regulation which are the followings:
  - a. exercising the right of freedom of expression and information;
  - b. compliance with a legal obligation which requires processing by Union or Member State law to which the Data Controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller;
  - c. public interest in the area of public health;
  - d. archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89 (1) of the 2016/679 EU Regulation in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
  - e. establishment, exercise or defence of legal claims.
5. **The right to restrict the processing:** Data subject is entitled to obtain from the Data Controller restriction of his or her personal data upon request as follows.
  - 5.1. If based on the underlying circumstances there is reason to believe that erasure would prejudice the legitimate interests of the data subject, the procession of data shall be restricted for a period of existence of such legitimate interest on the basis of which erasure was discounted for a period of existence of such legitimate interest on the basis of which erasure was discounted Restricted data

may only be processed for a period of existence of such legitimate interest on the basis of which erasure was discounted.

- 5.2. Pursuant to the EU Regulation restriction of processing shall be applied if
- a. the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
  - b. the Data Controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; or
  - c. the data subject has objected to processing; in such a case for the period of pending the verification whether the legitimate grounds of the Data Controller override those of the data subject.

5.3. Where processing has been restricted, such personal data shall, with the exception of storage, only be processed with the data subject's 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.

5.4. The Data Controller shall communicate the restriction of processing carried out to the data subject and to each recipient to whom the personal data for the purpose of processing have been disclosed. A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted. The Data Controller shall inform the data subject about those recipients if the data subject requests it. No communication is necessary if it does not prejudice legitimate interests of the data subject or if the communication proves impossible or involves disproportionate effort.

6. **Right to object:** The data subject is entitled to object to processing of his or her personal data in such a case the personal data shall no longer be processed for such purposes.
7. The Data Controller is obliged to suspend the processing and to evaluate the objection request submitted by the data subject within the shortest possible time, not exceeding 15 days from receipt of such request, and to notify the data subject of its decision in writing. If the objection of the data subject is relevant and reasoned, the Data Controller shall terminate processing and restrict the concerned data, furthermore the data controllers and data processors to whom such data was disclosed by the Data Controller before taking those measures of the objection and the measures made on the basis thereof by the Data Controller, and these persons shall make all measures necessary to enforce the right to object..
8. Should the data subject disagree the decision of the Data Controller or the Data Controller misses the deadline as of XI/14., the data subject shall be entitled to seek judicial remedy within 30 days from receipt of the decision or lapse of the missed deadline.
9. Data Controller draws the attention of the data subject that if they wish to exercise any of their rights, they can lodge their request by sending an email to the [dataprivacy.hu@syngenta.com](mailto:dataprivacy.hu@syngenta.com) or to other contact of the Data Controller.
10. The Data Controller shall provide information regarding the request to the data subject without undue delay and in any event within 15 days of receipt of the request, and delete/erase (restrict) the data or takes other action on the basis of the request.
11. Conditions of compensation and restitution under the relevant law: If the Data Controller processes the data subject's data in breach of the provisions of law or binding legislation on the processing of personal data or by breaching the data security requirements and this action or failure violates the data subject's privacy rights or other rights relating to personality, the data subject shall be entitled to claim for compensation and restitution.
12. No compensation shall be paid and no restitution may be demanded where the damage was caused by, or the violation of privacy rights or other rights relating to personality is attributable to, intentional or negligent conduct on the part of the person whose rights had been violated.

## **XII. RIGHTS OF THE STAFF MEMBERS – GUARANTEES IN CONNECTION WITH THE EMPLOYMENT RELATIONSHIP**

1. The Data Controller draws the attention of the Staff members to the following guarantees of the legal provisions related to the employment relationship, CCTV and access control system:
  - a. Inspection of the employer shall be considered lawful if deemed strictly necessary for reasons directly related to the intended purpose of the employment relationship and if proportionate for achieving its objective. [Section 9 (2) of the Labour Code]
  - b. Inspection of the employer and the means applied during thereof shall not violate the human dignity and employees' private life cannot be inspected. [Section 11 (1) of the Labour Code].
  - c. Processing of data is lawful if it is for clearly specified purposes and fair. [Section 4 (1)-(2) of Infotv.]
2. Based on the above:
  - a. No camera can be installed in order to observe only one employee and his or her activity.
  - b. It is unlawful to apply CCTV which aims at influencing the employees' behaviour on the workplace.
3. Further principle is that no camera is allowed to be installed in a room or space where the observing may violate the human dignity, in particular changing rooms, showers and lavatories.
4. No camera is allowed to be installed in rooms which is designated for the employees for spending their break time.

## **XIII. REMEDIES**

1. The Data Controller hereby informs the data subjects and the Staff members that in case of breach of their rights they can submit request to the Data Controller who is obliged to evaluate the request within the shortest possible time, not exceeding 15 days from receipt of such request and notifies the applicant on its decision in writing.
2. Should the data subject disagree the decision of the Data Controller the data subject shall be entitled to seek judicial remedy within 30 days from receipt of the decision.
3. Judicial remedy before the court: Data subject may file in an action to the court in case of breach of his or her right. The court shall hear such action in priority proceedings. The burden of proof to verify the lawfulness of processing lies with the Data Controller.
4. In case of breach of the right of informational self-determination notification or complaint may be lodged to:  
National Data Protection and Information Freedom Authority  
address: 1125 Budapest, Szilágyi Erzsébet fasor 22/C  
Phone: +36 (1) 391-1400  
  
Fax: +36 (1) 391-1410  
www: <http://www.naih.hu>  
e-mail: [ugyfelszolgalat@naih.hu](mailto:ugyfelszolgalat@naih.hu)

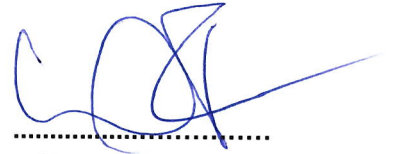
## **XIV. FINAL PROVISIONS**

1. The Data Controller reserves the right to amend this Regulation in order to harmonize it with the legal provisions as modified from time to time and with other internal regulations.



2. Annex I.-IX.- shall form integral part of this Regulation.
3. Paper copy of this regulation (as amended from time to time) is also available.
4. This Regulation shall enter into force on 2 October 2023.

dated: Budapest, 17 October 2023..



.....  
**Managing Director**  
**Ferenc Kalmár**

For further information and attachments, please contact the [dataprivacy.hu@syngenta.com](mailto:dataprivacy.hu@syngenta.com) e-mail address.