INFO COMMUNICATION TRADE UNION

www.iksz.eu – info@iksz.eu - +36309731370 – 4002 Debrecen, Madárbirs utca 7.

DATA PROTECTION AND DATA MANAGEMENT POLICY

Application of the data protection and data management regulations

Name of the organization: Info Communication Trade Union

Headquarters of the organization: 4002 Debrecen, Madárbirs utca 7.

The person responsible for the content of the regulations: Zsolt Tamás Nagy, president

Effective date of the policy: 02. January 2020.

This regulation establishes rules for the protection of natural persons with regard to the management of personal data and the free flow of personal data. The provisions of the regulations must be applied during specific data management activities, as well as when issuing instructions and information regulating data management.

Scope of the policy

This regulation is valid until withdrawn, and its scope extends to the organization's officials and employees.

Date: 02. January 2020.

.....

Zsolt Tamás Nagy (president)

Purpose of the policy

The purpose of these regulations is to harmonize the provisions of the other internal regulations of the Info Communication Trade Union (hereinafter: data manager) with regard to data management activities in order to protect the fundamental rights and freedoms of natural persons, and to ensure the appropriate management of personal data.

In the course of its activities, the organization intends to fully comply with the legal requirements for the management of personal data, in particular with the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council.

Furthermore, the important purpose of issuing the regulations is to enable the organization's employees to be able to legally manage the data of natural persons by familiarizing them with and following them.

Essential concepts and definitions in the conceptual framework of the GDPR

- GDPR (General Data Protection Regulation) is the General Data Protection Regulation of the European Union

- data controller: the natural or legal person, public authority, agency or any other body that determines the purposes and means of processing personal data independently or together with others; if the purposes and means of data management are determined by EU or member state law, the data controller or the special aspects regarding the designation of the data controller may also be determined by EU or member state law;

- data handling: any operation or set of operations performed on personal data or data files in an automated or non-automated manner, such as collection, recording, organization, segmentation, storage, transformation or change, query, insight, use, communication, transmission, distribution or making available in any other way through, alignment or connection, restriction, deletion or destruction;

- data processor: the natural or legal person, public authority, agency or any other body that processes personal data on behalf of the data controller;

- personal data: any information relating to an identified or identifiable natural person (data subject); a natural person can be identified directly or indirectly, in particular on the basis of an identifier such as name, number, location data, online identifier or one or more factors relating to the physical, physiological, genetic, mental, economic, cultural or social identity of the natural person identifiable;

- third party: the natural or legal person, public authority, agency or any other body that is not the same as the data subject, the data manager, the data processor or the persons who have been authorized to handle personal data under the direct control of the data manager or data processor;

- consent of the affected person: the voluntary, specific, and clear declaration of the will of the data subject based on adequate information, by which the data subject indicates through a statement or an act clearly expressing the confirmation that he gives his consent to the processing of personal data concerning one;

- restriction of data management: marking stored personal data for the purpose of restricting their future processing;

- aliasing: the processing of personal data in such a way that, without the use of additional information, it is no longer possible to establish which specific natural person the personal data refers to, provided that such additional information is stored separately and technical and organizational measures are taken to ensure that it is identified or this personal data cannot be linked to identifiable natural persons;

- registration system: the file of personal data in any way – centralized, decentralized or divided according to functional or geographical aspects – which is accessible based on specific criteria;

- data protection incident: a breach of security that results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to, personal data transmitted, stored or otherwise handled;

- health data: personal data relating to the physical or mental state of health of a natural person, including data relating to health services provided to a natural person, which carries information about the state of health of the natural person.

Data management guidelines

Personal data must be handled legally and fairly, as well as in a transparent manner for the data subject.

Personal data may only be collected for specific, clear and legitimate purposes, the legal basis for data management is ensured and can be verified during the entire life cycle of data management.

The purpose of processing personal data must be appropriate and relevant, and can only be to the extent necessary. The rights of the data subjects defined in the GDPR are guaranteed.

Personal data must be accurate and up-to-date. Inaccurate personal data must be deleted immediately.

Personal data must be stored in such a way that identification of the data subjects is possible only for the necessary period. Personal data may be stored for a longer period of time only if the storage is for the purpose of archiving in the public interest, for scientific and historical research purposes, or for statistical purposes.

The processing of personal data must be carried out in such a way that the appropriate security of personal data is ensured by the application of appropriate technical or organizational measures, including protection against unauthorized or illegal processing, accidental loss, destruction or damage of data.

The principles of data protection shall be applied to all information relating to identified or identifiable natural persons.

The organization's data processing employee is liable for disciplinary, compensation, violation and criminal liability for the lawful handling of personal data. If the employee learns that the personal data he is managing is incorrect, incomplete, or out of date, he must correct it or initiate its correction with the employee responsible for recording the data.

Management of personal data

Since natural persons can be associated with online identifiers provided by the devices, applications, tools and protocols they use, such as IP addresses and cookie identifiers, this data, combined with other information, is suitable and can be used to create a profile of natural persons and to for identification.

Data processing may only take place if the person concerned gives his voluntary, specific, informed and clear consent to the processing of data by means of a clear affirmative act, for example a written - including electronic - or oral statement.

Consent to data management is also considered if the person concerned ticks a relevant box while viewing the website. Silence, a pre-ticked box or inaction does not constitute consent.

Consent is also considered if a user makes relevant technical settings during the use of electronic services, or makes a statement or action that clearly indicates the consent of the person concerned to the processing of his personal data in the given context.

Children's personal data deserve special protection, as they may be less aware of the risks and consequences associated with the management of personal data and the related guarantees and rights. This special protection applies mainly to the use of the personal data of brain children for marketing purposes and for the purpose of creating personal or user profiles.

Personal data must be managed in a way that ensures an appropriate level of security and confidentiality, including in order to prevent unauthorized access to personal data and the tools used to manage personal data, as well as their unauthorized use.

In the course of assistance and other activities related to the performance of the data controller's duties, health personal data may only be processed by the person concerned, and children's personal data may only be processed with the express written consent of the legal representative.

All reasonable steps shall be taken to correct or delete inaccurate personal data.

Lawfulness of data management

The processing of personal data is lawful if:

▪ the purpose of data management is fair and legal,

▪ the legal basis of data processing according to the GDPR can be verified and remains the same throughout the data processing,

▪ the rights of those concerned are ensured,

▪ the security requirements of data management have been met.

The legal basis for data management is provided by Act CXII of 2011 on the right to self-determination of information and freedom of information. law and the GDPR.

Consent of the person concerned, conditions

▪ If the data management is based on consent, the data controller must be able to prove that the data subject has consented to the processing of his personal data.

▪ If the data subject gives his consent in the context of a written statement that also applies to other matters, the request for consent must be communicated in a way that is clearly distinguishable from these other matters.

▪ The data subject has the right to withdraw his consent at any time. Withdrawal of consent does not affect the legality of data processing based on consent prior to withdrawal. Before giving consent, the data subject must be informed of this. Withdrawal of consent should be possible in the same simple way as giving it.

▪ When determining whether the consent is voluntary, the fact must be taken into account to the greatest extent possible, among other things, whether the consent to the processing of personal data, which is they are not necessary for the performance of the contract.

▪ The processing of personal data in relation to information society-related services offered directly to children is legal if the child has reached the age of 16. In the case of a child under the age of 16, the handling of the children's personal data is legal only if and to the extent that the consent was given or authorized by the person exercising parental supervision over the child.

Data management that does not require identification

If the purposes for which the data controller processes personal data do not or no longer require the identification of the data subject by the data controller, the data controller is not obliged to retain additional information.

If the data controller can prove that it is not in a position to identify the data subject, it will inform the data subject accordingly if possible.

Information and rights of the person concerned

The principle of fair and transparent data management requires that the data subject receives information about the fact and purposes of data management.

If the personal data is collected from the data subject, the data subject must also be informed whether he is obliged to disclose the personal data, as well as the consequences of not providing the data. This information can also be supplemented with standardized icons in order for the data subject to receive general information about the planned data management in a clearly visible, easily understandable and legible form.

Information related to the handling of personal data concerning the data subject must be provided to the data subject at the time of data collection, and if the data was not collected from the data subject but from another source, it must be made available within a reasonable time frame, taking into account the circumstances of the case.

The data subject has the right to access the data collected about him and to exercise this right simply and at reasonable intervals in order to establish and check the legality of the data management. All data subjects must be guaranteed the right to know, in particular, the purposes of the processing of personal data and, if possible, the period for which the processing of personal data applies.

In particular, the data subject has the right to have their personal data deleted and no longer processed if certain conditions are met, if the collection or processing of personal data in another way is no longer necessary in connection with the original purposes of the data management, or if the data subjects have withdrawn their consent to the processing of the data.

If the processing of personal data is carried out for the purpose of obtaining direct business, the data subject must be guaranteed the right to object to the processing of his personal data for this purpose at any time free of charge.

Review of personal data

In order to ensure that the storage of personal data is limited to the necessary period, the data controller establishes deletion or regular review deadlines.

Regular review deadline established by the head of the organization: 1 year.

Duties of the data controller

The data controller applies appropriate internal data protection rules for the sake of legal data management. This regulation covers the powers and responsibilities of the data controller.

It is the duty of the data controller to implement appropriate and effective measures, as well as to be able to prove that the data management activities comply with the applicable legislation.

This regulation must be made taking into account the nature, scope, circumstances and purposes of data management, as well as the risk affecting the rights and freedoms of natural persons.

The data manager implements appropriate technical and organizational measures taking into account the nature, scope, circumstances and purposes of data management, as well as the variable probability and severity of the risk to the rights and freedoms of natural persons. On the basis of this regulation, other internal regulations are reviewed and, if necessary, updated.

The data manager or the data processor keeps an appropriate record of the data management activities carried out under its authority. All data controllers and data processors are obliged to cooperate with the supervisory authority and make these records available upon request in order to control the relevant data management operations.

Rights of data subjects

The right to request information

Through the contact details provided, you can request information from us on what data our company processes, on what legal basis, for what data management purpose, from what source, and for how long. Upon your request, we will send information to the e-mail address you provided without delay, but within 30 days at most.

Right to rectification

You can ask us to change any of your data via the contact details provided. Upon your request, we will act on this immediately, but within 30 days at the latest, and we will send information to the e-mail address you provided.

The right to erasure

You can ask us to delete your data via the contact details provided. At your request, we will do this immediately, but within 30 days at most, and we will send information to the e-mail address you provided. Deletion of data cannot be initiated, among other things, if the data management is necessary to fulfill an obligation under EU or member state law applicable to the data controller.

The possibility of legal enforcement related to data management

In the case of illegal data processing that you have experienced, notify our company so that it is possible to restore the legal status within a short period of time.

Legal remedy

1.) The person concerned may use the right to submit a complaint to the supervisory authority:

National Data Protection and Freedom of Information Authority

Address: 1125 Budapest, Szilágyi Erzsébet fasor 22/c

E-mail: ugyfelszolgalat@naih.hu

2.) you can apply to the court: Capital Court, 1055 Budapest, Markó utca 27.

The tasks of the organization for adequate data protection

- Data protection awareness. Professional preparation must be ensured to comply with the legislation. It is essential to prepare the staff professionally and familiarize them with the regulations.

- The purpose and criteria of data management, the concept of personal data management must be reviewed. Legal data management and data processing must be ensured in accordance with the data protection and data management regulations.

- Adequate information to the person involved in data management. It should be noted that - if the data processing is based on the data subject's consent - in case of doubt, the data controller must prove that the data processing has been consented to by the data subject.

- The information provided to the person concerned should be concise, easily accessible and easy to understand, therefore it must be formulated and displayed in clear and understandable language.

- The requirement of transparent data management is that the person concerned receives information about the facts and purposes of data management. The information must be provided before the start of the data management and the right to information belongs to the data subject until its termination during the data management.

- The main rights of the person involved in data management are the following:

▪ access to personal data relating to him;

▪ correction of personal data;

▪ deletion of personal data;

▪ limiting the processing of personal data;

▪ protest against profiling and automated data processing;

▪ the right to data portability.

- The data controller informs the data subject without undue delay, but at the latest within one month of receipt of the request.

- The data management carried out by the organization must be reviewed, the right to information self-determination must be ensured. At the request of the person concerned, their data must be deleted without delay, if the person concerned withdraws the consent that forms the basis of the data management, and there is no other legal basis for the data management.

- It must be clear from the consent of the person concerned that the person concerned consents to data management. If data management is based on the data subject's consent, in case of doubt, the data controller must prove that the data subject consented to the data management operation.

- In the case of personal data management of children, special attention must be paid to compliance with data management rules. The processing of personal data in relation to information society-related services offered directly to children is legal if the child has reached the age of 16. In the case of a child under the age of 16, the handling of the children's personal data is legal only if and to the extent that the consent was given or authorized by the person exercising parental supervision over the child.

- In case of illegal handling or processing of personal data, there is an obligation to report to the supervisory authority. The data controller must report the data protection incident to the supervisory authority without undue delay - no later than 72 hours after becoming aware of the data protection incident.

- In certain cases, it may be justified for the data controller to conduct a data protection impact assessment prior to data management. During the impact assessment, it is necessary to examine how the planned data management operations affect the protection of personal data. If the data protection impact assessment determines that data management is likely to involve a high risk, the data controller must consult with the supervisory authority before processing personal data.

- In the event that the main activities include data management operations that, due to their nature, scope or goals, require regular and systematic, large-scale monitoring of the data subjects, a data protection officer must be appointed. The appointment of a data protection officer aims to strengthen data security.

Data security

The data must be protected with appropriate measures, in particular against unauthorized access, alteration, transmission, disclosure, deletion or destruction, as well as against accidental destruction and damage, as well as against becoming inaccessible due to changes in the technology used.

In order to protect the data files managed electronically in the registers, an appropriate technical solution must be used to ensure that the data stored in the registers cannot be directly linked and assigned to the data subject.

When planning and applying data security, the current state of technology must be taken into account. Among several possible data management solutions, the one that ensures a higher level of protection of personal data must be chosen, unless it would represent a disproportionate difficulty for the data controller.

Data protection incident

A data protection incident is a breach of security that results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure or unauthorized access to personal data transmitted, stored or otherwise handled.

In the absence of appropriate and timely measures, a data protection incident can cause physical, financial or non-financial damage to natural persons, including the loss of control over their personal data or the restriction of their rights, discrimination, identity theft or identity abuse.

The data protection incident must be reported to the competent supervisory authority without undue delay, at the latest within 72 hours, unless it can be proven in accordance with the principle of accountability that the data protection incident is unlikely to pose a risk to the rights and freedoms of natural persons.

The affected person must be informed without delay if the data protection incident is likely to involve a high risk to the rights and freedom of the natural person, so that he can take the necessary precautions.

Data management for administrative and record purposes

The organization may also process personal data in cases related to its activities and for administrative and record-keeping purposes.

Data management is based on the voluntary and definite consent of the person concerned based on adequate information. After the detailed information - which covers the purpose, legal basis and duration of the data management as well as the rights of the person concerned - the person concerned must be warned about the voluntary nature of the data management. Consent to data management must be recorded in writing.

Data management for administrative and record-keeping purposes serves the following purposes:

- data management of the organization's members and employees, which is based on a legal obligation;

- data management of persons in a contractual relationship with the organization for contact, settlement and record keeping purposes;

- contact details of other organizations, institutions and businesses that have a business relationship with the organization, which may also include contact and identification data of natural persons;

The data management according to the above is based on the one hand on a legal obligation, and on the other hand, the data of the person concerned has expressly consented to the processing of his data (for example, for the purpose of an employment contract or registered as a partner on a website, etc.)

In the case of documents sent to the organization in written form – including personal data – (e.g. resume, job search application, other submissions, etc.), the consent of the person concerned must be assumed. After the case is closed - in the absence of consent or legal obligation for further use - the documents must be destroyed. The fact of destruction must be recorded in a protocol.

In the case of data management for administrative purposes, personal data are only included in the documents and records of the given case. The processing of these data lasts until the document on which the processing is based is disposed of.

In order to ensure that the storage of personal data is limited to the necessary period, data management for administrative and record-keeping purposes must be reviewed annually, and inaccurate personal data must be deleted immediately.

Compliance with the legislation must also be ensured in the case of data management for administrative and record-keeping purposes.

Data management for other purposes

If the organization wishes to carry out data management that is not included in these regulations, its internal regulations must be supplemented beforehand, and sub-rules corresponding to the new data management purpose must be attached.

Other documents belonging to the regulations

Documents and regulations that contain, for example, a written statement of consent to data management or, for example, describe the mandatory data management information in the case of websites, must be linked to the data protection and data management policy and managed together with it.