



**DATA PROCESSING INFORMATION NOTICE
ON THE RIGHTS OF THE DATA SUBJECT
REGARDING THE PROCESSING OF THEIR PERSONAL DATA**

TABLE OF CONTENTS

INTRODUCTION

DEFINITIONS

CHAPTER I – IDENTIFICATION OF THE DATA CONTROLLER

CHAPTER II – IDENTIFICATION OF DATA PROCESSORS

CHAPTER III – DATA PROCESSING RELATED TO EMPLOYMENT

CHAPTER IV – DATA PROCESSING RELATED TO CONTRACTS

CHAPTER V – DATA PROCESSING BASED ON LEGAL OBLIGATIONS

CHAPTER VI – SUMMARY OF THE DATA SUBJECT'S RIGHTS

CHAPTER VII – DETAILED INFORMATION ON THE DATA SUBJECT'S RIGHTS

CHAPTER VIII – SUBMISSION OF A REQUEST BY THE DATA SUBJECT,
ACTIONS OF THE DATA CONTROLLER

INTRODUCTION

The European Parliament and the Council (EU) Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC (hereinafter: Regulation), requires the Data Controller to take appropriate measures to ensure that all information relating to the processing of personal data is provided to the data subject in a concise, transparent, intelligible, and easily accessible form, using clear and plain language. The Data Controller must also facilitate the exercise of the data subject's rights.

The obligation to provide prior information to the data subject is also prescribed by Act CXII of 2011 on informational self-determination and freedom of information.

With this information notice, we fulfil our statutory obligations. The notice must be published on the Association's website or sent to the data subject upon request.

Definitions

For the purposes of this Policy, the definitions contained in Article 4 of the Regulation apply.

We highlight the main concepts:

1. "personal data": any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
2. "processing": any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure, or destruction.
3. "restriction of processing": the marking of stored personal data with the aim of limiting their processing in the future.
4. "profiling": any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural

person's work performance, economic situation, health, personal preferences, interests, reliability, behaviour, location, or movements.

5. "pseudonymisation": the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.
 6. "filing system": any structured set of personal data which is accessible according to specific criteria, whether centralised, decentralised, or dispersed on a functional or geographical basis.
 7. "controller": the natural or legal person, public authority, agency or any other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its designation may be provided for by Union or Member State law.
 8. "processor": a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.
 9. "recipient": a natural or legal person, public authority, agency or any other body to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall comply with the applicable data protection rules according to the purposes of the processing.
 10. "third party": a natural or legal person, public authority, agency or body other than the data subject, the controller, the processor, and persons who, under the direct authority of the controller or processor, are authorised to process personal data.
 11. "consent of the data subject": any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
 12. "personal data breach": a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.
-

CHAPTER I – IDENTIFICATION OF THE DATA CONTROLLER

Publisher and Data Controller:

Name: Hungarian Chemical Society (Magyar Kémikusok Egyesülete)

Registered seat: 1106 Budapest, Fehér út 10.

Registration number: 01-02-0000387

Tax number: 19815819-2-42

Representative: János Szabó dr.

Phone: +36307204417

Email: mail@mkeorg.hu

Website: mke.org.hu

(Hereinafter: Association)

CHAPTER II – IDENTIFICATION OF DATA PROCESSORS

A **data processor** is a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller (Regulation, Article 4(8)).

Engaging a data processor does not require the prior consent of the data subject, but the data subject must be informed. Accordingly, we provide the following information:

1. IT Service Providers of the Association

The Association engages data processors for the operation and maintenance of its website. They provide IT services (hosting) and, under the term of the contract, process the personal data submitted on the website by storing them on the server.

Data Processor:

Company name: MOLCOMP SYSTEM Kft.

Registered seat: 1192 Budapest, Gellért u. 17/3

Company registration number: 01-09-268709

Tax number: 10893087-2-43

Representative: István Molnár

Phone: +36 30 960 3049

Email: molnar@molcomp.hu

Company name: Etalon Bázis Kft

Registered seat: 2500 Esztergom, Mohácsy köz 4.

Company registration number: 11-09-007384

Tax number: 11917632-2-11

Representative: István Kuti

Phone: +36 20 92-59-363

Email: admin@hirlevelmanager.hu

2. Auditor / Accounting Service Provider

For fulfilling its tax and accounting obligations, the Association employs an external service provider who processes the personal data of natural persons who have contractual or payer relationships with the Association.

Data Processor:

Company name: TRIÁSZ-AUDIT Kft.

Registered seat: 1037 Budapest, Jutas u. 54

Company registration number: 01-09-685625

Tax number: 11966461-2-41

Representative: Eszter Ágnes Varga

3. Postal and Delivery Services

These processors receive the personal data necessary for delivering ordered products (name, address, phone number) and use them exclusively for delivery.

Service provider: Magyar Posta

CHAPTER III – DATA PROCESSING RELATED TO EMPLOYMENT

1. Employment and Personnel Records

1. **Only data strictly necessary** for establishing, maintaining, or terminating employment, or for providing social/welfare benefits may be requested or recorded.
2. The Association processes the following employee data based on the employer's legitimate interest (GDPR Article 6(1)(f)), for the purpose of establishing, performing, or terminating employment:
 - name
 - birth name
 - date of birth
 - mother's maiden name
 - address
 - nationality
 - tax identification number

- social security number
 - pension ID (for pensioners)
 - phone number
 - email address
 - ID card number
 - address card number
 - bank account number
 - online identifier (if applicable)
 - start/end of employment
 - job title
 - copies of educational or qualification certificates
 - photograph
 - CV
 - salary information, benefits
 - data related to lawful deductions
 - performance evaluation
 - reasons for termination
 - criminal record certificate (where job-specific)
 - results of medical fitness examinations
 - pension fund information (where applicable)
 - passport number (for foreign employees)
 - accident report data
 - welfare service–related data
 - data recorded by security cameras, entry systems, or geolocation systems
3. Data relating to **health** or **trade union membership** may only be processed when required by the Labour Code.
 4. Recipients: employer representatives, HR staff, data processors.
 5. Personal data of executive employees may be shared with the Association's owners.

6. Storage period: **3 years** after termination of employment.
 7. The data subject must be informed that the processing is based on the Labour Code and the employer's legitimate interest.
-

2. Data Processing Related to Medical Fitness Examinations

1. Only examinations required by law or necessary for the employer's legal obligations may be performed.
 2. Tests assessing job suitability may be used before or during employment.
 3. Large-scale psychological or personality testing must be **anonymous**, unless otherwise justified.
 4. Data processed: **the fact of job suitability** and conditions if applicable.
 5. Legal basis: **legitimate interest** of the employer.
 6. Purpose: establishing or maintaining employment, fulfilling job requirements.
 7. Recipients: examined employee and the professional conducting the test.
 8. Storage period: **3 years** after termination of employment.
-

3. Data of Job Applicants (Applications and CVs)

- Data processed: name, date/place of birth, mother's name, address, qualifications, photo, phone number, email, employer's notes.
 - Purpose: evaluating applications, selecting candidates, concluding an employment contract.
 - Legal basis: **consent** of the applicant.
 - Data recipients: authorised managers and HR staff.
 - Storage: until evaluation is complete; non-selected applicants' data must be deleted.
 - Retention beyond this is only allowed with explicit, voluntary consent.
-

4. Monitoring of Work Email Accounts

- Work email accounts may **only** be used for work purposes.

- Personal use is prohibited.
 - The employer may check the mailbox every **3 months**, based on legitimate interest.
 - Purpose: verifying compliance with work rules.
 - The employee must be informed of the inspection procedure and their rights.
 - Personal emails must be deleted by the employee; if they fail to do so, the employer may delete them.
-

5. Monitoring of Work Computers, Laptops, Tablets

- Devices provided for work may only be used for work.
 - No personal data may be stored on them.
 - Monitoring follows the same rules as work-email monitoring.
-

6. Monitoring of Workplace Internet Use

- Only work-related websites may be visited.
 - Personal browsing is prohibited.
 - Monitoring may be carried out based on legitimate interest.
-

7. Monitoring of Company Mobile Phones

- Personal use is prohibited.
 - The employer may access all outgoing call data and stored information.
 - Employees must report private use; they may be required to cover related costs.
-

8. GPS Tracking

- Legal basis: legitimate interest (work organisation, logistics, verifying employee duties).
- Data processed: vehicle ID, route, distance, usage time.
- GPS monitoring may only occur **during working hours**.

CHAPTER IV – DATA PROCESSING RELATED TO CONTRACTS

1

1. Processing of Data of Contracting Partners — Customer and Supplier Records

(1) The Association processes the following personal data of natural persons who enter into a contract with it as customers or suppliers, based on the legal basis of **contract performance**. The purposes are: concluding the contract, performing it, terminating it, and providing contractual discounts. The processed data include:

- name
- birth name
- date of birth
- mother's maiden name
- address
- tax identification number
- tax number
- entrepreneur registry number / primary producer certificate number
- ID card number
- address (residence)
- registered office, business address
- phone number
- email address
- website
- bank account number
- customer number, order number
- online identifier (customer or supplier lists, loyalty lists)

This data processing is also lawful when performed at the request of the data subject prior to entering into a contract.

Recipients: customer service staff, accounting/taxation staff, and data processors of the Association.

Storage period: 5 years after termination of the contract.

Information duty: the data subject must be informed that the processing is based on contract performance.

Information on data processors: the data subject must be informed about any transfer of their data to processors.

1

2. Contact Data of Representatives of Legal Person Clients, Customers, and Suppliers

(1) Personal data processed:

- name
- address
- phone number
- email address
- online identifier

(2) Purpose: fulfilment of the contract between the Association and the legal-person partner; business communication.

Legal basis: **consent** of the data subject.

(3) Recipients: customer-service employees of the Association.

(4) Storage period: **5 years** after the end of the business relationship or the representative's mandate.

1

3. Visitor Data Processing on the Association's Website

(1) Cookies are short data files stored on the user's device by the visited website. Their purpose is to facilitate or make the online service more convenient.

Cookies generally belong to two categories:

- **Session cookies** (temporary) – deleted when the session ends.
- **Persistent cookies** (e.g., language settings) – remain until the user deletes them.

According to EU guidelines, cookies **requiring consent** may only be placed with user permission.

(2) Cookies not requiring consent must be disclosed to the user upon first visit. Full text is not required — a link is sufficient.

(3) Cookies requiring consent may also be disclosed on first visit if they begin processing upon entering the page. Summary information and a link to full details is sufficient.

1

4. Information on the Use of Cookies

(1) The Association uses cookies on its website. A cookie is a small file with character data placed on the user's computer when visiting a website. It allows the website to recognise the user's browser on subsequent visits. Cookies may store:

- user settings (e.g., chosen language)
- other information (e.g., shopping cart contents)

Cookies enhance usability, prevent abuse, ensure smooth operation, and support quality service.

(2) During website use, the following data may be recorded:

- user's IP address
- browser type
- OS characteristics (e.g., language)
- date/time of visit
- visited subpages, functions, services

(3) Accepting cookies is not mandatory; users may block or manage them in browser settings.

The Association lists major browser cookie instructions. Certain services may not fully function without cookies.

(4) Cookies cannot identify the user directly.

(5) Types of cookies used:

1. Strictly necessary session cookies

- Purpose: ensure the proper functioning of the site.
- Deleted when the session ends.
- Data processed: *AVChatUserId, JSESSIONID, portal_referer*
- Legal basis: Act CVIII of 2001 (Elkertv.) §13/A(3)
- Purpose: website functionality.

2. Cookies requiring consent

2.1. Convenience cookies

Legal basis: user consent.

Purpose: improving efficiency, enhancing user experience.

Storage: **6 months**.

All above based on turn1search1.

5. Registration on the Association's Website

(1) Registration requires the user to give consent by ticking a checkbox—pre-ticked boxes are forbidden.

(2) Personal data processed:

- name (first and last)
- address
- phone number
- email address
- online identifier

(3) Purposes of processing:

1. Providing website services
2. Contacting the user (email, phone, SMS, post)
3. Informing about products, services, terms, promotions
4. Sending advertising materials (email or post)
5. Analysing website usage

(4) Legal basis: **consent** of the data subject.

(5) Recipients: customer service, marketing employees; IT service provider staff.

(6) Storage period: as long as registration exists, or until consent is withdrawn.

6. Newsletter Subscription

(1) Subscription requires explicit consent by ticking a checkbox (not pre-ticked). Unsubscription may occur via link, in writing, or by email, which withdraws consent — all data must be deleted immediately.

(2) Data processed:

- name (first + last)
- email address

(3) Purposes:

1. Sending newsletters on products/services
2. Sending advertisements

(4) Legal basis: **consent**.

(5) Recipients: marketing staff; IT service provider (hosting).

(6) Storage period: until newsletter service ends or consent is withdrawn.

1

7. Community Guidelines / Data Processing on the Association's Facebook Page

(1) Purpose: presenting and promoting the Association's products/services.

(2) Messages sent on Facebook do **not** count as official complaints.

(3) Personal data posted by visitors are **not processed** by the Association.

(4) Facebook's own Privacy and Service Terms apply.

(5) Illegal or offensive content may be removed without notice.

(6) The Association is not responsible for unlawful content posted by users or for any errors or malfunctions of Facebook.

CHAPTER V – DATA PROCESSING BASED ON LEGAL OBLIGATIONS

1

1. Data Processing for Fulfilling Tax and Accounting Obligations

(1) The Association processes personal data based on **legal obligation**, for the purpose of fulfilling statutory tax and accounting duties (bookkeeping, taxation). The processed personal data of natural persons engaged as customers or suppliers are those required by law, including:

- data required under the 2017 Act CXXVII on VAT (name, address, tax status, tax number),
- data required under Act C of 2000 on Accounting (issuer's name, address, signatures, etc.),
- data required under Act CXVII of 1995 on Personal Income Tax (entrepreneur certificate number, tax identification number).

(2) Storage period: **8 years** after termination of the legal basis.

(3) Recipients: employees performing taxation, bookkeeping, payroll, social security administration, and the Association's data processors.

2. Payer Data Processing

(1) Based on legal obligation, the Association processes data for fulfilling tax and social contribution obligations (tax advances, payroll computation, social security, pensions). This applies to: employees, their family members, contracted individuals, and anyone receiving benefits.

Processed data include:

- personal identification data (including former names, titles),
- gender, nationality,
- tax identification number,
- social security number (TAJ),
- and, where relevant under tax law, **health data** (e.g. deductions under PIT Act §40) and **trade-union membership** (PIT Act §47(2)b)).

(2) Storage period: **8 years** after end of legal basis.

(3) Recipients: employees performing tax, payroll, and payer administration; processors.

3. Archival Obligations under the Archives Act

(1) The Association processes personal data contained in documents classified as having **permanent value** under Act LXVI of 1995 (Archives Act). Purpose: ensuring long-term preservation for future generations.

(2) Storage period: until transfer to the public archives.

CHAPTER VI – SUMMARY INFORMATION ON THE RIGHTS OF THE DATA SUBJECT

(This chapter provides a short overview; details are in Chapter VII.)

1

The data subject has the right to:

- **Right to prior information** (Articles 13–14)
- **Right of access** (Article 15)
- **Right to rectification** (Article 16)
- **Right to erasure (“right to be forgotten”)** (Article 17)
- **Right to restriction of processing** (Article 18)
- **Notification obligation regarding rectification or erasure** (Article 19)
- **Right to data portability** (Article 20)
- **Right to object** (Article 21)
- **Right not to be subject to automated decision-making, including profiling** (Article 22)
- **Restrictions on rights** (Article 23)
- **Right to be informed about data breaches** (Article 34)
- **Right to lodge a complaint with a supervisory authority** (Article 77)
- **Right to an effective judicial remedy against the authority** (Article 78)
- **Right to an effective judicial remedy against the controller or processor** (Article 79)

CHAPTER VII – DETAILED INFORMATION ON THE DATA SUBJECT’S RIGHTS

1

Below are the detailed legal descriptions exactly as required by GDPR.

1. Right to Prior Information (Articles 13–14 GDPR)

The controller must provide detailed information at the time personal data is collected, including:

- identity and contact details of the controller and DPO,

- purposes and legal basis of processing,
- legitimate interests (where applicable),
- recipients, transfers to third countries, safeguards,
- storage period,
- rights of access, rectification, deletion, restriction, objection, portability,
- right to withdraw consent,
- right to lodge a complaint,
- whether providing data is mandatory,
- existence of automated decision-making or profiling.

If data is not collected directly from the data subject, additional rules apply regarding timing and method of notification.

2. Right of Access (Article 15 GDPR)

The data subject may request:

- confirmation of processing,
- access to personal data,
- information about purposes, categories, recipients, storage period, rights, data sources,
- information about automated decision-making and profiling,
- copies of processed data.

Additional copies may incur a reasonable fee.

3. Right to Erasure (“Right to be Forgotten”) (Article 17 GDPR)

Data must be deleted if:

- no longer needed for its original purpose,
- consent is withdrawn and no other legal basis exists,
- the data subject objects and there is no overriding legitimate interest,
- processing was unlawful,
- deletion is required under EU or Member State law,

- data were collected in relation to information society services offered to a child.

Exceptions apply (e.g. freedom of expression, legal obligation, public interest, research, legal claims).

Controllers must inform other controllers using the data (where reasonably possible).

4. Right to Restriction of Processing (Article 18 GDPR)

Applies if:

- accuracy of data is contested,
 - processing is unlawful and deletion is refused,
 - controller no longer needs the data but the subject needs it for legal claims,
 - the subject objects (pending verification).
-

5. Right to Data Portability (Article 20 GDPR)

Applies when:

- processing is based on consent or contract,
- processing is automated.

The data subject may receive the data in a machine-readable format and may request direct transmission between controllers, where technically feasible.

6. Right to Object (Article 21 GDPR)

The data subject may object at any time to processing based on:

- public interest tasks
- legitimate interest of controller or third party.

If objecting to **direct marketing**, the data **must not** be processed further.

7. Automated Decision-Making Including Profiling (Article 22 GDPR)

The data subject has the right **not** to be subject to decisions based solely on automated processing, except where:

- necessary for a contract,

- permitted by law,
- based on explicit consent.

Safeguards must include human intervention and the right to contest the decision.

8. Restrictions on Rights (Article 23 GDPR)

EU or national law may restrict certain rights for purposes such as:

- national security,
 - public safety,
 - crime prevention,
 - economic interests,
 - judiciary independence,
 - regulatory oversight,
 - protection of others' rights.
-

9. Information on Personal Data Breaches (Article 34 GDPR)

The data subject must be informed of any breach posing a high risk to rights and freedoms, except if:

- data were protected (e.g. encrypted),
 - subsequent measures eliminated the risk,
 - individual notification requires disproportionate effort (in this case: public notification).
-

10. Right to Lodge a Complaint (Article 77 GDPR)

The data subject may lodge a complaint with the supervisory authority in their place of residence, workplace, or location of the alleged infringement.

11. Right to Judicial Remedy Against Supervisory Authority (Article 78 GDPR)

If the authority does not act or issues a binding decision, the data subject may seek judicial remedy.

12. Right to Judicial Remedy Against Controller or Processor (Article 79 GDPR)

The data subject may bring proceedings before the courts where the controller/processor is established or where the data subject resides.

CHAPTER VIII – SUBMISSION OF REQUESTS AND ACTIONS OF THE CONTROLLER

1

(1) The controller must respond **within 1 month** of receiving a request.

(2) This period may be extended by **2 additional months** for complex or numerous requests; the data subject must be notified within the first month.

(3) If the request was submitted electronically, the response should also be provided electronically (unless requested otherwise).

(4) If the controller does not act, the data subject must be informed within 1 month, including the right to lodge a complaint or seek judicial remedy.

(5) Information and actions under Articles 13–22 and 34 are provided **free of charge**, unless requests are:

- manifestly unfounded, or
- excessive or repetitive — in which case a **6,350 HUF fee** may be charged or the request refused.

(6) The controller may request additional information if there are doubts regarding the requester's identity.