

HST Trainer

Information on the processing of personal data

pursuant to Regulation (EU) 2016/679 (GDPR)

Document version: 1.0

Language: English

1. Introduction

This information notice describes how the HST Trainer System processes the personal data of users who use the service.

The HST Trainer System is a digital tool designed to support educational activities, training exercises and personal development in the field of telegraphy reception (CW), as well as activities organized by groups, associations or organizations that use the service.

The processing of personal data is carried out in compliance with the principles established by:

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (GDPR);
- applicable national legislation on personal data protection.

The System is designed according to the principle of data minimization, collecting and using only the information necessary for the proper operation of the service.

Users' personal data are mainly used for:

- account management;
- management of group membership;
- access authorization;
- use of training tools;
- management of personal activity history;
- support of the learning path.

The System is not designed as a personal ranking system or a competitive evaluation system for users.

The activity history and results obtained have exclusively the following purposes:

- educational;
- training-related;
- organizational;
- supporting individual and group improvement.

Each user maintains control over their own learning path, and data relating to their activities are used exclusively within the purposes provided by the System.

2. Data Controller

The Data Controller of the HST Trainer System and of the processing of personal data is:

Alessandro Corsini (IK5MEP)

Legal address:

50019 Sesto Fiorentino (FI)

Italy

Contact email for requests relating to personal data:

ik5mep@libero.it

The Data Controller determines the purposes and methods of processing personal data and adopts the necessary measures to ensure that processing takes place in compliance with current legislation.

For any request relating to personal data, the data subject may contact the Data Controller through the indicated email address or through the procedures available within the System.

3. Purposes of personal data processing

The personal data collected through the HST Trainer System are processed exclusively for purposes related to the operation of the service, user management and the educational activities provided.

In particular, data may be used for the following purposes:

3.1 User account management

Data processing is necessary to:

- create and manage the user's personal account;
 - allow access to the System;
 - verify the user's identity through the provided email address;
 - manage access credentials;
 - keep the personal information necessary for the operation of the service updated.
-

3.2 Management of group membership

The System uses an organized structure based on working groups.

Data are used to:

- associate each user with their group;
- allow the Group Manager to perform organizational functions;
- manage access permissions;
- configure specific educational activities for the group.

Each user may belong exclusively to the groups for which they are authorized.

3.3 Educational activities and CW training

Personal data and data relating to performed activities are used to allow:

- use of the HST Trainer System;
 - configuration of exercises;
 - customization of training methods;
 - recording of completed activities;
 - monitoring of the individual learning path.
-

3.4 Personal activity history management

The System records the history of activities carried out by the user for the purpose of:

- allowing the user to monitor their own improvement;
- allowing the Group Manager to support the educational path;
- identifying possible difficulties;
- promoting progressive improvement of individual skills.

The personal activity history is not used for commercial purposes or user profiling.

3.5 Statistics and educational comparison

The System may process statistics relating to completed activities.

Such statistics have exclusively the following purposes:

- educational;
- training-related;
- organizational.

The comparison between members of the same group aims to:

- encourage collaboration;
- stimulate personal improvement;
- help the group grow in a consistent way.

No automatic publication of personal rankings is carried out and results are not used to create public evaluations of users.

3.6 Technical and organizational communications

Contact data may be used for communications necessary for the operation of the System, such as:

- registration confirmation;
- email address verification;
- account-related communications;
- technical information about the service;
- communications relating to account security.

No promotional or advertising communications are sent.

3.7 Security and administrative management

Data may be processed to:

- ensure the security of the System;
- prevent unauthorized access;
- manage possible technical issues;
- correctly administer users and groups.

Administrative access is regulated by specific authorization levels and, for accounts with elevated privileges, may include two-factor authentication systems.

4. Types of personal data processed

The HST Trainer System collects and processes exclusively the personal data necessary for the operation of the service and for the educational activities provided.

The principle adopted is that of data minimization; therefore, information that is not necessary for the declared purposes is not collected.

The processed data can be divided into the following categories.

4.1 User identification data

For account creation and management, the following data may be processed:

- name;
- surname;
- amateur radio callsign, if available;
- email address.

These data allow the identification of the user and the correct management of their participation in group activities.

4.2 Account-related data

To allow access to the System, the following data may be processed:

- internal user identifier;
- account status:
 - pending authorization;
 - active;
 - disabled;
 - deleted;
- information relating to authorizations;
- role assigned within the System.

Password data are not stored in readable form, but exclusively according to appropriate technical

protection methods.

4.3 Group membership data

For organizational management, the following data may be processed:

- group identifier;
- user's group membership;
- authorization status within the group;
- information necessary for management by the Group Manager.

The System does not use group membership to create personal rankings or evaluations other than those related to the intended educational purposes.

4.4 CW training activity data

During the use of the HST Trainer System, information relating to completed exercises may be recorded, such as:

- completed exercises;
- configurations used;
- training speed;
- characters used in exercises;
- results obtained;
- progress of activities over time.

These data constitute the user's personal history and are used exclusively for educational purposes.

4.5 Technical access and session data

To ensure the correct operation of the System, strictly necessary technical data may be processed, such as:

- information relating to the authenticated session;
- user's access status;
- technical information necessary for service security.

The System uses only the technical systems necessary for session management and authentication.

No commercial profiling tools or user activity monitoring systems are used for purposes other than the operation of the service.

4.6 Data relating to minor users

The System may also be used by minor users within activities organized by authorized groups or organizations.

The System processes only the data necessary for account management and does not collect additional age-related information, except where required for compliance with applicable obligations.

Authorizations relating to minors are managed according to the procedures adopted by the relevant group.

Documentation relating to parental consent or consent of persons exercising parental responsibility remains with the responsible group and is not stored within the System.

4.7 Data not collected

The HST Trainer System does not collect or process:

- health data;
- data relating to unnecessary personal conditions;
- financial data;
- commercial information;
- data used for advertising profiling.

Data collection is limited exclusively to what is necessary to provide the service.

5. Legal basis for processing

The processing of personal data carried out through the HST Trainer System takes place in compliance with the principles established by Regulation (EU) 2016/679 (GDPR) and is based on the applicable legal grounds in relation to the different activities performed.

5.1 Consent of the data subject

The main legal basis for processing is the consent of the data subject, expressed through the System registration procedure.

During registration, the user:

- views the Privacy Information Notice;
- accepts the System Terms of Use;
- provides consent for the processing of data necessary for account management.

Consent must be freely given, specific and informed.

5.2 Performance of the service requested by the user

The processing of data is also necessary to allow the provision of services requested by the user through the System.

In particular, data are necessary to:

- create and manage the personal account;

- authenticate the user;
- allow access to HST Trainer tools;
- associate the user with their group;
- manage the available educational functions.

Without the processing of the necessary data, it would not be possible to provide the requested service.

5.3 Organizational management of groups

The processing of data relating to group membership is necessary to allow the correct operation of the organizational model of the System.

Such processing allows:

- the Group Manager to manage authorized users;
 - configuration of the group's educational activities;
 - ensuring that each user accesses only the functions provided for their role.
-

5.4 Protection of System security

Some processing activities may be carried out to ensure System security and prevent unauthorized use.

These purposes include:

- access session management;
- account protection;
- verification of possible anomalies;
- management of administrative access.

These activities are necessary to ensure secure use of the System.

5.5 Minor users

In the case of minor users, data processing takes place in compliance with the authorizations required by applicable legislation.

Registration to the System may be carried out by the data subject or by the person responsible for registration, but account activation takes place only after verification by the Group Manager or the Administrator.

The relevant group manages any authorizations required by legislation, keeping the related documentation according to its internal procedures.

5.6 Withdrawal of consent

The data subject may withdraw consent to the processing of their personal data at any time.

Withdrawal of consent does not affect the lawfulness of processing carried out before the withdrawal request.

Withdrawal may result in the inability to continue using some or all System functions if data processing is essential for the operation of the service.

6. Personal data processing methods

The processing of personal data through the HST Trainer System is carried out using computer tools and organizational procedures designed to ensure the security, correctness and confidentiality of information.

Processing is carried out according to the following principles:

- lawfulness;
 - fairness;
 - transparency;
 - data minimization;
 - purpose limitation;
 - integrity and confidentiality.
-

6.1 Technical processing methods

Personal data may be processed through:

- System IT infrastructure;
- dedicated databases;
- authentication procedures;
- account management systems;
- tools necessary for the operation of HST Trainer.

Access to data takes place exclusively through authorized procedures and according to the role assigned within the System.

6.2 Separation of roles and permissions

The System adopts an access management system based on role separation.

Each subject may access only the information necessary to perform their assigned functions.

The following main access levels are provided:

User

The user may access:

- their own personal data;
- their own activity history;

- their own results;
- authorized educational functions.

The user cannot access the personal data of other users.

Group Manager

The Group Manager may access data relating to users belonging to the groups under their responsibility for organizational and educational purposes.

The Group Manager may:

- verify registration requests;
- authorize users;
- manage necessary group information;
- manage necessary user information;
- configure HST Trainer activities;
- monitor participants' educational progress.

Access is limited exclusively to users belonging to their own group.

System Administrator

The System Administrator manages the overall operation of the platform.

The Administrator may access the tools necessary for:

- System administration;
- group management;
- user management;
- System security;
- technical interventions.

Administrative access is protected by additional security measures, including the possibility of using two-factor authentication systems.

6.3 Information confidentiality

All subjects authorized to access personal data must use such information exclusively for the purposes provided by the System.

It is prohibited to:

- use data for personal purposes;
 - communicate information to unauthorized subjects;
 - disclose users' personal data;
 - use individual activity histories for purposes other than educational ones.
-

6.4 Information retention

Data are stored for the period necessary to achieve the purposes for which they were collected.

The System applies procedures to:

- keep accounts updated;
- disable users who are no longer active;
- delete data when no longer necessary;
- manage deletion requests.

Specific retention methods and periods are described in the following chapter dedicated to this topic.

6.5 Security of processing

The Data Controller adopts appropriate technical and organizational measures to protect personal data from:

- unauthorized access;
- accidental loss;
- unauthorized modification;
- improper disclosure.

The adopted measures are evaluated and updated according to the technical evolution of the System.

7. User and group management

The HST Trainer System uses an organizational model based on the division of users into working groups.

Each group represents an organized set of participants who follow a common educational path through the tools provided by the System.

User and group management is carried out according to security, confidentiality and access limitation principles.

7.1 User registration

The user may submit a registration request through the appropriate procedure available on the System.

During registration, only the information necessary for account creation is requested.

The procedure includes:

- entering the required personal data;
- indicating the group membership through the code provided by the Group Manager;
- verification of the email address through a link containing a temporary token;
- creation of the personal account.

Completion of the registration process does not automatically enable access to the System.

7.2 Account verification and authorization

After registration, the account is placed in the status:

"Pending authorization"

Access to System functions remains suspended until verification by authorized subjects.

Verification may be performed by:

- the Group Manager;
- the System Administrator.

The verification aims to confirm:

- correct membership of the indicated group;
 - accuracy of the entered information;
 - presence of required authorizations where applicable;
 - compliance of the registration with the organizational rules of the group.
-

7.3 User management by the Group Manager

The Group Manager may manage users belonging to their own group exclusively for organizational and educational purposes.

Within their permissions, the Group Manager may:

- verify registration requests;
- authorize or disable users;
- manage necessary user information;
- change group membership when required by organizational needs;
- update necessary group information;
- configure HST Trainer tools for the group;
- select characters used in exercises;
- configure available training parameters;
- monitor users' educational progress.

The Group Manager cannot access information relating to users belonging to other groups.

7.4 Group management

Each group has its own organizational configuration.

The Group Manager may:

- modify the group description;
- configure training methods;

- define HST Trainer parameters;
- select educational elements used by the group.

The Group Manager cannot:

- rename the group;
- permanently delete the group;
- modify general System settings.

Disabling a group, when necessary, is managed according to the established administrative procedures.

7.5 Separation of information between different groups

The System ensures logical separation of information belonging to different groups.

A user, Group Manager or authorized subject may access only information compatible with their assigned role.

Users' personal data and activity histories are not automatically shared between different groups.

8. Management of minor users

The HST Trainer System may also be used by minor users within educational activities organized by authorized groups or organizations.

The management of minor users follows the principles of personal protection and minimization of processed information.

The System does not automatically classify users based on age and does not use age as a standard criterion for organizing groups.

Any age-based subdivisions may only be adopted within specific external activities, such as competitions or events, according to the rules established by the event organizers.

8.1 Registration procedure for minors

The registration procedure for the System is the same for all users.

The account may be requested:

- directly by the data subject;
- through the procedures adopted by the group of belonging.

The technical creation of the account does not automatically allow access to the System.

Each new account remains in the status:

"Pending authorization"

until verification is carried out by the Group Manager or the Administrator.

8.2 Consent of the parent or person exercising parental responsibility

In the case of minor users, the relevant group manages the authorizations required by applicable legislation.

The parent or person exercising parental responsibility signs the authorization form at the reference group.

The documentation relating to consent:

- is kept by the responsible group;
- is not uploaded to the System;
- is not stored by the Data Controller.

The Group Manager verifies the presence of the required authorizations before enabling the account.

8.3 Limitation of processed data

For minor users, only information necessary for the operation of the System is processed.

The following are not collected:

- unnecessary additional personal data;
 - information relating to family circumstances;
 - health information;
 - data relating to personal aspects unrelated to educational purposes.
-

8.4 Responsibility of the group of belonging

The group hosting minor users plays a fundamental role in organizational management.

The Group Manager is responsible for:

- verifying correct user registration;
 - verifying the presence of required authorizations;
 - using data exclusively for the intended purposes;
 - ensuring confidentiality of available information.
-

8.5 External communication relating to minors

The HST Trainer System does not automatically publish data, images or results relating to minor users.

Any external communications, such as:

- presentation of activities;
- participation in events;
- publications;
- competitions or demonstrations;

must be managed separately by the organizing group and must comply with the required authorizations.

9. Roles and authorizations

The HST Trainer System adopts a role-based management system in order to ensure that each subject can access only the information necessary to perform their assigned functions.

The division of roles allows the application of the following principles:

- access control;
- limitation of authorizations;
- confidentiality of personal data;
- proper organizational management.

The main roles provided by the System are:

- User;
 - Group Manager;
 - System Administrator.
-

9.1 User role

The user uses the System to participate in the educational activities provided by their group.

The user may:

- access their personal account;
- view their personal information;
- use HST Trainer according to the configurations established by the group;
- consult their personal activity history;
- view their results and progress;
- view the activity history of members belonging to their working group;
- consult training charts and indicators relating to group members, exclusively for educational purposes and to support collective improvement;
- request modification of their personal information;
- request deletion of their data according to applicable legislation.

Consultation of the history and charts of other group members does not constitute a ranking system or competitive evaluation of users, but represents a tool intended to:

- encourage collaboration;
- stimulate personal improvement;
- share the learning path;
- allow the group to grow consistently.

The user cannot:

- independently modify their personal information stored in the System;
- modify other users' personal data;
- access personal data of users belonging to other groups;

- modify group configurations;
- modify general System parameters.

Requests for modification of personal data are managed by authorized subjects according to the procedures established by the System.

9.2 Group Manager role

The Group Manager performs organizational and educational functions for users belonging to their group.

The Group Manager may:

- verify registration requests;
- authorize users belonging to their group;
- manage necessary user information;
- modify group membership when necessary;
- update necessary group information;
- configure the group's HST Trainer settings;
- select characters used during training sessions;
- set speed parameters and exercise modes;
- monitor participants' educational progress.

The Group Manager cannot:

- access data of users belonging to other groups;
 - modify the group's identification name;
 - permanently delete a group;
 - modify general System settings.
-

9.3 System Administrator role

The System Administrator manages the overall operation of the System and ensures the correct technical and organizational functioning of the service.

The System Administrator may:

- manage users and groups;
- verify authorizations;
- intervene for technical requirements;
- manage System security;
- administer general configurations;
- support Group Managers in resolving operational issues.

Administrative access must be used exclusively for technical and organizational purposes.

The System Administrator does not use users' personal data for purposes other than those provided by the System.

9.4 Principle of separation of responsibilities

The management of the System is based on the principle that each subject receives only the permissions necessary for their role.

In particular:

- the user manages their own personal learning path;
- the Group Manager manages exclusively their own group;
- the System Administrator manages the general System.

This separation reduces the risk of improper access and provides greater protection of personal information.

10. Personal data retention

The HST Trainer System stores users' personal data for the period necessary to achieve the purposes for which the data was collected and according to the principles of necessity, proportionality and data minimization established by the GDPR.

Data retention periods vary depending on the status of the account and the user's activity.

10.1 Active account

Regularly authorized and used accounts are maintained active in order to allow the user to:

- access the System;
- carry out training activities;
- consult personal activity history;
- participate in the activities of the assigned group.

Data is retained for the entire period during which the user participates in the platform and in the related group.

10.2 Account inactivity

If a user does not access the System for a continuous period of 6 months, the account may automatically be placed in a suspended status.

Suspension is intended to:

- maintain proper user management;
- avoid indefinite retention of unused accounts;
- allow possible verification by the Group Manager.

The user may be re-enabled according to the procedures provided by the System.

10.3 Deletion of inactive accounts

After automatic suspension, if the account remains unused for an additional period of 12 months, the account and the personal data associated with it will be permanently deleted.

Deletion includes:

- user's identification data;
- account information;
- group association data;
- personal data connected to the System.

Technical data required for legal obligations or security purposes may be retained within the limits established by applicable legislation.

10.4 Deletion upon request of the data subject

The user may request deletion of their personal data at any time.

The request is processed without waiting for the automatic deletion periods described above.

Following verification of the request:

- the account is deleted;
- personal data is removed;
- references allowing identification of the user are deleted.

Deletion applies to all data directly attributable to the data subject, except where legal obligations require a different retention period.

10.5 Historical data and educational purposes

The management of activity history is carried out exclusively for educational purposes.

In the event of user deletion, personal data directly associated with the individual is removed according to the procedures provided.

Any data processing that no longer contains identifying elements may be retained only when necessary for statistical or technical purposes.

10.6 Management of disabled groups

A group may be disabled by the System Administrator when it is no longer operational.

Disabling a group results in suspension of group activities, preventing new accesses or new associations.

The subsequent management of users belonging to the disabled group is carried out according to the procedures applicable to inactive accounts.

11. Information security

The HST Trainer System adopts technical and organizational measures designed to protect users' personal data and ensure secure use of the service.

Security is achieved through a set of procedures, controls and technological tools designed to prevent:

- unauthorized access;
 - accidental loss of data;
 - improper use of information;
 - unauthorized modification of personal data;
 - disclosure to unauthorized subjects.
-

11.1 Account protection

Each user has a personal account associated with their access credentials.

The System adopts technical measures to protect:

- user identifiers;
- access credentials;
- personal information associated with the account.

Passwords are not stored in readable form, but through technical procedures that prevent direct access or visualization.

The user is responsible for maintaining the confidentiality of their credentials and must not disclose them to third parties.

11.2 Secure communications

Access to the System takes place through a protected connection.

Communications between the user's device and the System are performed using security protocols appropriate to the current state of available technology.

This reduces the risk of interception or unauthorized access to transmitted information.

11.3 Access session management

The System uses technical session mechanisms necessary to:

- maintain user authentication;
- verify access status;
- ensure the correct operation of available functions.

Sessions are managed according to security criteria and may be invalidated in case of:

- voluntary logout by the user;

- expiration of the session;
- security requirements of the System.

The System does not use user tracking mechanisms for purposes other than the technical management of the service.

11.4 Role-based access control

Access to information is regulated through a role-based authorization system.

Each user can access only information compatible with their authorization level.

In particular:

- the User accesses their own data and authorized training tools;
 - the Group Manager accesses the information necessary to manage their own group;
 - the System Administrator manages the System according to the established purposes.
-

11.5 Security of administrative access

Accounts with administrative privileges have higher authorization levels and are therefore subject to additional security measures.

The following tools may be adopted:

- multi-factor authentication;
- access verification procedures;
- internal control procedures.

Administrative accesses are used exclusively for platform management, maintenance and security activities.

11.6 Backup and data protection

The Data Controller adopts appropriate procedures to reduce the risk of data loss.

Backup and restoration procedures may be updated according to:

- technological evolution of the System;
 - operational requirements;
 - required security levels.
-

11.7 User responsibilities

Each user contributes to the security of the System through correct use of the service.

The user must:

- keep their credentials confidential;
 - not share their account;
 - report any anomalies;
 - use the System in compliance with the regulations.
-

12. Use of technical sessions

The HST Trainer System uses only the technical systems necessary for the proper operation of the service, in particular for managing users' authentication sessions.

Sessions allow the System to recognize an already authenticated user and maintain the connection between the user and the available functions while browsing.

12.1 Purpose of sessions

Technical sessions are used exclusively to:

- maintain user access after authentication;
 - verify that the user has the required permissions;
 - associate performed operations with the correct account;
 - ensure the correct operation of System functions.
-

12.2 Absence of profiling systems

The HST Trainer System does not use:

- commercial profiling cookies;
- advertising systems;
- user behavioral analysis tools;
- tracking systems aimed at creating personal profiles.

Technical information used during sessions has exclusively operational and security purposes.

12.3 Temporary technical data

During session management, only strictly necessary technical information may be processed, such as:

- session identifier;
- authentication status;
- information necessary for access security.

Such information is not used for purposes other than the operation of the System.

12.4 Session duration

Sessions are maintained for the period necessary to use the service.

A session may end:

- upon user's request through logout;
- due to inactivity;
- for security reasons;
- according to the technical settings adopted by the System.

At the end of the session, the associated temporary information is invalidated according to the established procedures.

12.5 Access through personal devices

Users may access the System through personal devices.

Users are responsible for:

- keeping their device updated;
 - using appropriate protection tools;
 - avoiding access from insecure devices;
 - logging out when using shared devices.
-

12.6 Changes to technologies used

If new technologies necessary for the operation of the System are introduced in the future, the Data Controller will update this information notice when required by applicable legislation.

Any new features involving additional processing activities compared to those described will be introduced in compliance with the principles of transparency and data minimization.

12.7 Recording of platform access

To ensure service security and allow technical verification, the HST Trainer System maintains a log of user authentication operations.

The System may record access-related information, including:

- user identifier;
- date and time of access;
- date and time of logout;
- result of the access request;
- IP address used for connection.

Access logging is carried out exclusively for:

- IT security purposes;

- prevention of unauthorized access;
 - analysis of possible anomalies;
 - technical and administrative support.
-

12.8 Use of access data

Access log data:

- is not used for user profiling;
- is not used for commercial purposes;
- is not used to evaluate users' skills or educational behavior.

Access to this information is restricted to authorized subjects according to their role and operational needs of the System.

12.9 Retention of access data

Access-related data is retained for a limited period proportional to the security purposes of the service.

The retention period may be defined according to:

- technical requirements of the System;
 - applicable legal obligations.
-

13. External communications

The CW Trainer platform uses users' contact details exclusively for communications necessary for the operation of the service and for the management of the planned activities.

Communications are carried out in compliance with the following principles:

- necessity;
- transparency;
- limitation of purposes;
- confidentiality of personal information.

13.1 Communications related to registration

During the registration procedure, technical communications may be sent to the email address provided by the user.

Such communications may include:

- confirmation of the registration request;
- sending of the link containing the verification token;
- confirmation of email address validation;
- information regarding the status of the account.

The link sent by email has the sole purpose of verifying the availability of the provided email address and

completing the required registration procedure.

13.2 Communications related to account authorization

When a user submits a registration request, the system may generate a notification intended for the authorized subjects responsible for user management.

The communication has the sole purpose of informing about the presence of a new request requiring verification.

The notification may be sent to:

- Platform Administrator;
- Group Manager indicated by the user.

The communications do not necessarily contain the personal data of the applicant, but may simply indicate the presence of a pending request to be verified by accessing the platform.

13.3 Technical and organizational communications

Users may receive communications related to:

- technical changes to the platform;
- service maintenance;
- account security;
- updates required for the correct use of the system;
- organizational information related to group activities.

Such communications are an integral part of the service and do not constitute promotional activities.

13.4 Absence of commercial communications

The CW Trainer platform does not use users' personal data for:

- sending advertisements;
- commercial communications;
- direct marketing;
- profiling of personal interests.

The email addresses collected are used exclusively for purposes related to the operation of the platform.

13.5 Communication of data to external parties

Users' personal data are not communicated to external parties, except in the following cases:

- obligations required by law;
- requests from competent authorities;
- technical requirements related to service providers that perform services necessary for the operation of the platform, when formally identified in accordance with applicable legislation.

Any future use of external service providers will be evaluated according to the requirements established by the GDPR.

13.6 Communications related to public activities or events

Participation in external activities, events, competitions or public presentations does not automatically result in the publication of users' personal data.

Any publication of:

- names;
- results;
- images;
- information relating to participants;

must be managed separately by the organizer of the activity and carried out in accordance with the required authorizations.

14. Rights of the data subject

Users of the CW Trainer platform, as data subjects whose personal data are processed, may exercise the rights provided for by Regulation (EU) 2016/679 (GDPR).

The Data Controller guarantees the possibility of exercising these rights through simple, transparent and accessible procedures.

14.1 Right of access to personal data

The data subject has the right to know:

- whether the processing of their personal data is taking place;
- which personal data are being processed;
- the purposes of the processing;
- the authorized subjects who may access the data;
- the expected retention period.

The data subject may request a copy of the personal data being processed.

14.2 Right to rectification and modification

The data subject has the right to request the correction of inaccurate or outdated personal data.

The request may concern:

- identification data;
- personal information associated with the account;
- data that are no longer correct compared to the current situation.

Changes are carried out according to the procedures provided by the platform and may be performed by subjects authorized to manage users.

14.3 Management of user modification requests

The user may request changes to their personal information.

Depending on the type of data, the modification may be:

- carried out directly by the user, when allowed by the platform;
- carried out by the Group Manager;
- carried out by the Platform Administrator.

Changes relating to organizational information or affecting group management may require intervention by authorized subjects.

14.4 Right to erasure of personal data

The data subject may request the deletion of their personal data.

The request involves:

- verification of the identity of the requester;
- deletion of the account;
- deletion of personal data associated with the user;
- removal of personal associations present within the platform.

Deletion is carried out without waiting for the timeframes established for the automatic deletion of inactive accounts.

14.5 Right to restriction of processing

The data subject may request the restriction of the processing of their personal data in the cases provided for by applicable legislation.

The restriction may involve the temporary suspension of certain processing operations while maintaining the information required for legal obligations.

14.6 Right to data portability

In the cases provided for by the GDPR, the data subject may request to receive the personal data provided in a structured, commonly used and machine-readable format.

The request will be assessed according to the nature of the processed data and the available technical procedures.

14.7 Procedures for exercising rights

Requests relating to personal data may be submitted through the dedicated privacy request section available within the platform.

Through this procedure, the data subject may request:

- access to personal data;
- modification or correction of personal information;
- restriction of processing where applicable;
- deletion of the account and personal data;
- information regarding the processing of personal data.

The request must contain the information necessary to identify the data subject and correctly manage the procedure.

Requests will be handled by the Data Controller according to the procedures required by applicable legislation.

For any additional communication or specific needs, the following email contact is also available:
ik5mep@libero.it

14.8 Relationship with the Group Manager

For organizational aspects related to participation in the group, the user may also contact the Group Manager.

The Group Manager may handle requests relating to information necessary for the management of group activities, while requests concerning rights provided by the GDPR remain under the responsibility of the Data Controller.

15. Request for modification or deletion of the account

The CW Trainer platform guarantees users the possibility to request, at any time, the modification or deletion of their personal data, in accordance with the rights provided by Regulation (EU) 2016/679 (GDPR).

Requests are managed through the dedicated procedure available in the privacy section of the platform.

15.1 Request for modification of personal data

The user may request the modification of their personal information when they consider that it is:

- incorrect;
- incomplete;
- outdated.

The request may concern, by way of example:

- identification data;
- contact information;
- account-related data.

The modification is carried out according to the type of information concerned:

- directly by the user, when allowed by the platform;
- by the Group Manager;
- by the Platform Administrator.

Changes affecting the organization of the group or the management of the account may require prior verification.

15.2 Request for deletion of personal data

The user may request the deletion of their account and the associated personal data at any time.

The request is processed without waiting for the periods established for the automatic deletion of inactive accounts.

Within account management, some data perform technical functions necessary for the correct operation of the platform:

- the first name and surname may be used as identification information and to support account recovery;
- the email address represents the user's primary identifier (username) and is also used for password recovery procedures.

The deletion of the email address associated with the account necessarily results in the deletion of the user account from the system, as the fundamental parameter required for authentication and access recovery is no longer available.

The first name and surname, when no longer necessary or upon request by the data subject, may be removed or modified according to the procedures provided by the platform, without necessarily requiring deletion of the account.

Following a request for complete account deletion, the necessary operations are carried out to:

- delete the user account from the platform;
- remove directly associated personal data;
- delete the association with the user's group;
- remove personal references stored within the platform systems.

Any data without identifying elements may be retained exclusively for technical or statistical purposes, where compatible with applicable legislation.

15.3 Verification of the request

To ensure the security of personal data, verification of the identity of the requester may be carried out before proceeding with modification or deletion.

Verification may take place through:

- user authentication on the platform;
- verification of the associated email address;
- additional procedures deemed necessary.

The verification has the sole purpose of preventing requests made by unauthorized persons.

15.4 Effects of deletion

Deletion of the account results in:

- loss of access to the platform;
- removal of the association with the group;
- deletion of personal data linked to the user.

Any data without identifying elements may be retained exclusively for technical or statistical purposes, where compatible with applicable legislation.

15.5 Management of the user within the group

In the case of users belonging to a working group, the request for modification or deletion is communicated and managed according to the procedures established.

The Group Manager may be involved exclusively for necessary organizational aspects, without replacing the Data Controller in the management of rights provided by the GDPR.

15.6 Deletion of users no longer belonging to the platform

Deletion may occur:

- upon direct request of the data subject;
- due to non-use of the platform according to the established periods;
- due to organizational deactivation of the account or the associated group.

Deletion is carried out according to the criteria defined in the chapter concerning data retention.

16. Personal Data Breach

The CW Trainer platform adopts technical and organizational measures aimed at preventing events that may compromise the security of users' personal data.

A personal data breach is defined as an event that involves, accidentally or unlawfully:

- unauthorized access to data;
- loss or destruction of data;
- unauthorized alteration of information;
- disclosure or availability of data to unauthorized persons.

16.1 Management of security incidents

In the event of a suspected or confirmed personal data breach, the Data Controller shall:

- analyze the event;
- identify the nature and extent of the breach;
- assess which data may be involved;
- adopt measures to contain or eliminate the consequences of the event;
- verify the need for any communications required by applicable legislation.

16.2 Risk assessment

Each event is assessed considering, among other aspects:

- type of data involved;
- number of potentially affected users;
- possible consequences for data subjects;
- possibility of unauthorized access or improper use of information.

Based on the assessment performed, the necessary actions are determined.

16.3 Communication to data subjects

If the breach presents a high risk to the rights and freedoms of users, the Data Controller shall inform the affected data subjects according to the provisions of the GDPR.

The communication may include:

- a general description of the event;
- information regarding the data involved;
- possible consequences;
- measures adopted to reduce risks;
- any operational instructions for users.

16.4 Communication to the competent authority

Where required by applicable legislation, the Data Controller shall notify the competent authority of the breach within the deadlines established by the GDPR.

The assessment of whether such notification is necessary is carried out based on the nature of the event and the level of identified risk.

16.5 Cooperation of authorized persons

Persons operating within the platform according to specific roles, such as:

- Administrator;
- Group Manager;

must promptly report any anomalies or situations that may compromise data security.

They must not:

- attempt to access data not required for their role;
 - disclose confidential information;
 - modify data without authorization.
-

17. Processing of personal data of minors

The HST Trainer System may also be used by minor users.

In the case of registration of a minor, the processing of personal data takes place exclusively after authorization by the person exercising parental responsibility, in compliance with applicable legislation.

The collected data are limited to those strictly necessary for registration, authentication and use of the System functionalities.

The Data Controller reserves the right to request, where necessary, documentation proving the consent provided by the parent or legal guardian.

18. Updates to the Privacy Notice

This Privacy Notice may be updated over time in order to keep the document consistent with:

- any regulatory changes;
- technical developments of the platform;
- introduction of new functionalities;
- changes in the methods of processing personal data.

Each update is carried out by the Data Controller, ensuring that the contents of the document remain compliant with the principles established by Regulation (EU) 2016/679 (GDPR).

18.1 Document version

Each revision of the Privacy Notice is identified through:

- version number;
- update date;
- brief description of the changes made.

The current version of the document is:

Version 1.0

18.2 Communication of changes

If updates involve substantial changes to the methods of processing personal data, users will be informed through the tools available on the platform.

Changes may concern, by way of example:

- new functionalities;
 - new data collected;
 - new methods of using information;
 - changes in authorized data processing subjects.
-

18.3 Acceptance of the new version

When necessary, users may be required to review the new version of the Privacy Notice before continuing to use the platform.

Failure to accept substantial changes may result in limitations to the use of the service, where the updated processing of data is essential for the operation of the platform.

18.4 Retention of previous versions

Previous versions of the Privacy Notice may be retained by the Data Controller for documentation purposes and to ensure traceability of the changes made.

End of Document 1

Privacy Notice on the processing of personal data

CW Trainer

Italian version – Document version 1.0

Data Controller:

Alessandro Corsini (IK5MEP)

Address:

50019 Sesto Fiorentino (FI) – Italy

Email:

ik5mep@libero.it