OSCE/ODIHR

Election Expert Database

Privacy Statement

Table of contents

1. What is the OSCE/ODIHR Election Expert Database?

The OSCE/ODIHR Election Expert Database is a tool created for the recruitment and management of experts and observers for ODIHR's election observation activities. The database is built around user profiles of experts, with search functions to facilitate ODIHR's selection of individuals for particular assignments based on specific criteria, such as experience, gender, languages, regional or thematic experience. The database serves as the main mechanism for users and ODIHR Election Department staff to add, update, and store information about individuals involved in ODIHR election-related activities.

The database falls under the responsibility of the ODIHR Head of Election Department. However, the collecting and processing of the data performed by OSCE participating States election observation focal points falls under the responsibility of their respective organisations.

Database information will be accessible by staff of ODIHR Election Department, ODIHR election observation activities, and national focal points, with different access rights. For details please refer to point *3*.

Registration occurs only at the initiative of the user. However, some information might be also passed to the roster by the national focal point.

2. What information do we collect, for what purpose and through which technical means?

In general, registration is mandatory to be able to be selected and participate in ODIHR election observation missions, training, and other electoral assistance activities. We store the information that you provide or that your organisation provides directly to us. By logging in and accessing accounts you are indicating your consent to the use of the data as described in this statement.

The data obtained from the registration process includes both personal details and details related to your professional background, skills, and election-related activities. Personal details include:

- Username
- Personal information
- Preferences, including sharing options with your country's election observation Focal Point
- Emergency Contact
- Professional Experience
- Professional Training
- Education
- Language Skills
- Computer Skills
- Publications
- References
- Travel Information

In case of selection for an assignment, you will be asked to provide additional information by submitting a **Registration Form**:

- Confirmation of airport of departure and return   [text field]
- Copy of passport (if not already uploaded)   [document to be uploaded]
- Photo (if not already uploaded)   [document to be uploaded]
- Accreditation Form (if required)   [document to be uploaded]
- Beneficiary Form (valid for 2 years)   [document to be uploaded]
- Supplier Registration Form (valid for 2 years)   [document to be uploaded]
- Other possible questions/documents.

This additional information, apart from the forms which are valid for 2 years, will be deleted after the completed mission, unless you wish to include it in your permanent profile. In such case you will not need to submit it for every mission and will be kept as long as your personal details (maximum 7 years since last update of your account).

We also store certain additional information (listed below) relating to the activity on your user account, so that we can protect both your identity and the integrity of the OSCE systems that you access.

We may collect the following additional data about each user:

- Date and time of:
    - o Last change of password
    - o Last password reset
- Number of good logins and failed attempts

When you login and/or change your password, we may record further information in log files, such as the IP address used, in line with the purposes stated above. This information can help in following up any doubtful activity relating to your account. It will not be used to monitor your activity, except to allow the removal of the account when no longer used.

3. Who has access to your information and to whom is it disclosed?

By registering to the database, you authorise the disclosure of the details you have entered in the user registration system to, ODIHR Election Department staff directly involved in the management and recruitment for the particular mission, your participating State election observation focal point, and system managers of the database who take care of the IT part of the system. ODIHR missions' staff will not have direct access to the database; however they will be provided by ODIHR with the information directly relevant for the conduct of the mission. If your registration form is submitted by your national focal point (i.e. in case of secondment), your consent is assumed to have been given (implicitly or explicitly) for the transfer of your details.

> ODIHR **will not** divulge your information to any other third parties.

Your password is stored only in an irreversible form. Apart from your password, the service administrators can view all of the data pertaining to a particular user. This helps them to perform duties such as helping users with problems and diagnosing suspected security incidents.

Types of access			
	ODIHR Staff	**IT Company maintaining the application**	**Participating States Focal Points***	**Core Team and administrative staff of election-related activity**
	Up to 20 people	Up to 5 people	Up to 5 people per focal point	Up to 10 people
Basic Account Information, Personal Information, Travel Information, Emergency Contact, Mission Registration Form	Full access and processing of data	Exceptional access for maintenance purposes	Limited to nationals of the relevant participating State	Limited to the specific election-related activity**
Other profile information	Full access and processing of data	Exceptional access for maintenance purposes	-	Limited to the specific election-related activity**

* – Focal Points will be allowed to access your data only if you explicitly allow for such access in the Preferences section of the profile.
** – Offline access. Offline users are instructed to handle personal information in strict confidentiality and to delete it both in electronic and in printed form at the end of their assignment.

4. How do we protect and safeguard your information?

Processing of the personal data of mission participants happens only under the authorisation and control of ODIHR. Personal data is treated as confidential, accessed only by the staff directly involved in the management of the mission, and only to the extent that is strictly necessary for the management of the mission.

Personal data is protected by appropriate technical and organisational measures from being copied, altered, removed, disclosed or erased in unauthorised way. Any copies of personal data regarding the mission participants are deleted or physically destroyed after the end of their necessary use for the purpose of the particular mission.

ODIHR stores your personal information in secure computers and your information can only be accessed by authorised persons. When you login, the password is always encrypted on the network and is decrypted for checking against the stored password by the authentication service.

Similarly, certain users are allowed to reset their password using e-mail. They should bear in mind that anyone else with access to their e-mail (because of automatic forwarding, delegation or other reasons) will be able to reset the password. If you have any reason to believe that your password has been compromised – for example, if your password appears to have been changed without your knowledge – you should notify your normal support contact or contact ODIHR as described on the website.

Notes:
- In principle, and especially if you have access to sensitive systems, you should never reveal your password to anybody else: it is a secret only you should know.
- When you enter your password, make sure your browser indicates (usually by means of a padlock or other icon) that you are on a secure connection and that you are connected to an ODIHR site address.

5. How can you verify, modify or delete your information?

You will be able to change and remove any personal information on-line. If you were ever selected for a mission, ODIHR will keep the information relative to your participation in missions for statistical and historical purposes. The data preserved in the database will include your name, date of birth, gender, nationality and name and type of mission in which you participated. Additionally, ODIHR can maintain some information for statistical purposes but only in anonymised version (separated from your name, date of birth and other personal information which will be deleted).

6. How long do we keep your data?

The roster keeps your data for as long as you are recorded as an active user and for a period of seven years thereafter. In case your account has not been updated for seven years, you will receive a message on the e-mail account registered in the roster, informing you that your data will be deleted from the roster.

> **Important:** ODIHR will consider you active as long as you log in and update your account at least once in seven years.

If you do not react to the message, your data, apart from the information mentioned in point *5*, will be deleted. It will not be possible to restore the deleted information.

7. Contact Information and recourse

If you wish to ask a question or submit a complaint about the service with respect to the use of your personal information, you should contact:

Deputy Head, Election Department
OSCE Office for Democratic Institutions and Human Rights (ODIHR)
Miodowa 10 | 00-251 Warsaw
Email: dataprotection.electionexpert@odihr.pl