M-16018/30/2021-SS-III

श्रम एवं रोजगार मंत्रालय
GOVERNMENT OF INDIA
MINISTRY OF LABOUR & EMPLOYMENT

e-Shram
S h r a m e v   J a y a t e
NATIONAL DATABASE OF UNORGANISED WORKERS

Guidelines on Data Integration/ Sharing through eShram Portal with Central Government Ministries

682492/2023/MOLE

Table of Contents

1. Introduction to eShram

Ministry of Labour & Employment (MoLE) has developed eShram portal for creation of a comprehensive National Database of unorganized workers (NDUW) verified by Aadhaar eKYC for all types of unorganized workers such as Construction Workers, Agricultural Workers, Domestic Workers and other sub-group of unorganized workers. The registration of workers in the portal has commenced from August 2021.

The data on eShram portal is proposed to be shared with the Central Government Ministries for extending social security benefits/welfare schemes to the workers registered on the eShram portal.

2. Key Objectives of the Guidelines

The key objectives of the Guidelines are as under:

- To clearly define the process to be followed during data sharing.
- To clearly define the roles and responsibilities of the Central Government Ministries for using eShram data.
- To provide necessary provisions and guidelines related to the privacy and security of eShram data being shared with the Central Government Ministries.
- To list out the precautions to be taken regarding storage, handling and utilization of the data being shared from eShram.
- To provide transparency and remove any ambiguity related to procedure and nuances of the data sharing activity from eShram to the Central Government Ministries and vice versa.

3. Key Points for sharing eShram data

The following are the key points for sharing of eShram data with any of the Central Government Ministries:

- All Central Government Ministries are encouraged to build a system for exchanging data to and from eShram through API.
- Those Central Government Ministries which require eShram data, will send their specific request to MoLE in the prescribed requisition form attached herewith.

M-16018/30/2021-SS-III

- The Ministries/ Departments shall verify and validate the data shared by eShram before extending any benefit/scheme to any eShram registrant. The responsibility of verification and validation of data will be with the Ministry using it.

- The Ministries are encouraged to seed corresponding UAN of the worker as per eShram data in their databases after required mapping, verification, and validation of the data.

- The Ministries using the data will share the verified eShram data record with eShram portal along with unique Id, if any generated in their database, of that worker.

- Once eShram receives verified data from the user Ministries, the verified fields will be stored in the secondary table in eShram database. The unique Id of the worker generated from the user Ministry database will be stored in the existing field earmarked for this in the eShram database.

- The verified data of the Central Government Ministries shared with eShram database will also be available to the eShram registrant for viewing along with the eShram data and as per his/her entries.

- The anonymised eShram data may be utilized for research activities by authorized government research institutes and their associated bodies only with approval of MoLE.

- Sharing and verification of eShram data have also been initiated with all the State/UT Governments. It is expected that MoLE shall receive verified data from the States/UTs in due course of time based on verification done by respective verification officers. Such verified data received from States/UTs shall also be made available to Central Government Ministries. However, if any Ministry desires to use eShram data for any benefit transfer or policy formulation, the verification onus lies with that Ministry using the data.

- eShram registrant will be able to update his/her data on eShram even after receipt of his/her verified record from the Central user Ministry: -
    - Only data collected through eShram will be available for updation. The same will be sent to Central Government Ministries through API for re-verification.
    - In case of updation of verified data of workers in any Central Government Ministry database, the same will be communicated to eShram through API. If user Ministry's verified data is already existing in eShram secondary table, the same will get overwritten with the latest updated and verified data received from that ministry for a particular worker.
    - The user Ministry should also provide date of updation and verification along with the verified data records.

- Matching and tagging of any Central Government Ministry records with eShram data as well as taking consent of workers for sharing their data with eShram will be the responsibility of the concerned Central Government Ministry.

It is proposed to share data with the Central Government Ministry through following two methods:

i. Provision 1 – Data Sharing through API with any Ministry having their own portal for registration and maintaining database of citizens.
ii. Provision 2 – Data Sharing through Data Sharing Portal (DSP) with any Ministry not having their own portal for registration and maintaining database of citizens based on any category or parameter.

4. Data Sharing Provision 1: Data exchange through API

For API based data exchange following activities will be carried out:

- Common API description document shall be shared by MoLE with the Central Government Ministry. For each Ministry, API shall be created by both eShram and respective Central Government Ministry for exchange of data from eShram to the corresponding Ministry databases and vice versa.
- API parameters and responses to the API calls shall be defined through appropriate API documentation between technical team of the user Ministry and the eShram team.
- The APIs for data sharing will have various authorisation mechanism such as token-based authorization etc.

4.1 Scenario 1 - Central Government Ministries having Aadhaar seeded Database

Steps to be followed for sharing of existing data

Step - 0 - The Central ministry should de-duplicate their database on the basis of Aadhaar to ensure that there is single record corresponding to unique Aadhaar.

Step - 1 - eShram data with hashed Aadhaar number for the respective Ministry will be shared through API for matching of both the Databases. However, if the user Ministry Database already has UAN number seeded into it, data exchange would be done based on eShram UAN only. The fields to be shared from eShram are as per **Annexure-I**.

M-16018/30/2021-SS-III

Step - 2 - Based on the hashed Aadhaar comparison, each registrant in eShram and Central user Ministry database will be uniquely identified and mapped. The data shared from eShram shall be stored in a separate table in the concerned Central Government Ministry database.

Step - 3 - The user Ministry shall have to verify and validate eShram data and thereafter, UAN will be seeded in user Ministry database for mapped data alongside Unique ID of the concerned Ministry (If available) as additional field of common identifier along with the validated and verified data.

Step - 4 - The user Ministry will return the verified data to eShram after required verification/ validation and consent of workers. The fields to be shared by the Ministry are as per **Annexure-II**.

Step - 5 - A separate table shall be created in eShram database wherein the verified data coming from the user Ministry database shall be stored along with the UAN and Unique Ministry Id of the worker. Unique Ministry ID will get tagged in the original eShram database table also against the corresponding UAN number as a common identifier. Hence, UAN and Unique Ministry ID shall be present in both the tables in eShram as common identifier.

Step - 6 - Data sharing activity shall be done periodically and incremental data from the point of last sharing shall be sent to the user Ministry. Additionally, if any fields for which data have already been shared with the Ministry is updated by a worker in eShram shall again be resent for re-verification purpose. Similarly, in case of updation of verified data of workers in Central Government Ministry database, the same will be communicated to eShram through API. If Central Government Ministry's verified data is already existing in eShram secondary table, the same will get overwritten with the latest updated and verified data received from the Central Government Ministry for a particular worker.

4.2 Scenario 2 - Central Government Ministries that have non-Aadhar seeded Database

Steps to be followed for sharing the data from eShram to the Central Government Ministry portal and vice versa

Step - 1 - eShram data for that Central Government Ministry will be shared through API for the fields as per **Annexure-I**.

Step - 2 - Based on the comparison of the data shared from eShram and Central Government Ministry databases, the user Ministry will uniquely identify and map the common registrant in both the databases.

Step - 3 - The data shared from eShram shall be stored in a separate table in the user Ministry database.

Step - 4 - The Central Government Ministries shall have to verify and validate eShram data and thereafter, UAN will be seeded in the user Ministry database alongside Unique Ministry ID as additional field of common identifier.

Step - 5 - User Ministries will return the verified data to eShram after required verification/ validation and consent of workers. The fields to be shared from Central Government Ministries are as per **Annexure-II**.

Step - 6 - A separate table shall be created in eShram database wherein the verified data coming from the Central Government Ministry database shall be stored alongwith the UAN and unique Ministry ID of the worker. Unique Ministry ID will get tagged in the original eShram database table against the corresponding UAN number as a common identifier. Hence UAN and Ministry ID shall be present in both the tables in eShram as common identifier.

Step - 7 - Data sharing activity shall be done once in a quarter and incremental data from the point of last sharing shall be sent to Central Government Ministries. Additionally, if any fields for which data have already been shared with user Ministry is updated by a worker in eShram shall again be sent for re-verification purpose. Similarly, in case of Updation of verified data of workers in user Ministry database, the same will be communicated to eShram through API. If user Ministries' verified data is already existing in eShram secondary table, the same will get overwritten with the latest updated and verified data received from the user Ministry for a particular worker.

5. Data Sharing Provision 2: Through Data Sharing Portal (DSP)

The Ministry of Labour and Employment envisages to provide Display and Download provision of Central Government Ministry specific eShram data to the Ministries not having their own database. In this regard, separate DSP within the eShram portal will be created. This DSP intends to provide exclusive access to the user Ministries to view and download the Ministry specific data of unorganized workers registered on eShram portal only on need basis.

The process for display, download/ Sharing of data will be as under:

▪ A single common DSP will be prepared under eShram and the same will be hosted centrally along with eShram portal.

M-16018/30/2021-SS-III

- This DSP will enable any Central Government Ministry to get role-based access of the eShram registrant data for view/ download purpose.
- The role-based access will be controlled centrally at MoLE through permissions based on requests received from the concerned user Ministry.
- Central Admin at MoLE can control the data access limit (specific State or district and number of parameters, etc) and type of access (only view or download or both).
- This DSP will have user management (user creation, assignment of specific State/district data visibility/downloading, assignment of specific parameters for access, activating/ deactivating user privileges, etc.) with centralised control.
- User Ministry will be required to nominate an officer not below the rank of Joint Secretary to receive user id and password with view and/or download provision from the data sharing portal of eShram. The nominated officer will also be required to do biometric authentication to access the data sharing portal.
- In order to avoid large data files, the last 7 days' data will be made available for view and/or download provision. This duration will be customizable as per the specific requirement.
- The data download link will be sent to registered email id of authorized user. After the secured access by the authorized user inside the date sharing portal, the data file will be available for 20 minutes (configurable as per requirement) for download, after which file will become unavailable. The password to open the secured file will be sent to registered email id of authorized user in a separate mail.
- The download/view action on eShram data by any authorized user can be tracked and all actions will get logged in the system which can be seen by the user and the Central eShram administrator as well.
- For the purpose of incorporating Multi Factor Authentication, all the users shall also be authenticated through Aadhaar biometric authentication for logging into the system. In case of change of officer, the relieving officer shall authenticate the next officer for access to the DSP.

6. Terms and Conditions of Data Sharing

6.1   MoLE shall not be liable for any incorrectness of the eShram data or resultant losses to the concerned Central Government Ministry upon use of eShram data without prior verification because the eShram data is based on self-declaration by the registrant.

6.2 The Central Government Ministry shall:

i. use the data only for the purpose of extending social security scheme/benefits/messaging and formulation of any policies for the workers by the concerned Ministry.

ii. not re-share eShram data with any other Agency, Department, individual or other Ministries without prior explicit approval of MoLE.

iii. comply with all rules & regulations brought out by Government of India, UIDAI, court rulings etc. regarding privacy and security of the individual data shared through eShram.

iv. follow the Guidelines and all the subsequent amendments/corrigendum to these Guidelines.

v. return the eShram data shared with the user Ministry after due verification and validation, UAN wise and along with Unique Ministry Id if any.

vi. make necessary arrangement for storage of the shared data in a secured environment.

vii. have the complete responsibility for the protection of eShram data from any leakage, theft, phishing or other cyber-attack on the data, once downloaded from the eShram data sharing portal or once transferred through API.

viii. mandatorily verify the data received from MoLE in terms of deduplication, cleansing, physical/ online verification etc. before use of data for any purpose/ benefits or schemes which are intended to be provided to the eShram registrant.

ix. make a provision to flag most probable duplicate records in their system based on self-reporting by individuals or ministries for necessary verification and validation.

The Central Government Ministry headed by Secretary shall be the focal point for sharing the data and for carrying out the obligations as indicated above.

7. Data Security, Protection and Privacy guidelines for the Central Government Ministries

Data security, protection and privacy guidelines advised to be followed by the Central Government Ministries while handling the eShram data in their environment are as under:

i. The user Ministry shall use appropriate antivirus for the system where data is stored.

ii. The user Ministry should ensure Intrusion Detection and Prevention system to be in place for the environment where the eShram Data is stored or used.

iii. The user Ministry should ensure whitelisting of only required ports/IPs in their network's firewall.

iv. The user Ministry should ensure OS hardening in the host system where eShram registrant data will be sent.

v. The user Ministry should ensure latest patches and updates of all the system software are implemented timely and on regular basis.

vi. The user Ministry should carry out periodic security audit of the application and infrastructure used in data sharing though Cert-In empanelled agency.

vii. Security Audit of the user Ministry system wherein the data is stored may be assessed by MoLE or its designated agency at any point in time.

viii. The user Ministry in discussion with eShram team should ensure encryption of the data, through Public and Private key combination for encrypting and decrypting while exchange and storage of data.

ix. The user Ministry should ensure that there is regular Vulnerability Assessment of servers used in transfer and receiving of data.

x. Aadhaar storage guidelines to be followed by user Ministries with whom data is being shared including creation of vaults and so forth.

xi. User Ministries shall ensure that data resides in a data centre located in India. In case, cloud services are used, the services of only NIC Cloud or MeitY empanelled Cloud Service Providers (CSPs) will be utilized. At no point, the data should be stored or replicated outside India.

xii. The data/reports downloaded on individual systems from Data Sharing Portal should be deleted after its intended use.

xiii. All the relevant acts related to data sharing, data protection, data privacy and their subsequent amendments will also be applicable in addition to the data sharing guidelines mentioned in this document.

xiv. User Ministries should ensure that Personal Identifiable Information is not visible to any unauthorised officials, persons, individuals etc. and such information shall be masked to ensure privacy of data.

*****

Fields To be shared with Central Government Ministries from eShram

Sl No.	Fields To be shared with Central Government Ministries from eShram
1	Hashed Aadhaar (SHA 512)
2	Hashed Aadhaar (SHA 256)
3	UAN No.
4	Name of the person
5	Mobile Number
6	DoB
7	Gender
8	Father's/ Husband's name
9	PIN Code - Permanent Address
10	LGD code of District in Permanent Address
11	LGD code of State/UT of Permanent Address
12	LGD code of District in Current Address
13	LGD code of State/UT of Current Address
14	Current Address
15	PIN Code - Current Address
16	Primary Occupation - NCO Code
17	Secondary Occupation - NCO Code
	Mandatory Master Tables to be Imported from eShram
1	Master table of Income Slab
2	Master table of Disability Type
3	Master table of Education Qualification
4	Master table of Gender
5	Master table of Social category
6	Master table of NCO code

682492/2023/MOLE

Fields to be shared by Central Government Ministries with eShram

Sl. No.	Fields to be shared by Central Government Ministries with eShram
1	Hashed Aadhaar (SHA 512)
2	Hashed Aadhaar (SHA 256)
3	Central Ministry Unique ID
4	Father's/ Husband's name
5	Mobile Number
6	Social Category Code
7	Income Slab Code
8	Is Migrant Worker?
9	PIN Code - Permanent Address
10	LGD code of District in Permanent Address
11	LGD code of State/UT of Permanent Address
12	LGD code of District in Current Address
13	LGD code of State/UT of Current Address
14	LGD code of Domicile State/UT
15	PIN Code - Current Address
16	LGD Code of Domicile District
17	Occupation - NCO Code
18	LGD code of Sub-District
19	LGD code of Village
20	Education Qualification Code
21	Bank account – Verified
22	IFSC Code of Bank account – Verified
23	Death of Registrant
24	Disability Type
25	Disability status
26	Is BOCW

M-16018/30/2021-SS-III

eShram Data Requisition Form

PART A

(To be filled by Data Requestor & submitted to Ministry of Labour & Employment (Data Owner), Government of India)

1.	Requestor Ministry / Department	
2.	Data Required through (Data Sharing Portal / API)	
3.	Purpose of the Requirement *(Indicate how data will benefit)*	
4.	Data Requestor Name	
5.	Data Requestor Designation	
6.	Data Requestor Email Id	
7.	Data Requestor Contact No.	
8.	List of data fields required *(Enclose list of fields as per data sharing guidelines)*	
9.	Period of data	From: DD/MM/YYYY To: DD/MM/YYYY

A. Terms and Conditions of Data Sharing

1.   MoLE shall not be liable for any incorrectness of the eShram data or resultant losses to the concerned State/UT/Central Government Ministry upon use of eShram data without prior verification because the eShram data is based on self-declaration by the registrant.

2.   The State/UT/Central Government Ministry shall:

  i.   use the data only for the purpose of extending social security scheme/benefits/messaging and formulation of any policies for the workers by the concerned Ministry/Department.

  ii.   not re-share eShram data with any other Agency, Department, individual or other Ministries without prior explicit approval of MoLE.

  iii. comply with all rules & regulations brought out by Government of India, UIDAI, court rulings etc. regarding privacy and security of the individual data shared through eShram.

iv. follow the Guidelines and all the subsequent amendments/corrigendum to eShram Data Sharing Guidelines.

v. return the eShram data shared with the user Ministry/Department after due verification and validation, UAN wise and along with Unique Ministry/State Id if any.

vi. make necessary arrangement for storage of the shared data in a secured environment.

vii. have the complete responsibility for the protection of eShram data from any leakage, theft, phishing or other cyber-attack on the data, once downloaded from the eShram data sharing portal or once transferred through API.

viii. mandatorily verify the data received from MoLE in terms of deduplication, cleansing, physical/ online verification etc. before use of data for any purpose/ benefits or schemes which are intended to be provided to the eShram registrant.

B. Data Security, Protection and Privacy guidelines for the States/UTs/Central Government Ministries

Data security, protection and privacy guidelines advised to be followed by the States/UTs/Central Government Ministries while handling the eShram data in their environment are as under:

i. The user Ministry/Department shall use appropriate antivirus for the system where data is stored.

ii. The user Ministry/Department should ensure Intrusion Detection and Prevention system to be in place for the environment where the eShram Data is stored or used.

iii. The user Ministry/Department should ensure whitelisting of only required ports/IPs in their network's firewall.

iv. The user Ministry/Department should ensure OS hardening in the host system where eShram registrant data will be sent.

v. The user Ministry/Department should ensure latest patches and updates of all the system software are implemented timely and on regular basis.

vi. The user Ministry/Department should carry out periodic security audit of the application and infrastructure used in data sharing though Cert-In empanelled agency.

vii. Security Audit of the user Ministry/Department system wherein the data is stored may be carried out by MoLE or its designated agency at any point in time.

viii. The user Ministry/Department in discussion with eShram team should ensure encryption of the data, through Public and Private key combination for encrypting and decrypting while exchange and storage of data.

M-16018/30/2021-SS-III

ix. The user Ministry/Department should ensure that there is regular Vulnerability Assessment of servers used in transfer and receiving of data.

x. Aadhaar storage guidelines to be followed by user Ministry/Department with whom data is being shared including creation of vaults and so forth.

xi. The user Ministry/Department shall ensure that data resides in a data centre located in India. In case, cloud services are used, the services of only NIC Cloud or MeitY empanelled Cloud Service Providers (CSPs) will be utilized. At no point, the data should be stored or replicated outside India.

xii. All the relevant acts related to data sharing, data protection, data privacy and their subsequent amendments will also be applicable in addition to the data sharing guidelines.

xiii. User Ministry/Department should ensure that Personal Identifiable Information is not visible to any unauthorised officials, persons, individuals etc. and such information shall be masked to ensure privacy of data.

Name:

Designation:

Signature:

Date:

M-16018/30/2021-SS-III

eShram Data Requisition Form

PART B

(To Be Filled by Data Owner (MoLE) & forwarded to NIC along with Part A)

(In case Data Owner is itself Data Requestor, both filled Part A & Part B to be forwarded to NIC)

1.	Data request of Part A approved by	
	a) Approval Authority Designation	
	b) Relevant e-Office Computer Number	
2.	Mode of data sharing: Data Sharing Portal / API	
3.	Approved Data-fields of Part A *(Enclose list)*	
4.	Approved sharing Period of data:	From: DD/MM/YYYY To: DD/MM/YYYY

Name:

Designation:

Signature:

Date:

15