How Mission East Process Applicants & Staff Personal Data

Contents

Mission East IT Security and Data Protection policy applies to all information provided by you to us, virtue of your role as candidate for a job we have advertised, employee, intern, volunteer, board member or consultant contracted by us.

At Mission East, we take care of the personal data you provide when interacting with us. In this Document, you can read more about the data we collect along your journey with Mission East, why and how we process your data, how long we store it, and which security measure we have in place. We will also present you with your rights and ways to claim them, should it be necessary.

Please read this Document and contact us if you do not agree to its contents, either in part or wholly. The current version of the Policy is available at missioneast.org at any time.

1 Data Controller

1.1 Organisation

The organisation responsible for processing your personal data is:

Mission East

Kastaniehuset - Bernstorffsvej 20C.1, 2900 Hellerup

Missioneast.org

CVR number: 1472 3692

(Hereinafter "Organisation")

1.2 General framework

The general legal framework for our processing of personal data is European General Data Protection Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC, including regulation. Additionally, we comply to the Danish Data Protection Act No. 502 of 23/05/2018 which contains additional provisions to the Regulation on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Exchange of Such Information.

1.3 Commitment

This Document commits Mission East while processing your Personal Data. All queries regarding this Document, the processing of your data and any suspicion of non-compliance should first be directed to:

Pierre Vernet, HR Director – complaints@missioneast.org.

2 Definitions

Personal Data is defined by the European GDPR as all kind of information upon a person (you) which alone or combined can lead to the identification of you as a physical person, disregard of the way data is stored and processed (electronically or not).

Public Data are any of information about you that can be made freely accessible by anyone or is already (e.g., social media, public records, press releases, and promotional materials). These data can be collected and processed without consent as long as there are used in accordance with the purpose of their original publication, and the Data Subject is informed of the source we have used to collect them.

Confidential Data are any of your personal information that are neither public nor sensitives. Such data requires elevated access permissions and often yours consent. Bank account, family relationships, private phone number and e-mail are example of such data.

Special Categories of Personal Data revealing your racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of your genetic data, biometric data for the purpose of uniquely identifying you as a natural person, data concerning your health or data concerning a natural person's sex life or sexual orientation. Such data may only be collected if absolutely required and with yours informed consent.

Processing data means every operation which is performed on your Personal Data 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.

Data Controller is defined as agency or other body which alone or together with other defines the purpose and the mean for gathering your Personal Data. Mission East is the Data Controller of your Personal Data held as supporters, local partners, donors, recipient of marketing activities, third parties and other contacts used for our activities.

Data Processor is defined as the physical or legal identity, authority, institution or other organisation which manages personal data on behalf of Mission East. Where Mission East, as of its activity, receives, store and process personal data for the purpose of others, Mission East is the Data Processor.

Data Subject is, for the purpose of this Document, you (the individual who can be identified behind data content).

Authorised Users or **Data Users** are Staff who need access to information to complete the tasks they are assigned to and reach the purpose of their role.

Pseudonymisation means the processing of your Personal Data in such a manner that the personal data can no longer be attributed to you 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 you.

Personal Data breach means 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

3 What happens with Your Data

3.1 Purpose of processing Your personal data

1 When we process Your personal data, it is to:

- Qualify and make the final decision regarding our cooperation with you
- Comply with our Due Diligence duty to safeguard staff and external stakeholders, and to fulfil donors' requirements
- Establish and manage your contract incl. placement in our salary scale
- Administrate your insurance and pension
- Pay your salary and benefits as well as income taxes and other mandatory contributions
- Administrate Gross Salary Arrangements if any
- Manage absences and vacation in compliance with law and agreements
- Manage your access to our systems and ensure IT security incl. data protection
- Support and administrate your skills & career development
- Enhance cooperation and performance across the organisation
- Enhance social relations and job satisfaction
- Administrate staff statistic and report to Mission East's Board and authorities
- Support work permit and visa application if necessary
- Manage crisis if it should happen
- Document our processes
- Manage Mission East's resource which includes plans, budget, follow-up and reporting
- If it should happen, manage crisis or ensure security at our premises and investigate any breach.

3.2 Your personal data that we process

3.2.1 Personal Data

2 The information we collect directly from You when you apply to a job is your name, private contact information, education, career, professional and personal profile test answers and whatever information you decide to share with us to demonstrate your qualification to the job.

3 Before concluding a contract with employees or consultant, we retrieve references from former employers/clients and colleagues and gather information about Your behavior in work situations (work and decision styles and preferences, social and professional contributions in groups, behavior in critical situations or under pressure, gender and intercultural sensitivity, involvement as subject of concerns in sexual exploitation, abuse or harassment case). We do also screen your name against Sanction and COTER lists, PEP register and media. Mission East does not contact references or process due diligence check without your Consent.

4 We may ask for a profile photo or descriptions of work behavior (by filling out a professional or personal profile and through interviews); We may also ask for civil information and a copy of Your passport to confirm your identity and support work permit or visa application. And We ask for a criminal report if you will work with or close to children.

5 The information we collect directly from You when you start is your birthday, gender, information about next of kind, spouse/partner and children, civil registration and tax numbers, bank information.

6 During your work relationship with Mission East, we process information about Your salary, absences, performance, skills and professional interests or activities you participate in.

7 At some of our locations, we have video surveillance around the office, at the entrance or/and in some offices, recording traffic and some meetings to document the transparency and fairness of negotiations.

3.2.2 Special Categories of Personal Data that we only process with Your Consent

8 We may gather health information in case of long-term illness, to arrange your work and travel conditions or to comply with our duty of care in case of accident or crisis; the information includes your blood type and if you have allergies or specific nutritional needs.

9 Mission East runs regular job satisfaction assessments, feedback processes and surveys, and we may gather some personal comments which can sometimes be considered as Special Categories of Personal Data. You may always decide whether to participate or not without further consequences regarding your employment at Mission East, and surveys are always anonymous (generally, only the system can identify you to administrate response rate).

10 If you chose facial or fingerprint recognition as a sign-in method to log in to the electronic devices we provide, we process this biometric data, but it is only stored on the device concerned.

11 We may also ask you about other Special Categories of Personal Data like sexual orientation, religion and ethnic origin; in this case it will be totally anonymous, and it will never be possible to link your answers to You. That information is necessary to monitor the implementation of our Diversity Policy.

3.3 Why we may process Your Personal Data (legal basis)

12 We must have a legal basis for processing Your Personal Data

12.1 When you become a Mission East employee, enter into any kind of working agreement with us, or have queries prior to entering into such an agreement with us, we process some of Your Personal Data to fulfil our contractual commitment with you. The legal basis of processing these data is then a contractual interest as defined in GDPR Art 6.1.b. Some examples of data that fall under a contractual interest are Your contact information, salary, bank information, information about spouse/partner and children (to administrate benefits) or next-of-kind and health information (in relation with our duty of care).

12.2 We may also process your Personal Data because we have a legitimate interest in doing so, cf. GDPR Art. 6.1.f, unless your right to have your Personal Data protected takes precedence over our legitimate interest in processing your data. Our legitime interests are, for example, the selection of the best candidate for a job, the maintenance of a healthy and supportive work environment, the performance and development of individuals and the organisation, the documentation of our processes and added value, our Due Diligence duty to comply with the sector's standard and donors' requirements, staff and other stakeholders' safeguarding, conflict management or breach investigation.

12.3 In certain cases, we may also have a legal interest (GDPR Art. 6.1.c), as we have the legal obligation to process Your Personal Data, for example when we process and store Your employment contract and data regarding Your salary due to the Danish Bookkeeping Act and the European Commission's documentation requirements (for people working on projects funded by EC) or we report your income and other benefits incl. your civil registration number to Tax Authorities. Finally, it is a legal requirement to check child abuse records for people working close to or with children.

12.4 We may have your vital interest (as defined by GDPR Art. 6.1.d) in mind when we process health information to ensure the proper intervention in case of injury or crisis during duty travel if it should happen.

12.5 We need your Consent on a legal basis (GDPR Art.6.1.a) to process some Personal Data including Special Categories of Personal Data, References, criminal records and Due Diligence screening output, Personified portrait photo and portrait or group photo where You are easily identifiable biometric data.

3.4 Sharing your Personal Data

13 When we share your Personal Data, it is always limited to what is necessary for the specific purposes of the agreed process and aligned with our legitim, legal or contractual interest. Sharing is based on clearly defined roles and signed Data Processor or corresponding agreements. You can see the list of the organisations we may share your Personal data with at the end of this document.

13.1 We may share your Personal Data with our suppliers and partners who contribute to delivering our services to you in relation to our IT operations, payroll, legal advice and audit processes.

13.2 We may also share your data with our Pension, Insurance, Broker companies or Benefits delivery companies so they can establish a direct relation to You.

13.3 We also share some of Your Personal Data when we manage Your Information within IT systems hosted, delivered or supported by a third party.

13.4 In addition to the above, we share your data to the extent that we are obliged to do so, for example due to requirements to report to public authorities such as the tax or migration authorities.

3.5 Sharing your Personal Data with recipients outside the EU/EEA

14 As international NGO, we do operate with own offices as well as partners and donors outside the European Union (EU) and the Europe Economic Area (EEA). We have also suppliers outside the EU/EEA. For these reasons, we may transfer your Personal Data outside the EU/EEA. It is generally the case for Personal Data concerning natural persons in our countries of operations, and it happens occasionally with European citizens' personal data.

You can see the list of the organisations based outside the EU/EEA that we may share your Personal data with at the end of this document.

14.1 We share your Personal Data to the recipient outside the EU/EEA if one of the conditions below is fulfilled:

- our local representation or office has signed and adopted our Binding Corporate Rules (GDPR Art.47)
- we have agreed on appropriate safeguard and standard data protection provisions passed by the European Commission with the recipient receiving your Personal Data (GDPR Art. 46).
- the recipient is either signatory of a Code of Conduct as per GDPR Art.40-2 or Art. 40-3 or has a certification in accordance with GDPR Art.42, and we have signed a Data Transfer Agreement.
- the relevant country or international organisation has a sufficient level of protection as defined by the European Commission (GDPR Art.45)

14.2 When any of the conditions above are fulfilled, we may also share your Personal Data outside the EU/EEA based on contractual, legal, vital or public interest. If the transfer is based on our legitim interest or a previous consent you gave us, we will ask your formal consent highlighting the data transfer (GDPR Art.49).

14.3 You may at any time request information about or a copy of the required guarantees that form the basis of sharing personal data with recipients outside of the EU/EEA and, if exceptions apply according to the description in GDPR Art.49, the exceptions that form the basis for any such sharing of Personal Data.

3.6 Storage and deletion of Your Personal Data

15 We store and process Your Personal Data if there is a legal and legitimate reason for doing so. Wherever possible, we use automated deletion and pseudonymization processes in our systems. Where our systems do not allow us to use such automated deletion and pseudonymization processes, we have established ongoing controls to ensure that personal data is reviewed and deleted/pseudonymized.

15.1 Candidates' Personal Data are stored in specialized HR Software and deleted or pseudonymized six months after the date of hiring of the final candidate unless You have given your consent to prolong this period.

15.2 Most of Employees' and some Consultants' and Volunteers' Personal Data is stored in specialized HR Software, where there are deleted or pseudonymized six months after the date of Your end of contract. Warning letters are deleted one year after the end of the period noticed in the letter.

15.3 Payments and related information are stored in a specialized ERP system and related apps as well as in dedicated pay roll systems and are stored normally for 8 years plus the period until June for the purpose of eventual audit in accordance with EU requirements.

15.4 Some of Your Personal Data that are included in overviews upon, for example, selected candidates, payroll, insurance or survey answers are stored in Excel file in access restricted folders in SharePoint and OneDrive and stored normally for 8 years plus the period until June for the purpose of eventual audit in accordance with EU requirements.

15.5 Correspondence and chats in Microsoft Teams and Outlook are usually deleted after one year.

15.6 Criminal records are deleted as soon as they have been checked.

15.7 In Mission East IT infrastructure, your Identification (credential) will be deleted one month after the date of Your end of contract. Before your departure, you must activate an automatic e-mail reply which redirects the sender of professional mail to your manager or colleague, and private mail to your own e-mail address.

15.8 Your mailbox can exceptionally be accessed with the authorization of the HR Director by IT staff who are committed to not investigating private mails or to IT investigator who may access the whole hard disk.

4 Your rights

16 If you want to claim one of your rights or opt for one of the possibilities described below, please, send your request by writing to the HR Director at personnel@missioneast.org.
We will always follow up without undue delay (normally considered as one month), informing you about the action we have taken or engaging in a dialogue to clarify any question or issue, for example if we have any legal interest to process your Personal Data that conflicts with your request.

4.1 Insight

16.1 You are entitled to gain insight into the personal data we process about you, including which data we have registered about you, how we process them and the purposes for which such data has been collected.

4.2 Correction and deletion

16.2 You are entitled to request that the personal data we process about you be corrected (GDPR Art.16) or, on grounds relating to your personal situation, deleted (GDPR Art.17). You have also the right to "be forgotten", which means that you request us not to contact you anymore. We will comply with your request as soon as possible to the extent necessary. If, for some reason, we are not able to comply with your request, we will contact you.

4.3 Limitation or objection of processing

16.3 In certain circumstances and in accordance with GDPR Art. 18 & 21, you are entitled to request a limitation on processing your Personal Data, like limiting the type of data we may process or the purpose we process them for.

16.4 In some extent defined by GDPR Art. 22, you have also the right not to be subject to a decision based solely on automated processing, including profiling. During recruitment with many candidates, we use such process based on the collected answers to mandatory questions; We use also automated processing and profiling in our employee's satisfaction or performance surveys.

16.5 You are also entitled to ask us not to process your Personal Data in cases where the processing is based on our legitim interest, public interest or exercise of authority (GDPR Art.6.e). The extent to which we process your data for such purposes appears from this Policy.

4.4 Withdraw you consent

16.6 You are entitled to revoke your consent at any time (GDPR Art.17.b), and we will stop processing your Personal Data without undue delay unless there is another legal ground for processing. Your revocation does not affect the legitimacy of processing that was carried out prior to revoking your consent.

16.7 If we are unsure of the identity of whom the consent revocation comes from, we may ask you to identify yourself. This is free of charge, except for the ordinary costs of communication.

4.5 Data portability

16.8 You are entitled to receive your Personal Data (only information about yourself that you have provided to us) in a structured, commonly used and machine-readable format (data portability – GDPR Art. 20).

4.6 Potential consequences of not providing Personal Data

16.9 If we need you to provide your Personal Data by yourself, it will appear in places where we collect such data. You may not wish to provide us with these Personal Data; as consequence we may be not able to answer your request, consider your application, engage or execute your contract.

5 How we create security around your data

17 Internally in our Organisation, our processing of personal data is subject to our IT Security & Data Protection policy. This policy also contains rules for the conduction of risk and impact assessments of existing, new or changed processing activities.

18 Only selected, qualified and trained staff members have access to Your information (HR, Finance, etc.); we have implemented internal rules and procedures to ensure an appropriate level of security from the time of collecting personal data until deletion, incl. Access Management, data protection impact assessments of existing and new data management systems.

19 Externally, processing of personal data is always carried out by Data Processors maintaining at least the same level of security standard as ours and who use Access Management, Transparent Data Encryption for storing personal data, including backup data. HTTPS (Secure Sockets Layer) is used to encrypt data during transmission. Single Sign On (SSO) or Multi Factor Authentication (MFA) are used to sign-in. Data Loss Prevention and Penetration Tests are part of platforms security management. Servers are hosted in ISO certified data center.

6 How to Complaint

20 You may at any time exercise your right to complain:

- first by contacting us at complaints@missioneast.org.
- secondly at the Danish Data Protection Agency, "Datatilsynet" - Carl Jacobsens Vej 35, DK-2500 Valby; phone: 3319 3200, email: dt@datatilsynet.dk, electronic form: https://www.datatilsynet.dk/english/file-a-complaint

7 Update of this Document

21 Mission East is committed to complying with the fundamental principles of personal data protection and privacy. Therefore, we regularly review our IT Security and Data Protection policy as well as this Document to keep it up to date and in accordance with applicable principles and legislation.

22 Any future changes in this Document will be published on this site and can be sent to you by e-mail if you so wish.

8 Sharing list

Following organisations, companies or systems are our regular providers and covered by either a Data Processor (within EU/EEA) or a Data Transfer Agreement (outside EU/EAA) or a contract that contains corresponding terms.

Organisations, companies or systems	Purpose	Location
BambooHR	HR Management & Recruitment	Ireland
Microsoft (Office tools, SharePoint and related apps…)	Operations & Administration	Germany
Business Central and related apps	Economy management	Ireland
Danløn / Trekroner Revisor	Denmark Payroll	Denmark
Partena	Belgium Payroll and employees' administration	Belgium
PFA	Denmark Pension and Health Insurance	Denmark
AXA	Belgium Injury insurance	Belgium
Mensura	Belgium Health & Work Environment	Belgium
EdenRed	Belgium benefits (Lunch vouchers)	Belgium
Cigna Healthcare	Expatriates Health Insurance	Belgium
Sompo	Duty Travel Insurance	Belgium
Lexis Nexis Risk	Due Diligence Screening	Ireland
Any previous employer (based on consent)	References & Due Diligence Screening	Any country