### European Disability Forum

### Data Protection Policy

**OBJECTIVE**

**The European Disability Forum** (“**EDF**,” “**we**,” or “**us**”) is committed to privacy and data protection. EDF needs to gather and use certain information about Data Subjects. These can include members, partners, sponsors, suppliers, business contacts, employees, participants in our events, and other people the organisation has a relationship with or may need to contact.

This Data Protection Policy (the “**Policy**”) to set out the standards and procedures we apply when Processing Personal Data, in accordance with our obligations under the EU General Data Protection Regulation and its national implementing laws (“**GDPR**”). Amongst others, this Policy helps to ensure that EDF:

* Complies with the GDPR and follows good practice;
* Employees are informed about their responsibilities when handling Personal Data; and
* Handles data breaches appropriately.

**DEFINITIONS**

“**Personal Data**” means any data relating to an identified or identifiable individual, including, for example, name, contact information, identification number, location data, online identifier, IP address etc.

“**Data Subject**” is the individual to whom the Personal Data relates.

“**Processing**” means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

**POLICY SCOPE**

This Policy applies to all our staff members, including Board members, Committee members, (temporary) employees, interns, volunteers, consultants or contractors, regardless of the office or workplace (hereinafter referred to as “**Employees**”, “**you**” or “**your**”).

**EFFECTIVE DATE**

This Policy is applicable as of January 25th 2021 following staff training. The Policy has been reviewed by the executive committee and approved on May 28th 2021.

**CONTACT FOR QUESTIONS**

If you have any questions regarding this Policy, please contact our Data Protection Officer (“**DPO**”), Muriel Davia, at muriel.davia@edf-feph.org.

1. **PRIVACY PRINCIPLES**

Each Employee who Processes Personal Data is required to comply with the following privacy principles:

* 1. **PURPOSE**
		1. Employees may only Process Personal Data for specified, explicit and legitimate purposes (e.g., to maintain our website and its member area to organise events and send event invitations, to arrange travel accommodation for speakers), and not further Process the data in a manner that is incompatible with those purposes. Any new purpose must first be approved by our DPO, which will indicate whether you need to provide the Data Subject with an opportunity to opt-in[[1]](#footnote-1) or opt-out from the new purpose. If you are not sure whether a purpose or use of Personal Data is new, please contact our DPO.

* 1. **LEGAL BASIS**
		1. Personal Data may only be Processed when one of the below legal bases is provided:
* ***Consent:*** The Data Subject has provided his or her free, specific, informed and unambiguous consent (e.g., by ticking a non-pre-ticked checkbox after being provided with sufficient notice about the Processing).
* ***Contract or memorandum of understanding (MOU):*** The Processing is necessary for the performance of a contract to which the Data Subject is a party or in order to take steps at the request of the Data Subject prior to entering into a contract.
* ***Legal obligation:*** We are required by law to Process the Personal Data.
* ***Legitimate interest:*** We, or a third-party, have a legitimate interest in Processing the Personal Data for that specific purpose (e.g., in some cases, fraud prevention may be considered a legitimate interest). Please contact our DPO to help you determine whether we have a legitimate interest in Processing Personal Data as intended.
	+ 1. Legal basis for specific Processing activities:
* ***Marketing (including newsletters and policy papers):*** As a general rule, sending electronic marketing communications to individuals requires obtaining the individual’s prior consent. In addition, marketing communications should contain a mechanism by which the recipient can object to receiving further marketing communications (e.g., an opt-out/unsubscribe link in a marketing email). Before sending marketing communications to Data Subjects, you must obtain the authorisation of your line manager or our DPO.
* ***Sensitive Personal Data[[2]](#footnote-2), such as health data and information regarding disabilities:*** As a general rule, the Processing of sensitive Personal Data is only allowed in very limited cases. If you consider that the Processing of sensitive Personal Data is absolutely necessary, you should obtain authorisation from our DPO prior to such Processing.
* ***Children’s Personal Data:*** If you intend to Process Personal Data of children under the age of 13, you should obtain authorisation from our DPO prior to such Processing as we need to implement additional safeguards for such Processing.
	1. **NOTICE**
		1. Our Privacy Policy[[3]](#footnote-3) informs Data Subjects about how we Process their Personal Data. If you plan to carry out a new Personal Data Processing activity, you should verify if the Personal Data Processing is covered by the Privacy Policy, and contact our DPO if this is not the case.
	2. **RECORDS OF PROCESSING ACTIVITIES AND DATA PROTECTION IMPACT ASSESSMENTS**
		1. If you plan to carry out a new Personal Data Processing activity, you should inform your line manager or our DPO to ensure that we update our records of processing activities (also referred to as ‘data maps’ or ‘article 30 records’). Our DPO will also verify if a Data Protection Impact Assessment (“**DPIA**”) needs to be completed for that activity.
	3. **PRIVACY SAFEGUARDS**
		1. **Privacy by design:** You must take into account privacy considerations when developing new products and services and strive to make the product or service as privacy-friendly as possible.
		2. **Privacy by default:** You must ensure that the default settings of our products and services are as privacy-friendly as possible.

* + 1. **Data integrity:** You must limit the collection and usage of Personal Data to that which is relevant for the intended purposes for which it was collected, and ensure that such Personal Data is reliable, accurate, complete, current and kept up-to-date.
		2. **Data retention:** We must delete Personal Data when it is no longer necessary for the purpose for which we collected it, unless we are required by law to keep it for a longer period or if we anonymise the data so that it no longer constitutes Personal Data.[[4]](#footnote-4) A new purpose for which the data is useful is not a justification for keeping the data for a longer period of time.

Please note that the data retention periods are different depending on the purpose for which Personal Data is used. Please refer to ***Appendix 1 – Data Retention*** for more information on the different retention periods that apply to each purpose. If the purpose for a Processing of Personal Data is not listed in Appendix 1 , please contact our DPO and request updating Appendix 1 to include the new purpose and the applicable data retention period.

* + 1. **Profiling and automated decision-making:** You must obtain approval from our DPO before engaging in any profiling of Data Subjects, or automated decision-making which produces legal effects concerning a Data Subject or significantly affects a Data Subject.
	1. **DATA SECURITY AND CONFIDENTIALITY**
		1. Any Personal Data you Process must be protected in accordance with ***Appendix 2 - Data Security***. Any questions regarding information security may be directed to the Muriel Davia who liaise directly with our IT manager.
		2. Employees who Process Personal Data must have committed themselves to confidentiality contractually or are under an appropriate statutory obligation of confidentiality (e.g., legal secrecy obligations such as for medical professions).
		3. You must take all reasonable and appropriate actions in their conduct at EDF to maintain the confidentiality of Personal Data, including by not disclosing any Personal Data without the appropriate executive, legal or DPO approval.
		4. Any accidental or unauthorised access to Personal Data must be communicated without delay to our DPO, who will take appropriate measures to mitigate the incident and notify supervisory authorities and Data Subjects, where required.
		5. You must keep all data, including, but not limited to Personal Data secure, by taking sensible precautions and following the guidelines set forth in Appendix 2.
	2. **AGREEMENTS AND DATA SHARING**
		1. Agreements with recipients of Personal Data of EEA and Swiss Data Subjects should include certain privacy and data protection clauses. This includes both contracts with service providers who will process Personal Data on our behalf (also referred to as “**processors**”) (e.g., data hosting providers, marketing agencies, accountants), as well as organizations to whom we disclose Personal Data, but who will Process the data for their own business purposes (also referred to as “**independent controllers**”) (e.g., European Institutions and third party contractors in the context of event organization).
		2. We are responsible for compliance with applicable laws for EEA Personal Data that we receive or disclose to third parties on our behalf. Any data disclosure to independent controllers may only be done in compliance with the principles set forth in ***Appendix 3 – Data Sharing***.

* + 1. You should consult with our DPO before entering into such agreements.
	1. **INTERNATIONAL DATA TRANSFERS**
		1. EDF must provide adequate protection when transferring Personal Data from the EEA or Switzerland to a location outside the EEA or Switzerland. You should consult with our DPO before conducting such international data transfers to ensure that EDF put in place the appropriate data transfer safeguards prior to the transfer.
	2. **REQUESTS AND NOTIFICATIONS:**
		1. **Requests from Data Subjects:** If you receive a claim or request from a Data Subject (e.g., a website visitor, another employee, a job applicant, vendor or other partner, or any other Data Subject), regarding his or her Personal Data, you must immediately communicate that claim or request to our DPO at muriel.davia@edf-feph.org with the subject line ‘Data Subject Request’, who will handle this request as per our Data Subject Request Handling Policy for more details.

Please see ***Appendix 4 – Data Subjects’ Rights*** to this Policy for information on the rights that Data Subjects’ have with regard to their Personal Data under GDPR.

* + 1. **Notifications from Service Providers:**  If you receive a notification from a service provider (or processor) regarding the Personal Data that the service provider Processes on our behalf must immediately forward such notification to our DPO.
		2. **Requests from Public Authorities:** If you receive a request from a public authority regarding the Personal Data we Process, you must immediately forward such request to our DPO. Our DPO will respond expeditiously to complaints. The response will address whether the complaint has merit and, if so, how EDF will rectify the problem.
1. **TRAINING AND AWARENESS**
	1. All our Employees handling Personal Data receive periodic privacy and data protection training covering the standards of this Policy to help them understand their responsibilities when handling Personal Data.
	2. Our DPO will monitor developments with regard to privacy, data protection and information security legislation and inform and advise EDF and our Employees about data protection obligations, including through awareness-raising campaigns and training.
2. **DATA PROTECTION OFFICER**
	1. In addition to the specific tasks laid out in the other sections of this Policy, the DPO is also responsible for:
* Keeping our board updated about EDF’s data protection responsibilities, risks and issues;
* Reviewing all data protection procedures and related policies;
* Handling data protection questions from staff and anyone else covered by this policy;
* Dealing with requests from Data Subjects, including when they request to exercise their rights under GDPR; and
* Maintaining and updating our internal records of Processing;
* Advising on the due diligence and engagement of third parties, who’s services may involve Processing Personal Data (such as data storage providers).
	1. The Data Protection Officer may be contacted via: muriel.davia@edf-feph.org.
1. **AUDIT**
	1. Our Employees will cooperate with any (internal) audit of our data processing facilities.
2. **FAILURE TO COMPLY**
	1. Failure to comply with this Policy may result in disciplinary actions against you, up to and including termination of employment, in accordance with the applicable employment agreement, work rules, labour laws or any other applicable rules or regulations, and/or civil or criminal penalties.

**Appendix 1 – Data Retention**

This Appendix forms an integral part of the EDF Data Protection Policy (“**Policy**”). Any terms capitalised in this Appendix, but not defined herein, shall have the meaning given to them in the Policy.

Employees must comply with the retention periods listed below and with the principles set out in the Policy. If the Personal Data you are Processing is not listed below or if you have a question about this Appendix, please consult our DPO.

Unless a longer or shorter retention period is required by law or otherwise provided in this Policy, the standard retention period for Personal Data is minimum five (5) years after the moment of collection. Personal Data must be deleted, destroyed or anonymised as soon as reasonably practical following the expiration of the applicable retention period.

|  |  |
| --- | --- |
| **Type of Personal Data** | **Retention Period** |
| Financial records  | Minimum 7 years following the taxable period to which the data relates |
| Invoicing details  | Minimum 7 years following the taxable period to which the data relates |
| Business contact information (e.g., from vendors, business partners, contact persons of European Institutions) | Maximum 1 year after termination of the relationship; or within 30 days of notification that a business contact is no longer employed by the relevant party, vendor, partner or institution |
| Information collected from Data Subjects in relating to events (including registration details, invoices for transport etc) | Minimum 7 years following the taxable period to which the data relates  |
| Information collected from event speakers or participants to arrange travel accommodation  | Maximum 1 year after the end of the year of the event  |
| Data collected on the EDF website via cookies or similar technologies  | Maximum 1 year from collection or the last interaction recorded from the website visitor; or upon withdrawal of consent by Data Subject |
| E-mail  | We keep e-mails on the Microsoft cloud , except where personnel have filed the e-mail into their personal folder, or a longer period applies due to a litigation hold. [[5]](#footnote-5) |
| Personnel records (including work details, performance reviews, records of leave or absence, maternity/paternity records, health and safety records, etc.) | Minimum 5 years following the creation of the data |
| Payroll and wages  | Minimum 7 years following the taxable period to which the data relates |
| Recruitment  | Minimum 1 year or minimum 5 years if there is a risk of a discrimination claim |
| Personnel employment lifecycle (including employment agreement, hiring / resignation letter, disciplinary sanctions, dismissal documents, etc.) | Minimum 7 years as from the end of the employment contract |
| Personal Data relating to legal claims | Minimum 10 years for claims against persons; or 30 years for other claims unless otherwise provided |
| Personal data related to EDF membership applications | To be kept for the duration of membership and reviewed each 5 years for accuracy  |
| Personal data related to governing body elections in EDF | To be kept for the duration of the mandate of the elected role (up to 4 years) |
| Personal data related to EDF internal structures including Board, committees and working groups  | To be kept for the duration of the mandate of the elected or committee role (up to 4 years) |
| Personal data included in EDF videos, conference reports, etc | Minimum 7 years from the production or publication  |

**Appendix 2 – Data Security**

This Appendix forms an integral part of the EDF Data Protection Policy (“**Policy**”). Any terms capitalized in this Appendix, but not defined herein, shall have the meaning given to them in the Policy.

EDF must implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the Processing. In determining those measures, we should take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of Data Subjects.

1. **Do’s and Don’ts for Employees**

Employees must comply with the following technical and organizational measures at all times:

* When not required, paper or files should be kept in a locked drawer or filing cabinet.
* Make sure paper and printouts are not left where unauthorized people could see them (e.g., on a printer).
* Data printouts should be shredded and disposed of securely when no longer required.
* When data is stored electronically, it must be protected from unauthorized access, accidental deletion and malicious hacking attempts.
* Personal Data should be protected by strong passwords that are changed regularly and never shared between Employees.
* If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.
* Data should only be stored on designated drives and servers and should only be uploaded to an approved cloud computing services.
* Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
1. **Security principles**

In addition to the measures listed under 1, EDF applies the following types of technical and organizational security measures:

1. **Physical access control –** Technical and organizational measures to prevent unauthorized persons from gaining access to the data processing systems available in premises and facilities (including databases, application servers and related hardware), where Personal Data are Processed, include:
	* Establishing security areas, restriction of access paths; EDFs office is in the Mundo Madou building- with a reception which managed access to the whole building and only allows entry to agreed visitors
	* Establishing access authorizations for employees and third parties; EDF staff have access cards and keys, and third parties need to be approved by EDF before having access.
	* Key management, card-keys procedures; all staff have access to the EDF office (via a key) and building (via a card). If you loose your key or card it must be reported to Mundo Madou and our DPO immediately.
	* Door locking ;
	* Reception staff available during office hours.
	* Securing decentralized data processing equipment and personal computers is done by our IT company off site.
2. **Virtual access control –** Technical and organizational measures to prevent data processing systems from being used by unauthorized persons:
	* User identification and authentication procedures are in place;
	* ID/password security procedures (special characters, minimum length, change of password) are applied;
	* Automatic blocking (e.g. password or timeout) after 10 attempts to log in;
	* Monitoring of break-in-attempts and automatic turn-off of the user ID upon several erroneous passwords attempts;
	* All servers and computers containing data are protected by approved security software and a firewall (Sophos);
	* Creation of one master record per user, user-master data procedures per data processing environment; and
	* Encryption of archived data media.
3. **Data access control –** Technical and organizational measures to ensure that persons entitled to use a data processing system gain access only to such Personal Data in accordance with their access rights, and that Personal Data cannot be read, copied, modified or deleted without authorization, include:
	* Internal policies and procedures;
	* Control authorization schemes;
	* Differentiated access rights (profiles, roles, transactions and objects);
	* Monitoring and logging of accesses;
	* Disciplinary action against employees who access Personal Data without authorization;
	* Reports of access;
	* Servers containing Personal Data should be sited in a secure location, away from general office space; and
	* Encryption.
4. **Disclosure control –** Technical and organizational measures to ensure that Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media (manual or electronic), and that it can be verified to which companies or other legal entities Personal Data are disclosed, include:
	* Encryption/tunneling;
	* Logging; and
	* Transport security.
5. **Entry control –** Technical and organizational measures to monitor whether Personal Data have been entered, changed or removed (deleted), and by whom, from data processing systems, include:
	* Logging and reporting systems; and
	* Audit trails and documentation.
6. **Control of instructions** – Technical and organizational measures to ensure that Personal Data are Processed by service providers and third parties in accordance with the instructions of EDF include:
	* Unambiguous wording of the contract;
	* Formal commissioning (request form); and
	* Criteria for selecting the Processor.
7. **Availability control –** Technical and organizational measures to ensure that Personal Data are protected against accidental destruction or loss (physical/logical) include:
	* Backup procedures;
	* Mirroring of hard disks (e.g. RAID technology);
	* Uninterruptible power supply (UPS) at the data centre;
	* Remote storage;
	* Anti-virus/firewall systems;
	* Data should be backed up frequently. Those backups should be tested regularly, in line with the company’s standard backup procedures; and
	* Disaster recovery plan.

**Appendix 3 – Data Sharing**

This Appendix forms an integral part of the EDF Data Protection Policy (“**Policy**”). Any terms capitalized in this Appendix, but not defined herein, shall have the meaning given to them in the Policy.

When disclosing Personal Data to third parties (who are independent controllers), Employees must comply with the following principles:

* To the extent reasonably practicable, Employees should request Data Subjects whether EDF may connect them to the third party recipient directly (e.g., to organize travel accommodation);
* To the extent reasonably practicable, Personal Data should be de-identified (and ideally anonymized) prior to disclosure;
* A written data sharing agreement should be concluded between the third party recipient and EDF, which should include appropriate privacy and data protection clauses. These clauses should cover at least:
	+ the categories and types of data intended to be shared;
	+ the purpose of the data disclosure;
	+ that the Personal Data should be Processed in compliance with applicable data protection law;
	+ an obligation for the third party to only use or otherwise Process the Personal Data for the purpose for which it is disclosed and to delete or destroy the Personal Data as soon as it is no longer necessary to achieve that purpose; and
	+ that any access to the data should be limited to the third party’s employees on a need to know basis.

**Appendix 4 – Data Subjects’ Rights**

Under GDPR, Data Subjects have a number of rights to their Personal Data.

Below is a general description of these rights. Please note that each right is subject to exceptions and limitations, and any Data Subject inquiry related to these rights should be handled in accordance with this policy.

* ***Right of access***: Data Subjects may submit a request to access any Personal Data we hold about them, or ask us to confirm whether we Process Personal Data about them. We should provide a copy of the Personal Data requested by the Data Subject in a commonly used electronic form. Data Subjects may also ask us questions as to how and why we Process their Personal Data.
* ***Right to rectification***: Data Subjects may submit a request to ask us to update, complete and correct inaccuracies in the Personal Data we hold about them.
* ***Right to erasure***: Data Subjects may ask us to delete the Personal Data we hold about them in specific cases such as when we no longer need that information, when the Data Subject withdraws his or her consent to the Processing and there is no other legal basis to Process their Personal Data, when they object to the Processing, when their Personal Data has been processed unlawfully, or when we are required by law to delete it. Some further exceptions may apply.
* ***Right to object to the Processing***: Data Subjects may object to the Processing of their Personal Data based on EDF’s or a third party’s legitimate interest if they provide grounds relating to their particular situation, unless we demonstrate compelling legitimate interests that override the Data Subject’s interests and rights or we need their Personal Information in connection with a legal claim. Data Subjects may at any time object to the Processing of their Personal Data for marketing purposes without providing reasons for the objection. In addition, Data subjects may opt-out from the use of their Personal Data for materially different purposes or to the disclosure of their Personal Data to third parties in accordance with the Privacy Shield principles.
* ***Right to restriction of the Processing***: Data Subjects may ask us to restrict our use of their Personal Data in specific cases, such as while we need to verify its accuracy to reply to their request or while we need to assess their objection to our Processing of their Personal Data.
* ***Right to data portability***: Data Subjects may ask us to send them a copy of the Personal Data that they provided to us (to be sent in a structured, commonly used, and machine-readable format), in some specific cases and to the extent this will not undermine the rights of others. Data Subjects may also ask us to have their Personal Data transmitted directly to another organization where technically feasible.
* ***Right to withdraw consent***: Data Subjects may, at any time and free of charge, withdraw any consent they previously provided to us regarding the Processing of their Personal Data. We will apply their preferences going forward and this will not affect the lawfulness of the Processing before the consent withdrawal.
* ***Right to receive a copy of our data transfer agreements***: The legal department will provide Data Subjects, upon request, with a copy of our data transfer agreements. Confidential or commercial information may be removed from the copy, on the conditions set out in the relevant data transfer agreement.
1. In principle, opt-in is required if Personal Data will be Processed for an incompatible purpose, or if the Processing concerns sensitive data (i.e., Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning an individual’s sex life or sexual orientation). Opt-out will be sufficient if non-sensitive data will be Processed for a compatible purpose. [↑](#footnote-ref-1)
2. This covers data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health and data concerning a natural person's sex life or sexual orientation. [↑](#footnote-ref-2)
3. As available online at the following URL: https://www.edf-feph.org/edf-privacy-statement/ [↑](#footnote-ref-3)
4. As long as Personal Data can be linked back to the individual, it remains Personal Data. Pseudonymized data is still Personal Data and does not qualify as anonymized data. [↑](#footnote-ref-4)
5. Back-up copies of e-mails are not currently addressed well by our IT service provider an this needs to be reviewed in our IT contact. [↑](#footnote-ref-5)