MAX PLANCK FOUNDATION
for International Peace and
the Rule of Law

Data Protection Policy

Contents

1. Introduction

The Max Planck Foundation for International Peace and the Rule of Law (hereinafter 'the Foundation') takes its responsibilities with regard to the management of the requirements of the EU General Data Protection Regulation (GDPR) very seriously. This Policy sets out how the Foundation manages those responsibilities.

The Foundation obtains, uses, stores and otherwise processes personal data relating to potential, current and former staff, student assistants and interns, contractors, website users and contacts, collectively referred to in this Policy as data subjects. When processing personal data, the Foundation is obliged to fulfil individuals' reasonable expectations of privacy by complying with GDPR and other relevant data protection legislation (data protection law).

This Policy therefore seeks to ensure that staff are clear about how personal data must be processed and the Foundation's expectations for all those who process personal data on its behalf.

The main terms used are explained in the glossary at the end of this Policy (Appendix 2).

2. Scope

This Policy applies to all personal data the Foundation processes regardless of the location where that personal data is stored (e.g. on an employee's own device) and regardless of the data subject. All staff and others processing personal data on the Foundation's behalf must read it. A failure to comply with this Policy may result in disciplinary action.

3. Principles

The Foundation is responsible for, and must be able to demonstrate compliance with, the data protection principles set out in the GDPR.

Those principles require personal data to be:

a) processed lawfully, fairly and in a transparent manner (Lawfulness, fairness and transparency). Detail on how to achieve this can be found in Appendix 1;

b) collected only for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes (Purpose limitation). Detail on how to achieve this can be found in Appendix 1;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (Data minimization). Detail on how to achieve this can be found in Appendix 1;

d) accurate and where necessary kept up to date (Accuracy). Detail on how to achieve this can be found in Appendix 1;

e) not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the personal data is processed (Storage limitation). Detail on how to achieve this can be found in Appendix 1;

f) processed in a manner that ensures its security, using appropriate technical and organizational measures to protect against unauthorized or unlawful processing and against accidental loss, destruction or damage (Security, integrity and confidentiality). Detail on how to achieve this can be found in Appendix 1.

4. Accountability

The Foundation must implement appropriate technical and organizational measures in an effective manner to ensure compliance with data protection principles. The Foundation is responsible for, and must be able to demonstrate compliance with, the data protection principles.

The Foundation must therefore apply adequate resources and controls to ensure and to document GDPR compliance including:

a) appointing a suitably qualified Data Protection Coordinator (DPC);

b) implementing privacy by design when processing personal data and completing a data protection impact assessment (DPIA) where processing presents a high risk to the privacy of data subjects;

c) integrating data protection into the Foundation's policies and procedures, in the way personal data is handled by the Foundation and by producing required documentation such as Privacy Notices, records of processing and records of personal data breaches;

d) training staff on compliance with data protection law and keeping a record accordingly; and

e) regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

5. Management Responsibilities

As the data controller, the Management of the Foundation is responsible for establishing policies and procedures in order to comply with data protection law.

6. Data Protection Coordinator Responsibilities

The DPC, a staff member of the Foundation, is responsible for:

a) advising the Foundation Management and staff of their obligations under GDPR;
b) monitoring compliance with the GDPR and other relevant data protection law;
c) monitoring training and audit activities related to such compliance;
d) providing advice where requested on data protection impact assessments;
e) liaising with the Data Protection Officer of the Max Planck Society.

7. Staff Responsibilities

Staff are responsible for familiarising themselves with the Privacy Notice provided when they register with the Foundation.

Staff who process personal data about present or former staff, applicants, donors, partners or any other individual must comply with the requirements of this Policy. Staff members must ensure that:

a) all personal data is kept securely;

b) no personal data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorized third party;

c) personal data is kept in accordance with the Foundation's retention schedule;

d) any queries regarding data protection, including subject access requests and complaints, are promptly directed to the DPC;

e) any data protection breaches are swiftly brought to the attention of the DPC.

Where senior staff are responsible for supervising other staff doing work which involves the processing of personal information, they must ensure that those staff members are aware of the data protection principles.

Staff who are unsure about who are the authorized third parties to whom they can legitimately disclose personal data should seek advice from their Project Manager and the DPC.

All staff must sign a confidentiality agreement that sets out their data protection responsibilities.

8. Third-Party Data Processors

Where external companies are used to process personal data on behalf of the Foundation, responsibility for the security and appropriate use of that data remains with the Foundation.

9. Contractors, Short-Term and Voluntary Staff

The Foundation is responsible for the use made of personal data by anyone working on its behalf. Managers who employ contractors, short term or voluntary staff must ensure that they are appropriately vetted for the data they will be processing. In addition, managers should ensure that:

a) any personal data collected or processed in the course of work undertaken for the Foundation is kept securely and confidentially;

b) all personal data is returned to the Foundation on completion of the work, including any copies that may have been made. Alternatively that the data is securely destroyed and the Foundation receives notification in this regard from the contractor or short term / voluntary member of staff;

c) the Foundation receives prior notification of any disclosure of personal data to any other organization or any person who is not a direct employee of the contractor;

d) any personal data made available by the Foundation, or collected in the course of the work, is neither stored nor processed outside the EU unless written consent to do so has been received from the Foundation;

e) all practical and reasonable steps are taken to ensure that contractors, short term or voluntary staff do not have access to any personal data beyond what is essential for the work to be carried out properly.

10. Disclosure of Data to Third Parties

In the absence of consent, a legal obligation, other legal basis of processing or an emergency, personal data may not be disclosed to third parties unrelated to the Foundation. Some bodies have

a statutory power to obtain information. Staff should seek confirmation of any such power before disclosing personal data in response to a request.

11. Data Transfers to Countries outside the EU

The GDPR restricts data transfers to countries outside the EU in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. This applies when personal data is 1. transmitted or sent to a different country or 2. viewed/accessed in a different country.

Personal data may only be transferred outside the EU if one of the following conditions applies:

a) the European Commission has issued a decision confirming that the country to which the Foundation transfers the personal data ensures an adequate level of protection for the data subjects' rights and freedoms. The countries currently approved can be found here: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en;

b) appropriate safeguards are in place such as binding corporate rules, standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism;

c) the data subject has provided explicit consent to the proposed transfer after being informed of any potential risks; or

d) the transfer is necessary for one of the other reasons set out in the GDPR including:

   (i) the performance of a contract between the Foundation and the data subject;

   (ii) reasons of public interest;

   (iii) to establish, exercise or defend legal claims; or

   (iv) to protect the vital interests of the data subject where the data subject is physically or legally incapable of giving consent.

Staff should seek guidance from their Project Manager and the DPC before any transfer of personal data to countries outside the EU takes place.

12. Record Keeping

The GDPR requires the Foundation to keep full and accurate records of all data processing activities. Staff must keep and maintain accurate corporate records reflecting the processing, including records of data subjects' consents and procedures for obtaining consents, where consent is the legal basis of processing.

These records should include, at a minimum, the name and contact details of the Foundation as data controller and the DPC, clear descriptions of the personal data types, data subject types, processing activities, processing purposes, third-party recipients of the personal data, personal data storage locations, personal data transfers, the personal data's retention period and a description of the security measures in place.

Records of personal data breaches must also be kept, setting out:

a) the facts surrounding the breach;

b) its effects; and

c) the remedial action taken.

13. Training and Audit

All Foundation staff must undergo adequate training to enable them to comply with data protection law. The Foundation must also regularly test the systems and processes to assess compliance.

14. Data Privacy by Design and Default and Data Protection Impact Assessments (DPIAs)

The Foundation is required to implement privacy-by-design measures when processing personal data, by implementing appropriate technical and organizational measures (like pseudonymization) in an effective manner, to ensure compliance with data-protection principles. The Foundation must ensure therefore that by default only personal data which is necessary for each specific purpose is processed. The obligation applies to the volume of personal data collected, the extent of the processing, the period of storage and the accessibility of the personal data. In particular, by default, personal data should not be available to an indefinite number of persons.

As well as complying with Foundation-wide practices designed to fulfil reasonable expectations of privacy, staff should also ensure that their own data-handling practices default to privacy to minimize unwarranted intrusions in privacy e.g. by disseminating personal data to those who need to receive it to discharge their duties.

The Foundation must also conduct data protection impact assessments (DPIAs) in respect of high-risk processing before that processing is undertaken.

A DPIA should be conducted in the following circumstances:

a) the use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);

b) automated processing including profiling; and

c) large-scale processing of sensitive (special category) data.

A DPIA must include:

a) a description of the processing, its purposes and the data controller's legitimate interests if appropriate;

b) an assessment of the necessity and proportionality of the processing in relation to its purpose;

c) an assessment of the risk to individuals; and

d) the risk-mitigation measures in place and demonstration of compliance.

15. Data Subjects' Rights

Data subjects have the following rights:

a) where the legal basis of the Foundation's processing is consent, to withdraw that consent at any time;

b) to ask for access to the personal data that the Foundation holds;

c) to object to the processing of personal data in limited circumstances;

d) to ask to erase personal data without delay:

(i) if it is no longer necessary in relation to the purposes for which it was collected or otherwise processed;

(ii) if the only legal basis of processing is consent and that consent has been withdrawn and there is no other legal basis on which to process that personal data;

(iii) if the data subject objects to the processing where the legal basis is the pursuit of a legitimate interest or the public interest and the Foundation can show no overriding legitimate grounds or interest;

(iv) if the processing is unlawful;

e) to ask to rectify inaccurate data or to complete incomplete data;

f) to restrict processing in specific circumstances e.g. where there is a complaint about accuracy;

g) to ask for a copy of the safeguards under which personal data is transferred outside of the EU;

h) not to be subject to decisions based solely on automated processing, including profiling, except where necessary for entering into, or performing, a contract, with the Foundation; it is based on the data subject's explicit consent and is subject to safeguards; or is authorized by law and is also subject to safeguards;

i) to prevent processing that is likely to cause damage or distress to the data subject or anyone else;

j) to be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;

k) in limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine readable format; and

l) to make a complaint to the regulator foreseen by law.

The identity of an individual requesting data under any of the rights listed must be verified. Requests (including for data subject access) must be complied with, usually within one month of receipt.

16. Data Subject Access Requests

Data subjects have the right to receive copy of their personal data which is held by the Foundation. In addition, an individual is entitled to receive further information about the Foundation's processing of their personal data as follows:

a) purposes;
b) categories of personal data being processed;
c) recipients/categories of recipients;
d) retention periods;
e) their rights;
f) details of the relevant safeguards where personal data is transferred outside the EEA;
g) any third-party source of the personal data.

The entitlement is not to documents per se, but to such personal data as is contained in the document. The right relates to personal data held electronically and to limited manual records.

Personal data may not be altered, concealed, blocked or destroyed once a request for access has been made. The DPC should be contacted before any changes are made to personal data which is the subject of an access request.

17. Reporting a Personal Data Breach

Any personal data breach where there is a risk to the rights and freedoms of the data subject needs to be reported to the DPC. Where the personal data breach results in a high risk to the data subject, he/she also has to be notified unless subsequent steps have been taken to ensure that the risk is unlikely to materialize, security measures were applied to render the personal data unintelligible (e.g. encryption) or it would amount to disproportionate effort to inform the data subject directly. In the latter circumstances, a public communication must be made or an equally effective alternative measure must be adopted to inform data subjects, so that they themselves can take any remedial action.

Staff members who know or suspect that a personal data breach has occurred should immediately contact the DPC. All evidence relating to personal data breaches must be retained in particular to enable the Foundation to maintain a record of such breaches, as required by the GDPR.

18. Changes to this Policy

This Policy including any amendments will be made accessible to all staff members. The Foundation reserves the right to change the Policy at any time without notice.

This Policy was approved on 24 July 2018 by the Management and the DPC of the Foundation and by the Data Protection Officer of the Max Planck Society. It will be reviewed by 24 July 2019.

Appendix 1: GDPR Principles

Principle 1 of the GDPR – Processing Personal Data Lawfully, Fairly and Transparently

1. Lawfulness and Fairness

Personal data may only be processed fairly and lawfully and for specified purposes. These restrictions are not intended to prevent processing, but ensure that the Foundation processes personal data for legitimate purposes without prejudicing the rights and freedoms of data subjects. In order to be justified, the Foundation may only process personal data if the processing in question is based on one (or more) of the legal bases set out below. The legal basis that is being relied on for each processing activity must be identified and included in the Privacy Notice provided to data subjects.

Legal Bases for Processing Non-Sensitive Personal Data

The legal bases for processing non-sensitive personal data are as follows:

a) the data subject has given his or her consent. A data subject's consent should only be obtained if there is no other legal basis for the processing. consent requires genuine choice and genuine control. A data subject consents to processing of his/her personal data if he/she indicates agreement clearly either by a statement or positive action to the processing. Silence, pre-ticked boxes or inactivity are therefore unlikely to be sufficient. If consent is given in a document that deals with other matters, the Foundation must ensure that the consent is separate and distinct from those other matters. Data subjects must be able to withdraw consent to processing easily at any time. Withdrawal of consent must be promptly honoured. Consent may need to be renewed if the Foundation intends to process personal data for a different and incompatible purpose which was not disclosed when the data subject first consented, or if the consent is historic. The Foundation should keep a record of all consents obtained so that it can demonstrate compliance;

b) the processing is necessary for the performance of a contract with the data subject (e.g. monitoring academic performance in order to provide the relevant qualification for which the student has enrolled);

c) to meet the Foundation's legal compliance obligations;

d) to protect the data subject's vital interests (i.e. matters of life or death);

e) to pursue the Foundation's legitimate interests (or another's legitimate interests) which are not overridden because the processing prejudices the interests or fundamental rights and freedoms of data subjects. The specific legitimate interest or interests that the Foundation is pursuing when processing personal data will need to be set out in relevant Privacy Notices. This ground can only be relied upon for private functions, e.g. marketing or fundraising, and not for public functions.

Legal Bases for Processing Sensitive Personal Data, including Special Category Data

Special Category Personal Data is data revealing:

a) racial or ethnic origin;

b) political opinions;

c) religious or philosophical beliefs;

d) trade union membership.

It also includes the processing of:

a) genetic data;

b) biometric data for the purpose of uniquely identifying a natural person;

c) data concerning health;

d) data concerning a natural person's sex life or sexual orientation.

Personal data relating to criminal convictions and offences including the alleged commission of offences or proceedings for offences or alleged offences should be treated in the same way to special category data.

The processing of sensitive personal data by the Foundation must be based on one of the following (together with one of the legal bases for processing non-sensitive personal data as listed above):

a) the data subject has given explicit consent (requiring a clear statement, not merely an action);

b) the processing is necessary for complying with employment law;

c) the processing is necessary to protect the vital interests of the data subject or another person where the data subject is physically or legally incapable of giving consent;

d) the processing relates to personal data which are manifestly made public by the data subject;

e) the processing is necessary for the establishment, exercise or defence of legal claims;

f) the processing is necessary for reasons of substantial public interest (provided it is proportionate to the particular aim pursued and takes into account the privacy rights of the data subject);

g) the processing is necessary for the purposes of preventive or occupational medicine, etc. provided that it is subject to professional confidentiality;

h) the processing is necessary for reasons of public interest in the area of public health, provided it is subject to professional confidentiality;

i) the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes if it is subject to certain safeguards (i.e. pseudonymization or anonymization where possible, the research is not carried out for the purposes of making decisions about particular individuals (unless it is approved medical research) and it must not be likely to cause substantial damage/distress to an individual and is in the public interest).

Processing sensitive personal data represents a greater intrusion into individual privacy than when processing non-sensitive personal data. Special care must be taken when processing sensitive personal data, ensuring compliance with the data protection principles (as set out in the main body of this Policy), in particular in ensuring the security of the sensitive personal data.

2. Transparency (Notifying Data Subjects)

Under the GDPR the Foundation is required to provide detailed, specific information to data subjects depending on whether the information was collected directly from data subjects or from elsewhere. That information must be provided through appropriate Privacy Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a data subject can easily understand what happens to their personal data.

Whenever the Foundation collects personal data directly from data subjects, for example for the recruitment and employment of staff, at the time of collection the Foundation must provide the data subject with all the prescribed information which includes:

a) the Foundation's details;

b) contact details of the DPC;

c) purposes of processing;

d) legal basis of processing;

e) where the legal basis is legitimate interest, identify the particular interests (e.g. marketing, fundraising);

f) where the legal basis is consent, the right to withdraw;

g) where statutory/contractual necessity, the consequences for the data subject of not providing the data of non-provision.

When personal data is collected indirectly (for example, from a third party or publically available source), the Foundation must also provide information about the categories of personal data and any information on the source. The data subject must be provided with all the information required by the GDPR as soon as possible after collecting/receiving the data. The Foundation must also check that the personal data was collected by the third party in accordance with the GDPR and on a basis which contemplates the Foundation's proposed processing of that personal data.

Principle 2 of the GDPR – Purpose Limitation

Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

Personal data cannot be used for entirely new, different or incompatible purposes from those disclosed when it was first obtained unless the Foundation has informed the data subject of the new purposes. Where the further processing is not based on the data subject's consent or on a lawful exemption from data-protection law requirements, it should be assessed whether a purpose is incompatible by taking into account factors such as:

a) the link between the original purpose/s for which the personal data was collected and the intended further processing;

b) the context in which the personal data has been collected, in particular the Foundation–data subject relationship, taking into consideration if the data subject would reasonably anticipate the further processing of his/her personal data;

c) the nature of the personal data, in particular whether it involves special categories of personal data (i.e. sensitive) or personal data relating to criminal offences/convictions;

d) the consequences of the intended further processing for the data subjects;

e) the existence of any appropriate safeguards, e.g. encryption or pseudonymization.

Provided that prescribed safeguards are implemented, further processing for scientific or historical research purposes or for statistical purposes will not be regarded as incompatible. Safeguards include ensuring data minimization (e.g. pseudonymization or anonymization where possible), the research will not be carried out for the purposes of making decisions about particular individuals and it must not be likely to cause substantial damage/distress to an individual.

Principle 3 of the GDPR – Data Minimization

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. The Foundation should not therefore collect large volumes of personal data that are not relevant for the purposes for which they are intended to be processed. Conversely, personal data must be adequate to ensure that the Foundation can fulfil the purposes for which it was intended to be processed.

Staff may only process personal data when performing their job duties requires it. They should not process personal data for any reason unrelated to their job duties.

The Foundation must ensure that when personal data is no longer needed for specified purposes, it is deleted or anonymized in accordance with the Foundation's data retention Policy and schedule.

Principle 4 of the GDPR – Accuracy

Personal data must be accurate and, where necessary, kept up to date. It should be ensured that personal data is recorded in the correct files.

Incomplete records can lead to inaccurate conclusions being drawn and in particular, where there is such a risk, it should be ensured that relevant records are completed.

The accuracy of any personal data must be checked at the point of collection and at regular intervals thereafter. The Foundation must take all reasonable steps to destroy or amend inaccurate records without delay and should up-date out-of-date personal data where necessary (e.g. where it is not simply a pure historical record).

Where a data subject has required his/her personal data to be rectified or erased, the Foundation should inform recipients of that personal data that it has been erased/rectified, unless it is impossible or significantly onerous to do so.

Principle 5 of the GDPR – Storage Limitation

Personal data must not be kept in a form that allows data subjects to be identified for longer than needed for the legitimate educational/research or Foundation business purposes or other purposes for which the Foundation collected it. Those purposes include satisfying any legal, accounting or reporting requirements. Records of personal data can be kept for longer than necessary if anonymized.

The Foundation will take all reasonable steps to destroy or erase from the Foundation's systems all personal data that is no longer required in accordance with all relevant Foundation records, retention schedules and policies. The Foundation has a document retention Policy.

The Foundation will ensure that data subjects are informed of the period for which their personal data is stored or how that period is determined in any relevant Privacy Notice.

Principle 6 of the GDPR – Security, Integrity and Confidentiality

The Foundation is required to implement and maintain appropriate safeguards to protect personal data, taking into account in particular the risks to data subjects presented by unauthorized or unlawful processing or accidental loss, destruction of, or damage to their personal data. Safeguarding will include the use of encryption and pseudonymization where appropriate. It also includes protecting the confidentiality (i.e. that only those who need to know and are authorized to use personal data have access to it), integrity and availability of the personal data. The Foundation will regularly evaluate and test the effectiveness of those safeguards to ensure security of the Foundation's processing of personal data.

Personal data must be handled in a way that guards against accidental loss or disclosure or other unintended or unlawful processing and in a way that maintains its confidentiality. Particular care must be exercised in protecting sensitive personal data from loss and unauthorized access, use or disclosure.

Staff must comply with all procedures and technologies put in place by the Foundation to maintain the security of all personal data from the point of collection to the point of destruction.

Staff must comply with all applicable aspects of the Foundation's Data Protection Policy, and comply with and not attempt to circumvent the administrative, physical and technical safeguards implemented and maintained in accordance with the data protection law standards to protect personal data.

The Foundation may only transfer personal data to third-party service providers (i.e. data processors) who provide sufficient guarantees to implement appropriate technical and organizational measures to comply with data protection law and who agree to act only on the Foundation's instructions. Data processors should therefore be appointed subject to the Foundation's standard contractual requirements for data processors.

Appendix 2: Glossary of Terms

Automated Decision-Making (ADM): when a decision is made which is based solely on automated processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits automated decision-making (unless certain conditions are met) but not automated processing.

Profiling: any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of automated processing.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the processing of personal data relating to them.

Data Controller: the person or organization that determines when, why and how to process personal data. It is responsible for establishing practices and policies in accordance with the GDPR. The Management of the Foundation is the data controller of all personal data relating to it and used delivering education and training, conducting research and all other purposes connected with it including business purposes.

Data Subject: a living, identified or identifiable individual about whom the Foundation holds personal data.

Data Protection Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of privacy by design and should be conducted for all major system or business change programs involving the processing of personal data.

Personal Data: any information identifying a data subject or information relating to a data subject that can be identified (directly or indirectly) from that data alone or in combination with other identifiers the Foundation possesses or can reasonably access. Personal data includes sensitive personal data and pseudonymized personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach: any breach of security resulting in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to, personal data, where that breach results in a risk to the data subject. It can be an act or omission.

Privacy by Design and Default: implementing appropriate technical and organizational measures in an effective manner to ensure compliance with the GDPR.

Privacy Notices: separate notices setting out information that may be provided to data subjects when the Foundation collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee, student and project partner privacy notices or the website privacy Policy) or they may be stand-alone, one-time privacy statements covering processing related to a specific purpose.

Processing or Process: any activity that involves the use of personal data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing

also includes transmitting or transferring personal data to third parties. In brief, it is anything that can be done to personal data from its creation to its destruction, including both creation and destruction.

Pseudonymization or Pseudonymized: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Contact

For more information please contact:

- The Data Protection Coordinator of the Foundation, Dr. Frauke Lachenmann (Tel. +49 (6221) 91404-48, Email: lachenmann@mpfpr.de);
- The Data Protection Officer of the Max Planck Society, Ms Heidi Schuster (Tel. +49 (89) 2108-1554, Email: datenschutz@mpg.de).