NWO-I Privacy Policy

Privacy policy text of NWO-I (the Institutes Organisation of the Dutch Research Council), as adopted by resolution of the Foundation Board on 2 November 2021.

Contents

1 Introduction

Privacy is increasingly the subject of attention. On 25 May 2018, the General Data Protection Regulation (GDPR) came into effect, succeeding the previous Directive that had served as the basis for the Dutch Personal Data Protection Act (PDPA) (*Wet bescherming persoonsgegevens*, Dutch acronym Wbp). NWO-I aims to meet all of its GDPR obligations by drawing up a privacy policy and updating it on a regular basis.

The use of personal data is necessary for the operations of NWO-I. Personal data should be stored and processed with the utmost care because its abuse can cause great harm to employees and other data subjects. As the data controller, the Foundation Board of NWO-I is legally responsible for the proper processing of personal data.
With the measures described in this policy document, NWO-I assumes its responsibility to optimise the processing and security of personal data and thus to comply with relevant privacy laws and regulations.

Definitions and abbreviations are given in Appendix A.

1.1 Scope and purpose of the privacy policy

The privacy policy is important for all employees, researchers and all other contacts of NWO-I. It has consequences for the work of all employees who handle personal data. The privacy policy covers the processing of personal data of all data subjects within NWO-I, including all employees, guests, visitors and external contacts (i.e. hiring of outside staff/outsourcing).

The privacy policy does not cover the processing of personal data for personal or household use, such as personal work notes or a collection of business cards. The conducting of research also falls outside the scope of this privacy policy. Where the nature and sensitivity of the research data make it necessary to develop additional policy, a privacy policy for conducting research will be drawn up for each institute. A code of conduct will also be drawn up if necessary, by analogy with the VSNU “Code of conduct for using personal data in research”, version 0.9.
The privacy policy covers the fully or partially automated and/or systematic processing of personal data undertaken under NWO-I responsibility, as well as the underlying documents (electronic or physical). The privacy policy also applies to the non-automated processing of personal data contained or intended to be contained in a filing system.

At NWO-I, the protection of personal data is considered in close connection with other obligations and policy objectives. In particular, an important relationship and partial overlap exists with the policy area of information security, which concerns the availability, integrity and confidentiality of data, including personal data. Attention is paid to the interfaces between the two areas and coordination is sought with regard to both planning and content.

The purpose of the privacy policy is to optimise the processing and security of personal data while striking a good balance between privacy, functionality and security.

The aim is to respect the privacy of data subjects as much as possible. Based on the fundamental right to the protection of one’s data, the data relating to a data subject must be protected against unlawful or unauthorised use and against loss or abuse. This implies that the processing of personal data must comply with relevant laws and regulations and that personal data held by NWO-I must be

secure.

The privacy policy explains to employees and other data subjects how privacy is organised at NWO-I. It also helps to raise awareness about the importance and necessity of protecting personal data.

The privacy policy aims to:

- Provide a framework for testing current and future personal data processing against a set standard and for clearly allocating duties, powers and responsibilities within the organisation.
- Enable the Foundation Board to assume responsibility by laying down the principles and organisation of personal data processing within NWO-I.
- Facilitate the decisive implementation of the privacy policy by making clear choices in terms of policy measures and actively monitoring their implementation.
- Ensure compliance with Dutch and European legislation.

In addition to the above specific objectives, a more general aim is to raise awareness of the importance and necessity of protecting personal data, partly in order to avoid risks arising from non-compliance with relevant laws and regulations.

The Foundation Board's approval of this privacy policy has resulted in a uniform privacy policy within NWO-I. Previous policy documents will be declared no longer applicable upon adoption of the present privacy policy.

2 Policy principles for personal data processing

NWO-I aims to handle personal data with care. This covers personal data in the context of research by the NWO Institutes, personal data of employees and data such as that of users of research facilities, for example. The framework consists of the General Data Protection Regulation (GDPR), the GDPR Implementation Act, the Telecommunications Act and other applicable statutory regulations, as well as national and international research standards and internal NWO-I regulations. The basis for information security within NWO-I is ISO27001. Without information security, there can be no protection of privacy. Of course, there are also issues that relate purely to the protection of privacy and not to information security. However, information security does play an important role; it is an essential tool for the protection of privacy. This is why the GDPR includes an obligation to engage actively in information security by taking appropriate technical and organisational measures. Responsibility for practical implementation of the GDPR in the context of research and location-based activities lies with the Institutes, while responsibility for operations lies, in principle, with the Foundation Board. There is close collaboration between NWO-I and NWO-D in the field of GDPR, especially through the shared Data Protection Officer (DPO).

As a general policy tenet, personal data must be processed properly and carefully in accordance with relevant laws and regulations. A good balance should be struck between the interests of NWO-I in processing personal data and the interests of data subjects in making their own decisions with regard to their personal data in a free environment.

To comply with the above policy tenet, NWO-I applies the following principles derived from the GDPR:

- Personal data are processed only for explicitly described and legitimate purposes. These purposes are specific and are set out before processing begins (Art. 5 GDPR).
- Processing of personal data is based on one of the legal grounds as stated in the General Data Protection Regulation (Art. 6 GDPR).
- The amount and type of personal data processed are restricted to those data that are necessary for the specific purpose. Data should be adequate, relevant and restricted to what is necessary in relation to that purpose (data minimisation).
- Personal data are processed as non-intrusively as possible and should be reasonably proportionate in relation to the intended purpose (purpose limitation).
- Measures are taken to ensure as far as possible that the personal data to be processed are accurate and up to date.
- Personal data are appropriately protected in accordance with applicable security standards.
- Personal data are not further processed in a manner incompatible with the initial purposes for which they were obtained.
- Personal data are not processed for longer than is necessary for the purposes of the processing, taking into account the applicable periods for storage and destruction.
- Every data subject has a legal right to access, correct, add to, delete or restrict their personal data in individual processing operations as well as, in certain cases, the right to object and the right to data portability.
- Privacy by design and privacy by default are applied at the start of a new process, project or system.

3 Responsibilities of the privacy organisation

For a structured and coordinated approach to the processing of personal data, certain responsibilities have been assigned to specific units and officials within the NWO-I organisation.

3.1 Board, Director NWO-I, directors of Institutes, Director of Operations

The Board is the highest body within NWO-I and is thus ultimately responsible for its overall functioning. Responsibility for day-to-day management lies with the Director NWO-I. The directors of the Institutes and the Director of Operations are accountable to the Director NWO-I. The Institute directors are responsible for ensuring compliance with the NWO-I privacy policy within their institute. The directors of the Institutes are authorised and responsible by mandate for processing operations within their institute. The Director of Operations is authorised and responsible by mandate for the implementation and further development of the NWO-I privacy policy and processing operations within the office.

3.2 Privacy Coordinator (first line)

The Privacy Coordinator (PC) has first-line responsibility for designing, monitoring and – to an extent – implementing the privacy policy within the institute or office, working closely with the Central Privacy Coordinator and the DPO. In addition, the PC can provide support in charting risks, for example by conducting a Data Protection Impact Assessment (DPIA). The PC also plays an important role on the work floor: for example, like the IT Manager, the PC advises the departmental teams and can answer questions such as: “How should we share this data?”; “Which rules should we follow?”; “Which measures should we impose on an outside party?”. The PC also has an important role in raising awareness and in organising or providing training. Another key role of the PC is in data breach incidents, including information gathering, communication and organising or implementing measures.

Duties of the PC[1]:

- Within the institute or office, is responsible for practical implementation of privacy-related policies and documentation (policies, regulations, education and communication plan, fact sheets), including reviewing sector- and department-specific regulations and policies, such as codes of conduct.
- Ensures privacy awareness and consciousness (education, knowledge sessions, training and communication).
- Monitors progress of data inventories and the processing register, risk analyses and DPIAs. Gives advice and answers questions, enabling line managers to provide the correct input for these privacy products.
- Answers ad hoc questions.
- Handles access, correction and deletion requests from data subjects in cooperation with the relevant privacy officers.

[1] The privacy coordinator of the research institute or office manages its processing register decentrally and ensures that further privacy documentation is channelled to a central point.

- Advises the various departments within an institute or office.
- Supports the various departments and privacy officers in conducting data inventories, DPIAs and risk analyses.
- Manages the privacy officers.
- Reviews partnerships and processor's agreements, if necessary in consultation with lawyers of NWO-I and/or CPC, where the PC does not have a legal background.

To ensure that departments and teams are GDPR-compliant, these duties have been (and will be) assigned to privacy officers where necessary. The privacy officers must supervise the process, create awareness and support, identify cases of non-compliance and safeguard information within the department. However, these officers all have the same duties. As first-line staff, they are accountable to their line managers. However, they can also be held accountable by the privacy coordinator for the duties they perform with regard to privacy.

Duties of the privacy officer:

- Contributes to the drafting of departmental privacy regulations, codes of conduct, fact sheets, work instructions and other communications.
- Identifies privacy-sensitive or high-risk processing operations, discusses these with the PC and implements any measures to be taken.
- Contributes to raising privacy awareness within the department (e.g. by putting it on the agenda of team or departmental meetings).
- Acts as a first-line point of contact for ad hoc questions from the department regarding privacy or personal data.

3.3 Central Privacy Coordinator (second line)

The Central Privacy Coordinator (CPC) is responsible for coordinating GDPR activities, liaising between different parts of NWO-I, arranging monthly meetings between the privacy coordinators, DPO and CISO and advising on various GDPR issues. The CPC plays a key role in connecting individuals with different GDPR roles and ensuring that as much as possible is streamlined and (where possible) tackled jointly. The CPC also supports the handling of data breaches and is a member of the data breach team (as part of the NWO-I privacy team). In addition, the CPC has an important role in advising the institutes and the office.

Duties of the CPC:

- Supervises the privacy coordinators with their team of local privacy officers.
- Ensures coordination between the privacy coordinators, DPO and CISO in the area of GDPR documentation.
- Provides tools and practical advice.
- Advises the institutes and office as required.
- Raises awareness and provides training.
- Acts as a privacy envoy.
- Acts as functional manager for the privacy coordinators.
- Supports the privacy coordinators in handling access, correction and deletion requests from data subjects.
- Supports the privacy coordinators in conducting data inventories, DPIAs and risk analyses.
- Carries out DPIAs in cooperation with the process or project manager.
- Is part of the NWO-I privacy team.
- Handles data breaches in close coordination with the data breach team.
- Holds monthly consultations with the DPO and CISOs.
- Holds monthly consultations with the privacy coordinators of the research institutes, the DPO and the CISO.

3.4 Data Protection Officer (third line)

The GDPR requires NWO-I to appoint an internal "supervisor" for the processing of personal data. This supervisor is called the Data Protection Officer (DPO). NWO-D and NWO-I share the DPO. The DPO supervises the application of and compliance with privacy legislation within all parts of NWO. The statutory duties and powers of the DPO give this officer an independent position in the organisation.

The DPO advises and informs the entire organisation and its individual units concerning the application of privacy legislation. The DPO contributes to the provision of information on the processing of personal data to employees and managers. The DPO promotes privacy awareness among staff, for example by posting information and blogs.

The DPO is the contact and enquiry point for anyone with queries about the protection of personal data. Together with the CISO, the DPO manages the register of reports of personal data processing operations (processing register).

The DPO is part of the audit team of NWO-D and NWO-I, reports to the vice president of the Executive Board/Foundation Board and conducts his/her activities independent of instruction.
Duties of the DPO:

- Acts as a privacy envoy.
- Coordinates with the Director of Operations and the CISO on privacy matters.
- Participates in the Privacy Team and Data Breach Team.
- Is involved in the handling of data breaches and other incidents.
- Drafts an annual privacy report including recommendations.
- Independently monitors the application of and compliance with privacy legislation and advises all levels within the organisation accordingly as required. Prepares reports for management and the Foundation Board.
- Acts as the organisation's contact person for the Dutch Data Protection Authority with regard to all data protection issues.
- Informs and advises the organisation about GDPR obligations.
- Submits DPIAs (subsequently) to the DPO for an opinion.

3.5 Chief Information Security Officer

NWO-I has a Chief Information Security Officer (CISO). The CISO is closely involved in implementing the privacy policy. The careful handling of personal data is covered in part by the general rules on information security.

The CISO is responsible for the development and implementation of information security and for determining the necessary measures (where organised centrally), and advises the institutes as required on security issues for which responsibility lies with the institutes.

The CISO's task is to oversee and coordinate the entire spectrum of information security. The CISO has an organisation-wide perspective on security. The purpose of the post, based on the generally accepted standard ISO27001, is to provide a coherent package of technical and organisational measures to safeguard the confidentiality, integrity and availability of information within the organisation. Risk analysis, an eye for operations and compliance with legal requirements are key concepts in this respect.

Duties of the CISO:

- Policy and coordination. The CISO can be seen as the programme manager for the strategic programme on information security.
- Advice and reporting. Acting as project manager for security projects, which involves managing project leaders within organisational units. Providing advice as required to the leadership of

the organisation and line management about the measures to be taken. Reporting to the management of the organisation about the policy pursued with regard to information security.

- As in the case of privacy, the CISO has regular consultations with the Security Officers (SOs) and Information Security Officers (ISOs) of the institutes.
- In addition, the CISO participates in the overarching consultations on privacy and information security matters described under “Duties of the PC”.

3.6 Privacy consultation and central privacy team

The central privacy team, consisting of the NWO-I Director of Operations, DPO, CISO, CPC and Head of Information Technology and Automation NWO-D, meets once a month to discuss and streamline ongoing issues. Where necessary, the central privacy team gives feedback to the PCs and IMs (information managers) on the topics to be discussed.

The Privacy Coordinators, Central Privacy Coordinator, DPO and CISO meet once a month for privacy consultations to discuss current issues and to further streamline the implementation, where possible.

4 Lawful and careful processing of personal data

4.1 General principles of personal data protection

All processing carried out by, within or on behalf of NWO-I involving personal data must comply with the principles of personal data protection. These principles are taken into account in all processing operations.

The processing of personal data must be based on one of the legal grounds as described in Article 6 of the GDPR. The data controller defines the purposes of the processing in advance. These purposes must be clear and specific. The extent to which the processing of personal data is necessary is assessed for each processing operation. The various interests are weighed up and expediency, proportionality and subsidiarity are examined.

Personal data are not further processed in a manner incompatible with the initial purposes for which they were obtained. If a processing operation is not part of the statutory duties of NWO, or in the absence of a legal obligation, an agreement or a legitimate interest, the explicit consent of the data subject is required.

NWO-I takes the necessary measures to ensure that personal data are correct and up to date in view of the purposes for which they are collected or subsequently processed.

Where infrastructure changes are made, processes introduced or revised, or new systems purchased, privacy is taken into account from the outset by conducting a Data Protection Impact Assessment (DPIA), where necessary. See Appendix E for the DPIA checklist to assess whether a DPIA is necessary.

In its implementation, NWO-I applies the principles of Privacy by Design and Privacy by Default. See also Appendix D.

4.1.1 Lawfulness, appropriateness and transparency

Personal data must be processed in a manner that is lawful, appropriate and transparent with regard to the data subject. According to this principle, all processing of personal data must firstly be lawful and appropriate. This means that all operations involving the processing of personal data must comply with the law. This refers both to the GDPR itself and to national law. Secondly, all processing operations must be transparent. This means primarily that the data subject must be aware of the processing. Operations in which personal data are processed in an unreasonable or unlawful manner, for example if the data subject was not informed about the processing, are therefore generally contrary to this principle.

4.1.2 Purpose limitation

Personal data should be collected only for specified, explicitly described and legitimate purposes and may not be further processed in a manner incompatible with those purposes.

The principle of purpose limitation requires that the purposes of processing be specifically defined prior to the processing. In particular, the purposes should not be formulated too vaguely or too broadly, and they may not be changed after the data have been collected.

Within NWO-I, the purpose of personal data processing must remain within the framework of:

- research;
- operational support.

4.1.3 Data minimisation

Thirdly, the principle of data minimisation requires that data be adequate, relevant and limited to what is necessary for the purposes of processing.

In essence, this means that personal data may only be processed if processing is necessary. Personal data that are not necessary should in principle not be collected. If several different processing operations are carried out, the principle of data minimisation applies to each separate operation.

In addition, the principle of data minimisation implies that only employees who need access to specific personal data in order to perform their duties are permitted to view these categories of personal data. Where access to personal data is not necessary, access should not be possible.

4.1.4 Accuracy

In addition, data should in principle be accurate and updated when necessary. All reasonable steps must be taken to ensure that personal data that are inaccurate, given the purposes for which they are being processed, are erased or rectified without delay.

The principle of accuracy means primarily that all data relating to a person must be correct. If data are found to be incorrect, they should be corrected or supplemented as soon as possible. This applies both to data that were already incorrect at the time of collection and to data that need to be adjusted as a result of a change in situation.

4.1.5 Storage limitation and retention periods

Personal data are kept for no longer than necessary for the purposes for which they were collected or are to be used. Personal data must be removed from the active records system after the storage period has expired. NWO-I will destroy personal data after the retention period has expired; alternatively, if the personal data are intended for historical, statistical or scientific purposes, NWO will store the data in an archive, provided that appropriate technical and organisational measures are taken to protect the rights and freedoms of the data subject.

4.1.6 Integrity and confidentiality

The principle of integrity and confidentiality requires that appropriate technical or organisational measures be taken. In addition to appropriate security, personal data must also be protected against unauthorised or unlawful processing and against intentional loss, destruction or damage.

This means that NWO-I and any processors brought in will handle personal data with care. Care means firstly that employees who handle personal data will treat them confidentially and secondly that NWO-I will take technical and organisational measures to further safeguard and protect those data.

4.1.7 Accountability

NWO-I is responsible for compliance with the above principles and is able to demonstrate this. NWO-I must demonstrate that the data processing principles are correctly and properly observed. If NWO-I does not fulfil its obligations, or does not fulfil them properly, it will be held accountable.

4.2 Lawfulness

NWO-I must be able to demonstrate that each processing operation is based on a legal ground as stated in the GDPR. The processing of personal data is therefore lawful only if NWO-I can demonstrate that one of the conditions in Article 6 GDPR applies. In short, the processing of personal data by NWO-I is permitted only if the processing is based on one of the following grounds:

4.2.1 Consent

In the case of consent, processing of personal data is lawful only if the data subject has consented to the processing of their personal data for one or more specific purposes. Consent is valid only if it is informed, voluntary and specific.

The data subject may withdraw consent at any time. Withdrawal of consent does not adversely affect the lawfulness of the processing that took place before the consent was withdrawn. Processing of personal data must of course cease immediately as soon as consent is withdrawn, unless the processing operations can be based on another legal ground.

4.2.2 Performance of an agreement

Personal data may also be processed if processing is necessary in order to perform an agreement, or to conclude an agreement at the request of the data subject. This applies, for example, to processing related to the performance of agreements between NWO-I and its partners.

NWO-I may invoke this legal ground only if the data requested are actually necessary for the performance of the agreement. This condition does not apply where no data, or no additional data, are required.

4.2.3 Legal obligation

NWO-I may process data if it is legally obliged to do so. A number of legal obligations may apply. NWO-I is mainly obliged to process data in order to meet its obligations as an employer and on account of tax obligations.

4.2.4 Vital interests

Personal data may be further processed if the processing is necessary in order to protect the vital interests of the data subject or another natural person. This condition applies especially in medical emergencies: for example, in an emergency situation such as unconsciousness, the person's consent may not be required before their identity data are passed on to the hospital.

4.2.5 Task carried out in the public interest

Data processing is also permitted if NWO-I processes personal data in connection with the performance of a task carried out in the public interest or in the exercise of official authority vested in it. This condition applies only if the personal data are actually necessary for the processing connected with the performance of a task carried out in the public interest.

4.2.6 Legitimate interests

Personal data may be further processed if NWO-I can demonstrate a legitimate interest, i.e. if the processing is necessary in order to protect the legitimate interests of NWO-I or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject.

Legitimate interests may include business interests, providing the interest is sufficiently strong. However, the existence of an interest is not sufficient in itself. This condition can only be applied if data security measures are taken, and if the proportionality and subsidiarity of the processing is guaranteed. The interests of the data controller and the data subject must therefore be carefully balanced. The balancing of interests must be justified and documented.

4.3 Reporting and documenting of data processing

Any fully or partially automated processing of personal data should be reported to the Privacy Coordinator of the research institute or office. The Privacy Coordinator, in cooperation with the CPC, assesses whether the data recording is lawful. The Privacy Coordinator ensures that the data recording is properly documented.

4.3.1 Responsibility

1. Data processing operations within NWO-I (research institutes and operations) are reported to the relevant Privacy Coordinator.
2. The Privacy Coordinator is responsible for entering these reports in the processing register.
3. The DPO/CISO are responsible for keeping an inventory of reports of data processing operations.

4.3.2 Reports

4. Every report of a data processing operation must contain at least the following information:
- Name of the process/operation;
- Functional name of the system in which processing takes place;
- Holder of the system;
- External parties involved;
- Purpose of processing;
- Which (categories of) personal data belonging to which categories of data subjects are recorded;
- Retention periods to be observed, which may differ for each type of personal data;
- Description of the security measures taken;
- List of national and international organisations to which personal data are provided.

5. The purpose of the processing must include the legal basis:
- Consent of the data subject;
- Performance of an agreement;
- A legal obligation;
- To safeguard a vital interest of the data subject;
- Performance of a public duty;
- Justified interest of the controller or third party to which data has been provided.

6. Information systems that do not use personal data are not reported.

4.4 The organisation of security

NWO-I ensures an adequate level of security and implements appropriate technical and organisational measures to protect personal data against loss or any form of unlawful processing. These measures are aimed in part at preventing the unnecessary or unlawful collection and

processing of personal data.

A risk analysis focusing on the protection of privacy and information security is part of the internal risk management and control system of NWO-I. This is done via the classification of an application.

4.5 Confidentiality

NWO-I classifies all personal data as confidential. Everyone should be aware of the confidentiality of personal data and act accordingly.

Persons not already bound by a duty of confidentiality on account of their office, profession or a statutory provision are also obliged to maintain confidentiality with regard to any personal data coming to their knowledge, unless an obligation of disclosure arises under a statutory provision or in the course of their duties.

4.6 Special data and criminal offence data

Special categories of personal data are particularly sensitive. These categories of personal data receive special protection, because their disclosure might have a negative impact on the data subject.

The processing of special categories of personal data is prohibited in principle, unless one of the exceptions in Article 9(2) GDPR applies. Exceptions include a legal basis, explicit consent of the data subject and a substantial public interest. The security of these categories of personal data is also subject to stricter requirements. Where the basic level of protection is insufficient, additional measures must be taken, tailored to each individual information system.

Special categories of personal data include data concerning a person's religious or philosophical beliefs, race, political opinions, health, sex life and trade union membership.

In addition to special data, there are also sensitive data. These are mainly data that are regarded as sensitive in view of their content or nature: for example, they may concern someone's financial situation or internet surfing behaviour, or they may relate to minors. NWO-I always handles sensitive data with special care. In addition, the citizen service number (BSN) of the data subject is processed only if required by law.

Criminal offence data may be only processed under strict conditions. Criminal offence data may be processed only under government supervision or where a legal provision allows NWO-I to process it.

4.7 Transfer of personal data to third parties

4.7.1 Outsourcing of processing to a processor

If NWO-I has personal data processed by a processor, the processing is governed by a written agreement between NWO-I, the controller and the processor. A standard template is available for a processor's agreement.

4.7.2 Transfer of personal data within the European Union

NWO-I provides personal data to third parties only if the transfer has a legal basis (Art. 6 GDPR) and the third party also has a basis for receiving the data. Special categories of personal data are not provided to third parties unless NWO-I can invoke one of the exceptions in Article 9 GDPR.

4.7.3 Transfer of personal data outside the European Union or international treaty organisations

NWO-I provides personal data to third parties located in a country outside the European Union only if that country as a whole or the business/institution concerned specifically guarantees an appropriate level of protection. To determine whether countries have an appropriate level of protection, NWO-I uses the list of countries with regard to which the European Commission has adopted an adequacy decision. Or where the transfer of employees' personal data is necessary for the purposes of working with internationally recognised treaty organisations[2].

NWO-I provides personal data to countries without an appropriate level of protection only on the basis of a statutory exception. One such exception is "unambiguous consent", where the person whose personal data are being transferred has given clear and unambiguous consent. Another statutory exception is transfer on the basis of a model contract (as drawn up by the European Commission). Changes or additions to the model contract require approval from the Minister of Justice and Security.

4.7.4 Third parties to which NWO-I transfers personal data

When NWO-I provides personal data to a third party, NWO-I always ensures by way of an agreement that the data may not be used for purposes other than those for which NWO-I has provided the data. In this agreement, NWO-I also stipulates that data must be removed as soon as these are no longer necessary. NWO-I has a standard exchange agreement for this purpose.

4.8 Data Protection Impact Assessment (DPIA)

A Data Protection Impact Assessment (DPIA) – also called a Privacy Impact Assessment (PIA) – is mandatory for high-risk processing of personal data. To determine whether processing is high-risk, the following factors should be considered: type of processing, whether the processing uses new technologies, nature, scope, context and purposes of the processing.

A DPIA is required in the following four cases:

- a systematic and extensive evaluation of personal aspects relating to persons which is based on automated processing, provided this results in decisions that produce legal effects for the person, such as profiling;
- processing on a large scale of special categories of data or of personal data relating to criminal convictions and offences;
- a systematic monitoring of a publicly accessible area on a large scale; or
- the processing operations for which the Dutch Data Protection Authority has indicated that a DPIA is required.

If a DPIA is carried out, NWO-I will give details of the processing operations and the associated purposes. The DPIA will also include an assessment of the necessity of the processing operations, the risks posed by the processing and the measures envisaged to address these risks. Finally, NWO-I carries out a review to assess if processing is performed in accordance with the recommendations and conclusions in the DPIA. Before a process requiring a DPIA is carried out, the DPIA must first be submitted to the DPO of NWO-I for an opinion. To assess whether a DPIA is necessary for new or existing processing operations, systems or partnerships, NWO-I has drawn up a DPIA checklist. See Appendix E.

[2] Such as ESA and CERN.

4.9 Privacy by Design and Default

Privacy by Design (PbD) means that the risk to privacy is considered before starting any new processing operation, for example in the case of a new project, a partnership, or the acquisition of software involving personal data. This analysis is translated into specific security requirements and measures that NWO-I takes to protect personal data appropriately.

PbD is a method used throughout NWO-I to guarantee the privacy of data subjects as thoroughly as possible. PbD means at the very least that data minimisation and pseudonymisation are central to processing by NWO-I. The following measures also play a role in designing the security of personal data:

- encryption of personal data;
- ensuring the confidentiality, integrity and availability of systems and services;
- restoring the availability of personal data promptly in the event of an incident;
- a procedure for testing, assessing and evaluating security measures.

NWO-I uses a Privacy by Design checklist. See Appendix D.

5 Personal data incidents

Every complaint or report regarding the processing of personal data within NWO is a privacy incident. The best-known form of such incidents is a data breach.

This section describes the policy for reporting, recording and handling incidents or suspected incidents during normal operations and in special circumstances.

5.1 Reporting and recording

NWO-I employees must immediately report any actual or suspected data breach or other privacy incidents. This is done via the data breach reporting point **datalek-nwoi@nwo.nl**.

A record is kept of each incident and its handling. Reports are treated as confidential. The person making a report can trust that there will be no personal consequences for them as a result. Until the incident has been handled, the person making the report must treat the report as confidential and not communicate about it with those involved or other parties.

5.2 Handling

The purpose of incident handling is to resolve the problem, limit the damage, comply with legislation and learn as an organisation. NWO-I has a separate team for data breaches (consisting of the DPO, CISO and IT department staff) that assesses whether an incident constitutes or might constitute a data breach. This data breach team is part of the privacy team.

If the incident constitutes a data breach, it is reported in accordance with the rules of the Dutch Data Protection Authority (DPA). A report to the DPA must be made without undue delay and within 72 hours of discovery, unless it can be reasonably assumed that the data breach (breach of privacy) is unlikely to result in a risk to the data subject.

Where informing data subjects is mandatory under DPA rules or otherwise desirable, communication is carried out by the relevant research institute, office or department in consultation with Communication. The person reporting the incident is informed about its handling and also receives feedback about how it was handled and the lessons we can learn from this as an organisation.

The full procedure for reporting data breaches is set out in Appendix B.

5.3 Evaluation

It is important to learn from incidents. Recording of incidents, periodical reporting, training and promotion of appropriate behaviour are all part of a professional approach to the processing of personal data. Reporting on personal data incidents is therefore a fixed part of the annual privacy report produced by the DPO.

6 Communication and awareness

Awareness is the first step towards achieving desired behaviour. Awareness is usually followed by motivation (to change) after which people are ready for the (new) knowledge (by informing and with some help in interpreting). If, in addition, (new) skills are needed, then safe practice is needed after which new behaviour effectively can be applied in 'real' practice. Especially with these last steps, there are often obstacles that must be solved by the organisation and/or communication in the area of motivation, capacity and opportunity (Triad of Poiesz). Think of barriers such as worries, lack of support or hours, demotivating context, a brochure, etc.

Communication play a powerful role in identifying and addressing all of these distinctive issues, their dependencies and sequencing. In this way, communication can help implement continuous AVG implementation and assurance through knowledge, skills and behaviour, both among current and, for example, new employees. The means and interventions to be deployed at any given moment in time are created agile and in close consultation with all those directly involved, of course preceded by the definition of target groups, objectives and strategies.

This continuous attention to communication can best be ensured by including a communication advisor in both, the organisation-wide and local privacy teams and during regular meetings of, for example, the CPC with PCs.

Data leaks and security incidents

Communication during and after data breaches and security incidents deserves extra attention, in order to let the organisation learn from things that went wrong or almost went wrong. In addition to informing and reporting on reported and registered situations, learning sometimes requires more like a training course or a good (and safe!) discussion (meeting).

Communication in the long term helps to further optimise and secure the quality of the processing and security of personal data, at the end to help NWO-I comply with the relevant privacy legislation. Which is good for our own organisation and certainly also for science in general, which is perhaps more than ever under a social magnifying glass.

Appendix A - Definitions and abbreviations

AP	Autoriteit Persoonsgegevens (the Dutch Data Protection Authority)
Controller	The natural person, legal entity or any other person or body who, alone or jointly with others, determines the purposes and means of the processing of personal data.
Criminal personal data	Personal data relating to criminal convictions and offences or related security measures.
Data breach	It is a breach of security that results in the accidental or unlawful disclosure of personal data. A data breach involves the destruction, loss, alteration or unauthorised disclosure of, or access to, data transmitted, stored or otherwise processed.
Data subject	An individual and natural person to whom personal data relates.
DPIA	Data Protection Impact Assessment. See Privacy Impact Assessment.
DPO	Data Protection Officer
GDPR	General Data Protection Regulation (EU) 2016/679. The European successor to the Wet bescherming Persoonsgegevens (Dutch data protection act), applicable as of 25 May 2018.
Opt-in	With opt-in, a data subject has given explicit and demonstrable consent to receive e-mail from a certain mailing list.
Opt-out	With an opt-out system, data subjects are automatically placed on a mailing list for a newsletter and have the possibility to unsubscribe from it.
Personal data	Any information relating to an identified or identifiable natural person.
Privacy by default	When users are offered a choice between different options, the default setting gives the best privacy guarantees.
Privacy by design	The management of the entire life cycle of personal data, from collection to processing and deletion, paying systematic attention to comprehensive safeguards concerning the accuracy, confidentiality, integrity, physical security and deletion of personal data.
Privacy Impact Assessment	A tool that helps identify privacy risks and provides the tools to reduce these risks to an acceptable level.

Processing of personal data	Any operation or set of operations in relation to personal data, personal data including in any case the collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or any other form of making available, alignment or combination, blocking, erasure or destruction of data.
Processor	An organisation who processes personal data on behalf of the controller.
Proportionality	The purpose of processing personal data must be proportionate to the invasion of privacy of those concerned.
Special categories of personal data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership. And the processing of genetic data, biometric data with a view to the unique identification of an individual, or data concerning health, or data concerning a person's sexual behaviour or orientation.
Subsidiarity	The intended purpose of the processing cannot be achieved in a less intrusive manner and/or by less intrusive means.
Third party	Any person other than the data subject, the controller or the processor, or any person under the direct authority of the controller or the processor, who is authorised to process personal data.