NWO Privacy Policy
2020–2021

# Table of contents

NWO privacy statement .................................................................................................................. 4

Introduction ................................................................................................................................ 5

1.1 Scope and purpose of the privacy policy .................................................................................. 5

2 Policy principles for personal data processing ............................................................................ 7

3 Laws and regulations ..................................................................................................................... 8

3.1 Government information security baseline (BIO) ...................................................................... 8
3.2 General Data Protection Regulation (GDPR) .............................................................................. 8
3.3 Dutch Public Records Act and Decree ...................................................................................... 8
3.4 Telecommunications Act .......................................................................................................... 8
3.5 Copyright Act .......................................................................................................................... 8

4 Roles and responsibilities in relation to processing of personal data .......................................... 9

4.1 Executive Board ....................................................................................................................... 9
4.2 Portfolio holder for Operations and Finances .......................................................................... 9
4.3 Director of Operations and Finances ...................................................................................... 9
4.4 Manager(s) ............................................................................................................................ 9
4.5 Overlap with information security ............................................................................................ 9
4.6 Data Protection Officer .......................................................................................................... 9
4.7 The application owner ............................................................................................................ 10
4.8 Affiliated institutions .............................................................................................................. 10

5 Implementation of privacy policy ................................................................................................ 11

5.1 Division of responsibilities ..................................................................................................... 11
5.2 Awareness raising and training ............................................................................................... 11
5.3 Monitoring and compliance .................................................................................................... 11

6 Lawful and careful processing of personal data .......................................................................... 12

6.1 Basis, purpose limitation and weighing of interests ................................................................ 12
6.2 Reporting and documenting of data processing .................................................................... 12
6.3 The organisation of security ................................................................................................ 12
6.4 Confidentiality ......................................................................................................................... 12
6.5 Storage/destruction periods by type of data .......................................................................... 13
6.6 Special categories of personal data ...................................................................................... 13
6.7 Transfer of personal data to third parties .............................................................................. 13

7 Personal data incidents ............................................................................................................. 15

7.1 Reporting and recording ........................................................................................................ 15
7.2 Handling .................................................................................................................................. 15
7.3 Evaluation ............................................................................................................................. 15
Appendix A Definitions and abbreviations ................................. 16

Appendix B Procedure for compulsory notification of data breaches ...... 17

Introduction ...................................................................................................................................................................................... 17
Area of application: controller and processor .................................................................................................................................. 17
The notification procedure ............................................................................................................................................................... 18
What constitutes a data breach? ..................................................................................................................................................... 19
Analysing a data breach and advising on follow-up ......................................................................................................................... 19
Analysing the data breach ................................................................................................................................................................ 20
Notifying the data subject(s) ............................................................................................................................................................ 21

Appendix C Privacy rules ........................................................................................................................................ 24
1 Privacy rules – Recording of data processing operations ................................................................. 24
2 Privacy rules – Website(s) .............................................................................................................................................................. 25
3 Privacy rules – Operations ............................................................................................................................................................. 25
4 Privacy rules – Camera surveillance ........................................................................................................................................ 26
5 Privacy rules – Confidentiality concerns .............................................................................................................................. 27
NWO privacy statement

NWO respects the privacy of grant applicants, researchers, employees and all other NWO contacts. Information is stored for no longer than necessary, for the purpose for which it was collected, and is not used for purposes incompatible with the initial objective. NWO processes personal data in accordance with the General Data Protection Regulation (GDPR, Dutch acronym AVG).

When processing personal data, NWO adopts the concepts of subsidiarity and proportionality. Regarding subsidiarity, NWO considers whether the purposes for which it processes personal data can also be achieved in another way, using less personal data, or personal data that are less invasive of the privacy of the data subject(s). Processing of personal data must also be proportionate to the intended purpose. NWO collects no more data than it needs for the intended purpose.

Personal data are appropriately protected and treated with the utmost care. NWO pays attention to privacy within all its processes and activities.

This privacy policy explains to employees and data subjects how privacy is organised at NWO.
1 Introduction

Privacy is increasingly under the spotlight. 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 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 NWO operations. Personal data should be stored and processed with the utmost care because its abuse can cause great harm to employees and other data subjects. The NWO Executive Board, as the data controller, is legally responsible for the proper processing of personal data.

With the measures described in this policy document, NWO 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 NWO privacy policy is important for all employees, researchers, grant applicants and all other NWO contacts. 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, including all employees, guests, visitors and external contacts (i.e., hiring of outside staff/outourcing).

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 privacy policy covers the fully or partially automated and/or systematic processing of personal data undertaken under NWO 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.

NWO applies a broad interpretation of the protection of personal data. 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 far as possible. Based on the fundamental right to protection of his or her 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 must be secure.

The privacy policy explains to employees and other data subjects how privacy is organised at NWO. 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 tasks, powers and responsibilities within the organisation;
- Enable the Executive Board to assume responsibility by laying down the principles and organisation of personal data processing within NWO;
- 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 to avoid risks arising from non-compliance with relevant laws and regulations.
2 Policy principles for personal data processing

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 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 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.
- In all recording operations not strictly necessary for an operating process, the data subject will be offered a clear opt-out procedure insofar as this is technically possible.
3 Laws and regulations

NWO is subject to the following laws and regulations in the context of data protection:

3.1 Government information security baseline (BIO)
The basic rules from the National government information security (BIR) Decree drawn up by the Dutch government are used as a guideline for the Information Security Policy. The basic rules from the Government Information Security Baseline (BIO) drawn up by the Dutch government are used as a guideline. NWO has set up a system of measures to guarantee the confidentiality, integrity and availability of data and of information systems. This system is maintained and periodically evaluated as described in the NWO Information Security Policy 2020–2021. This policy guides the implementation of day-to-day activities and the responsible handling of information. The Executive Board (EB) is ultimately responsible for the Information Security Policy. The Chief Information Security Officer (CISO) shapes and supervises the implementation of that policy.

3.2 General Data Protection Regulation (GDPR)
NWO has met its legal requirements (including the lawful and careful processing of personal data and the taking of appropriate technical and organisational measures to combat loss and unlawful processing of data or personal data) by adopting this privacy policy and the Information Security Policy 2020-2021.

3.3 Dutch Public Records Act and Decree
NWO complies with the rules on retention periods as laid down in, for example, the Dutch Public Records Act, and with the Dutch Public Records Decree as regards the handling of information contained in digitised or physical documents, information systems, websites, etc. The legal requirements have been implemented by means of the Public Records Management Regulations and the Selection List of NWO and its predecessor as from 1 April 1950. The Executive Board (EB) is ultimately responsible for the Public Records Management Regulations and the Selection List. Implementation is directed by the Chief Information Officer (CIO) and shaped in practice by the Information Manager.

3.4 Telecommunications Act
The Telecommunications Act covers topics including the rules applying to cookies on websites.

3.5 Copyright Act
The Copyright Act provides *inter alia* that the publication of images, photographs and videos is not permitted if a reasonable interest on the part of the person concerned allows it to be opposed. This is also referred to as portrait rights.
4 Roles and responsibilities in relation to processing of personal data

For a structured and coordinated approach to the processing of personal data, certain roles and responsibilities have been assigned to officials in the existing organisation.

4.1 Executive Board
The Executive Board (EB) is ultimately responsible for the lawful and careful processing of personal data within NWO and lays down the processing policy, measures and procedures by means of this privacy policy. Under the NWO Authorisation Rules 2017, each domain board is responsible by mandate for processing operations within its own domain.

4.2 Portfolio holder for Operations and Finances
The portfolio holder for Operations and Finances is the Executive Board member whose portfolio includes privacy. The portfolio holder has final responsibility for the protection and security of personal data within NWO.

4.3 Director of Operations and Finances
The Director of Operations and Finances is responsible for the implementation of privacy policy within NWO. The director is also responsible for personal data entered from NWO into an application. The director is supported by the privacy team, which consists of the CISO, Data Protection Officer and head of Information and Automation (I&A) in addition to the director.

4.4 Manager(s)
Awareness raising and compliance with the privacy policy are part of overall operations (including within the domains). The duties of all managers are to:

- ensure that their staff are aware of the privacy policy and its aspects that are relevant to them;
- ensure that their staff are sufficiently privacy-aware;
- supervise compliance with the privacy policy by their staff;
- periodically raise the topic of privacy for discussion in work meetings.

4.5 Overlap with information security
The Chief Information Security Officer (CISO) is closely involved in the implementation of the privacy policy. The careful handling of personal data is covered in part by the general rules on information security (NWO Information Security Policy 2020–2021).

4.6 Data Protection Officer
The GDPR requires NWO to appoint an internal “supervisor” for the processing of personal data. This supervisor is called the Data Protection Officer (DPO). The DPO supervises the application of and compliance
with privacy legislation within 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 is responsible for providing 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 on JOOST.

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 duties of the DPO are to:
- ensure, together with the CISO, that data processing records are maintained;
- be responsible for awareness raising and training;
- act as a resource person with regard to privacy;
- coordinate with the Director of Operations and Finances and the CISO on privacy matters;
- participate in the Privacy Team and Data Breach Team;
- be involved in the handling of data breaches and other incidents;
- draft an annual privacy report including recommendations;
- review the privacy policy frequently to reflect new developments.

4.7 The application owner
The application owner is responsible for ensuring that the application and associated ICT facilities effectively support the operating process for which the application owner is responsible. The application owner is also responsible for compliance with the privacy policy. This means that the application owner ensures that the application meets the requirements and wishes of users and complies with laws and regulations, both now and in the future.

4.8 Affiliated institutions
Institutions affiliated to NWO are responsible for compliance with privacy legislation. It is up to the affiliated institution to achieve compliance. NWO will stress the importance of compliance and request details of how it has been achieved.

Affiliated institutions can contact the NWO DPO and CISO for advice.
5 Implementation of privacy policy

The Executive Board is responsible for processing operations involving personal data for which it determines the purpose and means of processing. The Executive Board is considered as the “controller” within the meaning of the GDPR. However, the actual processing of personal data is carried out in various places within NWO.

Governance, the effective, efficient and responsible management of an organisation, includes in particular the relationship with the organisation’s main stakeholders, such as employees and society. Good governance ensures that all stakeholders know their rights and obligations and act accordingly.

5.1 Division of responsibilities
The Executive Board holds final responsibility for all data processing by NWO. Line responsibility lies with the domains and services, with each employee having their own responsibility according to their role.

See Section 4, Roles and responsibilities in relation to the processing of personal data.

Privacy is a line responsibility. This means that managers bear primary responsibility for the careful processing of personal data within their team. This includes the choice of measures and their implementation and enforcement. Line responsibility also encompasses the task of communicating the policy on the processing of personal data to all relevant parties, as far as is reasonable. Privacy is everyone’s responsibility. Employees and third parties are expected to behave with integrity and to handle personal data with care.

5.2 Awareness raising and training
Policies and measures are not sufficient to rule out all risks associated with the processing of personal data. Employee awareness of privacy (and security) must be honed constantly to increase knowledge of risks and encourage good behaviour. Good practices can be shared with others in the organisation, for example via the NWO Academy.

Regular awareness campaigns are held for employees and third parties as part of the implementation of the privacy policy.

Raising employee awareness of security and privacy is the responsibility of managers, supported by the DPO and CISO.

5.3 Monitoring and compliance
The DPO oversees compliance with privacy legislation and the privacy policy, including the allocation of responsibilities, awareness raising and staff training.

In addition, compliance audits carried out by the internal audit department allow NWO to check the effectiveness of the policy and the measures taken.

The processing of personal data is an ongoing process. Technological and organisational developments both inside and outside NWO require us to check regularly that our privacy policy is still sufficiently on track.
6 Lawful and careful processing of personal data

6.1 Basis, purpose limitation and weighing of interests
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 legitimate interest, the explicit consent of the data subject is required.

NWO 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 or new systems purchased, privacy is taken into account from the outset by conducting a Privacy Impact Assessment (PIA).
In its implementation, NWO applies the principles of Privacy by Design and Privacy by Default.

6.2 Reporting and documenting of data processing
Any fully or partially automated processing of personal data should be reported to the NWO DPO and/or CISO. The DPO assesses whether the data recording is lawful and, together with the CISO, ensures that it is properly documented.

6.3 The organisation of security
NWO 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. This is done via the classification of an application.

6.4 Confidentiality
NWO 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.

6.5 Storage/destruction periods by type of data

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 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.

6.6 Special categories of personal data

Processing of special categories of personal data is prohibited unless there is a legal basis, explicit consent from the data subject, or 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, trade union membership and criminal convictions or offences.

6.7 Transfer of personal data to third parties

6.7.1 Outsourcing of processing to a processor

If NWO has personal data processed by a processor, the processing is governed by a written agreement between NWO, the controller and the processor. A standard format is available from the Legal Affairs department.

6.7.2 Transfer of personal data within the European Union

NWO provides personal data to third parties only if the transfer has a statutory basis (Art. 6 GDPR) and the third party also has a statutory basis for receiving the data.

Special categories of personal data are not provided to third parties without the explicit consent of the data subject.

6.7.3 Transfer of personal data outside the European Union

NWO 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 uses the list of countries with regard to which the European Commission has adopted an adequacy decision. This includes the EU/US Privacy Shield Program.

NWO 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.

6.7.4 Third parties to which NWO transfers personal data

In light of the statutory duties assigned to NWO, NWO provides data to Dutch universities provided they use these data (exclusively) for analysis purposes. NWO also provides data to external research agencies to enable them to evaluate NWO activities, thus continuously improving the performance of its statutory duties. NWO also provides data to ZonMw, to the extent necessary for the joint performance of statutory duties. NWO can also exchange data with third parties in connection with its role in monitoring scientific integrity (Scientific Integrity Desk).

13
Where NWO provides personal data to a third party, it always concludes an agreement specifying that data may not be used for purposes other than those for which they were provided by NWO. In this agreement, NWO also states that data must be deleted as soon as they are no longer needed.
7 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 an incident 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.

7.1 Reporting and recording

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

7.2 Handling

The purpose of incident handling is to resolve the problem, limit the damage and comply with legislation. NWO has a separate team for data breaches (consisting of the DPO, CISO and I&A staff) that assesses whether an incident constitutes 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 domain or department in consultation with NOW’s central communication department (V&C). The person reporting the incident is informed about its handling.

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

7.3 Evaluation

It is important to learn from incidents. Recording and periodically reporting on incidents are 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.
**Appendix A Definitions and abbreviations**

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data subject</td>
<td>An individual and natural person who is the subject of personal data.</td>
</tr>
<tr>
<td>Data breach</td>
<td>Personal data falling into the hands of third parties who do not (or should not) have access to it.</td>
</tr>
<tr>
<td>DPA</td>
<td>Dutch Data Protection Authority <em>(Autoriteit Persoonsgegevens)</em>.</td>
</tr>
<tr>
<td>DPO</td>
<td>Data Protection Officer</td>
</tr>
<tr>
<td>Opt-in</td>
<td>In an opt-in system, a data subject has given explicit and demonstrable consent to receive email from a particular mailing list.</td>
</tr>
<tr>
<td>Opt-out</td>
<td>In an opt-out system, data subjects are automatically placed on a mailing list (e.g. of a newsletter) and have the option to unsubscribe.</td>
</tr>
<tr>
<td>PIA</td>
<td>Privacy Impact Assessment.</td>
</tr>
<tr>
<td>Privacy by Default</td>
<td>Where users are offered a choice of options, the default setting gives the best privacy guarantees.</td>
</tr>
<tr>
<td>Privacy by Design</td>
<td>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.</td>
</tr>
<tr>
<td>Privacy Impact Assessment</td>
<td>A tool that helps to identify privacy risks and provides the necessary support to reduce these risks to an acceptable level.</td>
</tr>
<tr>
<td>Controller</td>
<td>A natural or legal person or any other person or body which, either alone or with others, determines the purpose and means of the processing of personal data. At NWO, the Executive Board is the controller.</td>
</tr>
<tr>
<td>Processor</td>
<td>A person or body which processes personal data on behalf of the controller, without being under the controller’s direct authority.</td>
</tr>
<tr>
<td>Processing</td>
<td>Any operation or set of operations relating to personal data, where personal data includes the collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data.</td>
</tr>
</tbody>
</table>
Appendix B Procedure for compulsory notification of data breaches

Introduction
The compulsory notification of data breaches came into effect on 1 January 2016. At the time, this requirement was a new element of the Dutch Personal Data Protection Act (PDPA, Dutch acronym Wbp). Compulsory notification of data breaches means that organisations must notify the Dutch Data Protection Authority immediately in the event of a serious data breach during which personal information has been leaked or lost.

As from 25 May 2018, the new General Data Protection Regulation (GDPR, Dutch acronym AVG) is in effect. This Regulation prescribes that non-serious data breaches must also be notified to the Dutch Data Protection Authority, unless it can be reasonably assumed that the data breach (breach of privacy) is unlikely to result in a risk to the data subject (Art. 33 GDPR).

The PDPA/GDPR defines a data breach as a “breach of security”. Examples of a possible data breach include a stolen laptop, a hacker attack, a malware infection or a disaster (e.g. fire) in a data centre. However, these examples only fall under the definition of data breach if personal data are lost or unlawfully processed. To assess this, a number of steps need to be taken. These steps are described in this procedure. The purpose of this document is to identify the parties involved and describe their roles at the different stages of this procedure.

Area of application: controller and processor
NWO is an organisation that processes personal data to which the GDPR applies. This means that compulsory notification of data breaches also applies to NWO as the data controller. In addition, NWO works with processors for the processing of personal data. In principle, processors also include IT service providers which process personal data. In these cases too, the controller (NWO) must ensure that the processor provides sufficient guarantees regarding compliance with the requirement to notify data breaches. To this end, a processor’s agreement must be drawn up containing written arrangements between the controller and the processor.

NWO is obliged to guarantee the compulsory notification requirements in current and future contracts with processors/suppliers of NWO. The arrangements with processors should focus on how an identified data breach via the processor is reported in the standard notification process as described in this document. In addition, the arrangements with processors should state that any costs incurred due to the processor’s negligence in complying with the requirement to notify data breaches can be recovered from the processor. This was achieved in January 2018 by means of the standard processor’s agreements (available from Legal Affairs).
The notification procedure

The procedure for notifying a data breach to the Dutch Data Protection Authority and the data subject(s) is outlined below. This procedure comprises a number of steps that are also described in the guidelines of the Dutch Data Protection Authority:

Detecting a data breach:
- determining whether a data breach has actually occurred, analysis and advice on follow-up;
- notification to the Dutch Data Protection Authority;
- notification to data subject(s).

This appendix briefly describes each step, the action to be taken and the parties responsible for carrying it out. At the start of the process, when a data breach is detected, employees, processors/suppliers and application owners have a responsibility to report signs of a data breach as quickly as possible.

On initial detection of a data breach, it is reported to a central reporting point as quickly as possible. This point is the meldpunt-datalek@nwo.nl, through which the data breach team can be reached. Speed is important because the three working days within which data breaches must be notified, start from the time the data breach is detected. As a basic principle, therefore, the relevance of the reports received under compulsory notification is analysed by the data team, not by the domain or department within which the data breach occurred.

In the event of a large-scale security incident, a crisis organisation is set up in order to take appropriate action and resolve the incident quickly.

The basic principle is that reports are made via meldpunt-datalek@nwo.nl. This ensures that reports reach the data breach team as quickly as possible. However, some reports may also be received via the Service Desk. Examples of direct reports to the data breach team include (a) signs of abuse or possible abuse of confidential information, and (b) theft of data carriers (e.g. telephones, laptops, tablets, but also paper files, etc.). Reports from external parties will usually come in via the service desk. The service desk will forward all reports to meldpunt-datalek@nwo.nl.

The data breach team is responsible for recording incoming reports, analysing the detected breach and advising on its assessment. The data breach team examines whether the report is such that it must be notified to the Dutch Data Protection Authority and the data subject(s). When a report is received, the data breach team also informs the Director of Operations and Finances. The Data Protection Officer or, in the latter’s absence, the CISO, makes the notification to the DPA unless it can be reasonably assumed that the data breach (breach of privacy) is unlikely to result in a risk to the data subject. The Director of Operations and Finances is informed subsequently. The data subject(s) is/are informed by one of the directors after receiving relevant information from the data breach team.
What constitutes a data breach?

A data breach involves “access to or destruction, alteration or release of personal data within an organisation without it being the organisation’s intention. A data breach therefore includes not only the release (leaking) of data, but also the unlawful processing of data”. NWO must also take account of how systems are set up and data are used in ISAAC, SharePoint, SURFdrive, etc.

A data breach involves a breach in the security of personal data. This is the case where personal data:

• are exposed to a risk of loss or unlawful processing; and
• it cannot reasonably be ruled out that personal data have indeed been lost or unlawfully processed.

Sometimes an immediate assessment can be made as to whether a loss or unlawful processing has occurred. In this case, the data breach team will quickly reach a verdict. The data breach team can also call on other relevant expertise where necessary, such as IT and the DPO. In certain complex cases, external expertise may also be required. Examples are cases where systems have been infected with malware. Specialist knowledge may be required to assess this. The data breach team will assess the need for additional or external expertise, and which type of expertise, on a case-by-case basis. This assessment will involve the Director of Operations and Finances.

Analysing a data breach and advising on follow-up

If a data breach that has to be notified to the Dutch Data Protection Authority has been established, it must then be assessed whether the breach is of such a nature or severity that it must also be notified to the data subject(s). At this stage, the data breach team takes the lead. The data breach team analyses the breach and makes the notification to the Dutch Data Protection Authority.
Analysing the data breach

Does the data breach involve serious adverse consequences for the protection of personal data? The data breach team will make a well-founded judgment on this. The Dutch Data Protection Authority suggests two considerations in this respect:

- Have personal data of a sensitive nature been leaked?
- Do the nature and scope of the breach lead to (a significant risk of) serious adverse consequences?

Certain categories of personal data are considered as sensitive data, including BSN numbers. The DPA guidelines discuss this in detail, and it should be taken into consideration in determining the nature and scope of the breach.

The data breach team records certain information concerning the data breach for reporting purposes. The Dutch Data Protection Authority stipulates a retention period of at least one year for these records.

How and when should a data breach be notified to the Dutch Data Protection Authority?

The Dutch Data Protection Authority has a web form that can be used to notify data breaches. The form contains questions that make it clear which information is required for a notification.

A data breach should be reported without undue delay. This means that some time may be taken for investigations after a breach has been discovered. The notification must be made to the Dutch Data Protection Authority within 72 hours after discovery of the incident. This period starts from the time when the controller or processor becomes aware of the incident in question. At the end of this period, there may not yet be a full understanding of what happened. In this case, the notification must be made on the basis of the information available at the time. The notification can later be supplemented or withdrawn.

Besides a notification to the Dutch Data Protection Authority, the data breach may also be such that the data subject(s) must be notified. This requires a number of additional considerations, which are set out in more detail below.
Notifying the data subject(s)

At this stage, it has already been established that the data breach must be notified to the Dutch Data Protection Authority. The following considerations apply in determining whether to notify the data subject(s):

- Do the technical protection measures taken offer sufficient protection that it is not necessary to notify the data subject? (if the answer is yes, the notification may be omitted).
- Is the data breach likely to adversely affect the privacy of the data subject? (if the answer is no, the notification may be omitted).
- Are there compelling reasons not to notify the data subject? (if the answer is yes, the notification may be omitted)
- The first-mentioned consideration, concerning suitable technical protection measures, requires specialist expertise. The Dutch Data Protection Authority cites a number of aspects to be considered:
  - Exposure to destruction or compromise: if personal data are destroyed or compromised (measures such as encryption do not protect against this), the data subject must be informed.
  - Unlawful processing also falls under this category and is also a reason to inform the data subject if there are adverse effects on the latter’s privacy.
  - Encrypted at the time of the breach: if this is not the case, the data subject should be informed.
  - Is the encryption adequate: this is a strict standard that must take account of the technological state-of-the-art.
  - Is the residual risk acceptable? If the answer is yes, the notification may be omitted. NWO should form its own opinion on this, based on the previous points for attention. It should take into account the consequences for the data subject’s privacy if a malicious party were to gain knowledge of the personal data concerned, either now or in the future.

When assessing whether the data breach may have adverse consequences for personal privacy, the nature of the personal data concerned must be taken into consideration. If the data are of a sensitive nature, it can be assumed that the data subjects must be informed.

If data subjects have to be informed, the Director of Operations and Finances notifies the domains/departments concerned. The personal data breach will be notified to the data subject(s) by the domain/department which is the application owner or in which the data breach was identified. Other expertise (Communications) can be called upon if necessary.

How and when should a data breach be notified to the data subject(s)?

The notification to the data subject must include the following:

- the nature of the breach;
- the body or bodies from which the data subject may obtain further information on the breach;
- measures recommended to the data subject to limit the adverse consequences of the breach.

These include the recommendation to change the data subject’s usernames and passwords (including those for accounts outside the affected system if the data subject uses the same passwords and usernames for different services). In the vast majority of cases, the controller (NWO) will have the necessary contact details for data subjects and can contact them individually to inform them.

In the case of large-scale incidents, a combination of general information and individual notification of data subjects may be used (e.g. general information on the website combined with an email to all affected data subjects, or possibly through other channels). A report in the media is often not sufficient; data subjects must be made aware of measures and information that can help to limit the consequences of the breach.

The data breach should be notified to the data subject(s) without undue delay. This means that some time may be taken for further investigations after the data breach has been discovered, to ensure that data subjects can be properly and carefully notified. However, because the data subject must be sent recommendations on how to limit the breach, the notification should be made as soon as possible. As in the
case of notification to the Dutch Data Protection Authority, the data subject may initially be informed on the basis of the information available at the time, and then more detail provided at a later stage. This decision is made by the Director of Operations and Finances, who oversees this part of the procedure. As mentioned above, the notification itself comes from the area/department concerned.

What if the data subject directly reported the breach to the data breach team?

Certain incidents are reported to the data breach team (see previous description). If an employee has directly reported abuse of confidential information to the data breach team, the team will inform the data subject whether the report is considered worthy of investigation. If this is the case, the data breach team will keep the data subject informed of the handling of the investigation and the outcome.

Examples of data breaches are:

- a lost, unencrypted USB flash drive containing personal data;
- a lost or stolen unencrypted phone/laptop/tablet (private or business) containing personal data or access to an NWO account containing personal data;
- printed-out documents containing personal data left unattended beside a photocopier;
- anonymous survey results that nevertheless prove traceable to respondents;
- unauthorised access to personal data that are traceable to natural persons;
- hacker intrusion into a computer containing personal data or access to an NWO account containing personal data;
- circulation of a list of employees’ names, telephone numbers and home addresses;
- unauthorised persons accessing camera images.

Examples of other privacy incidents include:

- data collection that has not been reported to the DPO;
- unsafe working practices that could easily lead to data breaches;
- data collection on the basis of the data subject’s consent without such consent being actually requested or recorded.
Appendix C Privacy rules

Specific privacy rules are necessary in some areas. Employees can restrict themselves to the privacy rules relevant to them. Formally defining these privacy rules makes it possible to assess their implementation. Specific privacy rules have been defined for the following areas:

1. Recording of data processing operations
2. Website(s)
3. Operations
4. Camera surveillance
5. Confidentiality concerns

1 Privacy rules – Recording of data processing operations

Introduction

The privacy policy states that specific privacy rules are necessary in some areas. One of these areas concerns the recording of data processing operations (Art. 30 GDPR).

Responsibility

1. Data processing operations within NWO (domains and operations) are reported to the DPO and/or CISO.
2. The DPO/CISO are responsible for entering these reports in a processing register.
3. The DPO/CISO are responsible for keeping an inventory of reports of data processing operations.

Reports

4. Every report of a data processing operation must contain at least the following information:
   - Functional name of the system;
   - 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 data;
   - Description of the security measures taken;
   - List of 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.
2 Privacy rules – Website(s)

Introduction
The privacy policy states that specific privacy rules are necessary in some areas. One of these areas concerns the NWO websites.

Responsibility
1. The Communications department is responsible for implementing the privacy policy on the websites.
2. Websites on subdomains are the responsibility of the relevant domain and the Communications department advises them proactively.
3. The Communications department informs website operators of the relevant privacy rules where operators use forms to collect personal information.

Tracking of visitors
4. Visitors are tracked only if there is a good reason to do so; the proportionality principle is applied.
5. The websites clearly state how and for which purpose visitors are tracked.
6. The websites clearly state which data are collected.
7. The websites clearly state how visitors can visit the website without being tracked.

Forms
8. Forms on the websites request no more personal information than is necessary for the purpose for which it is being collected.
9. Each form states the purpose or purposes for which the requested information will be used.
10. Each form is part of an information system which is subject to the Privacy rules – Recording of data processing.

IP addresses
11. IP addresses are not used to track visitors.
12. IP addresses are logged and can be used to resolve security incidents and/or technical failures.
13. IP blocks can be used for statistical analysis.

Hosting
14. The above rules apply to both hosting on our own infrastructure and hosting with a supplier.
15. If hosting with a supplier is used, the supplier should meet the conditions set by NWO for SaaS services and a processor’s agreement should be completed and signed.

3 Privacy rules – Operations

Introduction
The privacy policy states that specific privacy rules are necessary in some areas. One of these areas concerns operations. The Security Rules: Information Systems included in the Information Security Policy 2020-2021 are applicable.

Responsibility
1. The holder of an information system is responsible for compliance with the privacy rules.
Acquisition
2. At or before the start of the project, a classification is carried out in accordance with the Classification Guideline for Information and Information Systems, as described in the Information Security Policy. The results can help to determine the requirements for the information system.
3. If sensitive personal data (e.g. BSN numbers) are processed, a Privacy Impact Assessment (PIA) is carried out. The results are incorporated into the business case for the project. The extent to which the processing of personal data is necessary is assessed. This includes a weighing up of the various interests.
4. The CISO is present or involved in the implementation of the PIA. The results of the PIA are sent to the DPO for an opinion.
5. If an external processor is brought in, a processor’s agreement will be concluded first (in consultation with the Legal Affairs department).

Implementation
6. The principles of Privacy by Design and Privacy by Default are applied. This means that privacy is taken into account from the start of the design process and that data minimisation is applied.
7. The holder reports the data processing to the DPO before the system is put into operation.
8. Data storage periods are specified to ensure that personal data are not kept for longer than necessary.
9. The holder notifies data subjects of the data processing.
10. The holder sets up a process to ensure that the right of access and the right to amend, add to, delete or restrict data can be exercised in good time, i.e. within four weeks.
11. As a rule, no production data are used for testing purposes, except to reproduce observed problems. Where production data are used for an acceptance test, the authorisation matrix must be the same as that of the production environment.

4 Privacy rules – Camera surveillance

Introduction
The privacy policy states that specific privacy rules are necessary in some areas. Camera surveillance at NWO is governed by the following rules in addition to the Privacy rules – Operations.

Responsibility
1. As the holder of camera surveillance, the Director of Operations and Finances is responsible for compliance with the privacy rules concerning camera surveillance at NWO.

Purpose and Transparency
2. The data are used exclusively for the following purposes:
   a. Protecting the health and safety of natural persons;
   b. Monitoring entrances to buildings and sites;
   c. Surveillance of items located in buildings or on land;
   d. Recording of incidents.
3. Cameras are clearly visible, or it is indicated on the spot, for example by stickers, that camera surveillance is being used.

Access
4. Live images are only accessible to employees responsible for security and surveillance at NWO.
5. Access to recorded images is possible only in a specially equipped room.
6. Only the head of the responsible department and his or her deputy have access to recorded images.
7. The employees concerned have a duty of confidentiality with regard to data that are traceable to individuals.

Storage
8. Recorded camera images are stored in such a way that they are not accessible to others.
9. Recorded camera images are kept for no longer than two weeks. Camera images recorded on behalf of the NWO facilities department are kept for a maximum of four days.

Incidents
10. If relevant visual material is available following an incident, the footage may be secured and kept for as long as is necessary for the resulting investigation.
11. In the event of a reasonable suspicion of an unlawful act, a written order of the Executive Board may permit the use of hidden cameras without informing those involved.
12. Images are provided to third parties only if NWO interests require this and after a decision to that effect by the Executive Board. The police may obtain images only when in possession of a warrant, or with the permission of the public prosecutor or acting public prosecutor.

5 Privacy rules – Confidentiality concerns
1. **Authorisation.** It is important to ensure that only those persons who need confidential information have access to it. This can be done by introducing an authorisation policy. Be aware of any use of another person’s account, including in cases of temporary replacement such as maternity leave.
2. **Authentication.** Preventing someone from impersonating another person and accessing confidential information. Prevent employees from sharing or writing down passwords. Consider two-factor authentication.
3. **Access from outside the permanent workplace.** Working from home or from a different location can lead to additional risks. This can be prevented by filtering by IP address.
4. **Data entry.** Remember that notes and temporary documents may also contain confidential information. Ensure controlled disposal or destruction of such papers and files.
5. **Processing and consulting of data.** When an employee requests or adds information, confidential information not necessary for the action in question can be hidden or placed behind an additional button.
6. **Work interruptions.** Remember to use screensavers and avoid leaving confidential papers lying around in plain sight.
7. **Exchanging data with other systems.** Do not exchange any more data than necessary. If confidential information is provided, be sure that it remains confidential. Make clear agreements in advance.
8. **Producing reports.** The degree of confidentiality will have to be determined for each report. If a report is known to be confidential, this can be stated on it as standard.
9. **Storage of data.** Critical confidential information should be stored in encrypted form. In the case of centralised storage, this is important to prevent hackers or administrators from gaining access. In the case of decentralised storage, the more likely risk is that of viruses and theft. Paper bearing critical confidential information, such as a file, should be stored in a locked cabinet.
10. **Keeping emails.** Keeping confidential information in the email system means that the information remains accessible for a long time via any device, including phones and tablets. Examples are sick leave notifications, job applications and performance interviews. Delete emails containing confidential information as soon as possible.
11. **Archiving information.** Specify the retention period and the rules on access and destruction.
12. **Printing of data.** Paper bearing critical confidential information may be printed only if the employee is present; it must not be left lying around, or taken out of the office, and it must be disposed of or destroyed after use.
13. **Carrying digital data.** Information can be carried on USB flash drives, hard disks, laptops, etc. Consider first whether all of the information is necessary; can the confidential information be left out? Critical confidential information should be stored in encrypted form.
14. **Working in public spaces.** Unauthorised persons can read information on your screen or piece of paper without your knowledge.

15. **Avoid this when consulting confidential information.** Think about corridors, canteens, restaurants, waiting rooms, trains, airplanes, etc.

16. **Discussing information.** When discussing information, including by telephone, remember that other people may be listening in.

17. **Sending information.** Check that the person concerned does in fact need this information; try to minimise the information provided. Check that NWO is permitted to provide this information to the person concerned. Where confidential information is sent by email or other digital means, it must be encrypted.

18. **Audit trail.** A log file must be used to show who has had access to which confidential information.

19. **Theft of information.** If paper bearing confidential information or an information carrier (USB flash drive, tablet, etc.) is lost, which procedures apply? On the one hand, minimise further damage by changing passwords, etc. Further steps are detailed in the procedure for compulsory notification of data breaches.

20. **Writing procedures.** Include employee roles in procedures, rather than the names of individuals.

21. **Extending or redesigning/reequiring applications.** Consider in advance which security aspects play a role. The Classification Guideline and a PIA can help with this. Adding extra requirements halfway through a project increases costs.

22. **Testing applications.** Live data are often used to test an application, as this makes it more realistic. But for most tests, critical confidential information can easily be left out. This can be done by scrambling certain fields in a database, or overwriting them with other information, and by not using original confidential documents.

23. **Outsourcing work or using cloud services.** Make clear agreements and, if personal data are exchanged, conclude a processor’s agreement.
Dutch Research Council (NWO)

NWO The Hague
Laan van Nieuw Oost-Indië 300
2593 CE The Hague
PO Box 93138
2509 AC The Hague

+31 70 344 4471
www.nwo.nl

NWO Utrecht
Winthontaal 2
3526 KV Utrecht

www.nwo-i.nl

Email NWO privacy team:
privacyteam@nwo.nl