Policy document on the processing of Personal data at Wageningen University & Research

WAGENINGEN
UNIVERSITY & RESEARCH

Policy document on the processing of Personal data at Wageningen University & Research

Content

1 Introduction

Storage and Processing of Personal data is necessary for the business processes of education and research institutions. This should be done with the utmost care because abuse of Personal data can do a great deal of damage to students, staff members and others involved at Wageningen University & Research[1]. Wageningen University & Research as an organisation can also be charged with hefty fines when the responsibility for this is not carried out correctly. As a research institute, Wageningen University & Research attaches great value to protecting the Personal data which it is provided with as well as the way these Personal data are processed. The correct Processing of Personal data is the responsibility of the Executive Board[2] of Wageningen University & Research. In describing the measures in this Policy document, Wageningen University & Research takes responsibility for optimising the quality of the processing and the security of Personal data, thus adhering to the relevant privacy laws and regulations.

On 25 May 2016, the General Data Protection Regulation (GDPR) [3] entered into force. The GDPR has direct effect and therefore does not need to be incorporated into national legislation first. The overall applicability of the regulation is set for 25 May 2018. In this way, during a transitional period of 2 years, organisations that work with Personal data are given the opportunity to prepare themselves for the new regulation. However, measures that can be introduced earlier to ensure compliance with the GDPR must be introduced within the transitional period.

The GDPR stipulates the rules on the protection of natural persons in the field of Personal data and the free movement of Personal data. The regulation applies to the automatic or non-automatic Processing of Personal data, whether fully or partially, if these Personal data form part of a file or are intended for this.

On the basis of the GDPR (article 24), Wageningen University & Research must have a data protection Policy in place as is recorded in this Policy document.

1.1 Definitions

In the GDPR (article 4), definitions of commonly used terms are provided. For a complete overview and a more detailed definition, please refer to the regulation. For readability purposes, only a brief explanation of the most common concepts has been included in this Policy.

"Policy": the present Policy with regard to the Processing of Personal data at Wageningen University & Research.

"Data subject": an individual and natural person to whom the Personal data refers.

"Controller": the Executive Board of Wageningen University & Research, which establishes the purpose and tools for the Processing of Personal data.

"Processor": a (third) party, commissioned by Wageningen University & Research, which processes Personal data on behalf of Wageningen University & Research.

[1] Wageningen University & Research is a framework of cooperation between the public legal entity Wageningen University and the private Wageningen Research Foundation.

[2] With the Executive Board of Wageningen University & Research is meant: the Executive Board of Wageningen University and/or the Executive Board of Wageningen Research Foundation.

[3] http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN

"Personal data": any and all information regarding an identified or identifiable natural person.

"Processing of Personal data": any (automated) act or set of acts with respect to Personal data, including at least the collection, recording, organisation, storage, updating, modification, requesting, consultation, use, making available by forwarding, dissemination, or any other form of disclosing, bringing together, associating, as well as the blocking, erasure, or destruction of data.

"Third party": any party other than the Data subject, the Controller, and the Processor, or any person who falls under the direct supervision of the Controller or the Processor and who is authorised to process Personal data.

"Data leak/breach": a breach in security resulting in the destruction, loss, modification, unauthorised sharing of, or unauthorised access to data that have been sent, stored, or processed in any other way.

"Privacy by design": the management of the entire life cycle of Personal data, from collecting to the processing and removal, during which systematic attention is given to comprehensive safeguarding with regard to accuracy, confidentiality, integrity, physical safety, and disposal of Personal data.

"Privacy by default": in addition to Privacy by design, all business processes will be designed in such a way that risks of invasion of privacy are minimised as much as possible. When describing the purposes and the design of the business processes, data minimisation is the starting point for the organisation. Personal data are not communicated more widely than is strictly necessary.

"Privacy Impact Assessment (PIA)": a tool that helps in identifying privacy risks and provides guidelines to reduce these risks to an acceptable level.

1.2 Scope and objective of the Policy

The Policy covers the Processing of Personal data of all Data subjects within Wageningen University & Research, including at least all staff members, students, guests, visitors, and external relations (hiring/outsourcing), as well as other Data subjects of whom Wageningen University & Research processes Personal data.

In the Policy, the emphasis is on the fully or partially automated/systematic Processing of Personal data that takes place under the responsibility of the Executive Board as well as on the documents underlying this processing, which have been included in a file. Similarly, the Policy is applicable to the non-automatic Processing of Personal data which already have been or are intended to be included in a file.
At Wageningen University & Research, the protection of Personal data is broadly interpreted. There is an important relationship and partial overlap with the adjoining Policy area of information security[4], which focuses on the availability, integrity, and confidentiality of data, including Personal data. At the strategic level, attention is paid to these interfaces and alignment in both planning and content is sought after.
The Policy at Wageningen University & Research aims to improve the quality of the processing and optimise the security of Personal data, during which the right balance must be struck between privacy, functionality, and security.

The objective is to respect the personal life of the Data subject as much as possible. On the basis of the fundamental right to protection of the Personal data of a Data subject, the data relating to him/her must be protected against illegal and unauthorised use or abuse. This means that the Processing of Personal data must comply with relevant laws and regulations and that Personal data must be safe at Wageningen University & Research.

In concrete terms, the objective of the Policy for Wageningen University & Research is the following:

[4] https://www.wur.nl/en/Expertise-Services/Facilities/Information-security.htm

- Providing a framework: the Policy provides a framework to assess (future) Processing of Personal data in relation to an established "best practice" or standard; and to implement the tasks, competencies, and responsibilities in the organisation.
- Setting standards: the basis for the security of Personal data is ISO 27001.[5] Measures are based on "best practices" in higher education and are adopted on the basis of ISO 27002.[6]
- The Framework of Legal Standards Framework for (Cloud) Services in Higher Education[7] is used as a "best practice" for cloud services and other outsource contracts.
- Having the Executive Board take responsibility by recording the principles and the organisation of the Processing of Personal data for the entire organisation. Effective implementation of the Policy by making clear choices with regard to measures and applying active monitoring to the implementation of the Policy measures.
- Complying with the Dutch and European legislation.

In addition to the concrete objectives above, a more general aim is to create awareness of the importance and the need of protecting Personal data, partly in order to avoid risks resulting from not yet being fully compliant with the relevant laws and regulations.

[5] In full: NEN-ISO/IEC 27001: Information security requirements for management systems
[6] In full: NEN-ISO/IEC 27002: Code for information security
[7] SURF task force Cloud, established by the Executive Committee of the ICT & Operational Management Platform of 3 April 2014, and can be found via: https://www.surf.nl/kennisbank/2013/surf-juridisch-normenkader-cloudservices.html

2 Policy Principles on the Processing of Personal data

2.1 Starting point for Policy and Policy principles

The general starting point for the Policy is that Personal data are properly and meticulously processed in accordance with the relevant laws and regulations. In doing so, a good balance must be struck between the interest of Wageningen University & Research to process Personal data and the importance of the Data subject to, in a free environment, make own choices with respect to Personal data.

In order to comply with the abovementioned starting point for Policy, the following principles apply:

- Processing Personal data is permitted if at least one of the conditions mentioned in article 6, clause 1 of the GDPR are met.
- Personal data are only processed for explicitly described and justified purposes. These purposes are concrete and are formulated prior to processing.
- When processing Personal data, the amount and type of data is limited to the Personal data necessary for the specific objective. For the purpose of that objective, the data must be adequate, relevant, and not excessive.
- Processing of Personal data is done in the least intrusive manner and shall be in reasonable proportion to the intended purpose.
- There are measures in place to ensure as much as possible that the Personal data is correct and up to date.
- Personal data are adequately protected in accordance with the applicable security standards.
- Personal data are not further processed in a way that is incompatible with the purposes for which they were obtained.
- Personal data are not processed for a longer time than is necessary for the purposes of the processing, taking into account the applicable retention and destruction terms.
- Any Data subject has the right to review or improve, supplement, remove, or block their Personal data in the separate processing operations, and has the right to object, as stipulated in section 8 of this Policy.
- For all voluntary registrations, the Data subject must be offered an unambiguous opt-out procedure.

3 Legislation and Regulations

At Wageningen University & Research, relevant legislation and regulations are dealt with in the following way:

3.1 The Higher Education and Research Act

Wageningen University & Research has a quality assurance system, which (among others) ensure the careful handling of data in the Student Administration system and guarantees the study results. In addition, the behavioural and integrity codes for academic and non-academic staff are complied with and applied[8] and Personal data in research data are secured.

3.2 General Data Protection Regulation (GDPR)

By means of the Policy, Wageningen University & Research has implemented the legal requirements (including the lawful and meticulous Processing of Personal data and taking appropriate technical and organisational measures against loss and unlawful processing of data or Personal data).

3.3 Public Records Act

Wageningen University & Research adheres to the requirements of the Public Records Act (*Archiefwet*) and the Public Records Decision (*Archiefbesluit*) with regard to information recorded in (digitised) documents, information systems, websites, etc. This is part of the annual external auditor's reports.

[8] http://www.wageningenur.nl/nl/Over-Wageningen-UR/Corporate-Governance.htm

4 Roles and responsibilities regarding the Processing of Personal data

To handle the Processing of Personal data in a structured and coordinated way, Wageningen University acknowledges a number of roles that have been assigned to officers in the existing organisation.

4.1 Executive Board

The Executive Board is responsible for the lawful and meticulous Processing of Personal data within Wageningen University & Research and determines the policies, measures, and procedures in the field of processing.

4.2 Personal data security portfolio holder

Personal data security portfolio holder is the board member whose portfolio includes the Processing of Personal data.

4.3 Data Protection Officer

Wageningen University & Research is required to appoint an internal supervisor for the Processing of Personal data. This supervisor is referred to as the Data Protection Officer (DPO). Within Wageningen University & Research, the DPO supervises the application of and compliance with the GDPR. The legal tasks and competencies of the DPO give this officer an independent position at Wageningen University & Research.

4.4 System owner

The system owner is responsible for ensuring that the application and related ICT facilities offer good support to the process which the application is responsible for and that it is in line with the Policy. This means that the system owner will, both now and in the future, ensure that the application continues to meet the requirements and wishes of the users and the laws and regulations.

4.5 Supervisor

Creating awareness and compliance with the Policy on the Processing of Personal data is part of the integral operational management. Each supervisor has the task of:

- Ensuring that its employees are aware of the Policy;
- Ensuring compliance with the Policy by its employees;
- Periodically promoting the topic of the protection of Personal data in work meetings.

5 Implementation Policy

The Executive Board of Wageningen University & Research is responsible for the Processing of Personal data, for which it establishes the purpose and tools for processing. Within the context of the GDPR, the Executive Board is considered the Controller. However, the actual Processing of Personal data will be carried out at many different layers of Wageningen University & Research. The good, efficient, and responsible management of an organisation is often referred to with the term governance. It includes, among other things, the relationship with the most important stakeholders of Wageningen University & Research: staff members, students, third parties, and society as a whole. A good corporate governance Policy shall ensure the rights of all Data subjects.

5.1 Division of responsibilities

- The meticulous Processing of Personal data should be seen as a line responsibility: that means that the line managers (department heads/central staff services) carry the primary responsibility for the meticulous Processing of Personal data at their department/unit. This also includes the choice of measures as well as its implementation and enforcement. The line responsibility also covers the task of communicating the Policy with regard to the Processing of Personal data with all the relevant parties.
- The careful handling of Personal data is everyone's responsibility. Staff and students will be expected to behave with integrity. It is unacceptable that, by intentional or unintentional behaviour, unsafe situations can arise that lead to damage and/or image loss of Wageningen University & Research or of individuals. It is for this reason that codes of conduct have been formulated and implemented.[9]

5.2 Imbedding in the governance and coordination with the different levels

In order to ensure that the consistency in the organisation with regard to data protection is well expressed and to align the initiatives and activities in the field of processing Personal data within the different divisions, it is important to have structured consultations on this topic at different levels.

At the strategic level, guiding discussions will take place about governance and compliance as well as about goals, scope, and ambition in the field of privacy. The strategic level consists of the Executive Board.

At the tactical level, the strategy will be translated into plans, standards to be adhered to, and evaluation methods. These plans and instruments are a guide for the implementation. The tactical level consists of the Architecture Board (*architectuur board*).

At the operational level, the issues that concern the day-to-day operational management (execution) will be discussed. The operational level consists of the directors of the operational management meeting.

[9] https://www.wur.nl/en/About-Wageningen/Integrity.htm

5.3 Awareness and training

Policies and measures are not sufficient to exclude risks in the field of processing Personal data. It is necessary to continuously increase the awareness at Wageningen University & Research, so that knowledge of risks is increased and safe and reliable behaviour is encouraged. Included in the Policy are the regularly recurring awareness campaigns for staff members, students, and guests. These campaigns can link to nationwide campaigns in higher education, if possible in consultation with other security campaigns. Increasing awareness is the joint responsibility of all stakeholders of Wageningen University & Research, including in particular the Executive Board as the Controller, the line management, the Data Protection Officer, the (central) Information Security Officer, and the (local) Security Managers and privacy officers.

5.4 Monitoring and compliance

Audits make it possible to check the effectiveness of the Policy and the measures taken. Together with the (central) Information Security Officer and the internal auditor, the Data Protection Officer initiates the audit of the lawful and meticulous Processing of Personal data.

Any external audits are carried out by independent accountants. This is linked to the annual audit and is coordinated as much as possible within the normal Planning & Control cycle. Peer-reviews of SURF audits are part of the external audits of Wageningen University & Research.

In case the compliance with regard to the protection of data and privacy information is seriously inadequate, Wageningen University & Research can potentially sanction the employees involved with a penalty within the framework of the collective labour agreement (CAO) or other legal possibilities.

The Processing of Personal data is a continuous process. Technological and organisational developments inside and outside Wageningen University & Research make it necessary to periodically review if the Policy is sufficiently on track.

6 Lawful and meticulous Processing of Personal data

6.1 Basis, purpose, and balancing 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 Controller describes the purposes for the processing in advance. These purposes have been formulated in a concrete and specific way. With each processing, an assessment will take place to determine to what extent the Processing of Personal data is needed. During this assessment, the different interests will be balanced and the effectiveness, proportionality and subsidiarity will be considered. Personal data are not further processed in a way that is incompatible with the purposes for which they were obtained.

Wageningen University & Research shall take the necessary measures to ensure that Personal data are correct and accurate, with respect to the purposes for which they are collected or further processed.

In the case of (research) projects, infrastructural changes, or purchasing new systems, Privacy by design as well as performing a Privacy Impact Assessment (PIA) are taken into account from the start. In research projects, the best practices with regard to scientific research and privacy that are followed can be found on the website of the National Coordination Point for Research Data Management (LCRDM) https://www.lcrdm.nl/.

When purchasing and implementing new systems, Wageningen University & Research applies the following principles: "Privacy by design" and more generally speaking: "Privacy by default".

6.2 Reporting and documenting processing operations

A wholly or partly automatic Processing of Personal data must be reported to the DPO. The DPO will assess the validity of the registration and will take care of appropriate documentation.

Processing operations shall be adequately documented and published on media that is accessible to the Data subject, stating the purpose of the registrations and the Controllers.

6.3 The organisation of the security

Wageningen University & Research shall ensure an adequate level of security and submit appropriate technical and organisational measures to protect Personal data against loss or against any form of unlawful processing. These measures are partly aimed at preventing unnecessary or unlawful collection and Processing of Personal data.

A risk assessment of privacy protection and information security is part of the internal risk management and audit system of Wageningen University & Research.

Because of the significant material risks, the risk assessment of information security and privacy protection is included in the Governance Code of Wageningen University & Research and is therefore housed in the attention area of the Supervisory Board.

6.4 Confidentiality

At Wageningen University & Research, all Personal data are classified as confidential. Everyone should be aware of the confidentiality of Personal data and the responsibility to act accordingly.

Even people who are not already under the office, professional, or legal obligation of confidentiality are required to maintain the confidentiality of the Personal data that they have insight into, except when any legal regulation obliges them to report or if this obligation results from their task.

6.5 Retention periods/destruction deadlines for each type of data

Personal data will not be kept longer than is necessary for the purposes for which they were collected or for which they are used. After expiration of the retention period,[10] Personal data must be taken out of the active administration's reach. After the expiration of the retention period, Wageningen University & Research will destroy the Personal data or, if the Personal data are intended for historical, statistical, or scientific purposes, it will archive it adequately.

6.6 Sensitive Personal data

The processing of sensitive Personal data is prohibited, unless there is a legal basis (e.g. labour and social security law), explicit consent of the Data subject, or a substantial public interest. In addition, stricter requirements apply to the security of these Personal data. Wherever the basic protection is not satisfactory, individually-tailored extra measures must be taken for each information system.

Sensitive Personal data include data concerning a person's religion or belief, race, political affiliation, health, sexual life, trade-union membership, and legal data. From a given context, sensitive Personal data may be distilled from data that is not sensitive, causing these data to also be included under the qualification of sensitive Personal data.

6.7 Transfer of Personal data to third parties

6.7.1 Outsourcing processing to a Processor

If Wageningen University & Research commissions a Third party to process Personal data as a Processor, the act of processing will be regulated in a separate written agreement between Wageningen University & Research, the Controller, and the Third party in the capacity of Processor.

6.7.2 Transfer of Personal data within the European Union (including the EEA).

Wageningen University & Research will only provide Personal data to third parties if this transfer complies with the criteria laid down in chapter V of the GDPR (articles 44 to 50). Sensitive Personal data will not be provided to third parties without the explicit consent of the individual concerned.

[10] Retention periods can be legally determined, such as financial data or formal study results, but they can also be established by Wageningen University & Research, for example in an agreement between Wageningen University & Research and the Data subjects.

6.7.3 Transfer of Personal data outside the European Union

Wageningen University & Research will only provide Personal data to third parties who are located in a country outside the European Union, if that country as a whole or that company/that institute specifically guarantees an adequate level of protection.

Wageningen University & Research will only provide Personal data to countries without an adequate level of protection, if it has obtained a permit from the Minister of Security & Justice or has entered into a contract on the basis of a model contract (as prepared by the European Commission). In both cases, Wageningen University & Research will provide the Dutch Data Protection Authority with a notification on the transfer to a country outside the EU.

6.7.4 List of third parties (non-exhaustive) to whom Wageningen University & Research transfers data

- DUO
- Government institutions
- Municipalities
- Tax Authorities
- Internship companies/organisations
- Student housing corporations
- Study associations
- Student associations
- Sport associations

7 Incidents relating to Personal data

Any complaint or notification regarding the Processing of Personal data within Wageningen University & Research is an incident. The best-known form of such an incident is theft or hacking data carriers (laptop/phone/USB stick, etc.) or the servers of Wageningen University & Research. When Personal data are involved in theft or a hack, we speak of a data leak. This chapter describes the Policy with regard to the reporting, registration, and handling of incidents or suspected incidents in regular business operations and in special circumstances.

7.1 Reporting and registration

Incidents should be reported to the IT Service Desk or, in exceptional cases, to the confidential counsellor or student guidance of Wageningen University & Research. A mandatory, meticulous record will be kept of every incident, the handling of the incident, and the possible measures to be taken. The notification forms are provided by the IT Service Desk and can also be downloaded from the website of Wageningen University & Research.

An incident can be reported by a Data subject, a Processor, or a Third party.

7.2 Handling

Incidents will be forwarded to the department or person responsible as much as possible and will subsequently be handled in accordance with the established procedures.

If the Personal data of the Data subject(s) or the business processes, the finances, or the good reputation of Wageningen University & Research are at stake, at least the Executive Board, the (central) Information Security Officer, and the DPO will be informed.

In the case of serious data leaks, these will be handled in accordance with the specific provisions included in the relevant legislation and regulations.

7.3 Evaluation

It is important to learn from incidents. Registration of incidents and a periodic reporting about it are part of professionally Processing of Personal data. Reporting on incidents concerning Personal data is therefore a fixed part of the annual report of the Executive Board and of the DPO.

7.4 Special circumstances

To be prepared for (the threat of) incidents in the field of Personal data in special circumstances, Wageningen University & Research has set up a special operational team, Disaster Management Team (*Calamiteiten Management Team* - CMT).

This team's main task is to act when there are incidents involving Personal data in those cases in which the organisation cannot solve an incident through the standard procedures. This may be because the incident takes place outside the regular opening hours of Wageningen University &

Research, in a period in which the regular business processes are disrupted, or because the nature of the incident requires emergency measures and/or specific mandates to carry out these measures.

The Disaster Management Team works according to an operational model established by the Executive Board and has special mandates that correspond to the mandates of the DPO, for which the team always has to provide accountability in hindsight about why and how the team has made use of these mandates.

The team has a direct link to the Executive Board as the Controller in the framework of relevant laws and regulations.

8 Rights of Data subjects

8.1 Information obligation

General announcement
Wageningen University & Research aims at sharing the Policy on the Processing of Personal data with students, staff members, and other Data subjects by means of general announcements. In addition, in accordance with the law, Wageningen University & Research aims at giving rights to Data subjects under certain circumstances, with which the Data subjects can adequately protect their Personal data.

Wageningen University & Research provides the Data subject with at least the following:
- The identity and contact details of the Processor and, if applicable, those of the Data Protection Officer;
- The specific purposes of the processing operation for which the Personal data are intended, as well as information regarding the security of processing;
- The period during which the Personal data are stored, or if not possible, the criteria that serve the purpose of determining these terms;
- The existence of the right to demand of the Processor: access to and rectification or deletion of Personal data concerning the Data subject;
- The right to file a complaint with the Executive Board
- The recipients or categories of recipients of the Personal data.

Announcement of modifications
If the Policy is amended or changed substantially over time, Wageningen University & Research will share these modifications in a general way via the website, in order to ensure meticulous and proper processing (see also Chapter 8).

8.2 Right to inspect

Request for access
Any Data subject has the right to access processed Personal data concerning him. A request for this can be submitted in writing to the functional e-mail address privacy@wur.nl of the privacy team of Wageningen University & Research.

A request for inspection from minors who have not yet reached the age of 16 must be submitted by their legal representative.

Period
The written response to the request will be made as soon as possible, but no later than four weeks after submission. In doing so, Wageningen University & Research ensures the proper verification of the identity of the applicant.

Announcement
If data are processed, the content of the response of Wageningen University & Research will contain a full description of these in intelligible form, a description of the purposes of the processing operation, the categories of data to which the processing relates, and the categories of recipients, as well as available information on the origin of the data and how long the data will be stored.

Costs
Every first application can be submitted free of charge. For every additional request, Wageningen University & Research will charge the Data subject a fee of €25 for administrative costs.

8.3 Right to improvement, supplementation, removal, protection, and data portability.

Request for improvement, supplementation, removal, protection, and data portability.
With regard to their Personal data as recorded at Wageningen University & Research, every Data subject is able to request that this data be changed, improved, supplemented, removed, protected, or transferred.

A request for improvement, supplementation, removal, or protection from minors under the age of 16 must be submitted by their legal representative. For all voluntary registrations, the Data subject must be offered an unambiguous opt-out procedure.

Period
Within four weeks after receipt of the request, Wageningen University & Research shall inform the Data subject in writing whether their request is well-founded.

Notification
If the recorded Personal data of the Data subject are factually inaccurate, incomplete or irrelevant for the purpose(s) of the processing operation, or otherwise in violation of any law, the data administrator (functional manager, a.k.a. the Processor) will correct this data.

In addition, third parties to whom the data have been supplied prior to the correction, will be informed about this. The applicant may request an indication of the person to whom Wageningen University & Research has sent this notification.

Deadline for implementation
The data administrator will ensure that a decision for correction, supplementation, removal, or blocking is implemented as soon as possible.

8.4 Right of appeal/objection

Grounds for appeal/objection:
In connection with his or her personal circumstances, any Data subject may object to processing at Wageningen University & Research, if this processing has taken place on the basis of:

a. the completion of a public legal task of the data administrator; or
b. the representation of a legitimate interest of Wageningen University & Research or of a Third party to whom the data will be provided;
c. Personal data that are used for scientific or statistical purposes, unless it concerns studies that are of public interest.

Any Data subject is entitled to object to the use of their Personal data for direct marketing objectives and profiling. The Processor responsible is then no longer able to use the Personal data for these purposes.

Period
Within four weeks after receipt of the appeal or objection, Wageningen University & Research will assess whether this is justified. If the appeal is justified, Wageningen University & Research will take the measures needed to terminate the processing operation.

Costs
The costs that Wageningen University & Research charges for this shall not exceed the amount determined by the Controller. In case the appeal or opposition is found to be well-founded, the remuneration will be refunded.

8.5 Legal protection

General complaints
If the Data subject feels that the legal provisions concerning the protection of privacy or the provisions of the Policy that concern him are not correctly maintained, he can submit a written complaint to Wageningen University & Research.

Possibilities to object after submitting general complaint
If the answer of Wageningen University & Research to the Data subject does not lead to an acceptable result for them, the Data subject has the possibility to start an appeal at the court.

Possibilities to object after rejection of an application for inspection
If Wageningen University & Research has decided to dismiss a request for inspection or improvement, supplementation, removal, or blocking of Personal data, or if Wageningen University & Research has rejected the request of the Data subject, then the Data subject has the possibility to start an appeal procedure at the court.

Deadlines for submitting an appeal
Within six weeks after receipt of the response from Wageningen University & Research, the written request will be submitted to the court. If Wageningen University & Research has not replied within the prescribed period, the appeal must be submitted within six weeks after the end of the set deadline.

9 In conclusion

This Policy has been established by the Executive Boards of Wageningen University and Wageningen Research on 27 March 2017. Changes to this Policy will be announced via the website and the latest version has been published on the internet page of Wageningen University & Research.

For questions or comments regarding the Policy, you can contact the Data Protection Officer: functionarisgegevensbescherming@wur.nl.

To explore the potential of nature to improve the quality of life

Wageningen University & Research
P.O. Box 9101
6700 HB Wageningen
www.wur.nl/en/About-Wageningen/Integrity

The mission of Wageningen University & Research is "To explore the potential of nature to improve the quality of life". Under the banner Wageningen University & Research, Wageningen University and the specialised research institutes of the Wageningen Research Foundation have joined forces in contributing to finding solutions to important questions in the domain of healthy food and living environment. With its roughly 30 branches, 5,000 employees and 10,000 students, Wageningen University & Research is one of the leading organisations in its domain. The unique Wageningen approach lies in its integrated approach to issues and the collaboration between different disciplines.