Riwal Holding Group Internal Privacy Code of Conduct and Data Retention Policy

Applicable to: Riwal Holding Group and its affiliates and subsidiaries

1. Introduction

Riwal is a company that considers privacy to be of paramount importance. Riwal has therefore designed this Internal Privacy Code of Conduct to establish guidelines to which employees must adhere when processing data within the company.

Compliance with our privacy guidelines starts with awareness. It is important for employees to then gain a proper understanding of data subject rights, choose the proper grounds for the lawful processing of all data, regardless of the data processing activities, and understand the principles governing personal data processing enshrined in the General Data Protection Regulation (**GDPR**).

1.1 Definitions

Riwal	Riwal Holding Group B.V. and all its affiliates and subsidiaries in other countries
Customer	An entity or organization that will enter or has entered into a rental or purchase fleet contract with Riwal or whose rental or purchase contract has ended not longer than 2 years ago.
Supplier	A natural person, entity or organization that provides Riwal with services or products, related to the business of Riwal.
Personal Data	Any information relating to an identified or identifiable natural person (‘data subject”). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location data or an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Processing	Any activity that involves use of the data. Processing includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data, including organizing, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring Personal Data.
Special Categories of Personal Data	Racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation.
Data Subject	Any person whose personal data is being collected, held or processed.
Controller	The person who or organization that determines the purposes for and the manner in which any Personal Data is processed. The

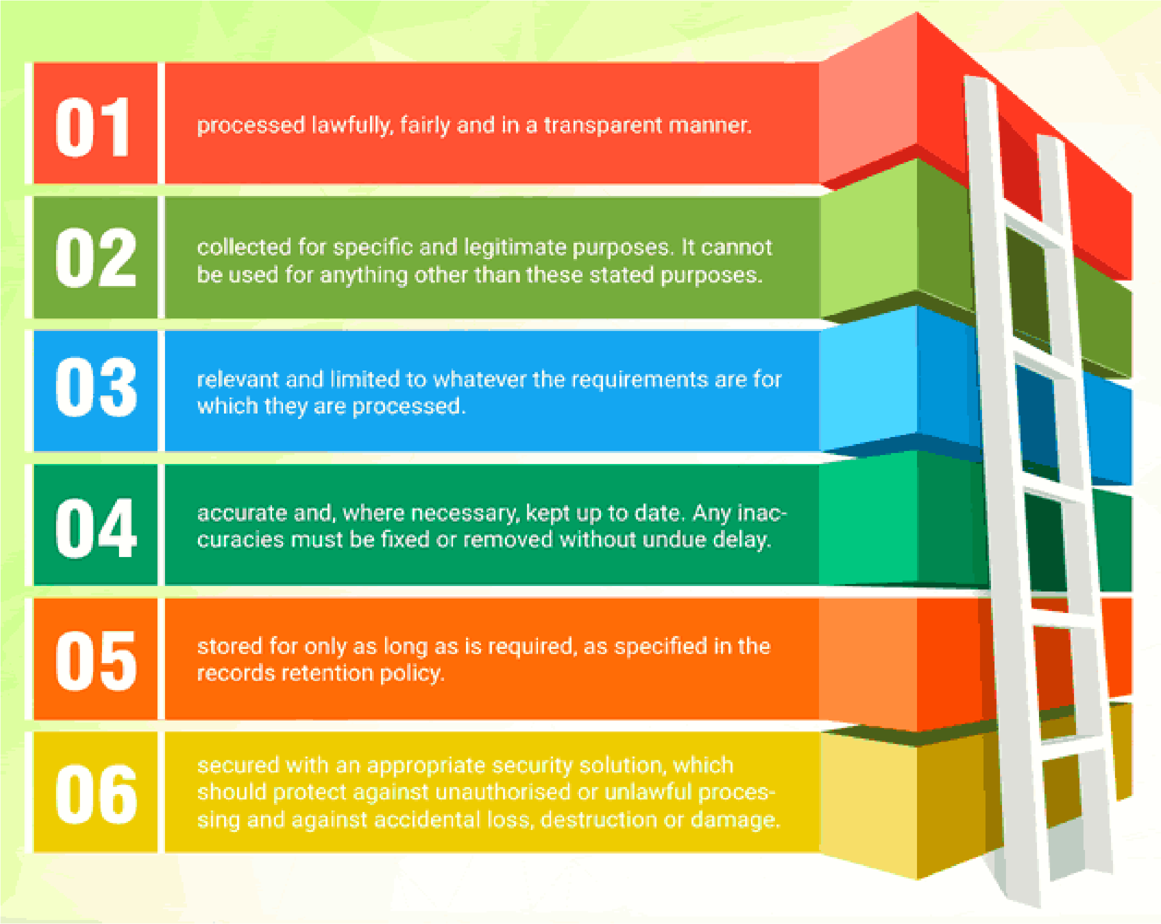
	Controller is responsible for establishing practices and policies in line with the GDPR.
Processor	A natural or legal person, public authority, agency or other body that processes Personal Data on behalf of the Controller.
Third Party	A natural or legal person, public authority, agency or body other than the Data Subject, Controller or Processor who is authorized to process personal data under the direct authority of the Controller or Processor.

1.2. Scope

This Privacy Code of Conduct is an internal guideline for Riwal employees and applies to the Processing of the Personal Data of Customers or Suppliers or other business partners.

2. The six principles governing Personal Data Processing

The GDPR is based on six general privacy principles that companies must follow when collecting, processing and managing personal data. These principles are described in the image below:



01 processed lawfully, fairly and in a transparent manner.

02 collected for specific and legitimate purposes. It cannot be used for anything other than these stated purposes.

03 relevant and limited to whatever the requirements are for which they are processed.

04 accurate and, where necessary, kept up to date. Any inaccuracies must be fixed or removed without undue delay.

05 stored for only as long as is required, as specified in the records retention policy.

06 secured with an appropriate security solution, which should protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Source: GDPR Awareness Coalition

2.1 Lawful, fair and transparent

Personal Data must be processed lawfully and you must therefore always ask yourself whether Riwal has a legal basis that legitimizes Processing. Personal Data should therefore only be processed if and insofar as doing so is consistent with at least one of the following legal grounds:

- the Data Subject has given **his or her unambiguous consent** to have the Personal Data processed;
- Processing is necessary **for the execution of an agreement** to which Riwal is a party, or in connection with pre-contractual measures undertaken at the request of the Customer and necessary to enter into an agreement with that Customer;
- Processing is **necessary to comply with a legal obligation** to which Riwal is subject;
- Processing is necessary to protect the vital interests of the Data Subject;
- Processing is necessary for the proper performance of **a public law duty** by the administrative body in question or by the administrative body to which the data are furnished; or
- Processing is in the legitimate interest of Riwal, except where such interest is overridden by the fundamental rights and freedoms of the Data Subject, in particular the right to privacy. An example is Riwal's direct marketing activities; however, if the Customer no longer wishes to receive a newsletter from Riwal, there must be an easy way for the Customer to unsubscribe.

In Riwal's case, the legal ground will generally be that Processing is necessary to execute a rental or purchase agreement with a Customer.

Fairness means, briefly, that there must be a fair balance between the Personal Data that Riwal processes and the reason why the Personal Data is being processed: it must be a fair game. If you want to process Personal Data in all fairness, then you should not hide anything: you must offer all necessary information concerning the Processing. For example, you should provide information about the Data Subjects' rights in relation to their Personal Data and what the consequences of Processing are.

Transparency means explaining why Riwal processes which Personal Data. Furthermore, transparency also requires that this information provided is expressed in easily comprehensible language and that it is easy for the Data Subjects to find.

2.2 Purpose limitation

Every Processing activity should have one (or more) purposes. These purposes should be explicit and legitimate and determined at the time of collection of the Personal Data. Every time you use Personal Data, then, ask yourself the purpose for which you are doing so (for example, to send out newsletters).

2.3 Data minimization

Once you have determined the purpose of Processing, you need Personal Data that serve this purpose but no more data than strictly necessary and relevant.

You therefore need to ask yourself whether you really need the data to accomplish your purpose (for example, you can send someone a newsletter without knowing their date of birth).

2.4 Accuracy

Personal Data should be correct and updated. In practice, this means that you should:

- take reasonable steps to ensure the accuracy of Personal Data;
- ensure that the source and status of the Personal Data is clear;
- carefully consider any challenges to the accuracy of the Personal Data; and
- consider whether it is necessary to periodically update the Personal Data.

The principle of accuracy therefore imposes certain duties and requires certain activities on your part. Accuracy should also be seen within the context of data management and data security, such as rectification mechanisms. If a Data Subject disagrees with the accuracy of his or her Personal Data, he or she can exercise the right to restrict Processing (see below).

2.5 Storage limitation

This principle includes the idea that Personal Data should not be retained for longer than necessary to achieve the purpose for which they were collected or for which they are being processed. If the data are no longer necessary for that purpose, then delete them. For specific data storage periods, please see our Data Retention Policy below.

2.6 Integrity and confidentiality

Processing of Personal Data should be done in such a way that a proper level of data security is guaranteed. This requires the right measures to be taken. Although the IT department has already introduced numerous security measures, please be aware that you also have a major role to play in this regard. For example, do not leave your laptop unattended, change your passwords regularly, and double-check the email address when sending data by email.

3. Accountability

Riwal must be able to demonstrate compliance with the above six privacy principles by documenting its privacy policies, keeping records of its Processing activities, maintaining a data breach notification register and, of course, complying with this Privacy Code of Conduct.

3.1 Restriction on transfers outside Riwal companies

You may share Personal Data with other recipients outside Riwal companies or transfer such data to such recipients subject to the following restrictions:

a) The data recipient may use the data only for the defined purposes and must have a valid legal basis for such use, unless the transmission is based on a legal obligation.
b) The data recipient must agree in writing (in a contract or in terms and conditions) to maintain a data protection level equivalent to this Privacy Code of Conduct and requirements under the GDPR.
c) If the data recipient is processing Personal Data on behalf of Riwal (for example a cloud provider), a data processing agreement must be concluded.

3.2 Restriction on processing Special Categories of Personal Data

You are prohibited from processing Special Categories of Personal Data unless the following applies:

a) the Data Subject has explicitly consented to having those Personal Data processed for one or more specified purposes; or
b) Processing is necessary for the purposes of meeting the obligations and exercising the specific rights of the Controller or of the Data Subject in the field of employment and social security and social protection law, in so far as such is authorized by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the Data Subject.

For example, pension records include the name and gender of the partner of an employee, thereby revealing the sexual orientation of that individual. However, Riwal is allowed to process this data to execute the employee's pension.

3.3 Rights of Data Subjects

A Customer or Supplier might request the execution of one of the following Data Subject rights:

a) **Right of access**
The Data Subject may request information on which Personal Data relating to him/her have been stored, how the data were collected and for what purpose. If Personal Data are transmitted to a Third Party, information must be given about the identity of the recipient.

b) **Right to rectification**
If Personal Data are incorrect or incomplete, the Data Subject can demand that they are corrected or supplemented.

c) **Right to withdraw consent**
Where Personal Data are processed on the basis of consent, the Data Subject can object to Processing at any time. These Personal Data must be omitted from the Processing to which the Data Subject has objected.

d) **Right to erasure**
The Data Subject may request deletion of his or her data if Processing of such data has no legal basis, or if the legal basis has ceased to apply.

The same applies if the purpose for which Processing was undertaken has lapsed or ceased to be applicable for other reasons. Existing retention periods and conflicting interests meriting protection must be observed.

e) **Right to object**
The Data Subject generally has a right to object to his/her data being processed and this must be taken into account if protection of his/her interests takes precedence over the interests of the Controller processing the particular Personal Data. This does not apply if a legal provision requires that the Personal Data must be processed, for example because the data are necessary to execute the rental agreement.

f) **Right to data portability**
The Data Subject has the right to request that the Personal Data that he/she has provided should be made available to him/her in an easily readable format, such as a Word or Excel document.

Riwal must immediately deal with any request to execute one of the above Data Subject rights and its actions may not result in any disadvantage to the Data Subject. Riwal must let the Customer know within a month of the date of request whether it will be able to comply with that request. In complex cases, Riwal may exceed this term by 1 to 3 months, but the Customer must be informed within a month that compliance will take longer.

If a Customer requests that you erase or rectify its Personal Data, you must do so without delay. In such a case, please send the request immediately to privacy@riwal.com. In addition, we ask you to send the following standard text (even if the request was made by telephone):

Dear Sir/Madam,

Thank you for your request.

We sent your enquiry directly to our privacy department and they will look into it. We will get back to you with our response within 1 calendar month.

Kind regards,

3.4 Confidentiality of Processing

Personal Data are subject to data secrecy. Any unauthorized collection, Processing, or use of such data by you as employee is prohibited. Any Processing undertaken by an employee that he/she has not been authorized to carry out as part of his/her legitimate duties is unauthorized. The “need-to-know” principle applies. Employees may have access to Personal Data only as appropriate for the type and scope of the task in question. This requires the careful breakdown and separation of roles and responsibilities as well as limitations.

You are forbidden to use Personal Data for your own private or commercial purposes, to disclose them to unauthorized persons, or to make them available in any other way. This obligation will remain in force even after your employment has ended. The employment agreements with Riwal employees therefore contain appropriate confidentiality obligations.

3.5 Processing Security

Personal Data must be safeguarded from unauthorized access or disclosure (whether caused internally or externally), unlawful Processing or accidental loss, modification or destruction. This obligation applies whether the data is processed electronically or in paper form. Apart from securing existing Personal Data in line with Riwal's relevant guidelines before the introduction of new methods of Processing, new IT systems or research approaches, technical or organizational measures to protect Personal Data must be defined and implemented. These measures must be based on the state of the art, the risk of Processing and the need to protect the data.

The technical and organizational measures for protecting Personal Data are part of our corporate (IT) security management and must be adjusted continuously to technical developments and advances as well as organizational changes. As a minimum, Riwal will process all Personal Data it holds in accordance with its (general) Code of Conduct and take appropriate security measures against unlawful or unauthorized Processing of Personal Data, and against the accidental loss of, or damage to, Personal Data. If a data breach occurs, the data breach protocol applies.

3.6 Data Protection Audit

Compliance with this Privacy Code of Conduct and the applicable data protection laws is checked regularly by means of data protection audits and other controls. The performance of such controls is the responsibility of the Privacy Coordinator.

3.7 Audit

Riwal's Customers also have audit rights under their agreements with Riwal. The results of the data protection audits must be reported to the Privacy Coordinator. On request, the results of data protection audits will be made available to the responsible data protection authorities.

3.8 Data Protection Incidents

You must inform your manager immediately about any violations of this Privacy Code of Conduct or other regulations concerning the protection of Personal Data, in accordance with the Data Breach Procedure in **Annex I**. Any failure to address serious failings under this Privacy Code of Conduct can also be reported to the Privacy Coordinator.

In the event of:

- improper transmission of Personal Data to a Third Party,
- improper transmission of Personal Data across borders,
- improper access, including by a Third Party, to Personal Data, or
- loss of Personal Data (including subsequent public disclosure of the data due to internal failures)

a data protection breach notification must be made immediately to ensure that: a) any reporting duties under national law can be complied with, b) any affected Customer can be informed and c) any stakeholder communication can be managed. Any data protection breach will also constitute an information security incident under the standard incident management process in Jira.

3.9 Responsibilities and Sanctions

The executive bodies of the respective Riwal companies are responsible for Processing in their area of responsibility. They are therefore obligated to ensure compliance with the legal requirements and those contained in this Privacy Code of Conduct, for data protection (e.g. national reporting duties). Management are responsible for ensuring that organizational, HR and technical measures are in place so that any Processing is carried out in accordance with these data protection requirements.

Compliance with these requirements is also the responsibility of the relevant employees. Improper Processing of Personal Data, or other violations of the data protection laws, can be

criminally prosecuted in many countries and result in claims for compensation of damage. In addition, violations for which individual employees are responsible can lead to sanctions under employment law.

1. Introduction

A vital part of Riwal’s Privacy Code of Conduct and practice is that personal data are retained for the appropriate period of time: neither too long nor too short. It’s Riwal policy to retain all information only for as long as specified in this Data Retention Policy.

This document lists the different categories of personal data and their specific retention periods.

Please note: if no minimum retention period is indicated, the data must be destroyed when they are no longer needed but no later than the end of the maximum retention period. On the other hand, data may be retained longer than the maximum retention period if Riwal has a good reason to do so. For instance, data from (former) employees may be retained for longer in the event of a dispute or if there is a lawsuit against the employee.

2. Retention periods

General business documents

Type of data	Minimum retention period	Maximum retention period	Commencement date
Annual accounts, auditor’s report and similar documents	7 years	8 years	From the date the document was created
Profit and loss account	7 years	8 years	From the date the document was created
Administration after dissolution of legal person	7 years	8 years	From the date of the dissolution
Dividend notes	5 years	6 years	From the date the document was created
Business data concerning real estate	9 years	10 years	From 1 January following the date Riwal started using the real estate
Subsidy administration	7 years	8 years	From the date that administration commences

<u>Tax documents</u>

Type of data	Minimum retention period	Maximum retention period	Commencement date
General ledger, debtor and creditor administration, purchase and sales administration, stock administration and payroll administration	7 years	7 years	From 1 January following the date the document was created
Invoices related to sales tax	7 years	7 years	From the date the invoice was produced
Payroll tax declaration	5 years	5 years	From 1 January following the date the employment has terminated.
Copy ID	5 years	5 years	From 1 January following the date the employment has terminated.

<u>Human Resource documents</u>

Type of data	Minimum retention period	Maximum retention period	Commencement date
Application letters, correspondence concerning the application, certificates and Certificate of Good Conduct	n/a	4 weeks without applicant’s permission 1 year with applicant’s permission	From the date of termination of the application procedure
Employment contracts and changes thereto	n/a	2 years	From the date of termination of employment
Correspondence about appointments, promotion, demotion and dismissal	2 years	2 years	From the date of termination of employment
Reports of performance reviews	2 years	2 years	From the date of termination of employment

Reporting within the context of the Gatekeeper Improvement Act	n/a	2 years	From the date of termination of employment
Payroll tax statements and copies of identity documents	5 years	5 years	From the date of termination of employment
Appointments concerning salary and employment conditions	7 years	7 years	From the date of termination of employment
Curriculum Vitae	1 month	1 year but only after receiving applicant's explicit written consent	From the date of rejection
Employee's personal details (name, address, civil state)	7 years	7 years	From the date of termination of employment
Data concerning early retirement	n/a	2 years	From the date of termination of employment
Works Council appointments	n/a	2 years	From the date of termination of membership
Data on ethnicity and origin	5 years	5 years	From the date of termination of employment
Identity papers of foreign nationals hired from third parties for which a work permit has been granted	5 years	5 years	From the end of the calendar year in which the work carried out by the hired foreign nationals terminates

Security

Type of data	Minimum retention period	Maximum retention period	Commencement date
Security cameras	n/a	24 hours, or as long as necessary to resolve the incident	From the date of recording

		and take disciplinary action	

IT documents

Type of data	Minimum retention period	Maximum retention period	Commencement date
Computer systems	n/a	6 months	From the date of use
E-mail and internet monitoring	n/a	6 months	From the date of monitoring
Audits and security incident reports	n/a	5 years	From the date of audit

Marketing/Commercial

Type of data	Minimum retention period	Maximum retention period	Commencement date
Supplier data	n/a	As long as necessary to execute the agreement with supplier but no longer than 2 years after termination	From the date on which the relationship with the supplier ends
Customer data	2 years	As long as necessary to execute the agreement with customer but no longer than 2 years after termination	From the date on which the relationship with the customer ends

Prospect – Customer data	n/a	1 year	From the date on which the marketing action ends or the prospect unsubscribes from the newsletter

Annex I - Data Breach Procedure

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data - a “data breach” – you must know what to do.

Data breach

First, you need to know which situations are designated as a data breach. Those situations include:

- access by an unauthorized third party;
- sending personal data to an unintended recipient;
- lost or stolen computing devices (including hard drives and USB sticks);
- unauthorized alteration of personal data;
- a cyber-attack where personal data have been captured

Responsibility

All employees of Riwal are required to be aware of and to follow this procedure in the event of a personal data breach.

Procedure

1. Alert

When a data breach is known to have occurred (or is suspected), any Riwal employee who becomes aware of this breach is obliged to report it to the person responsible for privacy, the Privacy Coordinator, within 24 hours. The information that should be provided (if known) includes:

- time and date when the data breach occurred;
- type of personal data involved;
- cause of the data breach; if unknown, how the breach was discovered;
- which systems are affected (if any);
- which department is involved;
- whether corrective action has been taken to remedy or ameliorate the data breach.

2. Assess and determine

Once notified of the aforementioned information, the Privacy Coordinator must consider whether a data breach has (or is likely to have) occurred and makes a preliminary judgement as to its severity.

The Privacy Coordinator must consider the following criteria to determine whether a data breach has occurred:

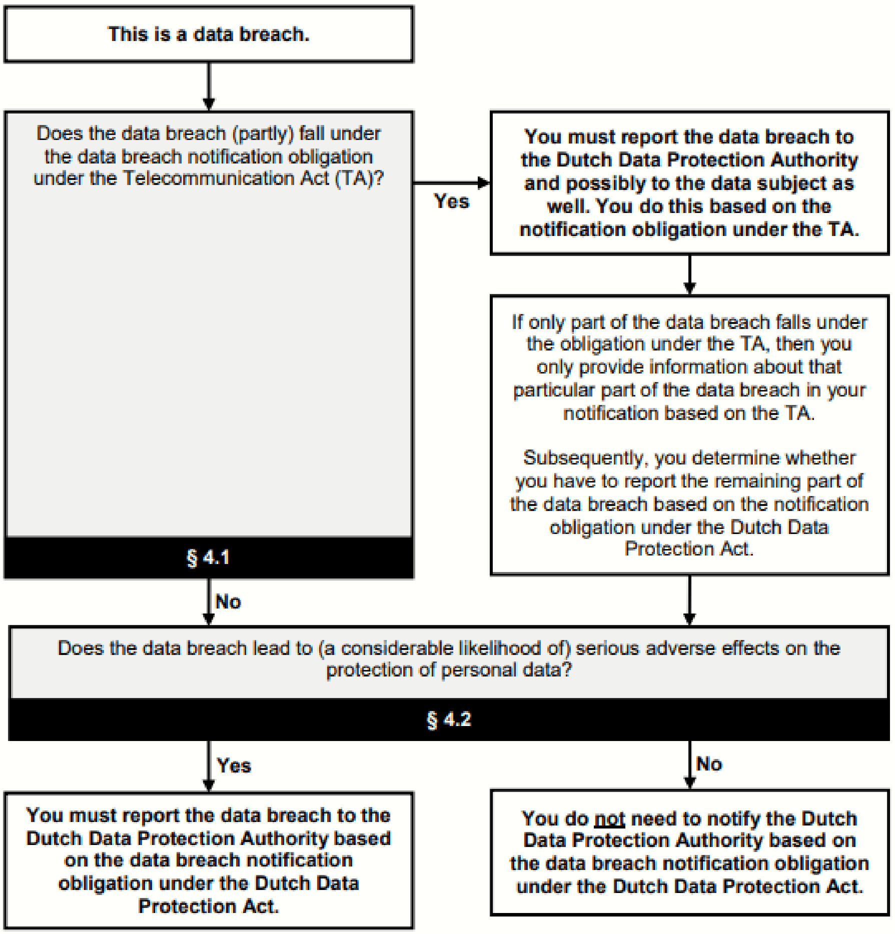
- Is personal data involved in the data breach?
- Is the personal data involved of a sensitive nature?
- Has there been unauthorized access to personal data, or loss of personal data in circumstances where unauthorized access to the information is likely to occur?

Furthermore, the Privacy Coordinator must consider the following criteria to determine the severity of the incident (if applicable):

- the type and extent of personal data involved;
- whether multiple individuals have been affected;
- whether the information is protected by security measures;
- the person who has access now;
- whether there is a risk of serious harm being done to the data subjects affected (physiological, emotional, economic and/or financial, or reputation);
- whether the breach or suspected breach will draw media or stakeholder attention.

Taking all these factors into account, the Privacy Coordinator will take a preliminary decision as to whether the data breach (or suspected breach) must be reported to the supervisory authority. In the Netherlands, the supervisory authority is called the Dutch Data Protection Authority (in Dutch: *Autoriteit Persoonsgegevens*).

The Privacy Coordinator need only report a data breach to the supervisory authority if the breach puts the rights and freedoms of those involved at risk. If so, the Privacy Coordinator must notify the supervisory authority without undue delay, where feasible no later than 72 hours after having become aware of the breach. The diagram on the next page illustrates the questions that must be answered to determine whether a specific data breach should be reported to the supervisory authority:



This is a data breach.

Does the data breach (partly) fall under the data breach notification obligation under the Telecommunication Act (TA)?

You must report the data breach to the Dutch Data Protection Authority and possibly to the data subject as well. You do this based on the notification obligation under the TA.

If only part of the data breach falls under the obligation under the TA, then you only provide information about that particular part of the data breach in your notification based on the TA.

Subsequently, you determine whether you have to report the remaining part of the data breach based on the notification obligation under the Dutch Data Protection Act.

Does the data breach lead to (a considerable likelihood of) serious adverse effects on the protection of personal data?

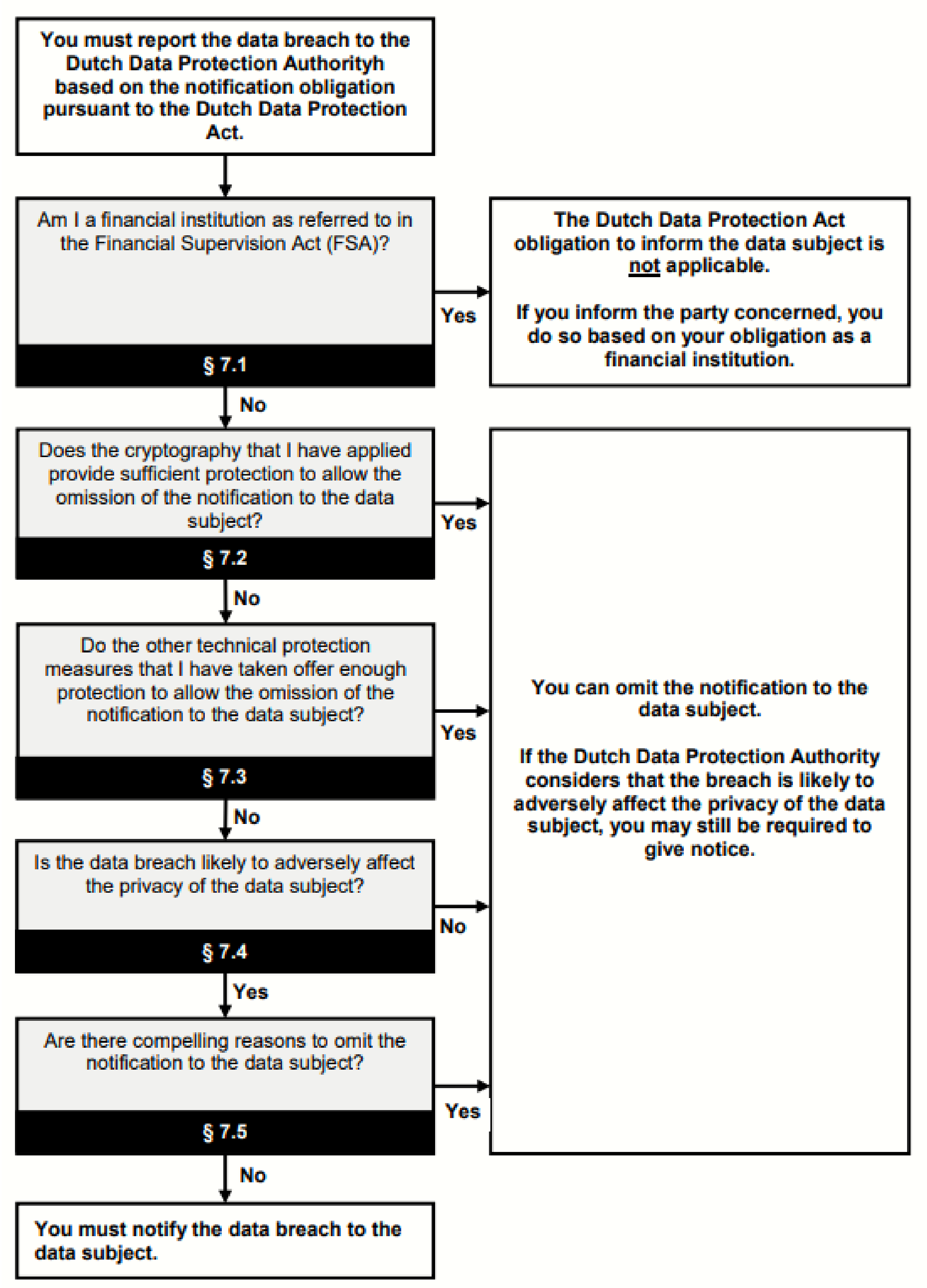
You must report the data breach to the Dutch Data Protection Authority based on the data breach notification obligation under the Dutch Data Protection Act.

You do not need to notify the Dutch Data Protection Authority based on the data breach notification obligation under the Dutch Data Protection Act.

Source: the Dutch Data Protection Authority (Policy rules for the data breach notification obligation)

If the Privacy Coordinator determines that the data breach must be reported to the Dutch Data Protection Authority, the following form must be completed: https://datalekken.autoriteitpersoonsgegevens.nl/melding/aanmaken?1.

Not all data breaches need to be reported to those involved. In principle, the relevant breach should be communicated directly to the data subjects affected unless doing so would involve a disproportionate effort. The diagram on the next page illustrates the questions that must be answered to determine whether a specific data breach should be reported to those affected:


You must report the data breach to the Dutch Data Protection Authorityh based on the notification obligation pursuant to the Dutch Data Protection Act.
Am I a financial institution as referred to in the Financial Supervision Act (FSA)?
§ 7.1
Yes
The Dutch Data Protection Act obligation to inform the data subject is not applicable.
If you inform the party concerned, you do so based on your obligation as a financial institution.
No
Does the cryptography that I have applied provide sufficient protection to allow the omission of the notification to the data subject?
§ 7.2
Yes
No
Do the other technical protection measures that I have taken offer enough protection to allow the omission of the notification to the data subject?
§ 7.3
Yes
No
Is the data breach likely to adversely affect the privacy of the data subject?
§ 7.4
No
Yes
Are there compelling reasons to omit the notification to the data subject?
§ 7.5
Yes
No
You must notify the data breach to the data subject.
You can omit the notification to the data subject.
If the Dutch Data Protection Authority considers that the breach is likely to adversely affect the privacy of the data subject, you may still be required to give notice.

Source: the Dutch Data Protection Authority (Policy rules for the data breach notification obligation)

1. Response team

There is no one way to respond to a data breach because incidents must be dealt with on a case-by-case basis. An assessment of the circumstances and associated risks informs the appropriate course of action. The person, or team, responsible for responding to a data breach could undertake the following steps:

- Immediately contain the breach. Corrective action may include: retrieval or recovery of the personal information, resetting passwords, disabling network access and shutting down or isolating the affected system.
- Evaluate the risks associated with the breach, including collecting and documenting all available evidence of the breach.
- Call upon the expertise of, or consult with, relevant Riwal staff.
- If needed, engage an independent cyber-security consultant. This will provide a fresh perspective on the existing practices and help to reassure customers and others with which Riwal does business.
- If needed, consider developing a communication or media strategy for any announcements made to Riwal staff and/or the media.
- All the above steps must take place in consultation with the Privacy Coordinator and within 48 hours.

It is then important to turn your attention to the following:

- Remedy any identified security flaws. Changes should be reflected in data security policies and other privacy-related documents (such as this data breach notification procedure).
- Prepare a security incident report for submission to the Board in association with the Privacy Coordinator.
- Consider the option of an audit to ensure necessary outcomes are effectuated and effective.
- Roll out training to relevant Riwal staff to ensure that everyone is up to speed on the latest practices.
- Review agreements with service providers to ensure that they are subject to appropriate data security obligations.

2. Documentation

All data breaches, including breaches that are not reported to the supervisory authority and/or to those involved, must be documented internally by the Privacy Coordinator.