

PANORAMIC

**DATA PROTECTION &
PRIVACY**

Netherlands



LEXOLOGY

Data Protection & Privacy

Contributing Editors

Aaron P Simpson and Lisa J Sotto

Hunton Andrews Kurth LLP

Generated on: September 5, 2025

The information contained in this report is indicative only. Law Business Research is not responsible for any actions (or lack thereof) taken as a result of relying on or in any way using information contained in this report and in no event shall be liable for any damages resulting from reliance on or use of this information. Copyright 2006 - 2025 Law Business Research

Contents

Data Protection & Privacy

LAW AND THE REGULATORY AUTHORITY

- Legislative framework
- Data protection authority
- Cooperation with other data protection authorities
- Breaches of data protection law
- Judicial review of data protection authority orders

SCOPE

- Exempt sectors and institutions
- Interception of communications and surveillance laws
- Other laws
- PI formats
- Extraterritoriality
- Covered uses of PI

LEGITIMATE PROCESSING OF PI

- Legitimate processing – grounds
- Legitimate processing – types of PI

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

- Transparency
- Exemptions from transparency obligations
- Data accuracy
- Data minimisation
- Data retention
- Purpose limitation
- Automated decision-making

SECURITY

- Security obligations
- Notification of data breach

INTERNAL CONTROLS

- Accountability
- Data protection officer
- Record-keeping
- Risk assessment
- Design of PI processing systems

REGISTRATION AND NOTIFICATION

Registration
Other transparency duties

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers
Restrictions on third-party disclosure
Cross-border transfer
Further transfer
Localisation

RIGHTS OF INDIVIDUALS

Access
Other rights
Compensation
Enforcement

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

SPECIFIC DATA PROCESSING

Cookies and similar technology
Electronic communications marketing
Targeted advertising
Sensitive personal information
Profiling
Cloud services

UPDATE AND TRENDS

Key developments of the past year

Contributors

Netherlands



Simmons & Simmons

Jaap Tempelman

jaap.tempelman@simmons-simmons.com

Alysia Hogaarts

alysia.hogaarts@simmons-simmons.com

Pien Kamps

Pien.Kamps@simmons-simmons.com

LAW AND THE REGULATORY AUTHORITY

Legislative framework

Summarise the legislative framework for the protection of personal information (PI). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments or laws of other jurisdictions on privacy or data protection?

In the Netherlands, the processing of personal data is primarily governed by [the General Data Protection Regulation \(EU\) 2016/679 \(GDPR\)](#), which has been directly applicable across the European Union since 25 May 2018. The GDPR establishes a harmonised legal framework for the protection of personal data within the EU.

The GDPR is given effect in the Netherlands by way of the [GDPR Implementation Act](#). This implementation act supplements the GDPR in areas where the Regulation permits or requires national legislative measures and ensures that it is effectively applied within the Dutch legal framework.

In addition to the GDPR, a separate EU instrument governs the processing of personal data by law enforcement and judicial authorities: Directive (EU) 2016/680. This directive has been transposed into Dutch law through the [Police Data Act](#) and the [Judicial Data and Criminal Records Act](#).

The GDPR operates within a broader European and international legal framework for the protection of privacy and personal data. Foundational instruments in this framework include article 8 of the European Convention on Human Rights, article 8 of the EU Charter of Fundamental Rights, and the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

Law stated - 12 May 2025

Data protection authority

Which authority is responsible for overseeing the data protection law?
What is the extent of its investigative powers?

The Dutch Data Protection Authority (DPA) is the independent public body tasked with supervising compliance with data protection legislation, including the GDPR and the GDPR Implementation Act.

The Dutch DPA has a wide range of powers to monitor and enforce compliance with data protection rules. These include the following:

- supervising the application of the GDPR and the GDPR Implementation Act;
- conducting investigations, either on its own initiative or in response to complaints;
- requesting access to information, documents, and IT systems;
- carrying out audits and on-site inspections;
- issuing warnings or reprimands for non-compliance;

- ordering specific corrective measures;
- imposing administrative fines; and
- advising on new legislation and policy relating to data protection.

The Dutch DPA operates independently and also plays a coordinating role at the European level through its participation in the European Data Protection Board (EDPB).

Law stated - 12 May 2025

Cooperation with other data protection authorities

Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

The GDPR establishes mechanisms to ensure cooperation among supervisory authorities and to promote a consistent regulatory approach across the Union. Chapter VII of the GDPR introduces a one-stop-shop mechanism for cases involving cross-border processing. Under this mechanism, organisations engaged in cross-border processing must primarily deal with a single lead supervisory authority, even if their activities affect individuals in multiple member states. The supervisory authority of the main or single establishment of a controller or processor is the lead supervisory authority for the cross-border processing carried out by that controller or processor. Each supervisory authority remains competent to handle complaints or infringements of the GDPR if they only relate to an establishment in its member state or substantially affect data subjects only in its member state and shall, in such event, inform the lead supervisory authority who can then decide whether or not to handle the case. Through the cooperation and consistency mechanisms, all supervisory authorities concerned are involved, enabling a coordinated and uniform application of data protection rules.

In addition, the Dutch DPA participates at the European level primarily through the EDPB. It also participates in standing committees responsible for coordinated supervision in areas such as law enforcement, judicial cooperation, and border control.

Law stated - 12 May 2025

Breaches of data protection law

Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

The Dutch DPA has a range of legal instruments at its disposal to respond to data breaches and enforce compliance with the General Data Protection Regulation (GDPR), enabling the Dutch DPA to respond proportionately to breaches of data protection law. Sanctions imposed by the Dutch DPA are determined by the nature, gravity and circumstances of the infringement, with a variety of corrective powers available to the Dutch DPA.

In cases of serious or repeated violations, the Dutch DPA can impose administrative fines of up to €20 million or 4 per cent of a company's total annual global turnover, whichever

is higher. One enforcement decision may include multiple fines if several distinct breaches are identified. The method used to calculate fines for private companies is based on the European Data Protection Board's [Guidelines on the calculation of administrative fines](#). Fines imposed on public sector bodies or individuals not acting in a business capacity are assessed in line with the Dutch DPA's [Fining Policy Rules 2023](#) (only available in Dutch). Administrative fines issued by the Dutch DPA are collected by the Central Judicial Collection Agency. The Dutch DPA does not keep these funds; they are transferred to the central government's general treasury, maintaining the financial neutrality of its enforcement activities.

In addition to financial penalties, the Dutch DPA may apply other corrective measures. These include processing bans, periodic penalty payments (used to encourage compliance where a breach continues), and formal warnings regarding planned processing activities that could potentially violate the GDPR.

If a breach is considered minor or incidental, the Dutch DPA may issue a reprimand instead of a fine. In determining whether this is the appropriate course of action, the DPA takes into account factors such as the duration and seriousness of the breach, whether it was intentional, the impact on individuals, and whether corrective steps have already been taken. This approach reflects the principle of proportionality.

The Dutch DPA will, in principle, publish its enforcement decisions, unless they concern reprimands. Its policy with respect to the publication of enforcement decisions and other aspects of its supervisory tasks are set out in its [Disclosure Policy](#) (only available in Dutch).

Law stated - 12 May 2025

Judicial review of data protection authority orders

Can PI owners appeal to the courts against orders of the data protection authority?

Data subjects, data controllers and data processors can, in first instance, appeal against decisions of the Dutch DPA with the Dutch DPA itself. The decision of the Dutch DPA on that appeal can subsequently be appealed before the competent Dutch administrative courts. The periods for appeal are generally six weeks from the date the decision was made known to the parties involved.

Law stated - 12 May 2025

SCOPE

Exempt sectors and institutions

Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

The processing of personal data by both public and private entities generally falls within the scope of the General Data Protection Regulation (GDPR) and the Dutch GDPR Implementation Act. The GDPR Implementation Act provides that the Act and the GDPR will also apply to the following:

- the processing of personal data in the context of activities not governed by EU law; and
- the processing of personal data by the Dutch armed forces in the context of their activities mandated under Title V, Chapter 2, of the EU Treaty, except where the Dutch Minister of Defence decrees otherwise in the context of the deployment of the Dutch armed forces to protect the interests of the Netherlands or the international legal order. A further general exemption concerns processing activities governed by the Dutch Intelligence and Security Services Act .

The Dutch GDPR Implementation Act provides for a general exemption from articles 12 up to and including 21 and article 34 of the GDPR where necessary and proportionate to safeguard (inter alia) national security, public safety, the prevention, investigation, detection, or prosecution of criminal offences, the execution of criminal penalties, the independence of the judiciary, the enforcement of professional standards in regulated professions, and the enforcement of civil law claims. Furthermore, in specific contexts, personal data processing for journalistic purposes, scientific research, or archiving may also be exempted from particular GDPR provisions under the Dutch GDPR Implementation Act.

Law stated - 12 May 2025

Interception of communications and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals?

The interception of electronic communications by public electronic communications services providers is generally forbidden except for specific exemptions provided under the [Dutch Telecommunications Act](#), and their processing of any such intercepted data is generally subject to the GDPR and the Dutch GDPR Implementation Act insofar as the provisions of the Dutch Telecommunications Act (and the rules promulgated thereunder) do not provide differently.

The interception of communications by law enforcement authorities is also governed by the Dutch Telecommunications Act, and the basis for their interception powers and restrictions as regards their processing of intercepted data are set out, inter alia, in the Dutch Code of Criminal Procedure and in the Dutch Intelligence and Security Services Act . The Dutch Code of Criminal Procedure and the Dutch Information and Security Services Act also provide the basis for other monitoring and surveillance activities with respect to individuals and the processing of personal data in that context.

While the GDPR Implementation Act generally also applies to the processing of personal data for the purposes of electronic marketing, specific rules on electronic marketing via public electronic communications networks and services are set out in the Dutch [Telecommunications Act](#), which implements the provisions of [Directive 2002/58/EC](#) (the ePrivacy Directive). With some specific exceptions, the use of automated systems without human intervention and electronic messages (including email) or other means for sending unsolicited communications for commercial, idealistic or charitable purpose is forbidden without the prior consent of the end user (whether a natural or legal person) of the electronic communication services concerned. A soft opt-in exemption applies to the use of electronic

contact details gathered from the customers of a sender in the context of the sale of goods or services insofar as it concerns communications concerning similar goods or services from that same sender, provided the customers are given the opportunity to easily object to such use of their contact details at the time the contact details were initially gathered by the sender and with each communication.

Law stated - 12 May 2025

Other laws

Are there any further laws or regulations that provide specific data protection rules for related areas?

The processing of personal data in the context of employee monitoring is primarily regulated by the GDPR as implemented in the Dutch GDPR Implementation Act . For organisations with works councils, the Works Councils Act provides that the consent of the works council is required to implement policies concerning the processing of employee personal data and the monitoring of employee presence, behaviour or performance.

In the Netherlands, the legal framework for establishing and managing health-related data registrations is governed by multiple layers of legislation. At the core are the Medical Treatment Contracts Act and the GDPR as implemented by the Dutch GDPR Implementation Act, in the context of which the former takes precedence over the latter. In addition to these general instruments, more specific laws apply in the healthcare context. Notably, the Electronic Data Exchange in Healthcare Act regulates digital data sharing between healthcare providers. In contrast, the Processing of Personal Data in Healthcare (Additional Provisions) Act sets out detailed rules concerning confidentiality, access, and logging obligations in medical data processing.

The Dutch Financial Supervision Act and the Dutch Anti-Money Laundering and Anti-Terrorist Financing and the rules promulgated thereunder may provide certain specific rules in relation to the processing of personal data by financial institutions and payment service providers that complement (and, in the event of a conflict, take precedence over) the general rules under the GDPR as implemented by the Dutch GDPR Implementation Act. For example, the Dutch Financial Supervision Act contains specific rules on access by payment service providers to the personal data of account holders. The Dutch Anti-Money Laundering and Anti-Terrorist Financing Act provides specific restrictions on the personal data that can be required and stored in the context of financial entities' screening policies.

The Dutch Telecommunications Act contains specific rules on the processing of personal data (including as comprised in location data or traffic data) by providers of public electronic communications networks and services in the context of their communications services, which take precedence over the rules under the GDPR and the Dutch GDPR Implementation Act.

Law stated - 12 May 2025

PI formats

What categories and types of PI are covered by the law?

The GDPR defines personal data as any information relating to an identified or identifiable natural person. This definition is unchanged under the Dutch GDPR Implementation Act . Both the GDPR and the GDPR Implementation Act apply to fully or partly automated processing, as well as to manual processing where the data are part of, or intended to be part of, a structured filing system.

Data relating to legal entities or deceased persons do not qualify as personal data unless the information also reveals something about a living, identifiable natural person. The GDPR defines processing broadly, encompassing a wide range of operations carried out on personal data, including collection, storage, disclosure, and erasure.

Law stated - 12 May 2025

Extraterritoriality

Is the reach of the law limited to PI owners and processors physically established or operating in your jurisdiction, or does the law have extraterritorial effect?

The Dutch GPR Implementation Act applies to the processing of personal data in the context of the activities of an establishment of a controller or processor in the Netherlands. The GDPR Implementation Act also applies with respect to the processing of personal data of data subjects in the Netherlands by a controller or processor established outside the European Union if the processing is related to:

- the provisions of goods or services to these data subjects (regardless of whether the provision is against remuneration); or
- the monitoring of the behaviour of data subjects insofar as such behaviour occurs in the Netherlands.

Law stated - 12 May 2025

Covered uses of PI

Is all processing or use of PI covered? Is a distinction made between those who control or own PI and those who provide PI processing services to owners? Do owners', controllers' and processors' duties differ?

Both the GDPR and the Dutch GDPR Implementation Act apply to all processing of personal data insofar as the processing is automated or forms part of a structured filing system. The GDPR draws a clear distinction between controllers, who determine the purposes and means of processing, and processors, who process personal data solely on behalf of the controller and in accordance with its instructions. The duties of controllers and processors differ. Controllers are primarily responsible for ensuring compliance with the GDPR, including the legal basis, transparency obligations, and the protection of data subject rights, while processors must adhere strictly to the controller's instructions and ensure appropriate security measures.

Law stated - 12 May 2025

LEGITIMATE PROCESSING OF PI

Legitimate processing – grounds

Does the law require that the processing of PI be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

The processing of personal data is only permitted if there is a legal ground. The General Data Protection Regulation (GDPR) provides an exhaustive list, which also applies under the Dutch GDPR Implementation Act:

- the data subject has given consent to the processing of their personal data for one or more specific purposes;
- the processing is necessary for the performance of a contract to which the data subject is party;
- the processing is necessary for compliance with a legal obligation to which the controller is subject;
- the processing is necessary to protect the vital interests of the data subject or another natural person;
- the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; and
- the processing is necessary for the purposes of the legitimate interests pursued by the controller.

Law stated - 12 May 2025

Legitimate processing – types of PI

Does the law impose more stringent rules for processing specific categories and types of PI?

In accordance with article 9 of the GDPR, the processing of special categories of personal data is prohibited under the GDPR Implementation Act. These specific categories include personal data revealing racial and ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, as well as genetic data, biometric data (to uniquely identify a natural person), health data and data concerning a natural person's sex life or sexual orientation.

The processing of these special categories of personal data is generally prohibited unless one of the specific conditions under article 9 of the GDPR is met. Some of these conditions allow for national implementation. In the Netherlands, the relevant implementation is detailed in articles 22-30 of the Dutch GDPR Implementation Act. For example, taking into account article 25 of the Dutch GDPR Implementation Act, the prohibition on processing personal data revealing racial or ethnic origin does not apply if the processing is to assign a privileged position to persons of a particular ethnic or cultural minority group in order to eliminate or reduce factual disadvantages related to the ground of racial or ethnic origin, and only to the extent that:

- the processing is necessary for that purpose;
- based on the data, it is possible to determine objectively whether a person belongs to a particular ethnic or cultural minority group; and
- the data subject has not objected to the processing in writing.

Law stated - 12 May 2025

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

Transparency

Does the law require owners of PI to provide information to individuals about how they process PI? What must the notice contain and when must it be provided?

The general rules under the General Data Protection Regulation (GDPR) apply, which require personal data controllers to provide information to data subjects about how their personal data is processed in a concise, transparent, intelligible and easily accessible form, using clear and plain language. In practice, this is done through a privacy notice.

This notice must contain at least the following information:

- identity and contact details of the controller and, if applicable, of the data protection officer;
- purposes and legal basis;
- (if applicable) the legitimate interests pursued;
- information on the recipients or categories of recipients;
- (if applicable) data transfers;
- retention periods;
- the existence of data subject rights;
- the existence of the right to withdraw consent;
- the right to lodge a complaint with a supervisory authority;
- whether the provision of personal data is obligated; and
- the existence of automated decision-making.

Concerning the information on recipients or categories of recipients of personal data, the Dutch Data Protection Authority (Dutch DPA) recently imposed a [fine](#) on Netflix. One of the violations was the failure to specify the names of the recipients in their privacy notice. In this respect, the Dutch DPA considered it relevant that this only involved a limited number of recipients. This indicates that it is advisable to include all the names of recipients in a privacy notice.

Under the GDPR, if the personal data is not obtained directly from the data subject, the controller must, in addition to the information listed above, provide details about the categories of personal data concerned and the source from which the personal data originates. This information should be provided within a reasonable period after obtaining

the personal data - no later than one month - or, if the personal data is shared with a third party, at the latest when it is first disclosed. If the personal data is used to communicate with the data subject, the information must be provided at the time of the first communication.

Law stated - 12 May 2025

Exemptions from transparency obligations

When is notice not required?

Under the GDPR, there are specific situations in which the obligation to provide notice about the processing of personal data may be exempt. These exemptions are outlined in article 13(4) of the GDPR and apply also in the Netherlands. For example, notice is not required if the data subject already has the relevant information.

In the Netherlands, additional key exemptions from certain GDPR provisions, including in respect of notice requirements, are outlined in the Dutch GDPR Implementation Act. Article 41 of the GDPR Implementation Act states that exemptions may be permitted when necessary and proportionate to protect various interests, such as national security, as well as other important objectives that serve the public interest. To invoke one of these exemptions, the data controller must consider several factors, including the purposes of the data processing, the categories of personal data involved, and the risks to the rights and freedoms of the data subjects.

Law stated - 12 May 2025

Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PI?

Article 5 (1)(d) of the GDPR states that personal data must be accurate and kept up-to-date. This means that a controller is obliged to take steps to ensure that personal data that is inaccurate is erased or rectified without delay.

Law stated - 12 May 2025

Data minimisation

Does the law restrict the types or volume of PI that may be collected?

Pursuant to the GDPR, the personal data being processed must be adequate, relevant, and limited to what is necessary for the specific purposes of the processing. This means that the controller should strictly limit the collection of personal data to what is directly relevant to the intended purpose. For example, collecting gender information to personalise marketing communications is not necessary for fulfilling a contract and, therefore, does not meet the requirement of being strictly relevant to the intended purpose.

Law stated - 12 May 2025

Data retention

Does the law restrict the amount of PI that may be held or the length of time for which PI may be held?

Dutch law specifies various legal retention periods, both minimum and maximum. In the Netherlands, some commonly applicable retention periods are:

- a minimum of seven years for business administration records (fiscal retention period);
- a minimum of five years for know-your-customer documentation (applicable to obliged entities under anti- money laundering legislation); and
- a maximum of two years for:
 - employee records, performance and appraisal interviews;
 - employment contracts and amendments thereto;
 - correspondence regarding appointment, promotion, demotion, and dismissal;
 - agreements on works council activities; and
 - certificates; absence frequency (note that salary administration records must be retained for seven years in accordance with the fiscal retention period mentioned above).

Law stated - 12 May 2025

Purpose limitation

Are there any restrictions on the purposes for which PI can be used by owners? If there are purpose limitations built into the law, how do they apply?

The principle of purpose limitation under the GDPR states that any processing of personal data must be conducted for specific, explicit and legitimate purposes. These purposes should be defined before any data processing begins. When the processing purpose is clear and specific, individuals know what to expect, which enhances transparency and provides legal certainty. Once personal data is collected for a specific purpose, it cannot be processed further in a way that is incompatible with that original purpose. Any new purposes for processing data that are not compatible with the original must have their own distinct legal basis, and they cannot rely on the fact that the data was initially obtained for a legitimate purpose.

Law stated - 12 May 2025

Automated decision-making

Does the law restrict the use of PI for making automated decisions without human intervention that affect individuals, including profiling?

According to the GDPR, individuals have the right not to be subject to decisions based solely on automated processing, including profiling, if such decisions have legal consequences or significantly impact them. A decision is considered solely automated if there is no human involvement in the decision-making process. For human intervention to qualify as meaningful, the controller must ensure that the oversight of the decision is meaningful. However, what makes human involvement meaningful has yet to be clearly defined. In light of recent developments in artificial intelligence, the Dutch Data Protection Authority is developing [guidelines](#) to determine whether human intervention can indeed be considered meaningful.

The GDPR states a few exceptions, such as when the data subject has given explicit consent, Article 22(2)(c). Under the Dutch GDPR Implementation Act, there is an exception to the GDPR prohibition of decisions based solely on automated processing of personal data, where such processing is necessary to comply with a legal obligation or for the performance of a task carried out in the public interest. These cases are, by definition, governed by article 6(1)(c) and (e) of the GDPR. However, it is important to note that this exception does not extend to profiling.

Law stated - 12 May 2025

SECURITY

Security obligations

What security obligations are imposed on PI owners and service providers that process PI on their behalf?

Pursuant to the General Data Protection Regulation (GDPR), controllers and processors are required to implement appropriate technical and organisational measures to protect personal data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

These measures must ensure an appropriate level of security, taking into account the condition, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the varying likelihood and severity for the rights and freedoms of individuals.

The following security measures, in particular, should be considered:

- implement pseudonymisation and encryption of personal data;
- ensure ongoing confidentiality, integrity, availability, and resilience of processing systems and services;
- maintain the ability to restore availability and access to personal data promptly after a physical or technical incident; and
- establish a process for regularly testing, assessing, and evaluating the effectiveness of security measures.

Law stated - 12 May 2025

Notification of data breach

Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

A data breach occurs when a security breach leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. Examples of data breaches include sending personal data to an incorrect recipient or the loss of an unencrypted USB drive containing personal data. The severity of a data breach depends on the nature and scope of the personal data involved. Certain breaches may have limited consequences, while others may pose significant risks to the rights and freedoms of the data subjects concerned.

In the Netherlands, a data breach must be reported to the Dutch Data Protection Authority (Dutch DPA) within 72 hours of the moment the breach being discovered. This notification must be submitted via the online form provided by the Dutch DPA.

Where a data breach is likely to result in a high risk to the rights and freedoms of the individuals concerned, the controller is also required under article 34 of the GDPR to inform the affected individuals without undue delay. An exception to this obligation is provided in article 42 of the Dutch GDPR Implementation Act, which stipulates that article 34 of the GDPR does not apply to financial institutions as defined in the Dutch Financial Supervision Act.

Law stated - 12 May 2025

INTERNAL CONTROLS

Accountability

Are owners or processors of PI required to implement internal controls to ensure that they are responsible and accountable for the PI that they collect and use, and to demonstrate compliance with the law?

To ensure accountability in the processing of personal data, controllers and processors must, under the General Data Protection Regulation (GDPR), implement internal controls and maintain records of the processing activities carried out under their responsibility and provide them to the supervisory authorities where requested.

Law stated - 12 May 2025

Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities? Are there any criteria that a person must satisfy to act as a data protection officer?

Under the GDPR, the appointment of a Data Protection Officer (DPO) is mandatory if:

- the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
- the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
- the core activities of the controller or the processor consist of processing on a large scale of special categories of data and personal data relating to criminal convictions and offences.

In other cases, organisations are not legally obliged to designate a DPO. However, the GDPR provides that controllers and processors may choose to voluntarily appoint a DPO while also allowing the possibility for member states to make such designation mandatory for more types of organisations than those foreseen under the regulation. The Netherlands has not made use of this option.

A DPO should be able to carry out their duties independently. Consequently, they should not receive any instructions from the organisation for which they work regarding the performance of their tasks. To safeguard this independence and ensure that DPOs are adequately protected in the execution of their responsibilities, they must not be dismissed or penalised by the controller or processor for fulfilling their role.

Law stated - 12 May 2025

Record-keeping

Are owners or processors of PI required to maintain any internal records relating to the PI they hold?

Record keeping is essential for ensuring compliance with the GDPR. Both data controllers and processors are required to maintain internal records of their processing activities.

For controllers, internal records should at least include the following:

- name and contact details of the controller;
- purposes of the data processing;
- categories of data subjects;
- categories of personal data;
- categories of data recipients;
- information about transfers of personal data to third countries;
- retention periods; and
- description of the implemented technical and organisational security measures.

For processors, records should include at least the following:

- name and contact details of the processor;
- categories of processing carried out on behalf of the controller.
- information about transfers of personal data to third countries; and

- description of the implemented technical and organisational security measures.

To accommodate the unique circumstances of micro, small, and medium-sized enterprises, the GDPR provides an exemption for organisations with fewer than 250 employees regarding record-keeping requirements.

Law stated - 12 May 2025

Risk assessment

Are owners or processors of PI required to carry out a risk assessment in relation to certain uses of PI?

When the processing of personal data is likely to result in a high risk to the rights and freedoms of individuals, the controller is required under the GDPR to conduct a General Data Protection Impact Assessment (DPIA) prior to proceeding with the processing. To determine if a DPIA is necessary, controllers should consider the nature, scope, context, and purposes of the data processing.

According to the GDPR, a DPIA should particularly be carried out in the following situations:

- the systematic and extensive evaluation of personal aspects relating to individuals based on automated processing, including profiling;
- the large-scale processing of special categories of data; and
- the systematic monitoring of publicly accessible areas on a large scale.

Additionally, the Dutch Data Protection Authority (Dutch DPA) has outlined specific types of processing operations that require a DPIA, including:

- assessing people on the basis of personal characteristics;
- automated decisions;
- systematic and large-scale monitoring;
- sensitive data;
- large-scale data processing operations;
- linked databases;
- data on vulnerable persons;
- use of new technologies; and
- blocking of a right, service or contract.

In essence, a DPIA should assess the likelihood and severity of the risks associated with the processing and outline the measures, safeguards and mechanisms envisaged to mitigate those risks. Furthermore, an assessment of any remaining high risks should be conducted. If the residual risks are still considered high, the Dutch DPA must be consulted beforehand.

Law stated - 12 May 2025

Design of PI processing systems

Are there any obligations in relation to how PI processing systems must be designed?

To ensure data security, the GDPR introduces key principles, including privacy by design and privacy by default. The core obligation is the implementation of appropriate measures and necessary safeguards that provide effective implementation of the data protection principles and, consequently, the rights and freedoms of the data subjects by design and by default.

Privacy by design means that controllers are required to implement appropriate technical and organisational measures that ensure compliance with data protection principles. When doing so, controllers must consider the state of the art, the cost of implementation and the nature, scope, context and purposes of the processing. Importantly, this principle is not limited to technical solutions; organisational measures, including mandatory privacy training for employees, are also examples of privacy by design.

Privacy by default requires controllers to configure processing settings and options so that only the personal information strictly necessary for each specific purpose is processed.

Law stated - 12 May 2025

REGISTRATION AND NOTIFICATION

Registration

Are PI owners or processors of PI required to register with the supervisory authority? Are there any exemptions? What are the formalities for registration and penalties for failure to do so?

Controllers and processors are not required to register with the Dutch Data Protection Authority (Dutch DPA). However, where a controller intends to process personal data relating to criminal offences and convictions and share this with third parties, they must obtain a permit from the Dutch DPA, as outlined in article 33(4)(c) of the Dutch GDPR Implementation Act. For instance, this applies when organisations intend to use and share a blacklist that includes such data. The Dutch DPA has published a [register](#) of organisations that have been granted a licence.

Law stated - 12 May 2025

Other transparency duties

Are there any other public transparency duties?

Dutch law does not prescribe any other transparency duties than those contained in the General Data Protection Regulation.

Law stated - 12 May 2025

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers

How does the law regulate the sharing of PI with entities that provide outsourced processing services?

The General Data Protection Regulation (GDPR) differentiates between controllers and processors. The controller is the natural or legal person who determines the purposes and the means of processing. At the same time, the processor is the natural or legal person who processes on behalf of the controller, following strict instructions. The primary consequence of being a controller is the legal responsibility for complying with the respective obligations under the GDPR. However, processors are also required to adhere to many of the same requirements that apply to controllers.

When outsourcing processing services, the GDPR provide that a data processing agreement must be established between the controller and the processor. This contract should clearly specify the subject matter, nature, purpose, and duration of the processing, as well as the types of personal data involved and the categories of data subjects. Furthermore, the agreement must clearly outline the obligations and rights of the controller.

Law stated - 12 May 2025

Restrictions on third-party disclosure

Are there any specific restrictions on the sharing of PI with recipients that are not processors or service providers?

The disclosure of personal data is governed by the general principles and requirements outlined in the GDPR. Any disclosure of personal data to a third party must align with the original purpose for which the personal data was collected. If the disclosure does not align with that purpose, it must be justified by one of the legitimate grounds for processing set forth in article 6(1) of the GDPR. This may be in certain cases the individual's consent.

Law stated - 12 May 2025

Cross-border transfer

Is the transfer of PI outside the jurisdiction restricted?

Transfers of personal data to recipients in third countries are governed by specific rules under the GDPR. The key requirement is to ensure the same level of protection as guaranteed by the GDPR. In general, such transfers are permitted only if one of the exceptions listed in the GDPR applies or if the European Commission has issued an adequacy decision, indicating that the third country provides an adequate level of protection.

If no adequacy decision has been issued, personal data can be transferred to a third country without specific authorisation from the supervisory authority, provided that the controller or processor has implemented appropriate safeguards. The GDPR specifies the following safeguards:

- legally binding and enforceable instrument between public authorities or bodies;
- binding corporate rules approved by a competent supervisory authority;

- standard data protection clauses adopted either by the European Commission or by a supervisory authority;
- codes of conduct approved by a competent supervisory authority, together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; and
- certification mechanisms approved by a competent supervisory authority, together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

In the absence of an adequacy decision or appropriate safeguards, personal data transfers to a third country are allowed under the GDPR only under the following conditions:

- the data subject has explicitly consented to the proposed transfer after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims; and
- the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.

Law stated - 12 May 2025

Further transfer

If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

The conditions outlined in articles 44-50 of the GDPR are equally applicable to transfers to service providers and onward transfers.

Law stated - 12 May 2025

Localisation

Does the law require PI or a copy of PI to be retained in your jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction?

There are no specific rules governing the retention of personal data or a copy of personal data in the Netherlands.

Law stated - 12 May 2025

RIGHTS OF INDIVIDUALS

Access

Do individuals have the right to access their personal information held by PI owners? Describe how this right can be exercised as well as any limitations to this right.

Pursuant to the General Data Protection Regulation (GDPR), individuals have the right to request confirmation from the data controller as to whether their personal data is being processed. If this is the case, the individual is entitled to access these data, as well as to receive information about:

- the purposes of the processing;
- the categories of personal data concerned;
- the recipients or categories of recipient to whom the personal data has been or will be disclosed;
- the envisaged retention period, or, if not possible, the criteria used to determine that period;
- the existence of the right to request from the data controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- the right to lodge a complaint with a supervisory authority;
- where the personal data is not collected from the data subject, any available information as to their source; and
- the existence of automated decision-making, including profiling.

The right of access aims to give individuals more control over their personal data. It allows data subjects to exercise their rights as laid down in articles 16-19, 21, 79 and 82 of the GDPR. In this respect, the right of access entails the ability for data subjects to obtain information from the data controller about the specific recipients who have received or will receive their data.

The right of access must not infringe upon the rights or freedoms of others, including business secrets and intellectual property rights. This means that confidential or protected information may need to be redacted or removed before providing it to the requesting data subject. Furthermore, article 41 of the Dutch GDPR Implementation Act contains several potential exceptions to the application of this right of access.

Law stated - 12 May 2025

Other rights

Do individuals have other substantive rights?

In addition to the right to access, data subjects have the following rights pursuant to the GDPR:

- the right to information;
- the right to rectification
- the right to removal of data;
- the right to restriction of processing;
- the right to data portability;
- the right to object;
- the right to human intervention in decision-making processes; and
- the right to complain to a national supervisory authority.

Law stated - 12 May 2025

Compensation

Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

In accordance with article 82 of the GDPR, any individual who suffers material or non-material damages as a result of an infringement of the provisions as laid down in the GDPR has the right to receive compensation from the data controller or processor.

This right to compensation also applies when a data subject experiences fear regarding the potential misuse of their personal data by third parties as a result of the infringement. In this context, there is no *de minimis* threshold. Furthermore, when determining the amount of compensation for non-material damages, it must be acknowledged that such damages caused by a personal data breach are not less significant than physical injury.

Law stated - 12 May 2025

Enforcement

Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

To exercise an individual's rights, a complaint can be submitted to the Dutch Data Protection Authority (Dutch DPA). The Dutch DPA has the power to impose administrative fines in cases of infringement of the data subject's rights. Additionally, the data subject can file a complaint with the data controller. If the response is unsatisfactory, the data subject has six weeks to submit a petition to the Dutch civil court. According to article 35(4) of the Dutch GDPR Implementation Act, this can be done without an attorney. In conclusion, data subjects can

exercise their rights through both the judicial system and enforcement by the supervisory authority.

Law stated - 12 May 2025

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described?

The Dutch GDPR Implementation Act imposes several additional exceptions and restrictions on the processing of personal data.

Firstly, there is an exception to article 22 of the General Data Protection Regulation (GDPR). In the Netherlands, automated individual decision-making is authorised in case it is necessary to comply with a legal obligation or to perform a task carried out in the public interest. However, it is important to note that this exception does not apply to profiling. Examples include adjusting the amount of student funding entitlement or determining a violation of the speed limit without human intervention.

Secondly, additional restrictions apply to the processing of the Dutch citizen service number (BSN). The Dutch GDPR Implementation Act stipulates that non-governmental organisations may use the BSN only if authorised by specific legislation.

Law stated - 12 May 2025

SPECIFIC DATA PROCESSING

Cookies and similar technology

Are there any rules on the use of 'cookies' or equivalent technology?

In the Netherlands, the rules on cookies and similar technologies are outlined in the Dutch Telecommunications Act, which stipulates that the storage of information on a user's device, such as cookies, or accessing already stored information is only permitted if the user has been provided with clear and comprehensive information in line with the General Data Protection Regulation (GDPR) and has given its consent.

This means that informed consent, obtained through an active opt-in process, must be acquired before placing cookies on a user's device. Consent is not required in specific situations, such as when the sole purpose of storing or accessing information is to transmit a message over a public electronic communications network. Additionally, consent is not needed if the storage or access is strictly necessary to provide the digital service explicitly requested by the user or if it has minimal impact on the user's privacy, such as when obtaining information about the quality or effectiveness of the provided service.

Law stated - 12 May 2025

Electronic communications marketing

Are there any rules on marketing by email, fax, telephone or other electronic channels?

In the Netherlands, sending unsolicited electronic communications for commercial, ideological, and charitable purposes is governed by specific rules in the Dutch Telecommunications Act, which implements the provisions of [Directive 2002/58/EC](#) (the ePrivacy Directive). As a general rule, the use of automated systems without human intervention and electronic messages (including email) or other means for sending unsolicited communications for commercial, idealistic or charitable purposes is forbidden without the prior consent of the end user (whether a natural or legal person) of the electronic communication services concerned. A soft opt-in exemption applies to the use of electronic contact details gathered from the customers of a sender in the context of the sale of goods or services insofar as it concerns communications concerning similar goods or services from that same sender, provided the customers are given the opportunity to easily object to such use of their contact details at the time the contact details were initially gathered by the sender and with each communication.

Law stated - 12 May 2025

Targeted advertising

Are there any rules on targeted online advertising?

The use of tracking cookies for the purposes of online advertising is subject to an opt-in regime. In practice, this is implemented via a cookie banner, where it is not allowed to have pre-ticked boxes. Furthermore, to secure valid consent for the placement of tracking cookies, the data subject must be informed about:

- the types of personal data;
- the purposes;
- the categories of businesses or third parties to whom data is provided;
- the retention period; and
- as much further information as necessary to give website visitors a fair view of the data processing.

The Dutch Data Protection Authority (Dutch DPA) has published a list with nine general rules to make a clear cookie banner.

These rules:

- provide information about the purpose;
- do not use pre-ticked choice options;
- use plain text;
- place the different choices on one layer;
- do not hide certain choices;
- do not let someone make additional clicks;

- do not use inconspicuous links in the text;
- be clear about the withdrawal of consent; and
- do not confuse consent with legitimate interest.

Law stated - 12 May 2025

Sensitive personal information

Are there any rules on the processing of 'sensitive' categories of personal information?

In line with article 9 of the GDPR, the processing of special categories of personal data is prohibited. These specific categories include racial and ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data (to uniquely identifying a natural person), health data and data concerning a natural's person's sex life or sexual orientation.

The processing of these special categories of personal data is generally prohibited unless one of the specific conditions under article 9 of the GDPR is met.

Law stated - 12 May 2025

Profiling

Are there any rules regarding individual profiling?

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

According to the GDPR, individuals have the right not to be subject to decisions based solely on automated processing, including profiling, if such decisions have legal consequences or significantly impact them. A decision is considered solely automated if there is no human involvement in the decision-making process. For human intervention to qualify as meaningful, the controller must ensure that the oversight of the decision is meaningful.

However, what makes human involvement meaningful has yet to be clearly defined. In light of recent developments in artificial intelligence, the Dutch DPA is developing [guidelines](#) to determine whether human intervention can indeed be considered meaningful.

Law stated - 12 May 2025

Cloud services

Are there any rules or regulator guidance on the use of cloud computing services?

There are no specific rules on the use of cloud computing services under Dutch law.

Law stated - 12 May 2025

UPDATE AND TRENDS

Key developments of the past year

Are there any emerging trends or hot topics in international data protection in your jurisdiction?

Over recent years, the Dutch Data Protection Authority (Dutch DPA) has focused on five key areas: algorithms and AI, Big Tech, freedom and security, data trade, and the digital government.

Additionally, the Dutch DPA has imposed several large fines on organisations in relation to infringements of the General Data Protection Regulation (GDPR). Among others, a fine of €290 million has been imposed on Uber for breaching article 44 of the GDPR, as Uber allowed transfers of personal data to the United States while not providing appropriate safeguards as stipulated in Chapter V of the GDPR.

Furthermore, at the beginning of 2024, the Dutch DPA announced its intention to enforce stricter measures against misleading cookie banners. The Dutch DPA plans to continue this trend in the coming year, so organisations should ensure their cookie banners comply with the GDPR.

Finally, a key topic was the implementation of the EU AI Act and its interaction with data-protection requirements.

Law stated - 12 May 2025