

VOORBEELD BEWAARTERMIJNEN BELEID – TEMPLATE DATA RETENTION POLICY

Inleiding

In de AVG wordt – net als in de WBP – bepaald dat *persoonsgegevens worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is* [...], art. 5 (1) e AVG.

In combinatie met de verantwoordingsplicht (“accountability”) die volgt uit art. 5 (2) AVG verder is uitgewerkt in art. 24 AVG is het opstellen, implementeren, evalueren en actualiseren van een Bewaartermijnenbeleid of Data Retention Policy een manier om te voldoen aan de verplichting tot opslagbeperking.

Bij het uitvoeren van DPIA is het eveneens een voordeel om te kunnen verwijzen naar een reeds geïmplementeerd Bewaartermijnenbeleid of Data Retention Policy.

Hierna volgt een Engelstalig voorbeeld van een Data Retention Policy. Dit beleid is niet enkel toegespits op de bewaartermijnen die volgen uit de AVG en andere wetgeving. Er is gekozen voor een bredere insteek waarbij aandacht is voor de omgang met informatie, al dan niet persoonsgegevens, binnen de gehele organisatie.

Als bijlage bij het voorbeeld is een lijst aangehecht met mogelijke van toepassing zijnde bewaartermijnen met verwijzing naar de vindplaats in wetgeving. In het daadwerkelijk te implementeren beleid kan deze kolom vervangen worden door de vindplaats van de betreffende gegevens in de systemen van uw organisatie.

LET OP: Informatie over bewaartermijnen dient ook te worden vermeld in de privacy policy / privacy statement (art. 12 en 13 AVG). Indien er gekozen wordt om de bewaartermijn niet te baseren op een concrete termijn, maar op een criterium aan de hand waarvan de bewaartermijn wordt bepaald, dan dient dit criterium te worden opgenomen in de informatie verstrekking aan de betrokkene, art. 13 (2) sub a AVG.

(DRAFT / EXAMPLE) DATA RETENTION POLICY

GENERAL BACKGROUND INFORMATION**1. Purpose of this Policy**

The purpose of this policy is to outline to all employees of [Company Name], you, how [Company Name] would like you to handle the information obtained, collected, used, and received in our systems. This policy is therefore an internal policy and should **not** be shared externally.

This policy is also to inform you how [Company Name], with you as a part of [Company Name], fulfills its data retention obligation as determined by GDPR (General Data Protection Regulation, in Dutch: AVG). This regulation is, as of May 2018, the new European privacy law which regulates how personal data should be processed, and for how long personal data can be stored. This period of use (storage) results in maximum retention periods which is one of the basic principles to obey under GDPR.

Just to make the link between GDPR and this retention policy more clear: as mentioned, GDPR is about the use of personal data. Personal data is all data which identifies or can identify a natural person. This includes, but goes beyond, name/address/email of natural persons. It also includes *[company specific example of customer/client/patient/member data]*. So, within [Company Name] the retention periods are most of the time set by the rules of GDPR as almost all information in our systems relates to identified or identifiable natural persons.

2. Scope of this Policy

This policy is applicable to all information in all of [Company Name]'s systems and applications.

Just for explanatory reasons **information** means:

- Electronic files in any kind of format
- Invoices
- Letters and correspondence
- Contracts
- Documents
- E-mails
- Contact files
- Performance reviews
- Notes, appointments, recordings in any kind of format
- *[Company specific examples]*

In [Company Name]'s systems and applications means accessible, stored, located, documented in:

- Any business systems within [Company Name] such as but not limited to *[name of Company systems used]*, your computer, intranet, mobile phones and so on
- Any business application within [Company Name] such as but not limited to *[specific Company applications used to process financial data, sales data, patients data, members data, marketing data]*, and so on

But please keep in mind that in general this policy also applies to all hand written, hard copy, documents that are not stored in a system as well. Meaning you also need to handle, store and destruct handwritten document, notes or hard copy files that are not stored or are also stored electronically with the utmost care. *[include a warning on clean desk policy or other specific Company rules on handling data, if applicable]*.

3. Primary reason to use information

The retention period for the information we use depends on several things. The primary reason for the use of information is based upon the specific purpose for obtaining, collecting, using, and receiving the information.

Under GDPR we are obliged to determine the purpose of use before obtaining the information. Once determined, we have to stick to that purpose. You cannot re-use information. Or keep it because it is “nice to have for some reason in the future”. If the purpose of use is accomplished, basically the information needs to be deleted after having checked whether there are other legitimate reasons to keep the information. You do not have to do this exercise yourself, we include a Retention Periods Schedule in this policy with maximum retention periods.

What you should however keep in mind:

- Do not re-use information for other purposes than the purpose for which the information is obtained!

For example:

[include a Company specific situation describing the capture of data and what kind of re-use is not allowed]

4. Secondary reason of processing

If and when the original purpose of use is fulfilled, there can be other legitimate reasons to not delete the information straight away. For example:

- Company know how
- Ensuring operational continuity
- Evidence of our rights and obligations
- Protection of our legal interest
- Legal requirements such as bookkeeping obligations, regulatory requirements, labour law related requirements

We have to comply with GDPR, but we also have to comply with other laws which might require us to keep the information in our systems.

What you should however keep in mind:

- If the original purpose of use is achieved, and the personal data in the information is no longer needed for the secondary reason of processing: Anonymize the information

5. Rights of erasure/deletion/ to be forgotten

Under GDPR the natural persons, (known as the **data subject**), do have rights towards *[Company Name]* on the information we have on them.

These rights include the right of erasure, rectification, the right to be forgotten and the right to restriction of processing. Do these rights determine our retention period? No, not on their own, but only if we have to take action on the request of a data subject. These rights are not absolute rights. Meaning that we need to assess on a case by case basis if *[Company Name]* needs to take action (delete) at the request of a data subject.

Therefore we must handle requests from data subjects with the utmost care. In order to exercise their rights, a data subject raises a data subject access request,. A procedure and guidance for this, as well as

template answers, are in place, and can be found [*reference to the place where information on SAR's is published or to the department handling SAR's e.g. the DPO*].

In some cases, requests to be deleted can be refused e.g.:

- if the person still has unpaid invoices
- if we have a dispute or litigation pending with this person
- [*include a company specific reason, check art. 23 GDPR and art. 41 UAVG*]

6. What if we do not follow the data retention rules?

This policy is not just a 'nice to have' set of rules. Both accidental or intentional destruction of information *during* their specified retention period as well as keeping the (personal data) information for longer than their specified retention period could result in:

- Fines and penalties (keeping information too long)
- Loss of rights (early destruction)
- Obstruction of justice charges (early destruction)
- Serious disadvantages in litigation (early destruction)

So we all have to be careful in determining the retention periods together. If possible we will set the retention periods in a system itself to automate the process.

RETENTION PROCEDURE

7. Information not in scope of this Policy

Some information you can discard or delete at your sole discretion. This information is therefore out of scope of this policy. This includes the following:

- Duplicates of originals that have not been annotated
- Preliminary drafts of letters, memo's, reports, worksheets and informal notes that do not represent significant steps or decisions in the preparation of an official record
- Books, manuals, training binders or other printed materials obtained from sources outside [*Company Name*] and retained primarily for reference purposes
- Spam and junk mail
- [*Company specific examples*]

8. Information we cannot store, zero retention period

Please note that there is a category of information which we cannot store at all in our systems. Information with a so called zero retention period. This information is:

- Confidential information from a source outside [*Company Name*], especially if and when disclosing means a violation of a legal or professional obligation of secrecy;
- Civil citizen numbers! Within [*Company Name*] only [*departments*], when [*activity*], can have a civil citizen number in files, which must to be stored in [*secured place, specific description*].

Please contact [*DPO/Legal/CEO/department*] if you come across the following information:

- Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and 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 relating to criminal convictions and offences or related security measures. This data is a special category of personal data (also known as sensitive data) which is prohibited to process unless [Company Name] can use an exemption.

9. Responsibilities for the management of data

[Responsible person, persons or department] is responsible for the correct use, storage and disposal of information in the systems used by [department, group, members]. This not only includes the business systems, business applications but the email boxes, desks, closets or drawer units as well!

[Description of the controls put in place to follow up this responsibility. For example a specific action taken yearly to check the data retention periods, data used etc]

10. How to store, destroy, handle data

Storage: The information should, during the allowed period of use, be stored in a safe, secure and accessible manner. This means that you need to follow the instructions on how to use the business systems and business applications as provided to you in [reference to the manner of place where this instruction is provided for, such as employee handbook]. [Consider to include a reminder on specific ways of storage within the Company].

Archive for documents: We store all contracts, agreements, [summary of company specific documents] and any other document with a legal implication for our company in [name of application or reference to specific location of storage]. This functions as our archive. You can find the instructions for proper filing in this system [reference to a document on how to ensure proper storage of this information].

Archive for databases: We have information in active databases in our business applications. This means that we still work on a regularly basis with this information. As soon as we no longer need to work with this information on a regularly basis, we [include the actions which should be taken]. [include explanation for this re-location action]. The maximum retention periods mentioned in the Retention Periods Schedule do include the archive periods as well. [include the responsible person/department for the decision on the re-locating action].

Special garbage: [if a special secured garbage bin or shredder is available within the company explain here when and how to use it, as well as where it is located].

Destruction: Destruction of information after expiry of its retention period means total irreversible destruction. On your computer this will mean deleting from a file, from your email box, from other files where you kept a copy, from all applications, withdrawing access rights granted if it was a shared document, going over to the other person with whom you shared the document and making sure they have also destroyed the document and, last but not least, emptying your computer bin.

11. Where to raise your questions on this Policy?

If you have any questions, suggestions, remarks, or ideas on how to improve our retention policy please do contact [department/person/DPO].

SCHEDULE OF RETENTION PERIODS

NOTE: this schedule is a dynamic document. Please contact [department/person/DPO] if you have suggestions, questions, and good ideas to improve or amend this schedule or the retention periods mentioned.

NOTE: the retention period is the *maximum* retention period. Within this period the [responsible person/department as indicated in this Policy] should decide when to move the information from the active database to the archive database!

LEGAL BASES below mentioned can be replaced by the physical place the data can be found within the Company

Customer/Patient/Member/Client information		
Type of information	Legal basis	Retention Period
<i>Leads/prospects</i> name address e-mail address telephone number	Art. 5 (1) e GDPR (AVG)	<i>[to be discussed, for how long does this information has value to your sales departement?]</i>
<i>Contracts</i> name address e-mail address telephone number IBAN number location transaction data invoice data <i>[other data related to the contract]</i>	Art. 2:10, 3:15i DCC (<i>Burgerlijk Wetboek</i>) art. 52 GTA (<i>Algemene Wet inzake Rijksbelastingen</i>) art. 5(1) e GDPR (AVG) art. 12, 13 Data Protection Exemption Decree (<i>Vrijstellingsbesluit. Weliswaar ingetrokken, maar wordt door AP ook nog steeds gebruikt om invulling te geven aan bewaartermijnen, geeft slechts een indicatie, goed onderbouwde andere termijnen zijn mogelijk</i>)	2 years after ending of the contractual relationship in active database (<i>depending on the guarantees/liabilities in the contract</i>) than move to archive. Personal data included to be deleted to the extent no longer relevant (unless needed longer to meet a statutory retention obligation) 7 years for recordkeeping purposes (maximum)
<i>Customer Care contact</i> name address e-mail address telephone number reason for contacting Customer Care	Art. 5 (1) e GDPR (AVG)	2 years after resolving the issue (unless deletion is requested earlier, provided that the issue is resolved)
<i>Information in marketing department</i>	Art. 5 (1) e GDPR (AVG)	until unsubscribe (after which new consent can be obtained, or new contracts can be

name address e-mail address		entered into creating a new legal basis to process and store the data for a renewed period)
<i>Subject access request</i> name address [other information obtained]	Art. 5 (1) e GDPR (AVG) Art. 12 (5) GDPR (AVG), in order to determine the repetitive character	12 months after completion of a request
<i>Login and logout data of visitors</i>	Art. 5 (1) e GDPR (AVG) Art. 37 Data Protection Exemption Decree (Vrijstellingsbesluit. Zie eerdere opmerking)	6 months after the data of visit
<i>Member data or benefactor data</i>	Art. 3 Data Protection Exemption Decree (Vrijstellingsbesluit. Zie eerdere opmerking)	3 years as from end of the membership or notice on the end of benefactor relationship
Recruitment information		
Type of information	Legal basis	Retention Period
<i>Applicant data</i> name address e-mail address telephone number resume photo motivation letter	Art. 5 (1) e GDPR (AVG) art. 5 Data Protection Exemption Decree (Vrijstellingsbesluit. Zie eerdere opmerking)	4 weeks after recruitment procedure has ended (meaning [Company Name] hired someone on this position) With freely informed actively given permission of the applicant: max 1 year after recruitment procedure has ended
Employee information		
Type of information	Legal basis	Retention Period
<i>Information regarding wage tax, withholding tax, including copy of employee ID including civil citizen number (BSN)</i>	Art. 12.1 (5), 7.5 (4) of the Implementing Regulations for the Wages and Salaries Tax Act 2011 (Uitvoeringsregeling Loonbelasting 2011)	5 years after termination of the employment agreement

<i>HR-data / employee file</i> Data of employment payslips employment contract user agreement lease contract declaration of commuting distance	Art. 52 (4) GTA (<i>Algemene Wet inzake Rijksbelastingen</i>)	7 years after termination of the employee agreement
<i>Copy of ID of a temporary agency worker who is non-EU/EEA citizen</i>	Art. 15 of the Foreign Nationals Employment Act (<i>Wet arbeid Vreemdelingen</i>)	5 years from the year following the year in which the temporary agency work of the foreign national was terminated at the recipient company
<i>Performance reviews</i> <i>Illness</i> Administrative data Date of reporting sick Date of recovery	Art. 5 (1) e GDPR (AVG) art. 7 Data Protection Exemption Decree (<i>Vrijstellingsbesluit. Zie eerdere opmerking</i>)	2 years after termination of the employee agreement
<i>Pension administration</i>	art. 169 Pension Act (<i>Pensioenwet</i>)	minimum 7 years after the financial year to which the information refers After termination of employment agreement in archive database permanently
Rehabilitation file	Par. 6.1 of the “Guidelines for processing health data of employees who are ill” – DDPA, 23 February 2016 (<i>De zieke werknemer – Beleidsregels voor de verwerking van persoonsgegevens over de gezondheid van zieke werknemers</i>)	2 years after the completion of the rehabilitation

Corporate information		
Type of information	Legal basis	Retention Period
<i>Information to employees</i> All policies, guidelines, statement and internal regulations, matrixes, plans (key), handbook, overviews, forms	Art. 5 (1) e GDPR (AVG)	3 years after validity has ended (or another period as determined internally)
annual plan including objectives, audit program, audit planning, internal audit report, external audit report	Art. 5 (1) e GDPR (AVG)	3 years after validity has ended (or another period as determined internally)
financial reports, company accounts, books of accounts and records, profit and loss accounts, information relevant to the company's tax position and tax liabilities	Art. 2:10, 3:15i DCC (<i>Burgerlijk Wetboek</i>) art. 52 GTA (<i>Algemene Wet inzake Rijksbelastingen</i>)	7 years Upon preparation of company accounts Once the profit and loss accounts has lost its actual value Following the fiscal year to which the information relevant to the company's tax position relates
register on security incidents, reports on security incidents	Art. 5 (1) e GDPR (AVG)	clean up every other year, due to the learning purpose of the register
results of penetration test	Art. 5 (1) e GDPR (AVG)	3 years after publishing
insurance claims, insurance disbursements, insurance contracts and policies, IP registrations, real estate documents, articles of incorporation, bylaws, board policies, resolutions, meeting minutes	Art. 5 (1) e GDPR (AVG)	permanent
Real estate documents	art. 34a VAT Act (<i>Wet op de Omzetbelasting</i>)	minimum 9 years following the year in which the relevant real estate was used by this the business for the first time

Business / operational information		
Type of information	Legal basis	Retention Period
<i>supplier list and files, corporate customer list and files</i> contracts / SLA NDA DPA supplier assessment form	Art. 52 GTA (<i>Algemene Wet inzake Rijksbelastingen</i>) Art. 1:32 General Customs Act (<i>Douanewet</i>) Art. 2:10, art. 3:15i DCC (<i>Burgerlijk Wetboek</i>)	2 years after contract has ended in active database (longer if liabilities continue after termination) than move to the archive 7 years for tax and bookkeeping reasons
Monitoring data		
Type of information	Legal basis	Retention Period
<i>Logging (ict)</i> use of business systems business applications use of devices provided by [Company Name]	Art. 5 (1) e GDPR (AVG)	6 months after capturing the data, unless the purpose of use is not accomplished yet
<i>Video- and audio, CCTV</i> video images	art. 38 (6) Data Protection Exemption Decree (<i>Vrijstellingsbesluit. Zie eerdere opmerking</i>)	4 weeks (unless there is a need to keep the data e.g. for law enforcement, investigation)
Miscellaneous		
Several specific member, patient, customer, client data	Several sector specific laws (o.a. 7:454 BW voor medische dossiers -15 jaar of Arbeidsomstandighedenbesluit inzake werken met bepaalde stoffen – 3 tot 40, 41, 42, 43 jaar na blootstelling)	various

Hulp nodig bij het op maat maken van een Bewaartermijnenbeleid of Data Retention Policy?

Wij helpen graag!

www.privacy-advocaat.nl

Alle informatie van www.privacy-advocaat.nl is met zorg samengesteld, maar wij garanderen niet dat de informatie juist, volledig en voor uw situatie passend is. De interpretatie van privacywetgeving is aan verandering onderhevig en hangt af van feiten en omstandigheden. Voor een passend en actueel advies verzoeken wij u contact op te nemen.