

Privacy in de organisatie

Asiya Baher, Meindert Boon, Whitney Naomi van den Brand,
Coosje Jeekel, Gerda Salaroe, Jean Paul van Schoonhoven,
Mike Tiernagan, Sébastian van der Veen

Privacy in de organisatie

Handboek voor AVG-compliance en
risicogestuurd eigenaarschap



Privacy in de organisatie

Jean Paul van Schoonhoven e.a.

Eerste druk, augustus 2026

Auteursfoto's: studio Viorica Cernica - vioricacernica.com

© Berghauser Pont Publishing, Amsterdam, 2026

www.berghauserpont.nl

ISBN: 9789493376236

NUR: 823



Behoudens de in of krachtens de Auteurswet van 1912 gestelde uitzonderingen mag niets uit deze uitgave worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand, of openbaar gemaakt, in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen of enig andere manier, zonder voorafgaande schriftelijke toestemming van de uitgever.

No parts of this book may be reproduced in any way whatsoever without the written permission of the publisher.

Voorwoord

Bij mijn eerste kennismaking met privacy, als student-assistent bij de vaksectie Recht en IT, raakte het onderwerp mij totaal niet. Zoals de meeste mensen heb ik behoefte aan een eigen identiteit en een eigen levenssfeer en daarmee ook affiniteit met dit onderwerp. Maar vage begrippen als ‘voorzover nodig’ om te bepalen of een verwerking wel of niet is toegestaan, kwamen mij als jurist en econoom toch wat onbepaald en dus ongemakkelijk voor.

Toch greep het onderwerp mij langzaamaan. Niet in het minst vanuit mijn vroegere rol als beleidsmedewerker bij het College bescherming persoonsgegevens. Maar het kriebelde en die jeuk is eigenlijk nooit overgegaan. Ik vroeg me vaak af: hoe kan ik van iets ongemakelijks iets positiefs maken? De mensen die mij wat beter kennen weten dat dit een rode draad is die al heel lang door mijn leven loopt.

In het verleden schreef ik al diverse artikelen en stelde ik een aantal publicaties samen zoals een uitsprakenbundel, wettenverzameling en een jurisprudentietijdschrift. Het idee voor dit handboek is dan ook niet recent. Tijd ervoor vrijmaken wel. Want zoals veel organisaties leg ik de lat voor mezelf hoger dan de beschikbare tijd en de vereiste diepgang samen toelaten. Toch is het uiteindelijk gelukt om van mijn ambitie een publicatie te maken waarmee elke lezer de open normen van privacyregelgeving concreet en beheersbaar kan maken. Privacy is geen ‘salononderwerp voor linkse juristen’ maar juist een wezenlijke bedrijfskundige factor die voor elke organisatie van belang is. Groot of klein, publiek of privaat.

Is dit boek helemaal af? Nee. De lezer zal ontdekken dat dit boek, net als het leven zelf, een te voltooien bouwwerk is. Dat geldt net zo goed voor de inhoud die ik samen met Asiya, Coosje, Gerda, Meindert, Mike, Sébastian en Whitney Naomi heb opgeschreven. Al ben ik persoonlijk wel blij dat ik, anders dan Antoni Gaudí, de voltooiing van dit bouwwerk nog bij leven heb mogen aanschouwen.

Tot slot een bijzonder woord van dank aan mijn vrouw Cosmina, voor het achter mijn broek aanzitten, voor het incasseren van mijn urenlange geplak achter de laptop en voor het meedenken over en samenstellen van de grafische afbeeldingen in dit boek. Te iubesc.

Jean Paul van Schoonhoven

1 juli 2026

Inhoudsopgave

Voorwoord	V
Inleiding	1
DEEL I	
PRIVACYMANAGEMENT ALS STRATEGIE	
1 Achtergrond van de AVG	
1.1 Privacy als begrip	7
1.2 De AVG	10
1.3 Waarom de AVG nodig was	10
1.4 Strategische en tactische inzichten voor het management	13
2 Waarom de compliancereis starten?	
2.1 Compliance als business enabler	15
2.2 De relatie tussen het Thomas-theorema, data-obesitas en systeem-denken	16
2.3 Compliance als systeemverandering	18
2.4 Het fundament van het Privacy Huis leggen	22
2.5 Strategische en tactische inzichten voor het management	22
3 Het bouwen van het Privacy Huis	
3.1 Van los zand tot fundament	25
3.2 Zorg voor governance, normenkaders en volwassenheid	27
3.3 De meest voorkomende valkuilen bij het bouwen	30
3.4 Wat maakt het bouwen wel tot een succes?	32
3.5 Het Privacy Huis en de governance volgens het Three Lines Model	33
3.6 Het fundament van het Privacy Huis	34
3.7 Strategische en tactische inzichten voor het management	34
4 Het leggen van het fundament	
4.1 Aantoonbaarheid als fundament	37
4.2 De PDCA-cyclus als onderdeel van het besturingsmechanisme	38
4.3 Risicosturing als fundament voor goed bestuur	41
4.4 Risicobereidheid en privacy-volwassenheidsniveaus	48
4.5 Passende technische en organisatorische maatregelen: opzet, bestaan en werking	55

4.6	De uitvoeringskosten van maatregelen laten meewegen	59
4.7	De governance van het risicogestuurd managen volgens het Three Lines Model	61
4.8	Strategische en tactische inzichten voor het management	66

DEEL II

HET PRIVACY HUIS ALS PRIVACY MANagementsYSTEEM

5 De bouwstenen van de AVG

5.1	Artikel 2-3: het materiële en territoriale toepassingsgebied van de AVG	71
~	Wanneer is de AVG van toepassing?	72
~	Checklist voor deze bouwsteen van het Privacy Huis	78
5.2	Art. 5-11: beginselen inzake verwerking van persoonsgegevens	81
~	De beginselen van de AVG	82
~	Hoe ga je om met de beginselen	84
~	De verantwoordingsplicht of het aantoonbaarheidsvereiste	105
~	Grondslagen van de verwerking	107
~	Gewone, gevoelige of bijzondere persoonsgegevens	119
~	Checklist voor deze bouwsteen van het Privacy Huis	123
5.3	Art. 12-14: Transparantie en communicatie	131
~	Transparantie vanuit het oogpunt van betrokkenen	132
~	Hoe moet informatie worden aangeboden?	133
~	Wanneer moet informatie worden aangeboden?	138
~	Welke informatie moet worden verstrekt?	140
~	Uitzonderingen op de informatieplicht	144
~	Checklist voor deze bouwsteen van het Privacy Huis	148
5.4	Rechten van betrokkenen (artikel 15-22 AVG)	151
~	De rechten van betrokkenen in het kort	152
~	Algemene regels bij elk verzoek	152
~	Recht op inzage (art. 15)	156
~	Recht op rectificatie (art. 16)	157
~	Recht op gegevenswissing, het 'recht op vergetelheid' (art. 17)	158
~	Recht op beperking van de verwerking (art. 18)	159
~	Kennisgevingsplicht (art. 19)	160
~	Recht op overdraagbaarheid van gegevens (art. 20)	161
~	Recht van bezwaar (art. 21)	162
~	Geautomatiseerde individuele besluitvorming en profilering (art. 22)	163
~	Checklist voor deze bouwsteen van het Privacy Huis	166

5.5	Uitzonderingen op de informatieplicht, de rechten en de meldplicht (artikel 23 AVG)	168
~	Uitzonderingen zijn mogelijk, maar nooit vanzelfsprekend	169
~	Een beroep op een uitzondering is tijdelijk	170
~	De noodzakelijkheids- en evenredigheidstoets	170
~	Checklist voor deze bouwsteen van het Privacy Huis	171
5.6	Het privacybeleid (artikel 24 AVG)	172
~	Privacybeleid	173
~	Opstellen en structuur van het privacybeleid	175
~	Vaststellen, implementeren, adopteren en beheren	177
~	Checklist voor deze bouwsteen van het Privacy Huis	178
5.7	Privacy by design en default (artikel 25 AVG)	180
~	Vooruitzien is ontzorgen	182
~	De elementen van artikel 25 AVG	183
~	De zeven basisprincipes van privacy by design	183
~	Ontwerpstrategieën om tot maatregelen te komen	183
~	Van strategie naar maatregel: een organisatiebrede aanpak	184
~	Verwerking van bijzondere of gevoelige persoonsgegevens	185
~	Checklist voor deze bouwsteen van het Privacy Huis	187
5.8	Privacy-overeenkomsten (artikel 26-28 AVG)	188
~	Het maken van schriftelijke afspraken	188
~	Het bepalen van de rollen	190
~	Het selecteren van verwerkers	195
~	Het monitoren van verwerkers	195
~	De verwerkersovereenkomst (artikel 28)	195
~	De onderlinge regeling (artikel 26)	196
~	De overeenkomst tussen twee zelfstandige verwerkingsverantwoordelijken	198
~	Checklist voor deze bouwsteen van het Privacy Huis	199
5.9	Het register van verwerkingsactiviteiten (artikel 30 AVG)	200
~	Inzicht met het verwerkingsregister	201
~	De verplichtingen voor de verwerkingsverantwoordelijke	201
~	De verplichtingen voor de verwerker	202
~	De uitzondering op de registerplicht	202
~	Naar een actueel, juist en volledig verwerkingsregister	202
~	Samenhang met andere verplichtingen	203
~	Tools en hulpmiddelen	205
~	Checklist voor deze bouwsteen van het Privacy Huis	205

5.10	Artikel 32: de beveiliging van persoonsgegevens	206
~	Beveiligen van informatie en persoonsgegevens	207
~	De eisen aan de beveiliging van persoonsgegevens	208
~	Het beoordelen van risico's	211
~	Governance en eigenaarschap	214
~	Checklist voor deze bouwsteen van het Privacy Huis	217
5.11	Artikel 33 en 34: de meldplicht datalekken	218
~	De meldplicht datalekken	219
~	De meldplicht bij de AP	222
~	De meldplicht bij betrokkene	223
~	Oorzaken datalekken	224
~	Kosten van een datalek	226
~	Beheersen van de risico's	227
~	Een stappenplan voor een effectieve werking van de meldplicht datalekken	229
~	Checklist voor deze bouwsteen van het Privacy Huis	232
5.12	Artikel 35: de gegevensbeschermingseffectbeoordeling (DPIA)	233
~	Achtergrond van de DPIA	234
~	Positionering en governance van de DPIA	235
~	Verplichte DPIA op grond van art. 35 lid 3 AVG	235
~	De criteria van de EDPB en de AP	236
~	De inzet van de pre-DPIA als beslisinstrument	242
~	Aan welke eisen moet een DPIA voldoen?	243
~	Het uitvoeren van het DPIA-proces	244
~	Het beheer van uitgevoerde DPIA's	248
~	Bundeling van vergelijkbare verwerkingen in één DPIA	249
~	Lessen uit de praktijk bij het uitvoeren van een DPIA	250
~	Checklist voor deze bouwsteen van het Privacy Huis	255
5.13	Artikel 36: de voorafgaande raadpleging	256
~	De verplichting tot voorafgaande raadpleging	256
~	De procedure bij de AP	258
~	Inhoudelijke beoordeling door de AP	258
~	Checklist voor deze bouwsteen van het Privacy Huis	261
5.14	Artikel 37-39: de FG	262
~	De FG als verplichte toezichthouder	263
~	Benoeming van de FG	265
~	Vrijwillige aanstelling of één FG voor meerdere organisaties	269
~	Professionele kwaliteiten en FG als externe dienstverlening	270
~	Positionering van de FG	271
~	Taken van de FG	277

~	De coördinerend FG binnen samenwerkingsverbanden	279
~	Strategische rol van de FG binnen het Privacy Huis	282
~	Checklist voor deze bouwsteen van het Privacy Huis	285
5.15	Internationale doorgiften (art. 44-50 AVG)	288
~	Wat is een internationale doorgifte?	289
~	Waarom rechtmatig doorgeven ertoe doet	290
~	De AVG verbiedt doorgifte niet, maar stelt randvoorwaarden	291
~	Hoe geef je rechtmatig door: de doorgifte-instrumenten	292
~	De rol van de Schrems-uitspraken en de transfer impact assessment	294
~	De huidige status: AP, EDPB en Europese Commissie	294
~	De relatie met het perspectief van het handboek	295
~	Checklist voor deze bouwsteen van het Privacy Huis	296

DEEL III

BEHEER EN ONDERHOUD VAN HET PRIVACY HUIS

6	Het beheren en onderhouden van het Privacy Huis	
6.1	Van bouwen naar beheren	301
6.2	Aantoonbaar voldoen via de PDCA-cyclus	304
6.3	Het Three Lines Model toegepast op beheer en onderhoud	306
6.4	Risicogestuurd kiezen wat je onderzoekt: de risicomatrix	311
6.5	De vier beheers- en onderhoudsacties	314
6.6	Veelvoorkomende valkuilen bij beheer en onderhoud	325
6.7	Groeien in privacyvolwassenheid door iteratie	326
6.8	Checklist voor beheer en onderhoud van het Privacy Huis	330
7	GenAI, de AI-verordening en andere data-ontwikkelingen: verandert de aanpak?	
7.1	Een veranderend landschap	333
7.2	De AI-verordening op hoofdlijnen	336
7.3	Waar de AI-verordening ingrijpt op het Privacy Huis	338
7.4	De vier onderhoudsacties toegepast op AI	340
7.5	De rol van de FG en de Privacy Officer	341
7.6	Andere data-ontwikkelingen op hoofdlijnen	342
7.7	Zijn de datawetten compatibel met de aantoonbare PDCA-aanpak?	344
7.8	Checklist voor AI- en datawetgeving in het Privacy Huis	347

8	Materieel voldoen aan de AVG: van het bouwen naar het bewonen van het Privacy Huis	
8.1	Formeel versus materieel voldoen	349
8.2	De dagelijkse praktijk: het probleem	350
8.3	Het materiële toetsingskader dat de eerste lijn kan leren	355
8.4	Checklist voor materieel voldoen aan de AVG	360
	Nawoord	363
	Trefwoordenregister	365
	Over de auteurs	371