Externe gegevensverwerkers – technische en organisatorische maatregelen

Precontractuele activiteiten, contractonderhandelingen en postcontractuele activiteiten

Door: Kennisgroep Privacy & GDPR

Privacy incidenten, datalekken van persoonsgegevens, boetes van nationale en internationale toezichthouders en veranderingen in (internationale) privacywetgeving zijn aan de orde van de dag. Voor privacy-professionals is het soms lastig om de impact hiervan op hun organisatie goed in te schatten. De kennisgroep Privacy & GDPR[1] zal de komende periode verschillende checklists uitbrengen rondom actuele privacy onderwerpen. Deze onderwerpen zijn gebaseerd op de ISACA ledenenquête in 2020. In dit artikel kijken we specifiek naar de technische en organisatorische maatregelen die nodig zijn bij de verwerking van persoonsgegevens door een externe gegevensverwerker (hierna 'verwerker').

De Algemene verordening gegevensbescherming[2] (AVG) heeft onder andere tot doel een vrij verkeer van persoonsgegevens in de EU te bewerkstelligen alsook hierbij een consistent niveau van bescherming te bieden bij de verwerking hiervan. De eindverantwoordelijkheid voor de verwerking van persoonsgegevens ligt bij de verwerkingsverantwoordelijke. Bij de verwerking van persoonsgegevens kunnen ook andere partijen betrokken zijn om namens de verwerkingsverantwoordelijke gegevens te verwerken.[3]
Art. 28 lid 1 AVG geeft aan dat een verwerkingsverantwoordelijke uitsluitend een beroep op een verwerker mag doen die afdoende garanties kan bieden met betrekking tot het toepassen van technische en organisatorische maatregelen. Voordat een verwerker gecontracteerd wordt, is het dus nodig om na te gaan of deze verwerker deze van toepassing zijnde organisatorische en technische maatregelen ter bescherming van de persoonsgegevens kan bieden (‘due diligence’[4] - zorgvuldigheidseisen), die tevens contractueel moeten worden vastgelegd. Deze stap voorkomt dat er bij of na contractonderhandelingen over de verwerking van persoonsgegevens discussies ontstaan omdat een verwerker niet in staat blijkt aan de contractuele verplichtingen te voldoen. Nadat een verwerker gecontracteerd is, zijn er tevens activiteiten nodig om, gedurende de verwerking van persoonsgegevens, te waarborgen dat de vereiste technische en organisatorische maatregelen adequaat geïmplementeerd zijn en gevolgd worden door de verwerker. Het selecteren van de juiste technische en organisatorische maatregelen kan via een risico-gebaseerde methode, waarbij bijvoorbeeld rekening gehouden wordt met de aard van de verwerking, de opslag van de gegevens en het land waarin de verwerker opereert.

Het proces van contracteren en managen van een nieuwe verwerker kan op verschillende manieren worden ingericht. In dit artikel laten we een proces om potentiële organisaties te identificeren (Request for Information (RFI) / Request for Proposal (RFP) en dergelijke) buiten beschouwing. In dit stuk wordt uitgegaan van de volgende fases:

---

[1] GDPR is de General Data Protection Regulation (Algemene verordening gegevensbescherming) en door middel van de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG) in Nederland geïmplementeerd.
[2] Verordening (EU) 2016/679 bescherming natuurlijke personen i.v.m. verwerking persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG.
[3] Art. 28 AVG.
[4] Reasonable steps taken by a person in order to satisfy a legal requirement, especially in buying or selling something.

- precontractuele activiteiten (due diligence) van een nieuwe verwerker die men op het oog heeft;
- het opstellen van het contract (inclusief de noodzakelijke verwerkingsovereenkomst[5]);
- postcontractuele activiteiten (waaronder verificatie dat de vereiste technische en organisatorische adequaat door de verwerker geïmplementeerd zijn).

Voor alle drie bovenstaande fases moet uiteraard (in redelijke mate) duidelijk zijn welke verwerkingsactiviteiten de verwerker gaat uitvoeren. Art. 28 lid 5 AVG geeft overigens aan dat aansluiting van de verwerker bij een goedgekeurde gedragscode of certificeringsmechanisme kan dienen om aan te tonen dat de verwerker voldoende garanties biedt in de zin van art. 28 lid 1 of lid 4 AVG. In dat geval kan wellicht de due diligence, maar ook het postcontractuele toezicht minder streng zijn omdat een verwerker door het voldoen aan de eisen van een gedragscode en/of certificering al adequate technische en organisatorische maatregelen genomen heeft en dit aan kan tonen.

Precontractuele activiteiten

Voordat een verwerkingsverantwoordelijke een contract met een verwerker afsluit, is het noodzakelijk om na te gaan of deze verwerker aan de door verwerkingsverantwoordelijke gestelde eisen kan voldoen. Dit is een situationele evaluatie, afhankelijk van bijvoorbeeld:

- wet- en regelgeving waaraan verwerkingsverantwoordelijke moet voldoen naast de AVG;
- de te treffen maatregelen die passen bij de aard en de gevoeligheid van de te verwerken persoonsgegevens, binnen de specifieke verwerkingsactiviteiten;
- eventuele transporten van persoonsgegevens (bijvoorbeeld elektronisch via Internet).

Een gebruikelijke methode is om de potentiële verwerker te vragen een standaard vragenlijst in te vullen. Via de vragenlijst worden dan de te verwachten technische en organisatorische maatregelen bevraagd. Het hoeft overigens niet zo te zijn dat de verwerker aan alle eisen moet voldoen. Als een organisatie bijvoorbeeld een verwerker contracteert om (uiteindelijk) geanonimiseerde vragenlijsten te verwerken met feedback van websites, dan geeft dat meestal een ander risicoprofiel in vergelijking met een verwerker die ingehuurd wordt om volledig identificeerbare medische dossiers te verwerken.
Indien een verwerker niet aan alle eisen voldoet, kan eventueel een organisatie in dit stadium een voorwaardelijke goedkeuring geven om de nieuwe verwerker te contracteren. Bijvoorbeeld onder voorbehoud dat de verwerker binnen een gestelde periode interne maatregelen gaat nemen om wel aan alle eisen te voldoen. Over het algemeen moet de verwerker de maatregelen adequaat geïmplementeerd hebben, voordat daadwerkelijk persoonlijke informatie verwerkt gaat worden. Indien de verwerking een hoog risico vormt voor de verwerkingsverantwoordelijke (bijvoorbeeld: veel gevoelige data, strikte wettelijke eisen) dan kan een precontractuele inspectie (‘audit’) op zijn plaats zijn.

Opstellen van het contract

Bij het opstellen van een contract zijn een aantal zaken belangrijk. Er zal allereerst gekeken moeten worden naar de verwerkingsactiviteiten en bijvoorbeeld de wettelijke, bedrijfsmatige, technische en organisatorische eisen die gesteld moeten worden aan de verwerking van persoonsgegevens. Als er risico's geïdentificeerd worden, bijvoorbeeld omdat deze al intern bepaald waren of specifiek bepaald worden bij het inschakelen van deze verwerker (al dan

[5] Art. 28 lid 3 en art. 28 lid 9 AVG.

niet in een gegevensbeschermingseffectbeoordeling[6]) kunnen die in het contract opgenomen worden met de mitigerende maatregelen. Een auditrecht moet standaard in het contract opgenomen worden, zodat de verwerkingsverantwoordelijke altijd kan nagaan of de verwerker zich aan de contractuele bepalingen houdt.
Er zal tevens voldaan moeten worden aan de overige eisen in art. 28 lid 3 en lid 9 AVG inzake de overeenkomst tussen de verwerkingsverantwoordelijke en de verwerker. Mochten persoonsgegevens internationaal en naar buiten de Europese Unie verplaatst worden, dan moet nagedacht worden over de te gebruiken transportmechanismen.[7] Het moge duidelijk zijn dat indien een verwerker die bijvoorbeeld IT-ondersteuning levert vanuit een derde land, zoals India, en daarbij wellicht persoonsgegevens ziet, dit ook als verwerken van persoonsgegevens beschouwd wordt.[8] Dit in het kader van de Schrems II beslissing.[9] De verwerker zal uiteraard goed notie moeten nemen van hoe de contractuele bepalingen geïmplementeerd moeten worden om te voldoen aan het contract, inclusief het eventueel teruggeven van gegevens of het (deels) vernietigen daarvan na beëindiging van het contract.

Postcontractuele activiteiten

Dan wellicht de meest belangrijke fase: de uitvoering van het contract. De verwerkingsverantwoordelijk blijft, ondanks de uitbesteding van de werkzaamheden, verantwoordelijk voor het verwerken van de persoonsgegevens die plaatsvinden door de verwerker. Er zal dus ook voldoende en regelmatig toezicht moeten plaatsvinden om te waarborgen dat de door de verwerker genomen technische en organisatorische maatregelen blijvend effectief zijn. Dit toezicht kan risico- maar ook kwaliteitgedreven zijn met kritieke prestatie indicatoren (KPIs). Uiteraard moet bepaald worden wat de risico's bij de verwerking zijn, deze risico's moeten waar nodig gekwantificeerd worden en waar nodig gemitigeerd en het restrisico uiteindelijk geaccepteerd door de verwerkingsverantwoordelijke. Deze risicoanalyse moet de hele levenscyclus van de verwerking van persoonlijke gegevens omspannen, van verzamelen, opslaan tot verwijderen.[10]
Over het algemeen zal de verwerkingsverantwoordelijke een plan moeten maken hoe het toezicht uitgeoefend gaat worden. Daarin kan onder andere bepaald worden:

- welke rapportage (kwaliteit, incidenten, klachten, uitoefening rechten) er periodiek moet plaatsvinden door de verwerker;
- eventueel inzien van documentatie die contractueel vereist zijn (beveiliging, data vernietigingscertificaten);
- de beveiliging van het transport van persoonlijke gegevens;
- hoe het monitoren van risico's plaats zal vinden;
- het verder contracteren en uitvoering door sub-verwerkers.

Hoe gedetailleerd een dergelijk plan van toezicht moet zijn is onder andere afhankelijk van: hoeveelheid persoonsgegevens, gevoeligheid van de gegevens, wettelijke eisen, interne/externe verwerking (bijvoorbeeld via internet), vastgestelde risico's, waar gegevens verwerkt worden en eisen gesteld aan de beveiliging.
Een onderdeel van en vaak sluitstuk bij de uitvoering van een contract is het uitvoeren van een audit tijdens de verwerking van persoonsgegevens. Ook hiervoor kan een risico-gebaseerde aanpak mogelijk zijn. Wellicht hoeft een derde partij waarbij, naar de aard van de verwerking, het verwerkingsrisico laag is, niet geauditeerd te worden. Een voorbeeld kan de

[6] Art. 35 AVG.
[7] Hoofstuk V AVG (Doorgiften van persoonsgegevens aan derde landen of internationale organisaties).
[8] Art. 4(2) "verwerking" is breed gedefinieerd.
[9] Schrems II refereert aan de uitspraak van het Hof van Justitie van de Europese Unie (HvJ-EU) op de klacht van dhr. Schrems (C-311/18). Zie de ISACA site voor meer informatie.
[10] Art. 4(2) AVG: "verwerking" is breed gedefinieerd.

verwerking van geringe hoeveelheden beperkte zakelijke gegevens zijn. Een derde partij die grote hoeveelheden gevoelige gegevens verwerkt, bijvoorbeeld medische gegevens, zal mogelijk periodiek en frequent geauditeerd moeten worden. Ook kunnen externe factoren hierbij een rol spelen alsook de uitslagen van vorige audits of indien een verwerker gecertificeerd is en de verwerkingsverantwoordelijke dit certificaat erkent.

ISACA Privacy Principes

Binnen onze beroepsorganisatie ISACA worden privacy ontwikkelingen over de gehele wereld gevolgd. Dit heeft in 2016 geleid tot de publicatie "ISACA Privacy Principles and Program Management Guide". In deze publicatie zijn naast privacy risico's ook de vereisten per regio en specifiek voor sommige landen opgenomen. Om zorg te blijven dragen voor een overzichtelijke aanpak van privacy is gekozen voor privacy principes die aansluiten bij het Core Cobit Framework.

Dit artikel is gemaakt door leden van de ISACA-kennisgroep Privacy & GDPR. Deze kennisgroep is in het leven geroepen om verdieping aan te brengen in de verschillende onderwerpen die er spelen rondom privacy, in het algemeen en specifiek de AVG. Vanuit een veertiental ISACA Privacy Principes lichten wij periodiek een belangrijk onderwerp rondom privacy op een begrijpelijke manier toe met praktische handvatten voor de ISACA-professional in de Nederlandse taal.

Een korte checklist[11] hieronder kan behulpzaam zijn bij de verdere invulling van maatregelen en de aandachtspunten bij het contracteren van een verwerker van persoonsgegevens.

ISACA Privacy Principe[12]	Verwerkingsverantwoordelijke	Verwerker van persoonsgegevens
1. Vrije keuze en toestemming	✓ Verwerkingsverantwoordelijke: ⬢ A: aanbieden van vrije keus, maar meestal alleen waar toestemming de wettelijke grondslag is (art. 7 AVG). ⬢ B: vragen van toestemming waar dat de wettelijke grondslag is (art. 6 AVG).	✓ Het ontwerp voor het geven van de vrije keus en eventueel vragen van toestemming kan (contractueel) gedelegeerd worden aan de verwerker.
2. Wettelijke grondslag, specificatie en beperking	✓ Het bepalen van de wettelijke grondslag (art. 6 AVG) en doeleinde van de verwerking is aan de verwerkingsverantwoordelijke.	✓ Over het algemeen geen rol voor de verwerker, tenzij de verwerker ook onder een wettelijke regeling valt (art. 6 lid 1 sub c AVG).
3. Levenscyclus gegevens	✓ Verwerkingsverantwoordelijke bepaalt bij de verwerking van persoonsgegevens het:[13] - vastleggen (verzamelen); - bewaren; - gebruiken; - delen; - archiveren; - verwijderen. ✓ Verwerkingsverantwoordelijke houdt toezicht op de gehele verwerking.	✓ De verwerker voert altijd alleen uit per contract of bij wet.

[11] Met de checklist beogen de auteurs de belangrijkste elementen in te vullen. Een checklist is geen garantie op volledigheid.
[12] https://www.isaca.org/resources/news-and-trends/industry-news/2017/using-isaca-privacy-principles-for-gdpr-compliance.
[13] Art. 4(2) AVG: "verwerking" is breed gedefinieerd.

ISACA Privacy Principe[12]	Verwerkingsverantwoordelijke	Verwerker van persoonsgegevens
4. Juistheid en kwaliteit	✓ Verwerkingsverantwoordelijke bepaalt de van toepassing zijnde criteria voor kwaliteit en nauwkeurigheid. ✓ Verwerkingsverantwoordelijke houdt toezicht.	✓ Over het algemeen als contractueel overeengekomen. ✓ Waar nodig rapportage aan de verwerkingsverantwoordelijke.
5. Openheid, transparantie, communicatie	✓ De verwerkingsverantwoordelijke is verantwoordelijk voor het verstrekken van informatie aan betrokkenen.[14]	✓ Verwerkingsverantwoordelijke kan aspecten van verstrekken van informatie delegeren aan de verwerker, per contract.
6. Rechten van betrokkenen	✓ Rechten van de betrokkenen zal (o.a. aan de hand van wettelijke grondslag) door verwerkingsverantwoordelijke bepaald moeten worden. ✓ Verwerkingsverantwoordelijke moet een proces inrichten zodat betrokkenen rechten kunnen uitoefenen.	✓ Waar contractueel gedelegeerd moet verwerker een proces inrichten van hoe betrokkenen rechten kunnen uitoefenen. ✓ Waar nodig zal verwerker een proces moeten inrichten zodat goedgekeurde verzoeken van betrokkenen geïmplementeerd kunnen worden.
7. Verant-woordelijkheden	✓ Verwerkingsverantwoordelijke is primair verantwoordelijk.	✓ Verwerker heeft contractuele verantwoordelijkheden en verder zoals gespecificeerd in art. 28 AVG.[15]
8. Beveiligings-maatregelen	✓ Verwerkingsverantwoordelijke zal adequate beveiligingsmaatregelen moeten inrichten of daarop moeten toezien (art. 32 AVG).	✓ Verwerker zal de contractuele gespecificeerde beveiligingsmaatregelen (minimaal) moeten implementeren.
9. Meten, monitoren, rapporteren	✓ Verwerkingsverantwoordelijke zal een plan moeten maken om na te gaan of de ingerichte controles (incluis bij de verwerker) adequaat zijn.	✓ Verwerker moet, zoals contractueel overeengekomen, van toepassing zijnde KPIs (kritieke prestatie indicatoren) en andere gespecificeerde metrics en data rapporteren aan de verwerkingsverantwoordelijke.
10. Voorkomen van schade	✓ Vereist geen additionele maatregelen. ⬢	✓ Vereist geen additionele maatregelen. ⬢
11. Derde partijen (verwerker)	✓ Verwerkingsverantwoordelijke moet een overeenkomst met verwerker(s) (de derde partij) afsluiten. ✓ De overeenkomst zal de verwerking en de te nemen maatregelen voldoende nauwkeurig moeten beschrijven.	✓ De verwerker mag alleen andere derde partijen als verwerker inschakelen na toestemming van de verwerkingsverantwoordelijke (art. 28 lid 2 AVG).

[14] Hoofdstuk III (Rechten van de betrokkene) AVG.
[15] Art. 30(2) (Register van de verwerkingsactiviteiten) en (indien van toepassing) 37 AVG geven nadere en zelfstandige verantwoordelijkheden aan de verwerker.

ISACA Privacy Principe[12]	Verwerkingsverantwoordelijke	Verwerker van persoonsgegevens
12. Inbreuken, incidenten	✓ Verwerkingsverantwoordelijke zal een proces moeten inrichten ter bijvoorbeeld: – Voorkoming van incidenten; – Detectie van incidenten; – Interne melding van incidenten mochten deze optreden; – Analyse en tijdige melding aan autoriteiten en/of betrokkenen; – Het bepalen van de oorzaak en nemen van maatregelen om een dergelijk incident opnieuw te voorkomen; – Het meten van de effectiviteit van bovenstaande maatregelen.	✓ Verwerker zal incidenten volgens de contractueel bepaalde termijnen aan de verwerkingsverantwoordelijke moeten melden. ✓ Waar nodig moet de verwerker maatregelen nemen ter voorkoming, detectie of oplossen van incidenten.
13. Security & Privacy by design	✓ Verwerkingsverantwoordelijke zorgt voor de toepassing van security en privacy by design & by default.	✓ De verwerkingsverantwoordelijke kan bij onderdelen van de verwerking de bijbehorende toepassing van security en privacy by design & default aan de verwerker delegeren.
14. Transport naar Landen & zones	✓ Waar nodig moet de verwerkingsverantwoordelijke (contractuele) maatregelen nemen als gegevens verwerkt worden in landen die geen passend beschermingsniveau waarborgen..	✓ Waar nodig moet de verwerker (contractuele) maatregelen nemen als gegevens verwerkt worden in landen die geen passend beschermingsniveau waarborgen.

Disclaimer NL

Alleen de auteurs zijn verantwoordelijk voor de standpunten die in dit artikel worden geuit. Het artikel vertegenwoordigt niet noodzakelijk de standpunten, besluiten of het beleid van het ISACA NL Chapter. De standpunten die in dit artikel worden geuit kunnen op geen enkele manier worden opgevat als een weergave van een officieel standpunt van het bestuur van ISACA NL Chapter.
De auteurs hebben alle redelijke voorzorgsmaatregelen genomen om de informatie in deze publicatie te verifiëren. Het gepubliceerde materiaal wordt echter verspreid zonder enige vorm van garantie, expliciet of impliciet. De verantwoordelijkheid voor de interpretatie en het gebruik van het materiaal ligt bij de lezer. De auteurs en het bestuur van ISACA NL Chapter zijn in geen geval aansprakelijk voor schade die voortvloeit uit het gebruik ervan.

Disclaimer ENG

The authors alone are responsible for the views expressed in this article and they do not necessarily represent the views, decisions or policies of the ISACA NL Chapter. The views expressed herein can in no way be taken to reflect the official opinion of the board of ISACA NL Chapter.
All reasonable precautions have been taken by the authors to verify the information contained in this publication. However, the published material is being distributed without warranty of any kind, either expressed or implied. The responsibility for the interpretation and use of the material lies with the reader. In no event shall the authors or the board of ISACA NL Chapter be liable for damages arising from its use.