Kennisinstituut cultuur & digitalisering

Stappenplan AVG leveranciers

Versie 2.1

Arvid van Bokhorst

Postbus 90407 | 2509 LK Den Haag | www.den.nl | (0)70 314 03 43 | den@den.nl

Inhoudsopgave

Inleiding en aanleiding 3

Adviezen 4

Stappenplan bestaande systemen 5

BIJLAGE 1 Template leverancier inventarisatie 6

BIJLAGE 2 Checklist nieuwe systemen 9

BIJLAGE 3 Meer informatie 10

- Belangrijke factoren om rekening mee te houden 10
- Waar moet je op letten in algemene voorwaarden of verwerkingsovereenkomst? 10

Inleiding en aanleiding

Veel organisaties hebben de afgelopen tijd, noodgedwongen door de coronacrisis, extra software en nieuwe systemen aangeschaft. In veel gevallen om werken op afstand mogelijk te maken, of om het delen van bestanden en onderlinge communicatie te vergemakkelijken. Door de snelheid waarmee deze keuzes moesten worden gemaakt, kan het zijn dat er niet voldoende rekening is gehouden is met informatieveiligheid en de eisen die de Algemene Verordening Gegevensbescherming (AVG) stelt bij het delen van gegevens via software of systemen.
We presenteren daarom een stappenplan dat jouw organisatie kan gebruiken voor het in lijn brengen van jullie huidige systemen met de eisen uit de AVG.

Om je systemen goed te kunnen gebruiken, moet je goede afspraken maken met je leverancier, maar ook je software op de juiste manier instellen en medewerkers goed instrueren. Het stappenplan geeft je de structuur om met deze aspecten aan de slag te gaan. Nadat je de stappen hebt doorlopen, weet je of je systemen AVG-proof zijn en waar nog eventuele aanpassingen nodig zijn.

Naast de acht stappen in het stappenplan bieden we je ook een template aan om per leverancier een check uit te voeren, een checklist voor nieuwe systemen en extra informatie over AVG en informatiebeveiliging.

Adviezen

De volgende adviezen zijn goed om te hanteren wanneer je een nieuw systeem of nieuwe software implementeert. Met deze adviezen leg je de basis voor het AVG-proof maken van je infrastructuur.

- Als een systeem de optie biedt, gebruik dan altijd 2-STAPSVERIFICATIE.
- Pas altijd de PRIVACYINSTELLINGEN aan. Standaard deel je vaak meer informatie dan nodig is om gebruik te kunnen maken van de dienst of software. Denk aan Google, Zoom en andere applicaties.
- INSTRUEER MEDEWERKERS hoe ze systemen veilig gebruiken. Denk aan het uitzetten van video bij Zoom of het niet opnemen van meetings.
- Gebruik alleen ZAKELIJKE E-MAILADRESSEN.
- Stel een DATAPROTOCOL (de do's en don'ts in omgang met gegevens) op.
- Verzamel nooit meer persoonsgegevens dan STRIKT NOODZAKELIJK voor wat je ermee van plan bent.
- Werk alleen met BETROUWBARE LEVERANCIERS. Deze zijn herkenbaar aan een onafhankelijk keurmerk als ISO of bewezen diensten bij collega's. Onzeker? Doe zelf onderzoek, bijvoorbeeld door de leverancier te vragen naar informatie over certificering of door bij collega-instellingen te vragen om ervaringen.

Vaak geïmplementeerde systemen zijn bijvoorbeeld:

Asana
Basecamp
Google Drive
Google Survey
Mailchimp
Microsoft (Teams, Sharepoint, etc.)
Slack
SurveyMonkey
WeTransfer
Zoom

Stappenplan bestaande systemen

Inventariseren, toetsen en herstellen van bestaande leveranciers

STAP 1	**BRENG JE LEVERANCIERS IN KAART.**	*Vraag je administratie en systeembeheerder om een lijst met leveranciers* *Houd rekening met "gratis" systemen als Google Analytics, Zoom en Dropbox.*
STAP 2	Stel vast welke leveranciers omgaan met **PERSOONSGEGEVENS OF BEDRIJFSGEVOELIGE GEGEVENS**.	*Zie template in bijlage 1.*
STAP 3	**VERWIJDER** alle leveranciers die niet voldoen aan de criteria van stap 2 uit de selectie.	*Voor de volledigheid zou je kort kunnen aantekenen waarom je deze leveranciers niet hebt meegenomen.*
STAP 4	Maak bij persoonsgegevens onderscheid tussen **INTERNE EN EXTERNE VERWERKINGEN**.	*Zie template in bijlage 1.*
STAP 5	**PRIORITEER** de leveranciers die overblijven op de impact die ze hebben op de doorgang van bedrijfsprocessen.	*Als deze leverancier omvalt, blijft de boel dan wel gewoon draaien?*
STAP 6	Maak een **OVERZICHT** van verwerkingen per leverancier.	*Zie template in bijlage 1.*
STAP 7	**CONCLUSIE** per leverancier.	*Zie template in bijlage 1.*
STAP 8	**MAAK EEN (actie)planning**.	*Welke eventuele onvolkomenheden pak je als eerste aan?*

BIJLAGE 1 Template leverancier inventarisatie

- Zorg dat je onderstaande gegevens beschikbaar hebt van leveranciers en gebruikte systemen
- Vergeet niet “gratis leveranciers” als *Google, Dropbox* etc., eigen systemen of Excellijsten die circuleren in je organisatie mee te nemen in dit overzicht.
- Pas het template aan de specifieke eigenschappen van je eigen organisatie aan.
- Check periodiek (bijvoorbeeld jaarlijks) of deze lijst nog up-to-date is
- Mocht je organisatie beschikken over een systeem voor contractmanagement (bijvoorbeeld een ERP-systeem, een Excelsheet of een overzicht in de boekhouding), dan is het aan te raden dit template ermee te combineren.
- Gebruik samenwerking en projectmanagementtools als TRELLO en ASANA om beheer makkelijker te maken. Let er daarbij op dat je ook bij deze systemen het stappenplan doorloopt voor een AVG-proof implementatie.

Naam leverancier		
BELANG leverancier voor organisatie		*Wat gebeurt er als deze leverancier wegvalt?*
RISICO data incident (BIV)		*Als er een incident is heeft dat dan effect op Beschikbaarheid, Integriteit of Vertrouwelijkheid van je informatie/organisatie?*
Welk SOORT gegevens verwerken ze?		*Bedrijfsgevoelige of persoonsgegevens. Zie bijlage 3: Meer informatie*
Met welk DOEL worden gegevens verwerkt?		*Bijvoorbeeld administratie, marketing etc.*
WELKE gegevens verwerken ze?		*Bijvoorbeeld naam, adres, geboortedatum etc.*
INTERNE of EXTERNE verwerking		*Intern (alleen de persoonsgegevens van jouw organisatie - denk aan medewerkers)* *Extern (ook persoonsgegevens buiten jouw organisatie - denk aan deelnemers aan een congres of mailinglijsten)*
Hoe GEVOELIG zijn deze gegevens?	Laag, middel, hoog	*Zie ook bijlage 3: Meer informatie*
Verwerkingsovereenkomst of algemene voorwaarden?		*Passage of document toevoegen aan administratie*
Bevatten voorwaarden KWETSBAARHEDEN?		*Denk aan aansprakelijkheid, verwerking buiten EU, doorgifte aan derden etc*
Is AANPASSING noodzakelijk?	Ja/Nee	
Moet de CONFIGURATIE worden aangepast?	Ja/Nee	*Denk bijvoorbeeld aan het uitzetten van zichtbare IP-adressen in Google Analytics*
Moeten medewerkers extra worden GEÏNSTRUEERD?		*Denk aan instructie over gebruik email of het delen van e-mailadressen*
Zijn er ALTERNATIEVEN voor deze leverancier	Ja/Nee	*Indien bekend: geef aan welke alternatieven*
Op welke termijn is ACTIE nodig	Nu, korte termijn, lange termijn	*Op welke termijn moet je actie ondernemen om te zorgen dat je software aan de eisen voldoet?*

Lege template om in te vullen per leverancier

Naam leverancier	
BELANG leverancier voor organisatie	
RISICO data incident (BIV)	
Met welk DOEL worden gegevens verwerkt?	
WELKE gegevens verwerken ze?	
INTERNE of EXTERNE verwerking	
Hoe GEVOELIG zijn deze gegevens?	Laag, middel, hoog
Verwerkingsovereenkomst of algemene voorwaarden?	
Bevatten voorwaarden KWETSBAARHEDEN?	
Is AANPASSING noodzakelijk?	Ja/Nee
Moet de CONFIGURATIE worden aangepast?	Ja/Nee
Moeten medewerkers extra worden GEÏNSTRUEERD?	
Zijn er ALTERNATIEVEN voor deze leverancier	Ja/Nee
Op welke termijn is ACTIE nodig	Nu, korte termijn, lange termijn

BIJLAGE 2 Checklist nieuwe systemen

Doorloop bij aanschaf van een nieuw systeem of dienst de volgende checklist.

1. Welke gegevens ga ik in dit systeem verwerken?
2. Zitten daar gevoelige gegevens bij? (Medisch, financieel, gegevens van kinderen (bijvoorbeeld op je educatie-afdeling))
3. Ga ik dit systeem inzetten voor verwerking van gegevens voor anderen? (Denk aan een kaartverkoopsysteem dat je voor anderen inzet)

DE ANTWOORDEN OP BOVENSTAANDE DRIE VRAGEN BEPALEN WAAR JE REKENING MEE MOET HOUDEN BIJ HET KIEZEN VAN EEN SYSTEEM.

Stel vervolgens de volgende zaken vast of beantwoord de volgende vragen:

4. Is het een betrouwbare leverancier die werkt voor vergelijkbare organisaties?
5. Is het een Europees systeem? (Systemen die in Europa opereren en gegevens van Europese burgers verwerken, zijn namelijk al direct verplicht om zich aan de wetgeving rondom gegevensbescherming te houden)
6. Heeft de leverancier een eigen verwerkingsovereenkomst; is de leverancier bereid om er een van jouw organisatie te tekenen of zijn verwerkingen onderdeel van algemene voorwaarden?
7. Is expliciet opgenomen dat geen gegevens worden doorgeven aan derden of gebruikt voor zaken anders dan overeengekomen?
8. Zijn ze benaderbaar in geval van een probleem of datalek?

DE ANTWOORDEN OP BOVENSTAANDE VRAGEN HELPEN BIJ HET MAKEN VAN EEN WELOVERWOGEN BESLUIT OF VERGELIJKING VAN VERSCHILLENDE LEVERANCIERS.

BIJLAGE 3 Meer informatie

Hierna volgt enige context ten aanzien van AVG en informatiebeveiliging van gebruikte systemen.

Belangrijke factoren om rekening mee te houden bij verwerking van persoonsgegevens

Wanneer je met persoonsgegevens of bedrijfsgevoelige gegevens werkt, zijn er een aantal “triggers” waar je extra alert bij moet zijn. Want hoe je het ook regelt, jij blijft volgens de AVG verantwoordelijk voor het verwerken van persoonsgegevens.

- Verwerk je gegevens voor je eigen organisatie of voor een andere organisatie (bijvoorbeeld wanneer je een dienst levert)?
- Zijn de gegevens die je verwerkt op een of andere manier gevoelig (medisch, minderjarigen, financieel etc.)?
- Worden ze opgeslagen in Europa?
- De Autoriteit Persoonsgegevens en de AVG eisen dat je persoonsgegevens verantwoordelijk, veilig en binnen de kaders van de wet persoonsgegevens verwerkt. Maar ook bedrijfsgevoelige gegevens als jaarrekeningen en prognoses wil je niet per ongeluk verkeerd delen. Het is belangrijk om je keuzes regelmatig te controleren en een plan te maken voor het oplossen van eventuele problemen om te blijven voldoen aan je eigen eisen en die van de AVG. Dat toont ook aan dat je professioneel met gegevens omgaat. Wanneer je als instelling subsidie ontvangt, maakt dit ook onderdeel uit van je risicobeheersing, waarover je jaarlijks in het bestuursverslag verantwoording aflegt.

Waar moet je op letten in algemene voorwaarden of verwerkingsovereenkomst?

Er zijn (juridische) experts die je kunnen helpen. Bij twijfel kun je de hulp van deze personen inschakelen. Daarnaast zijn er ook zaken waar je zelf al rekening mee kunt houden.

Wettelijk moet je een aantal zaken regelen:

- Het eigendom van gegevens

- Doorgifte en gebruik van gegevens
- Geheimhouding van gegevens
- (Informatie)veiligheid van gegevens

Hierover maak je afspraken. Vaak doe je dat als onderdeel van algemene voorwaarden bij grotere leveranciers als Google en Microsoft. Dan heb je zelf niet altijd voldoende opties om aan de AVG te blijven voldoen. Werk daarom als het even kan met een aparte geheimhoudingsovereenkomst en verwerkingsovereenkomst. Daarnaast kun je met sommige bedrijven in de leveringsvoorwaarden en met specifieke overeenkomsten ook van alles regelen. In dat geval is het zeker raadzaam om een (juridisch) expert in te schakelen.

Het is daarnaast ook raadzaam om regelmatig (bijvoorbeeld jaarlijks) te checken of er wijzigingen zijn in de voorwaarden van je leveranciers. Dit is voor gesubsidieerde instellingen ook onderdeel van je aanpak ten aanzien van je risicobeheersing.

We adviseren om de volgende passages in overeenkomsten extra zorgvuldig te lezen.

- AANSPRAKELIJKHEID - de AVG stelt dat zowel jouw instelling als de leverancier aansprakelijk zijn naar de betrokkene. Je kunt dus niet de volledige verantwoordelijkheid bij je leverancier neerleggen. Omgekeerd kan de leverancier dat ook niet volledig bij jou neerleggen.
- SOORT GEGEVENS - stel vast dat de gegevens die de leverancier zegt te verwerken, overeenkomen met wat je hebt afgesproken.
- VERWERKING OP EUROPEES GRONDGEBIED of volgens de in Europa geldende standaarden - Dit is een actueel punt: zorg ervoor dat je leverancier de persoonsgegevens in Europa verwerkt of zich aan goedgekeurde afspraken houdt. LET OP: *in de zomer van 2020 is een uitspraak van het Europees Hof gedaan, waarin werd gesteld dat de EU-VS Privacy Shield herzien moet worden. De EU-VS Privacy Shield is een overeenkomst over de bescherming van persoonsgegevens van burgers van de Europese Unie, die in de Verenigde Staten worden verwerkt. Voor Amerikaanse leveranciers als Google, Zoom en Microsoft kan deze veranderende wetgeving dus ineens heel actueel worden.*
- EIGEN VERWERKINGSOVEREENKOMST OF ONDERDEEL ALGEMENE VOORWAARDEN - je bent wettelijk verplicht om hier afspraken over te maken. Als er geen aparte verwerkingsovereenkomst is, dienen er minimale artikelen in de algemene voorwaarden te staan.

- **Geheimhouding** – het is altijd goed om te controleren of de voorwaarden stellen dat je leverancier alleen gegevens verwerkt voor het doel waarvoor ze worden verstrekt en er geen doorgifte aan derden plaatsvindt.
- **Beveiliging** – dit is geheel afhankelijk van je eigen kennis en het soort gegevens dat de leverancier verwerkt, maar je prikt er snel doorheen als een organisatie hier niet over nagedacht heeft. Een ISO- of NEN-norm is altijd een snelle check. Hoewel het niet hebben van een ISO- of NEN-certificaat niet automatisch betekent dat gegevens onveilig verwerkt worden.