AVG

STAPPENPLAN

Stappenplan Algemene Verordening Gegevensbescherming

Vanaf 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van toepassing. Dit betekent dat er vanaf die datum dezelfde privacywetgeving geldt in de hele Europese Unie (EU). De Wet bescherming persoonsgegevens (Wbp) is dan niet langer geldig. De AVG is ook wel bekend onder de Engelse naam: General Data Protection Regulation (GDPR).

Wat verandert er? De AVG versterkt de positie van de betrokkenen (de mensen van wie gegevens worden verwerkt). Zij krijgen nieuwe privacyrechten en hun bestaande rechten worden sterker. Organisaties die persoonsgegevens verwerken krijgen meer verplichtingen. Daar hoort bij dat je als organisatie moet kunnen aantonen dat je je aan de wet houdt.

Hoe zorg je ervoor dat jouw organisatie klaar is voor de AVG? Om je te helpen hebben we een stappenplan voor je gemaakt. Lees het door en ga ermee aan de slag!

Artikel 5 van de AVG

De meeste actiepunten om op te pakken volgen uit artikel 5 van de AVG. De belangrijkste passage uit dit artikel luidt als volgt: “Persoonsgegevens moeten worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is.” Rechtmatigheid, behoorlijkheid en transparantie zijn dus zaken waarmee je rekening dient te houden als je persoonsgegevens verwerkt en opslaat. Maar wat betekent dit concreet?

EXtreem veilig

MaXimaal beschikbaar

In principe moet iedere organisatie voor zichzelf bepalen hoe ze rechtmatigheid, behoorlijkheid en transparantie interpreteren. In deze whitepaper geven we je onze interpretatie en vertellen we welke stappen daaruit volgen. Je kunt er geen rechten aan ontlenen.

Rechtmatigheid

Data met persoonsgegevens opslaan is alleen toegestaan als dat het doel dient, behorend bij de visie, missie en strategie van de organisatie. Draagt het opslaan van bepaalde persoonsgegevens niet bij tot dat doel? Dan is er geen gegronde reden om die gegevens op te slaan. Dus ook geen rechtvaardiging.

Stap 1: Inventariseer alle data- en gegevensstromen

- Inventariseer alle persoonsgegevens met informatie die je daarbij opslaat
- Verbind de persoonsgegevens met gekoppelde informatie met het organisatorische doel, zodat de doelverbindingen per datatype inzichtelijk zijn.

Je eindproduct is een matrix met persoonsgegeven en datatypes met doelverbinding.

Behoorlijkheid

Behoorlijkheid gaat over de mate waarin we data met een verantwoorde doelverbinding veilig opslaan en bewerken. Je wilt beleidsmatig, organisatorisch en technisch de juiste maatregelen nemen om privacy en security (in)breuk te voorkomen. Ook wil je adequaat kunnen handelen als zich een privacy en/of security (in)breuk voordoet.

Stap 2: Maak een risicoanalyse

- Stel een matrix samen met persoonsgegevens en doelverbonden datatypes
- Bepaal de impact van privacy en security (in)breuk per doelverbonden datatype. Met andere woorden: wat is de impact als gegevens op straat komen te liggen en er ongeautoriseerd gebruik van wordt gemaakt?
- Bepaal het risico vanuit de huidige gang van zaken. Inventariseer de werkwijze per datatype. Hoe en door wie wordt data verwerkt en met welke systemen? Welke veiligheidsmaatregelen worden hierbij getroffen?

Stap 3: Bepaal de werkwijze per type data

Transparantie

Transparantie gaat over de vraag: hoe helder is het voor iemand dat er doelverbonden data van hem of haar wordt opgeslagen? Zowel voor, tijdens als na het opslaan. Het is belangrijk dat een medewerker, relatie of bezoeker weloverwogen toestemming kan geven voor het opslaan en bewerken van data die gekoppeld zijn aan persoonsgegevens.

Stap 4: Verwerk een matrix 'persoonsgegevens met doelverbonden datatypes' in het personeelsbeleid

- Vermeld voor ieder datatype dat je opslaat van een werknemer de doelverbinding in het personeelshandboek. Maak helder welke data je op welke wijze beheert en vermeld waarom die data relevant voor je zijn.

Stap 5: Verwerk een matrix 'persoonsgegevens met doelverbonden datatypes' in het klantbeleid.

- Vermeld voor ieder datatype dat je opslaat van een klant of leverancier de doelverbinding in de algemene voorwaarden, dienstbeschrijvingen, sla's en andere contracten met je klant of leverancier. Maak helder dat duidelijk is welke data je op welke wijze beheert en vermeld waarom die data relevant voor je zijn.

Overige acties

Naast de 5 genoemde stappen, zijn ook de volgende acties aan te bevelen in het kader van de AVG:

Definitie security breuk

Omschrijf de definitie van een security breuk. Wanneer is daar sprake van en wanneer niet? Zorg dat dit duidelijk is voor alle medewerkers die hiermee te maken kunnen krijgen. Zodat ze gepaste actie kunnen ondernemen als er sprake is van een security breuk.

Draaiboek wat te doen bij een security of privacy breuk

Leg vast wat werknemers moeten doen als zich een security of privacy breuk voordoet. Zij zullen dit moeten melden. Kunnen ze zelf maatregelen treffen om de risico's en impact te verkleinen? Dan moeten ze weten wat ze moeten doen.

Aanstellen verantwoordelijke voor privacy en security beleid en toezicht
Stel een data officer aan bij wie privacy en security breuken gemeld kunnen worden.

Risico's inventariseren in je huidige omgeving
Zet alle kwetsbaarheden op een rij en inventariseer hoe deze kwetsbaarheden op dit moment beschermd worden door BSU en andere leveranciers.

- BSU kan een scan uitvoeren en aangeven waar nog kwetsbaarheden zitten.
- BSU kan aan de hand van de momenteel afgenomen diensten aangeven hoe je nu beschermd bent.

Verwerkersovereenkomsten opstellen
Stel verwerkersovereenkomsten op met alle 3e partijen die gegevens verwerken in relatie tot persoonsgegevens van klanten of medewerkers.

Hulp nodig?
Heb je hulp nodig om deze stappen te doorlopen? Laat BSU je ondersteunen. Neem vrijblijvend contact op via 0413-243333. We vertellen je graag meer over onze aanpak.