Introductie

Per 25 mei zal de AVG worden gehandhaafd. Hier is een hoop nieuwe regelgeving en documentatie bij betrokken en bij DBHeroes begrijpen wij dat er behoefte is aan een eenvoudig overzicht van wat er zoal moet gebeuren. Hieronder hebben we de voor organisaties te nemen stappen samengevat en een korte uitleg toegevoegd.

Stap 1: Data Mapping

De eerste stap is om een overzicht te maken van wat voor (persoonlijke) data uw organisatie bezit. Vragen om te beantwoorden zijn:

- Waar bevindt de data zich?
- Wie heeft toegang tot de data?
- Zijn er (gedocumenteerde) procedures met betrekking tot de toegankelijkheid hiervan?
- Zijn er (gedocumenteerde) procedures met betrekking tot de data?

Stap 2: Wettelijke basis en grensoverschrijdende overdrachten

De verwerking van gegevens moet gebaseerd zijn op een van de gegeven redenen in artikel 6 van de AVG. Dit geldt voor alle persoonlijke gegevens waarvoor uw organisatie verantwoordelijk is. Zie voor de verschillen tussen verwerkingsverantwoordelijke en verwerker de volgende link: https://europadecentraal.nl/avg-deel-iii-verwerker-verwerkingsverantwoordelijke-en-verwerkersovereenkomst/

De zes wettelijke gronden zijn:

1. Toestemming: dit moet vrijwillig worden afgegeven en moet altijd opt-in zijn (dus geen vooraf aangevinkte vakjes). Meer informatie over toestemming (en de andere gronden) is te vinden via de volgende link: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/mag-u-persoonsgegevens-verwerken
2. Contract: de verwerking is noodzakelijk voor het uitvoeren van een contract of ter voorbereiding van een contract. Een voorbeeld kan de verwerking van persoonsgegevens zijn om een salaris te kunnen uitbetalen of wanneer een psychologische of fysieke test vereist is om iemand aan te nemen.
3. Naleving van een wettelijke verplichting: hierbij kan gedacht worden aan de verwerking van persoonsgegevens om te voldoen aan bijvoorbeeld belastingwetgeving.
4. Om de essentiële belangen van een persoon te beschermen waarbij het individu niet in staat is om toestemming te geven: dit is alleen van toepassing op humanitaire doeleinden in geval van een epidemie. Als het een andere persoon betreft, kan aan een ongeluk gedacht worden waarbij

DBHeroes B.V.
Utrechtseweg 310
6812 AR Arnhem
The Netherlands
www.dbheroes.eu
info@dbheroes.eu
T +31(0)88 888 6000

Administration
administration@dbheroes.eu
T +31(0)88 888 6002

Staffing
staffing@dbheroes.eu
T +31(0)88 888 6001

Rabobank
NL54 RABO 0303 1270 90

Chamber of Commerce
57289034
VAT The Netherlands
NL852518134B01

iemand medische hulp nodig heeft maar bewusteloos is. Voor de laatstgenoemde zou geen andere wettelijke basis beschikbaar moeten zijn.

5. Voor de uitvoering van een taak die wordt uitgevoerd in het openbaar belang of de uitoefening van het openbaar gezag door de voor de verwerking verantwoordelijke. Deze grond is van toepassing op de journalistiek en onderzoek.
6. Met het oog op legitieme belangen: bijvoorbeeld een marketingbedrijf. Zaak hierbij is dat de verwerking noodzakelijk moet zijn om het resultaat te bereiken, oftewel er is geen waarschijnlijk geen minder opdringerige manier beschikbaar.

Stap 3: Data Governance

Stel een Data Governance-structuur op (als uw organisatie er nog geen heeft). Zorg ervoor dat de procedures volgens de Plan-Do-Check-Act (PDCA) verlopen.

Stap 4: DPIA's en Privacy by Design & Default

DPIA staat voor een Data Protection Impact Assessment. Een DPIA is een verplichte vereiste volgens artikel 35 van de AVG. Dit artikel stelt wanneer een DPIA uitgevoerd moet worden:

> *Wanneer een soort verwerking, in het bijzonder een verwerking waarbij nieuwe technologieën worden gebruikt, gelet op de aard, de omvang, de context en de doeleinden daarvan waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen voert de verwerkingsverantwoordelijke vóór de verwerking een beoordeling uit van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens. Eén beoordeling kan een reeks vergelijkbare verwerkingen bestrijken die vergelijkbare hoge risico's inhouden.*

Wanneer uw DPIA een hoog risico identificeert dat u niet kunt beperken, moet u uw gegevensbeschermingsautoriteit (Authoriteit Persoonsgegevens) raadplegen. Als u besluit om geen DPIA uit te voeren, moet dit worden gedocumenteerd.

Privacy by Design is ervoor zorgen dat tijdens de ontwikkeling privacy als leidraad wordt genomen. Privacy by Default betekent dat de instellingen (standaard) zo moeten worden ingesteld dat er minimaal inbreuk wordt gemaakt op privacy. Onderdeel van Privacy by Design is de scheiding van de OTA-omgeving (Ontwikkel-, Test en Acceptatie) van de productieomgeving. Er mogen geen productiegegevens worden gebruikt in OTA.

Stap 5: Beleid voor het bewaren en bijhouden van gegevens

Leg vast hoe lang gegevens worden bewaard en hoe die periode is vastgesteld. Een ander deel van deze stap is dat er ook moet worden gedocumenteerd hoe gegevens worden bewaard en verwijderd.

DBHeroes B.V.
Utrechtseweg 310
6812 AR Arnhem
The Netherlands
www.dbheroes.eu
info@dbheroes.eu
T +31(0)88 888 6000

Administration
administration@dbheroes.eu
T +31(0)88 888 6002

Staffing
staffing@dbheroes.eu
T +31(0)88 888 6001

Rabobank
NL54 RABO 0303 1270 90

Chamber of Commerce
57289034
VAT The Netherlands
NL852518134B01

Stap 6: Transparantie

> *"De verwerkingsverantwoordelijke neemt passende maatregelen opdat de betrokkene de ... bedoelde informatie en ... communicatie in verband met de verwerking in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal ontvangt ..."* (artikel 12).

Met andere woorden: de informatie mag geen overdreven legalistische, technische of specialistische taal of terminologie bevatten. De informatie moet bovendien los worden gezien van andere niet-privacygerelateerde informatie, zoals contractuele bepalingen. Andere informatie die moet worden verstrekt zijn de rechten van de betrokkenen en hoe die rechten kunnen worden uitgeoefend.

Stap 7: Rechten van betrokkenen

Een persoon (of officieel genoemd: betrokkene) heeft verschillende rechten. Een organisatie moet een betrokkene in staat stellen om die rechten uit te oefenen en procedures (Data Governance!) opgesteld te hebben. Deze rechten zijn: Recht van toegang - Recht op rectificatie - Recht op wissen (ook wel "recht om vergeten te worden" genoemd) - Recht op beperking van verwerking - Recht op dataportabiliteit.
Een overzicht van die rechten (en de verordening zelf) is te vinden via de volgende link:
https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/rechten-van-betrokkenen

Stap 8: Procedures met betrekking tot incidenten en inbreuken

Documenteer de procedures met betrekking tot incidenten en inbreuken. Zorg ervoor dat het oefenen van de procedures onderdeel is van een (minstens) jaarlijkse routine.

Stap 9: Leveranciersbeleid

Een verwerkingsverantwoordelijke is verplicht om alleen samen te werken met gegevensverwerkers die "voldoende garanties bieden om passende technische en organisatorische maatregelen op zodanige wijze te implementeren dat de verwerking voldoet aan de vereisten van de [AVG] en de bescherming van de rechten van de betrokkenen waarborgt." Bovendien zijn verwerkingsverantwoordelijken verplicht om een schriftelijk contract - een gegevensverwerkingsovereenkomst - aan te gaan met alle verwerkers.

DBHeroes B.V.
Utrechtseweg 310
6812 AR Arnhem
The Netherlands
www.dbheroes.eu
info@dbheroes.eu
T +31(0)88 888 6000

Administration
administration@dbheroes.eu
T +31(0)88 888 6002

Staffing
staffing@dbheroes.eu
T +31(0)88 888 6001

Rabobank
NL54 RABO 0303 1270 90

Chamber of Commerce
57289034
VAT The Netherlands
NL852518134B01

Stap 10: Communicatie met de Authoriteit Persoonsgegevens (AP)

In de volgende situaties moet een organisatie een functionaris voor gegevensbescherming (FG) benoemen:

- De organisatie is een overheidsinstantie of publieke organisatie;
- De kernactiviteiten vereisen grootschalige, regelmatige en systematische monitoring van individuen; of
- De kernactiviteiten bestaan uit grootschalige verwerking van speciale categorieën gegevens of gegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten.

Landen kunnen de gronden uitbreiden waarbij een FG verplicht is. Ongeacht of een organisatie verplicht is om een FG aan te wijzen of niet moet de organisatie zorgen voor voldoende personeel en middelen om te voldoen aan de AVG.

Verder is een FG het contactpunt met de AP. Als ervoor gekozen wordt om geen FG te benoemen moet niet alleen de reden daarvoor worden gedocumenteerd maar moet de organisatie ook een communicatiekanaal met de AP tot stand brengen.

Tot slot

DBHeroes heeft geprobeerd om een zo duidelijk mogelijk overzicht te geven van de stappen die genomen moeten worden om te voldoen aan de AVG. Mocht u vragen of suggesties hebben of ondersteuning willen bij de uitvoer van de stappen, neem dan contact met ons op.

DBHeroes
www.dbheroes.nl
E-mail: info@dbheroes.eu
Telefoon: +31 88 888 6060

DBHeroes B.V.
Utrechtseweg 310
6812 AR Arnhem
The Netherlands
www.dbheroes.eu
info@dbheroes.eu
T +31(0)88 888 6000

Administration
administration@dbheroes.eu
T +31(0)88 888 6002

Staffing
staffing@dbheroes.eu
T +31(0)88 888 6001

Rabobank
NL54 RABO 0303 1270 90

Chamber of Commerce
57289034
VAT The Netherlands
NL852518134B01