Ministerie van Veiligheid en Justitie

Anticiperen op de Algemene verordening gegevensbescherming

Tien stappen voor een goede voorbereiding

De spelregels voor omgang met persoonsgegevens zijn aangescherpt. Vanaf 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing. In tien stappen bereidt u de procedures, systemen en processen in uw organisatie voor op de eisen van de AVG. Hoeveel menskracht en middelen u moet inzetten om deze stappen goed te doorlopen, hangt mede af van de mate waarin uw organisatie voldoet aan de eisen van de Wet bescherming persoonsgegevens (Wbp).

1 Bewustmaken; maak de omgang met persoonsgegevens tot onderwerp van gesprek

Breng de nieuwe privacyregels onder de aandacht van sleutelfiguren en beleidsmakers van uw organisatie. Laat hen een inschatting maken van de gevolgen van de AVG voor de processen en systemen. Breng in kaart wat de benodigde menskracht en middelen zijn voor de implementatie van de privacyregels.

2 Breng informatiestromen in kaart en registreer alle verwerkingen

De AVG introduceert een registratieplicht voor alle verwerkingen van persoonsgegevens. Welke persoonsgegevens worden voor welk doel verwerkt? Waar komen de gegevens vandaan en met wie zijn ze gedeeld? Hoe lang worden de gegevens bewaard? De registratie van de verwerkingen helpt u gedocumenteerd aan te kunnen tonen dat de gegevensverwerking op orde is.

3 Identificeer risico's van voorgenomen verwerkingen met behulp van een gegevensverwerkingseffectbeoordeling (GEB)

De GEB helpt u vroegtijdig risico's in kaart te brengen en maatregelen te nemen, afgestemd op het veiligheidsrisico en de behoefte aan beveiliging. In Nederland is de GEB verplicht bij nieuwe wetgeving, beleid of ICT-projecten waarin verwerking van persoonsgegevens een rol speelt. Het kabinetsbeleid dat is ingezet in 2013 wordt voortgezet en daarbij is voor de vereisten waaraan een GEB moet voldoen aangesloten bij de AVG. De AVG stelt een GEB verplicht als de verwerking een hoog privacyrisico voor betrokkenen inhoudt, in het bijzonder bij gebruik van nieuwe technologieën en in elk geval bij profilering, grootschalige verwerkingen van 'bijzondere' categorieën persoonsgegevens en stelselmatige monitoring in openbare ruimten. De resultaten van de GEB kunnen u verplichten contact op te nemen met de Autoriteit Persoonsgegevens (AP). Bij vergelijkbare verwerkingen met vergelijkbare risico's kan worden volstaan met één GEB.

4 Borg gegevensbescherming met 'privacy by design' en 'privacy by default'

Net als de Wbp verlangt de AVG passende maatregelen om de beveiliging van persoonsgegevens te borgen. De AVG gaat een stap verder en verlangt dat gegevensbescherming in het technische ontwerp van systemen wordt ingebouwd. Systemen moeten standaard op de meest privacy-vriendelijke manier worden ingericht, zodat gebruikers niet extra moeite moeten doen om gegevens beter te beschermen (gegevensbescherming by design). Ook moeten ze zo zijn ontworpen en ingericht dat er zo min mogelijk persoonsgegevens worden verwerkt (gegevensbescherming by default).

5 Betrek de functionaris voor gegevensbescherming bij voorgenomen verwerkingen

De AVG verplicht ook overheidsinstanties of -organen een functionaris voor gegevensbescherming (FG) te benoemen. Zo is zeker dat iemand in de organisatie (of een externe FG) toeziet op de naleving van de AVG en dat hij de kennis en bevoegdheid heeft om dit te doen. De FG rapporteert aan de hoogste leidinggevende en mag geen instructies krijgen met betrekking tot de uitoefening van zijn taak. Overheden kunnen met elkaar ook één gezamenlijke FG aanstellen.

6 Beoordeel bestaande contracten en breng ze zo nodig in lijn met de AVG

U moet de bestaande contracten met verwerkers en onderaannemers controleren en, waar nodig, in lijn brengen met de AVG.
De verwerking van persoonsgegevens mag alleen op basis van uw schriftelijke instructies plaatsvinden. De verwerker heeft ook uw toestemming nodig voor het inschakelen van een onderaannemer. In de overeenkomst moeten ook de geheimhouding en beveiliging geregeld zijn. Evenals de plicht van de verwerker om mee te werken aan inspecties die de gedragseisen verifiëren en aan verzoeken van betrokkenen aan uw adres.

7 Stem privacyverklaringen af op de doelgroep(en)

Implementeer de aangescherpte informatieplichten en zorg dat de verklaring voldoende is afgestemd op de doelgroep(en). Is de informatie beknopt, begrijpelijk en gemakkelijk toegankelijk? Vanaf mei 2018 moet de privacyverklaring bijvoorbeeld ook informatie bevatten over de wettelijke grondslag, bewaartermijnen, eventuele uitwisseling met landen buiten de EU, het klachtrecht van betrokkene bij de AP en mogelijke geautomatiseerde besluitvorming en profilering.

8 Implementeer nieuwe rechten van betrokkene

Beoordeel of de procedures zijn ingericht op alle rechten waarop betrokkene onder de AVG een beroep kan doen. Dat zijn de rechten die onder de Wbp gelden, aangevuld met nieuwe rechten als het recht van betrokkene om zijn gegevens te ontvangen in een gestructureerde gangbare en elektronische vorm (dataportabiliteit) en het recht op vergetelheid.

9 Controleer de manier waarop toestemming wordt gevraagd

Zorg dat de manier waarop toestemming wordt gevraagd, verkregen en geregistreerd in lijn is met de AVG. Zeker als het toestemming van kinderen betreft. De toestemming moet vrij, specifiek, geïnformeerd, ondubbelzinnig, actief en controleerbaar zijn. Uit zwijgen of niet-handelen mag geen toestemming worden afgeleid.

10 Breng procedures voor datalekken in lijn met de AVG

Controleer of de procedures voor datalekken (opsporen, onderzoeken, rapporteren, melden) aan de aangescherpte regels voldoen. Alle datalekken moet u registreren.

april 2017 - 102284