



Handreiking Privacy

Werkorganisatie Druten Wijchen

Functionaris Gegevensbescherming:
Annemarie Walraven
September 2018

Inleiding

Op 24 mei 2016 is binnen de Europese lidstaten de General Data Protection Regulation (GDPR) ingevoerd. In Nederland kennen wij de GDPR als de Algemene Verordening Gegevensbescherming, meestal afgekort als de AVG. De AVG regelt de bescherming van natuurlijke personen in het kader van de verwerking van persoonsgegevens binnen de gehele Europese Unie. Een groot pluspunt van de AVG is dat er uniformiteit ontstaat bij de lidstaten over de wijze waarop de privacy van burgers moet worden beschermd.

Aanleiding

Aanleiding om deze handreiking is dat de AVG een algemene regeling is voor alle lidstaten van de E.U. maar dat de toepassing in het dagelijkse werk vaak moeilijk is te duiden. De onbekendheid van veel van onze medewerkers met het juridische kader rond het werken met persoonsgegevens leidt tot vragen. Bijvoorbeeld of persoonsgegevens wel of niet en onder welke voorwaarden met anderen mogen worden gedeeld. De gevolgen hiervan kunnen zijn dat processen trager verlopen, beslissingen langere voorbereidingstijd nodig hebben, en er achteraf wordt getwijfeld of een verwerking van persoonsgegevens al dan niet toelaatbaar was.

Doelstelling

Doelstelling van deze handreiking is om de organisatie handvatten te bieden die de dagelijkse werkpraktijk ondersteunen.

Twee algemene uitgangspunten

De dienstverlening staat voorop

Ons eerste algemene uitgangspunt is dat we de dienstverlening voorop stellen. Het betekent dat we leveren waar de burger recht op heeft, dat we onze afspraken met ketenpartners nakomen, dat we zo nodig – ten gunste van de dienstverlening - de randen van het toelaatbare opzoeken, en dat we beslissingen over het al dan niet verstrekken van persoonsgegevens naar het juiste organieke niveau brengen. Het komt bij ons bijvoorbeeld niet voor dat een medewerker besluit om een dienstverleningsproces te stoppen, zonder dat de verantwoordelijke daar weet van heeft.

De dienstverlening staat voorop betekent ook dat de privacywetten er niet zijn om het werk te belemmeren of zelfs onmogelijk te maken. De AVG moet worden uitgelegd als een raamwerk dat over alle informatieprocessen heen ligt. Wanneer de wet bijvoorbeeld zegt dat er toestemming nodig is van de betrokkene, dan zullen we ons inspannen om die toestemming te krijgen. En als de toestemming niet wordt verleend dan zullen we de gegevens niet gebruiken. In dat geval moeten we onderzoeken of we de burger op een andere manier, zonder het gebruik van persoonsgegevens, verder kunnen helpen. We accepteren het dat de dienstverlening hierdoor moeizamer kan verlopen.

We houden ons aan de wet

Ons tweede algemene uitgangspunt is dat we ons bij het verwerken van persoonsgegevens houden aan wet- en regelgeving. Tenzij er zeer dringende redenen zijn om hiervan af te wijken. De redenen om van wet- en regelgeving af te wijken moeten in zwaarwegend belang zijn van de persoon van wie de gegevens worden verwerkt. Niet om bijvoorbeeld de efficiency van interne procedures te bevorderen.

De leidende wet is de Europese AVG, daarna nationale wetten zoals de wet basisregistraties en de wet openbaarheid van bestuur. Wanneer Europese en nationale wetten onvoldoende aanknopingspunten bieden, dan zijn de aanwijzingen van toezichthouders zoals de Autoriteit Persoonsgegevens (AP) en de Rijksdienst voor Identiteitsgegevens (RvIG) van toepassing.

Voordat wij besluiten om van wet- of regelgeving af te wijken wordt verplicht een risicoanalyse of een privacy impact assessment uitgevoerd. Het besluit om van regelgeving af te wijken moet zorgvuldig, gemotiveerd en op het juiste beslissingsniveau worden genomen. De interne functionaris die namens de verantwoordelijke voor de persoonsgegevens optreedt voor de onreglementaire gegevensverwerking, draagt zorg voor een deugdelijk en volledig dossier van de gebeurtenissen. Een onreglementaire verwerking van persoonsgegevens moet altijd bij de interne toezichthouder worden gemeld.

Continue aandacht voor privacy

De werkorganisatie Druten Wijchen heeft standaard aandacht voor privacy. Bijvoorbeeld wanneer er een nieuw informatiesysteem wordt aangeschaft, dan houden we er in het programma van eisen al rekening mee, dat er standaard veiligheidsinstellingen mogelijk moeten zijn. Als dat niet kan, dan zoeken we verder naar een systeem waarmee het wel kan.

Hetzelfde principe geldt voor bijvoorbeeld nieuwe werkprocessen. Wanneer we een nieuw werkproces ontwerpen, dan houden we er in de ontwerpfase al

rekening mee dat het proces veilig moet zijn. Bijvoorbeeld door er controlemechanismen en functiescheidingen in aan te brengen.

We zorgen er voor dat de organisatie en de besturing van ontwikkelprocessen ingericht zijn voor privacy. Het betekent dat de ontwikkelaars (vaak zijn dat de beleidsmakers) tijdens het ontwikkelproces integraal samenwerken met de teams en afdelingen die het nieuwe werk gaan uitvoeren, dusdanig dat eventuele tekortkomingen in het procesontwerp vroegtijdig kunnen worden opgemerkt, zodat deze niet in de uitvoering terecht kunnen komen.

Risicobeheersing

Risicobeheersing is een belangrijk aandachtspunt om veilig met persoonsgegevens te kunnen werken. Bijvoorbeeld het risico voor een burger als gevolg van een datalek, het risico van bedrijfsschade bij ons of bij een ketenpartner als gevolg van een privacy incident, en het risico dat we sowieso dragen vanwege onze verantwoordelijkheid als gegevenseigenaar. Risico's kunnen niet altijd worden verzekerd en moeten daarom worden afgedekt met beheersmaatregelen.

De werkorganisatie Druten Wijchen voert voordat een nieuwe risicovolle verwerking van persoonsgegevens wordt uitgevoerd een Privacy Impact Assessment (PIA) uit. Het doel van het assessment is om de mogelijke risico's van de verwerking in kaart te brengen, de risico's te wegen, en er beheersmaatregelen tegenover te zetten.

De werkorganisatie Druten Wijchen volgt het advies van de Autoriteit Persoonsgegevens om bij de uitvoering van een PIA de handreiking van de beroepsvereniging van auditors NOREA te gebruiken. Een verwijzing naar de handreiking is te vinden op de website van de autoriteit. Het assessment wordt uitgevoerd door een onafhankelijk deskundige.

Er wordt pas toestemming gegeven voor een nieuwe verwerking van persoonsgegevens na beoordeling door de Chief Information Security Officer (CISO). De CISO kan de proceseigenaar zo nodig nog aanwijzingen geven om de veiligheid te verhogen, en geeft tevens opdracht om de nieuwe verwerking van de persoonsgegevens te melden bij de toezichthouder Functionaris Gegevensbescherming (FG).

Werken aan bewustwording

De Europese privacywet betreft ingewikkelde materie die zich vaak moeilijk laat vertalen naar toepassing in de dagelijkse praktijk. We stellen dat het waarschijnlijk niet realiseerbaar is om alle medewerkers van de werkorganisatie Druten Wijchen wat privacy betreft op een hoogwaardig kennisniveau te brengen. Het best werkbaar is om diepgaande kennis van privacy te borgen bij de juristen

en de Functionaris Gegevensbescherming, zeer specialistische kennis zo nodig extern te betrekken, en basiskennis bij alle medewerkers. Bij deze policy passen de volgende beheersmaatregelen:

- Alle medewerkers moeten bij in dienst treden door de direct leidinggevende over worden geïnformeerd dat zij met gevoelige informatie in contact kunnen komen. Deze informatie mag niet zonder meer worden gedeeld met anderen.
- Elke medewerker is verplicht om een korte initiële training en een jaarlijks opfrustraining te volgen over het werken met gevoelige informatie.
- Onze interne specialisten worden doorlopend in de gelegenheid gesteld om hun kennis van privacy te onderhouden.
- Ontwikkelprocessen rond het verwerken van persoonsgegevens worden dusdanig ingericht dat voor het in productie stellen van het proces een privacy-specialist of de Functionaris Gegevensbescherming worden geconsulteerd.