Ipsos' inzet van Privacy en Databescherming

Context

De General Data Protection Regulation ("**GDPR**"), die is ingesteld door de Europese Unie en op 25 mei 2018 in werking treedt, is een nieuwe stap in de bescherming van de privacy-rechten van personen (zoals striktere beperkingen bij toestemming, het recht om te worden vergeten, type en hoeveelheid persoonlijke gegevens die gebruikt kunnen worden, toegang tot gegevens en veiligheid, etc.) naast de beschermende maatregelen die al enige tijd in de Europese Unie en vele andere landen wereldwijd gelden.

Voor Ipsos, als leider in de Marktonderzoeksindustrie en leverancier van informatie over mensen, is de bescherming van persoonlijke gegevens een topprioriteit. Dat is altijd zo geweest. Ipsos houdt zich aan de richtlijnen en bepalingen van de **professionele gedragscode die geldt voor alle geregistreerde markonderzoeksbureaus** (ICC/ESOMAR International Code on Market, Opinion and Social Research and Data Analytics) en aan alle huidige bestaande lokale wettelijke bepalingen, vooral bij de bescherming van gegevens van respondenten.

Daarbij hanteert Ipsos binnen haar bedrijf al vele jaren de **4Ss benadering**. De 4 S'en staan voor **Security, Simplicity, Speed and Substance.** Beleid voor IT Security en Informatiebeheer is al jarenlang een integraal onderdeel van het beleid van Ipsos.

Ipsos heeft een proactieve benadering gevolgd om de persoonlijke gegevens van haar klanten, respondenten en medewerkers te waarborgen en te beschermen. Ipsos heeft daartoe vorig jaar **een wereldwijd privacy-programma** gelanceerd **dat wordt aangestuurd door een multidisciplinair team** (bestaande uit de CPO, de afdelingen IT, Juridische zaken, Kwaliteit, HR en Marketing & Communicatie), voor de naleving van de GDPR met ingang van 25 mei 2018, dat zich in de eerste plaats op de landen in de European Economic Area (EEA) richtte. Verder is Ipsos van plan om eind 2018 ook in alle 89 landen waar zij actief is de GDPR vereisten te implementeren.

Ipsos heeft al veel acties ondernomen voor naleving van de GDPR. De belangrijkste acties zijn, onder andere, de volgende:

1. De aanstelling van een wereldwijde Chief Privacy Officer (CPO) en lokale Data Privacy Officers (DPOs)

Op 1 maart 2017 stelde Ipsos een wereldwijde Chief Privacy Officer aan, Rupert van Hüllen. De CPO heeft als rol het begeleiden en coördineren van Ipsos' wereldwijde inspanningen voor naleving van databescherming en privacy en het aansturen van de lokale Data Protection Officers die aangesteld zijn in alle landen waar Ipsos actief is. Hun mandaat omvat het waarborgen van de juiste behandeling en bescherming van persoonlijke gegevens.

2. Geanonimiseerde data en beveiligde toegang

- Voor respondenten

  Ipsos maakt gebruik van **anonimiserings-technieken** om de persoonlijke gegevens van respondenten tijdens dataverzameling te beschermen, zodat de veldwerkteams van uitvoerende afdelingen hier uitsluitend **op basis van *need to know*** toegang toe hebben. Ipsos past hetzelfde beleid en dezelfde zorgvuldigheid toe bij door klanten aangeleverde samples en bij leden van Ipsos panels en off-line respondenten.

- Voor onze medewerkers

  De toegang tot persoonlijke gegevens van medewerkers is strikt beperkt tot personeel dat verantwoordelijk is voor human resources management.

3. Medewerker training

Ipsos lanceert in maart-april 2018 een uitgebreid trainingsprogramma voor haar medewerkers om te zorgen voor een **sterke mate van aandacht voor databescherming en voor naleving van databescherming binnen de Ipsos groep**. Onze klanten verwachten dat Ipsos medewerkers de GDPR en andere toepasselijke wetgeving voor databescherming naleven. Ipsos implementeert een **wereldwijd trainingsprogramma over databescherming** (waaronder de GDPR vereisten) voor het personeel dat hiermee te maken heeft.

4. Encryptie

Ipsos heeft **verschillende encryptieoplossingen** geïmplementeerd, met name op de laptops van alle medewerkers. Bij [software]applicaties neemt Ipsos maatregelen om zowel bepaalde panelapplicaties te versleutelen als databases met speciale (gevoelige) categorieën persoonlijke gegevens, bijvoorbeeld over gezondheid, politieke mening, etc.
Tot slot, wat betreft haar medewerkers, is het belangrijkste managementsysteem voor het menselijk kapitaal van Ipsos, “iTalent”, volledig versleuteld.

5. Leveranciers

Ipsos volgt procedures voor het selecteren van leveranciers die persoonlijke gegevens verwerken om er zeker van te zijn dat ze voldoen aan de vereisten van Ipsos voor databescherming. Dat houdt in dat alle leveranciers een overeenkomst met Ipsos moeten ondertekenen, inclusief clausules voor databescherming die minimaal even streng zijn als degene die Ipsos ondertekent met haar klanten. Deze overeenkomst bepaalt dat geen enkele leverancier persoonlijke gegevens kan overdragen buiten de EEA, tenzij zij daarvoor akkoord zijn gegaan met passende waarborgen en toestemming van de klant hebben verkregen. Voorts mogen onze leveranciers hun diensten voor de verwerking van de persoonlijke gegevens niet gedeeltelijk uitbesteden aan onderaannemers zonder voorafgaande toestemming van Ipsos.

6. Gegevensoverdrachten

Ipsos heeft enkele contractuele maatregelen ingesteld voor gegevensoverdrachten binnen Ipsos over landsgrenzen heen en met haar leveranciers. Wanneer gegevensoverdracht vereist is in een land waarvan bekend is dat het geen adequaat databeschermingsniveau heeft, geeft Ipsos de verzekering dat de EU Standaard Contractuele Clausules van toepassing zijn, zodat de juiste technische en organisatorische maatregelen geïmplementeerd zijn voor de bescherming van de persoonlijke gegevens.
Ipsos zet zich voortdurend in voor de bescherming van persoonlijke gegevens van haar klanten, respondenten en werknemers. Als u vragen heeft of een verdere toelichting wenst, neem dan contact op met onze Data Protection Officer, te bereiken via DPO.Netherlands@ipsos.com.