General Data Protection Regulation (GDPR)

ALGEMENE VERORDENING GEGEVENSBESCHERMING (*AVG*)

Jaap Mengerink

8-4-2019

Why is GDPR important to Asahi?

Risks, Penalties and Benefits

Risk	Detail
Negative impact on sales, reputation and talent retention	Customers/employees are not comfortable sharing their data with Asahi; the brand is not trusted; confidence is lost
Enforcement regime	Fines up to €20,000,000 or 4% of total worldwide annual turnover
Individual and group action claims for compensation	More likely after GDPR (e.g. corporate reorganisation, mass redundancies)
Disgruntled employees/ex-employees and customers	Increased use of data protection rights as leverage in disputes
Criminal liability for Asahi and its directors (if imposed by local law derogations)	EU Member States may introduce other penalties applicable to infringements. In the UK, this means that Asahi and its Directors could face criminal liability for specific breaches
Regulators	Range of investigative, corrective, authorisation and advisory powers

Practical and commercial benefits of compliance:

1. differentiation from competitors;
2. instils trust and confidence in Asahi employees and customers that their personal data are in safe hands;
3. ability to be flexible and creative in how Asahi achieves compliance; and
4. helps to build a culture of awareness and responsibility.

Introduction to Asahi's new GDPR documentation (1)

Key new GDPR policies/documents:

Policy/document	Description
Privacy Policy (internal)	Contains the mandatory transparency information that Asahi must provide to employees, potential employees, interns and prospective interns under the GDPR. It describes: the information Asahi collects; how Asahi uses this personal data; the legal basis upon which Asahi process it; with whom it is shared; and how it is stored.
Privacy Policy (external)	Same as the internal privacy policy except that it applies to customers, website visitors, distributors, suppliers, personnel of suppliers and contractors.
Personal Data Protection and Handling Policy	Sets out Asahi's internal policy with regard to management and processing (which includes collection, storage, use, disclosure and transfer) of personal data of employees, contractors, customers and suppliers.

Wanneer geldt de AVG *(art 3. Personal Data Protection and Handling policy)*

Verwerkingen feitelijke handelingen* van;

- Persoonsgegevens dat op geheel of gedeeltelijk geautomatiseerde wijze geschiedt of in een bestand zijn opgenomen of daarvoor bestemd zijn

- in het kader van activiteiten van een vestiging in Nederland; of
- door een vestiging buiten EU: betrokkenen die zich in de EU bevinden en
  - Goederen of diensten aanbieden binnen de EU
  - Monitoren gedrag in de EU.

*Voorbeelden: verzamelen, opslag, kennisnemen van, met elkaar in verband brengen, analyseren

Definities *(art 3. Personal Data Protection and Handling policy)*

Persoonsgegevens: elk gegeven over geïdentificeerde of identificeerbare natuurlijke persoon

- Identificeerbaar = gekeken moet worden naar de middelen die redelijkerwijs inzetbaar zijn om identiteit te achterhalen
- Voorbeelden: NAW gegevens, e-mailadres, telefoonnummers, Profiel, foto, cv

Bijzondere persoonsgegevens: godsdienst of levensovertuiging, ras, politieke voorkeur; Gezondheid, seksuele leven, lidmaatschap van een vakbond, strafrechtelijk verleden, kopietje paspoort

Betrokkene: degene op wie de gegevens betrekking hebben, natuurlijke personen

Verantwoordelijke: heeft zeggenschap over doel en wijze van verwerking

Verwerker: verwerkt persoonsgegevens ten behoeve van de verantwoordelijke zonder aan haar of zijn rechtstreeks gezag te zijn onderworpen. Bijv. mailingbedrijf, administratiekantoor, outsourcing service provider, cloudleverancier.

Rechtsgrond *(art 5.1. Personal Data Protection and Handling policy)*

Alleen persoonsgegevens verwerken indien:

a) Toestemming
b) Overeenkomst (*nodig voor uitvoeren overeenkomst*)
c) Wettelijke plicht
d) Vitaal belang
e) Algemeen belang /Publieke taak
f) Gerechtvaardigd belang verantwoordelijke / derde dat vóór privacybelang betrokkene gaat

Toestemming (art. 10 Personal Data Protection and Handling policy and Guidance Note Consent Standards)

Toestemming: vrij, geïnformeerd en specifiek

a) De verantwoordelijke moet kunnen **aantonen** dat de betrokkene toestemming heeft gegeven;
b) De persoon moet bij het vragen van de toestemming worden **geïnformeerd over** het feit dat de toestemming altijd weer kan worden ingetrokken (NB: intrekking geldt voor toekomstige verwerkingen)
c) Het intrekken **moet net zo makkelijk** zijn als het geven van de toestemming
d) De toestemming moet door middel van een **uitdrukkelijke handeling** worden gegeven
e) De **toestemming is niet "vrij" als afhankelijk van levering dienst** en gegevens niet noodzakelijk voor overeenkomst
f) Toestemming is **niet "vrij" bij wanverhouding verantwoordelijke / betrokkene (werkgever, overheid)**
g) Als een verwerking meerdere doeleinden heeft, moet **voor elk doeleinde toestemming** worden gegeven
h) Als de betrokkene toestemming moet geven na een verzoek dat aan de betrokkenen is gericht via elektronische middelen, moet dat **verzoek duidelijk en kort zijn en niet onnodig storend voor het gebruik van de dienst**;
i) Als de toestemming wordt gevraagd in een schriftelijke verklaring, moet de toestemming voor het verwerken van de persoonsgegevens **duidelijk worden afgescheiden van de andere tekst**.

Informatieplicht (5.1 Personal data and protection policy and Fair Processing Notice)

Bestaande en nieuwe klanten dienen duidelijk te worden geïnformeerd over wat met hun persoonsgegevens wordt gedaan:

- online privacyverklaring *(algemene verklaring)*
- Eventueel fair processing note *(verkorte verklaring met specifieke informatie)*

Attenderen middels:

- Verwijzing naar privacyverklaring in contracten, introductiemateriaal en inschrijfformulieren
- Pop ups voor fair processing note bij webformulieren

Verantwoordingsplicht

De verantwoordelijkheid ligt bij organisaties om aan te tonen aan de privacyregels wordt voldaan.

o.a. door:

- Policy:
- Verwerking register: overzicht van de verschillende verwerkingen van persoonsgegevens die plaats vindt binnen Grolsch
  - welke persoonsgegevens
  - waarvoor worden deze verwerkt
  - dataretentie

De verwerkersovereenkomst (Template data processing clauses)

Indien een verwerker namens de verantwoordelijke persoonsgegevens verwerkt dan moet er een verwerkersovereenkomst worden gesloten (wettelijke verplichting)

Waarin onder andere opgenomen:

- *dat de verwerker de gegevens alleen in zijn opdracht verwerkt;*
- *voor passende technische en organisatorische beveiligingsmaatregelen zorgen;*
- *Toezien op naleving van de maatregelen (auditrecht).*

Datalekken (art 5.6. Personal Data Protection and Handling policy)

Datalekken meldplicht – “indien mogelijk binnen 72 uur” aan AP (autoriteit persoonsgegevens)

Datalek: Onbevoegde toegang, onbevoegde wijziging, vernietigd / verloren, onbevoegd verstrekt
Bijvoorbeeld: Hack, Gegevensdrager weg (telefoon, laptop etc.), Datacenter afgebrand zonder back-up

Nieuwe procedure:

- **Melden datalek middels Topdesk onmiddelijk na ontdekken datalek**
- Incident response team (legal/IT) beoordeelt of datalek aan AP wordt gemeld en zorgt voor melding

rechten betrokkenen (art 4.4 and 9. Personal Data Protection and Handling policy and Guidance Note: Handling Request from Individuals)

Rechten van de betrokkenen honoreren:

- Zoals het recht op **inzage/kopie**, **correctie** van onjuiste persoonsgegevens en onder bepaalde voorwaarden het recht op **verwijdering**
- Een dergelijk verzoek kan op elke wijze worden ingediend (geen vormvereiste), Grolsch is verplicht dit verzoek in behandeling te nemen

Nieuwe procedure:

- **Melding verzoek betrokkenen registreren middels Topdesk** (*naam telefoon/e-mailadres*) en aangeven welke categorie (bijv. horecaklant)
- Melding komt bij de betreffende aangewezen verantwoordelijke voor afhandeling en wordt afgewikkeld