

ALGEMENE VERORDENING GEGEVENSBESCHERMING (AVG)

Vanaf 25 mei 2018 geldt voor heel Europa één privacyregeling. De nationale wetgeving komt hierdoor grotendeels te vervallen. Dit heeft grote gevolgen voor de Rotterdamse Haven. Deltalinqs ondersteunt haar leden bij het samenstellen van een effectief en solide beleid rondom informatiebeveiliging en privacygevoelige gegevens.

Duidelijke regels over privacy en gegevensbescherming zijn van ongekend belang. De invoering van de Algemene Verordening Gegevensbescherming (AVG) betekent dat vanaf 25 mei 2018 voor heel Europa dezelfde regels gaan gelden ten aanzien van het verwerken van persoonsgegevens. Europa staat daarmee aan de vooravond van een omvangrijke herinrichting van de privacywetgeving. Dit heeft grote consequenties voor bedrijven in de Rotterdamse haven. Samengevat zal deze nieuwe algemene verordening meer bescherming bieden aan betrokken personen, maar ook meer verantwoordelijkheid neerleggen bij de gebruikers van persoonsgebonden gegevens (bedrijven en andere organisaties) met aanzienlijke administratieve rompslomp als gevolg.

Toestemming

Het uitgangspunt van de AVG is dat bedrijven persoonsgegevens niet zonder meer mogen verwerken en beheren. Elk bedrijf verwerkt, al dan niet bewust, persoonsgegevens. Denk aan namen, adressen en telefoonnummers van klanten, medewerkers, bezoekers en ingeleend personeel. Daarnaast zijn er veel data afkomstig van telemetrie, procesbesturingssystemen (SCADA, DCS) en logistieke informatie.

De verordening verplicht bedrijven waakzaam te zijn bij het beheren en verwerken van deze gegevens. Zo is het bijvoorbeeld vereist dat uw klant expliciet en ondubbelzinnig toestemming verleent, voordat u rechtmatig persoonsgegevens mag verwerken.

Stappenplan

De Autoriteit Persoonsgegevens (AP) zal de verantwoordelijkheden en bijbehorende zorgplicht die bedrijven krijgen opgelegd vanuit de AVG toetsen en handhaven. Om bedrijven te helpen bij de voorbereidingen op de nieuwe Europese privacywetgeving heeft de AP een 10-stappenplan opgesteld. Een belangrijke stap is het creëren van bewustzijn in de organisatie en het informeren van betrokkenen over hun rechten. Daarnaast adviseert de toezichthouder organisaties onder meer in kaart te brengen met welk doel zij bepaalde persoonsgegevens verwerkt, waar de gegevens vandaan komen en met wie de organisatie ze deelt. Onder de AVG moeten organisaties een register bijhouden om te kunnen aantonen dat ze in overeenstemming met de wet handelen.

Privacy Impact Assessment

U zult als bedrijf ook aan moeten tonen met welk rechtmatig doel u persoonsgegevens wilt gaan verwerken. Het is goed mogelijk dat u verplicht bent om een Privacy Impact Assessment (PIA) uit te voeren. De PIA is een instrument om vooraf de privacyrisico's van gegevensverwerking in kaart te brengen, om vervolgens maatregelen te kunnen nemen om de risico's te verkleinen. Zo'n assessment is verplicht als een gegevensverwerking waarschijnlijk een hoog privacyrisico oplevert voor de mensen van wie de organisatie gegevens verwerkt. Aangezien bepaalde typen bedrijven op grond van andere wetgeving, zoals havenbeveiliging (ISPS) of douanefaciliteiten (AEO) veelvuldig

persoonsgebonden gegevens verzamelen zal deze verplichting vrij snel van toepassing zijn.

Mogelijke knelpunten

Vanzelfsprekend willen bedrijven aan de geldende wet- en regelgeving voldoen. Tegelijkertijd zien ze zich vaak geconfronteerd met conflicterende wetgeving en andere belangen. Zo stelt de AVG grenzen aan het mogen verwerken van privacygevoelige informatie, terwijl havenbeveiligingswetgeving juist voorschrijft om persoonsgebonden informatie van bijvoorbeeld bezoekers te verifiëren. Ook bij het tewerkstellen van ingehuurd personeel, zoals bijvoorbeeld het geval is bij grote onderhoudstops, komen diverse regels en belangen met elkaar in botsing. Dat kan leiden tot onduidelijkheden in de praktijk. Om compliant te zijn aan de AVG en zeer forse boetes – maximaal 20 miljoen Euro of 4% van de mondiale omzet – te voorkomen, is het dus noodzakelijk om te inventariseren waar de dagelijkse praktijk tot knelpunten leidt en hoe je het beste kunt handelen.

Privacy Gedragscode

Alle bedrijven die hiermee te maken krijgen, hebben dus een gemeenschappelijk probleem. Daarom is het opstellen van één Privacy Gedragscode een goed middel om te beschrijven hoe bedrijven met vergelijkbare werkprocessen met privacygevoelige informatie omgaan. De AVG stimuleert het opstellen van een code die bijdraagt aan een juiste toepassing van de verordening en stelt dat daarbij de kenmerken en behoeften van de sector in acht kunnen worden genomen. De AVG vereist evenwel goedkeuring van de gedragscode door de Autoriteit Persoonsgegevens.



WAT DOET DELTALINQS?

1. BEWUSTWORDING EN KENNISUITWISSELING

Deltalinqs organiseert workshops voor haar leden over de impact die de AVG kan hebben voor de bedrijven in de Rotterdamse haven. De workshops zijn bedoeld om bewustwording te creëren en kennis uit te wisselen over de mogelijke gevolgen van de AVG voor werkprocessen zoals het aanmelden van bezoekers op ISPS-locaties, het beveiligen van de logistieke keten (AEO) en het toepassen van het XS-Key systeem (CargoCard, DSP).

2. INFORMATIEVERSTREKKING

Alle leden van Deltalinqs hebben recent een digitaal informatiepakket ontvangen met daarin onder meer de relevante wet- en regelgeving, het 10-stappenplan van de AP en enkele relevante artikelen.

3. ONTWIKKELEN PRIVACY GEDRAGSCODES

In de verschillende Deltalinqs-overlegorganen is de behoefte aan een eenduidig privacybeleid geuit. Het is namelijk goed mogelijk dat de verplichtingen van de AVG botsen met de regelgeving voor ISPS en/of AEO. Met de code kan een bedrijf bij het bevoegde gezag – de Autoriteit Persoonsgegevens – aantonen dat het alles in het werk heeft gesteld om zo goed mogelijk aan beide regimes te voldoen. Deltalinqs faciliteert en ondersteunt het (laten) opstellen van een Privacy Gedragscode door de onderneming Port Privacy BV, welke vooral gericht is op de leden van Deltalinqs die ISPS- en/of AEO-gecertificeerd zijn. In de begeleidende projectgroep zijn vertegenwoordigers van bedrijven uit verschillende sectoren betrokken evenals het Havenbedrijf Rotterdam, de Douane en de Zeehavenpolitie. De kosten voor

het opstellen en in stand houden van deze Privacy Gedragscode wordt volledig gedragen door de deelnemende ISPS- en/of AEO-gecertificeerde bedrijven. Daarnaast zullen zij ook jaarlijks ge-audit worden.

Verder onderzoekt Deltalinqs of het wenselijk is om een vergelijkbare Privacy Gedragscode te ontwikkelen voor knelpunten rondom het inzetten van inleenschakelingen (Wet ketenaansprakelijkheid en de Wet Arbeid Vreemdelingen). Deltalinqs voert hiertoe gesprekken met de directies van VOMI, VRC en TLN.

PLANNING

De AVG zal vanaf 25 mei 2018 van toepassing zijn.

In het voorjaar van 2018 zal een bijeenkomst worden georganiseerd die specifiek zal ingaan op de gevolgen van de AVG voor het inhuren en/of inzetten van flexibel personeel.

BETROKKEN PARTIJEN

VOMI, TLN, Secure Logistics BV, Port Privacy BV.

NASLAGWERK:

1. Algemene verordening gegevensbescherming (AVG), VERORDENING (EU) 2016/679.
2. Publicatie van de AVG: In 10 stappen voorbereid op de AVG.
3. Publicatie van de AVG: De AVG in een notendop.
4. Infazine over de bescherming van digitale gegevens.

CONTACT

Peter van Loo, Veiligheid & Security