Privacy - heden & toekomst

Wat je minimaal moet weten om privacy compliant te worden

Privacy en gegevensverwerking

Door de aangescherpte wet- en regelgeving verdwijnt privacy in een rap tempo uit de hoek van randvoorwaarden waaraan ondernemingen met minimale inspanning kunnen voldoen. Het op de juiste wijze gebruiken én beschermen van persoonsgegevens wordt een hygienefactor én een serieus bedrijfsrisico. Organisaties kunnen zich hier maar beter goed op voorbereiden. In deze whitepaper leest u hier meer over.

Het recht op privacy is sinds jaar en dag gewaarborgd in wetten en internationale verdragen. Maar steeds meer mensen maken zich zorgen over wat er met hun digitale data kan gebeuren. Ongemak dat alleen maar toeneemt sinds klokkenluider Edward Snowden onthulde dat de Amerikaanse veiligheidsdienst NSA via social media sites meekijkt in de privégegevens van gebruikers wereldwijd. De aankondiging in 2014 dat een Nederlandse grootbank klantgegevens en informatie over betaalgedrag zou gaan verkopen droeg verder bij aan de maatschappelijke onrust. Datzelfde geldt voor het recente bericht van een Nederlandse energieleverancier dat de gegevens over energiecontracten van twee miljoen huishoudens gestolen waren.

Wet bescherming persoonsgegevens

De belangrijkste regels voor de omgang met persoonsgegevens in Nederland zijn vastgelegd in de Wet bescherming persoonsgegevens (Wbp). Zo moet een organisatie die persoonsgegevens verwerkt, dit melden bij de Autoriteit Persoonsgegevens (AP), de interne Privacy Officer of de Functionaris Gegevensbescherming (FG). In Nederland is de Autoriteit Persoonsgegevens (AP) belast met het toezicht op de handhaving van de regels voor bescherming van persoonsgegevens. Op 1 januari 2016 is de Wbp aangescherpt met de Meldplicht datalekken. Deze is bedoeld om het grote aantal datalekken waar persoonsgegevens bij betrokken zijn in te dammen: naar schatting ieder jaar zo'n 62.000. Niet ieder incident leidt direct tot identiteitsfraude of andere ernstige inbreuken op de privacy. Maar dit gevaar loert altijd, dus moet je er goed op voorbereid zijn.

Meldplicht datalekken

Als door een inbreuk op de beveiliging een ernstig datalek ontstaat, moet een organisatie dit voortaan direct melden. Als dit ten onrechte niet gebeurt, kan de AP een boete opleggen. Deze meldplicht vereist dat een organisatie bij een reëel risico op verlies of onrechtmatige verwerking van persoonsgegevens snel en effectief kan aangeven waar het lek zich bevindt, welke data worden geraakt en wie er geïnformeerd dient te worden. Een andere belangrijke wijziging is de aanpassing van de bevoegdheden van de toezichthoudende autoriteit. Niet alleen zijn de boetebevoegdheden uitgebreid, ook de boetebedragen zijn verhoogd. Sinds 1 januari kan de AP organisaties die de Wet bescherming persoonsgegevens overtreden een boete opleggen tot maximaal 820.000,- euro of 10% van de jaaromzet.

De toekomst: één privacywet in de hele EU

Per 25 mei 2018 is de nieuwe Europese privacyverordening rechtstreeks van toepassing in alle EU-lidstaten: de Algemene Verordening Gegevensbescherming (AVG). Zij vervangt dan de Wbp. Alle organisaties in de publieke en private sector worden geacht om voor 25 mei 2018 hun bedrijfsvoering in overeenstemming met de AVG te brengen. Vanaf deze datum geldt in de hele EU nog maar één privacywet, in plaats van 28 verschillende nationale wetten. De AVG heeft belangrijke consequenties voor alle organisaties die persoonsgegevens opslaan en verwerken. Zo kan iedereen hen op de naleving van de AVG aanspreken en lopen de boeterisico's op tot 20 miljoen euro of maximaal 4% van de wereldwijde jaaromzet. Bedragen die de continuïteit van een organisatie ernstig in gevaar kunnen brengen.

Wat betekenen deze ontwikkelingen voor uw organisatie?

In de AVG wordt meer nadruk gelegd op de verantwoordelijkheid van organisaties om controle over de gebruikte persoonsgegevens te hebben. Zij dienen de bedrijfsprocessen op orde te hebben, en de data en datastromen aantoonbaar te identificeren, classificeren én beschermen. Vanwege deze accountability hebben organisaties een documentatieplicht. Nederlandse organisaties hoeven verwerkingen van persoonsgegevens straks niet meer bij de AP te melden. Wel zijn ze verplicht om met de bewerker van persoonsgegevens een bewerkingsovereenkomst te sluiten. Verder worden organisaties die dataverwerking als kernactiviteit hebben, verplicht om een functionaris voor de gegevensbescherming (FG) aan te stellen en om privacy impact assessments (PIA's) uit te voeren.

Privacybewustzijn

Waar het op neerkomt is dat iedereen die persoonsgegevens verwerkt, moet waken tegen elke vorm van inbreuk en misbruik. Zaak dus om een raamwerk te ontwikkelen dat u de zekerheid geeft over de bescherming van de persoonsgegevens die binnen uw organisatie worden verwerkt. Over de bescherming van data, de privacy en compliance. Maar u kunt de processen en systemen nog zo goed beveiligen, de praktijk leert dat de medewerker de zwakste schakel in de keten is. Uw medewerkers dienen zich bewust te zijn van de risico's en hun gedrag hierop aan te passen. Het is voor lang niet iedereen even vanzelfsprekend om vooraf na te denken over het type gegevens dat verwerkt wordt en de benodigde beschermingsmaatregelen. De bewustwording onder uw medewerkers is dus van groot belang.

Wat te doen?

Allereerst dient u de datastromen in kaart te brengen en te inventariseren in hoeverre u handelt in overeenstemming met de privacywetgeving en de aankomende AVG. Deze resultaten kunnen als uitgangspunt dienen bij het bepalen van privacy- en securitybeleid en eventuele aanpassingen in bedrijfsprocessen en data-architectuur. Zorgt u er ook voor dat uw medewerkers blijvend op de hoogte zijn van gewenste gedragsregels Hiervoor kunt u bijvoorbeeld awareness-trainingen inzetten. Verder dient u een risicoanalyse te doen en wellicht een FG/ Privacy Officer aan te stellen. Zo'n privacy professional met de juiste ervaring op het gebied van gegevensbescherming mag u ook op interim-basis inschakelen. DPA Privacy voorziet u graag van specialistisch advies en oplossingen voor privacy-compliance.

Vertrouwen en continuïteit

Het waarborgen van de privacy van uw relaties heeft twee kanten. Ja, het is een forse uitdaging om privacy te borgen in uw bedrijfsstrategie. En ja, het kost tijd en geld om aantoonbaar 'in control' en privacy-compliant te zijn. Maar bekijk het vooral ook van de andere kant. Met een gedegen privacystrategie wint u het vertrouwen van uw medewerkers, klanten en andere stakeholders. En zullen zij eerder geneigd zijn om data met u te delen. Zo beschikt u over actuele informatie die u in staat stelt om snel en gericht in te spelen op nieuwe ontwikkelingen en veranderende klantbehoeften. Op deze manier beschermt u niet alleen de belangen van de betrokkenen, maar ook de reputatie van uw organisatie en de continuïteit van de bedrijfsvoering.

Aantoonbaar in control en privacy-compliant zijn:

Privacyrechten van betrokkenen (degenen op wie de gegevens betrekking hebben):

- Informatie krijgen over de doeleinden van de verwerkingen;
- Inzage krijgen in verwerkingen;
- Recht op vergetelheid: verwijdering persoonsgegevens (AVG);
- Aanpassen en overdracht van persoonsgegevens naar andere organisatie (AVG);
- Recht op beperking of beëindiging van de verwerking.

Privacyverantwoordelijkheden voor organisaties:

- Rechtsgeldige grondslag voor verwerking;
- Aantoonbare geldige toestemming voor gegevensverwerking;
- De juiste organisatorische en technische maatregelen;
- Uitvoeren van privacy impact assessment (PIA);
- Aanstellen functionaris voor de gegevensbescherming (FG);
- Datalekken en inbreuken op persoonsgegevens melden.

Sancties

- Bij een datalek kan een bestuurlijke boete worden opgelegd met een maximum van 500.000 euro. In bijzondere gevallen kan de toezichthouder een hogere boete opleggen: tot 820.000 euro of, als dat niet passend is 10% van de netto jaaromzet van de onderneming.
- Bij niet naleving van de verplichting om een PIA uit te voeren: maximaal 10 miljoen euro of 2% van de wereldwijde omzet.
- Risico bij ernstige overtreding: maximaal 20 miljoen euro of 4% van de totale wereldwijde jaaromzet

Begrippenlijst

Persoonsgegevens
Alle gegevens die zo kenmerkend zijn voor een persoon dat hij/zij aan de hand van die gegevens geïdentificeerd kan worden. Naast NAW-gegevens zijn dit bijvoorbeeld telefoonnummers, e-mailadressen, bankrekeningnummers, inkomensgegevens, IP-adressen, (pas)foto's en vingerafdrukken.

Bijzondere persoonsgegevens
Gegevens die zo gevoelig zijn dat de verwerking iemands privacy ernstig kan aantasten. Dit zijn bijvoorbeeld gegevens over iemands ras, godsdienst, gezondheid, strafrechtelijk verleden, seksuele leven, lidmaatschap van een vakvereniging en het burgerservicenummer (BSN). Deze zijn door de wetgever extra beschermd.

Betrokkene
Degene(n) op wie de persoonsgegevens betrekking hebben.

Verwerking van persoonsgegevens
Elke handeling met betrekking tot persoonsgegevens. Ofwel: het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekking door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen en vernietigen van gegevens. Eigenlijk valt alles wat we met persoonsgegevens doen onder 'verwerking'.

Bewerkers- of verwerkersovereenkomst
De overeenkomst tussen verantwoordelijke en bewerker, waarin wordt vastgelegd hoe de bewerker met de persoonsgegevens moet omgaan.

Datalek
Bij een datalek zijn de persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking – dus aan datgene waartegen de beveiligingsmaatregelen bescherming moeten bieden. Daardoor kan inbreuk op persoonsgegevens worden gemaakt. Voorbeelden van datalekken zijn een kwijtgeraakte USB-stick met (persoons)gegevens, een gestolen laptop of een inbraak in een databestand door een hacker.

Meldplicht datalekken
Als een datalek tot aanzienlijke kans op ernstige nadelige gevolgen leidt of ernstige nadelige gevolgen voor de bescherming van persoonsgegevens heeft, dient het binnen 72 uur gemeld te worden bij de Autoriteit Persoonsgegevens en soms ook aan degenen van wie de persoonsgegevens zijn gelekt. De verantwoordelijke dient tevens een overzicht bij te houden van iedere inbreuk die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen of ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens.

Doelbinding
Persoonsgegevens mogen alleen voor welbepaalde, vooraf uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld. En vervolgens alleen worden verwerkt voor doeleinden die daarmee verenigbaar zijn. Degene van wie persoonsgegevens worden verwerkt (de betrokkene), moet ten minste op de hoogte zijn van de identiteit van de organisatie of persoon die deze persoonsgegevens verwerkt (de verantwoordelijke) en van het doel van de gegevensverwerking.

Rechtvaardigingsgronden
Voor elke verwerking van persoonsgegevens dient aan de wettelijke regels voldaan te worden. Bovendien dient ten minste één van de volgende zaken van toepassing te zijn: toestemming betrokkene, uitvoering overeenkomst, wettelijke verplichting, vitaal belang, publiekrechtelijke taak of gerechtvaardigd belang.

Functionaris voor de gegevensbescherming (FG)
Functionaris die binnen de organisatie toezicht houdt op de toepassing en naleving van de Wbp.

Privacy impact assessment (PIA)
Onderzoek met als doel om inzicht te krijgen in de risico's van de gegevensverwerking zodat passende maatregelen genomen kunnen worden.

Wilt u meer weten over de mogelijkheden van ondersteuning bij uw privacy-project? Neem dan contact op met ons op.

DPA Privacy
Paul Schraven
t +31 (0)652 30 22 40
paul.schraven@dpa.nl
www.dpa.nl/privacy