EEN INLEIDING OP

AVG

Wat betekent de nieuwe verordening inzake gegevensbescherming voor u en uw bedrijf?

Cordery® Legal.Compliance

Fellowes Brands™

Waar gaat de AVG eigenlijk over?

De Europese Unie (EU) heeft haar gegevensbeschermingsregels gewijzigd. Deze wijzigingen zijn rechtsgeldig en treden op 25 mei 2018 in de hele EU in werking. De nieuwe regelgeving heet Algemene Verordening Gegevensbescherming (AVG) en is overal van toepassing, van overheidsinstanties tot kleine en middelgrote bedrijven. Deze wijzigingen beïnvloeden de manier waarop we zakendoen.

Deze nota geeft een basisinleiding op AVG en in het bijzonder op de invloed ervan op het werken op een kantoor.

Wat is EU-gegevensbescherming?

In de EU bestaan wettelijke voorschriften voor de verzameling en verwerking van persoonsgegevens. Iedereen die persoonsgegevens verzamelt of verwerkt, moet deze beschermen tegen misbruik en zich houden aan diverse wettelijke voorschriften. De AVG bouwt de bestaande regelgeving verder uit.

Zijn deze nieuwe regels van toepassing op zowel elektronische als gedrukte gegevens?

Ja. De AVG is van toepassing op elektronische gegevens (zoals e-mail en databases) en gedrukte gegevens (met enkele uitzonderingen). Dit houdt in dat we ook verantwoordelijkheid hebben voor papieren bestanden - deze moeten veilig bewaard worden en wanneer we ze niet meer nodig hebben, veilig verwijderd worden (bijvoorbeeld in een beveiligde papiervernietiger).

U loopt het risico op een boete van

€20 miljoen

of 4% van uw jaarlijkse omzet

Welke boetes kunnen aan mijn bedrijf worden opgelegd als de voorschriften worden overtreden?

Onder de nieuwe regelgeving kunnen de toezichthouders voor gegevensbescherming hoge boetes opleggen voor het overtreden van de voorschriften. De boete is maximaal € 20 miljoen of 4% van de wereldwijde jaaromzet van een onderneming (afhankelijk van welk bedrag het hoogst is). Hoewel niet elke overtreding tot de hoogste boete zal leiden, is het krijgen van een boete absoluut geen optie - we moeten ervoor zorgen dat we ons houden aan de voorschriften.

Moeten bedrijven meer gaan doen?

Ja. Onder de nieuwe regels heeft elke organisatie meer verantwoordelijkheden en verplichtingen. Organisaties moeten in het bijzonder technische en organisatorische maatregelen nemen om te verzekeren dat ze gegevens correct verwerken. Er moet rekening worden gehouden met de verwerkingsrisico's, zoals het per ongeluk of op onrechtmatige wijze vernietigen van gegevens, om het juiste veiligheidsniveau te beoordelen. U moet kunnen aantonen welke maatregelen u hebt genomen wanneer de toezichthouder u hierom vraagt. Een belangrijk onderdeel is het controleren aan wie u persoonsgegevens toestuurt - u dient bijvoorbeeld ook de processen te controleren van personen en/of bedrijven met wie u werkt, zoals mailingbedrijven, versnipperingsbedrijven en uitzendbureaus.

Zijn er voorbeelden van gevallen waar men fouten heeft gemaakt?

- **Het niet naleven van de voorschriften kan pijnlijke gevolgen hebben.** De Britse toezichthouder voor gegevensbescherming, de 'Information Commissioner's Office' (ICO), heeft onlangs aan een gemeentelijke overheid een boete van £ 100.000 opgelegd wegens nalatigheid van het treffen van veiligheidsmaatregelen tegen het per ongeluk verliezen of vernietigen van gegevens. Het betrof documenten met de persoonsgegevens van ongeveer 100 personen (onder wie volwassenen en kinderen in kwetsbare omstandigheden), die werden aangetroffen door de koper van een leegstaand gebouw dat voorheen werd gebruikt door de gemeente. Dit gebeurde toen de gemeentelijke overheid verhuisde en daarbij een aantal documenten in het gebouw achterliet.

- In Nederland zijn enkele openbaarvervoerbedrijven door de toezichthouder voor gegevensbescherming beboet, omdat ze bepaalde transactiegegevens langer hadden bewaard dan nodig was. De toezichthouder gaf de bedrijven in eerste instantie opdracht om ofwel de transactiegegevens te verwijderen of deze te anonimiseren - zij besloten om de gegevens te bewaren, maar de anonimiseringstechnieken waren in ten minste één geval ontoereikend en een van de bedrijven kreeg een **boete opgelegd van € 125.000.**

- In Spanje hebben zich verschillende handhavingszaken voorgedaan waarbij documenten met persoonsgegevens in de vuilnisbak of op straat terechtkwamen - in ten minste één geval was de documentatie slechts gedeeltelijk versnipperd en in andere gevallen was het dumpen het gevolg van het nalaten van het versnipperen of correct vernietigen van de documenten.

Moet gegevensbescherming een centrale rol innemen in wat ik doe?

Ja. Privacy moet in alle processen worden ingebouwd. Bedrijven moeten procedures opstellen die ervoor zorgen dat er standaard alleen persoonsgegevens worden verwerkt waarvoor dat ook echt nodig is. Daarom moet u zich steeds afvragen:

- Heb ik deze persoonsgegevens nodig?
- Moet ik ze voor dit doel verwerken?
- Heeft iedereen die toegang heeft ook toegang nodig? (Voorbeeld: als alleen HR de papieren behoort te zien, moeten deze in een afgesloten dossierkast worden opgeborgen waarvan alleen HR de sleutels heeft.)
- Zijn de gegevens verouderd?

Is voor gegevensverwerking toestemming nodig?

Ja. In het algemeen moet er een legitieme reden zijn voor de verwerking van persoonsgegevens. Als voor de verwerking van gegevens toestemming moet worden gegeven, moet volgens de nieuwe regels de door de betrokkene gegeven toestemming een vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting zijn. Stilzwijgen, opt-out of inactiviteit kan niet als toestemming gelden. In plaats daarvan moet er een actieve procedure worden ingesteld, bijvoorbeeld het selecteren van vakjes. Bedrijven moeten bovendien kunnen aantonen dat de toestemming inderdaad is gegeven. Wees er zeker van dat alle procedures om aan al deze eisen te voldoen geïmplementeerd zijn.

Zijn er ook nieuwe rechten?

Ja. Er zijn diverse nieuwe rechten ingevoerd, zoals:

- Het recht op vergetelheid - personen mogen verzoeken dat hun persoonsgegevens worden verwijderd;
- Het recht op overdraagbaarheid van gegevens - personen mogen verzoeken dat hun persoonsgegevens die in een algemeen gebruikt formaat zijn opgeslagen, worden overgedragen; en
- Het recht van bezwaar – hieronder valt het recht om bezwaar te maken tegen geprofileerd worden. Indien persoonsgegevens worden verwerkt ten behoeve van direct marketing, kan hiertegen ook bezwaar worden gemaakt.

De implementatie van deze nieuwe rechten zal een uitdaging zijn voor organisaties, hoewel moet worden benadrukt dat al deze nieuwe rechten aan bepaalde beperkingen onderhevig zijn. Dit betekent dat er enkele uitzonderingen zijn waarvoor juridisch advies moet worden ingewonnen.

Hoe zit het met personen die verzoeken om inzage in hun gegevens?

Het recht dat personen hebben om hun gegevens in te zien, hetgeen technisch gezien een toegangsverzoek van betrokkene is, blijft van kracht onder de nieuwe regelgeving. Deze procedure geeft iedereen het recht op toegang tot gegevens die van hen worden bewaard. Onder de nieuwe regels moet binnen zes maanden na ontvangst aan een toegangsverzoek gehoor worden gegeven (hoewel deze periode in bepaalde omstandigheden met twee maanden kan worden verlengd). Verder is het recht van bedrijven om voor een toegangsverzoek geld in rekening te brengen afgeschaft. In de afgelopen jaren is het aantal toegangsverzoeken aanzienlijk gestegen. Wanneer toegangsverzoeken gratis worden, valt een sterke stijging van het aantal verzoeken te verwachten. Gezien de groei van e-mail- en cloud-toepassingen, zijn toegangsverzoeken nu ook duurder en gecompliceerder om te verwerken.

Het instellen van goede procedures voor de afhandeling van toegangsverzoeken zal daarom voor organisaties een essentieel onderdeel zijn van hun toekomstige strategie voor gegevensbescherming.

U moet goede processen opstellen voor het omgaan met **TOEGANGS-VERZOEKEN**

Moet ik een functionaris voor gegevensbescherming aanstellen?

Mogelijk wel. Onder de AVG moeten overheidsinstanties een functionaris voor gegevensbescherming aanstellen. Een functionaris voor gegevensbescherming moet ook worden aangesteld bij bedrijven zodat zij in bepaalde omstandigheden kunnen voldoen aan de voorschriften voor de gegevensbescherming. In dit geval is het beter om hierover juridisch advies in te winnen, afhankelijk van wat u doet en waar u het doet. Gezien het belang dat tegenwoordig wordt

gehecht aan naleving van privacy voorschriften dient zelfs een middelgrote onderneming die regelmatig gegevens verwerkt, te overwegen om een functionaris voor gegevensbescherming aan te stellen, zelfs als dit vanuit technisch oogpunt niet verplicht is.

Moet ik inbreuk op gegevens melden?

Ja. Ervoor zorgen dat gegevens veilig zijn, zoals de aanpak van inbreuk op gegevens, is een van de pijlers van de nieuwe regelgeving.

> Een inbreuk op gegevens kan betrekking hebben op een groot aantal situaties, waaronder de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot persoonsgegevens.

Inbreuk moet zonder onnodige vertraging en (indien haalbaar) uiterlijk binnen 72 uur nadat men ervan op de hoogte komt, worden gemeld (inclusief de stappen die zijn genomen om inbreuk te beperken) aan de relevante toezichthouder. Betrokkenen die door de inbreuk getroffen zijn, moeten hierover eveneens zonder onnodige vertraging worden ingelicht (hoewel hiervoor geen officiële termijn is gesteld) als de inbreuk waarschijnlijk zal resulteren in een hoog risico voor hun rechten en vrijheden. Voor het melden aan een toezichthouder en het informeren van personen gelden enkele beperkte uitzonderingen waarvoor goed juridisch advies moet worden ingewonnen.

Het melden van inbreuk op gegevens wordt nog verder gecompliceerd doordat:

- Bepaalde landen (waaronder Oostenrijk, Duitsland en Nederland) al een eigen meldingsplicht voor inbreuk op gegevens hebben;
- Het melden van inbreuk op gegevens volgens andere richtlijnen en voorschriften verplicht kan zijn, in het bijzonder in de financiële sector en de gezondheidssector; en
- Afzonderlijke aanvullende wetgeving zal worden geïmplementeerd in de EU in overeenstemming met Europese Richtlijn Cyberveiligheid.

Hoe zit het met aansprakelijkheid en schadevergoeding?

Als algemeen beginsel geldt dat iedereen die schade heeft geleden als gevolg van een schending van de nieuwe regelgeving, recht heeft op schadevergoeding van de degenen die de betreffende persoonsgegevens beheren of verwerken, behoudens enkele uitzonderingen. Gezien het extra risico dat een inbreuk op gegevens onder de nieuwe regelgeving met zich meebrengt, moeten bedrijven al het mogelijke doen om de kans op schadeclaims te minimaliseren.

Bedrijven moeten daarom de hoogste prioriteit geven aan de implementatie van een duidelijk actieplan en beleid tegen de inbreuk van gegevens en hun personeel hiervoor opleiden

Moeten er beoordelingen van de gevolgen voor de privacy plaatsvinden?

Ja. Onder de nieuwe regelgeving worden deze beoordelingen privacy effectbeoordelingen genoemd. Wanneer een soort verwerking (in het bijzonder een verwerking waarbij nieuwe technologieën worden gebruikt) een hoog risico inhoudt voor de rechten en vrijheden van personen, moet vóór de verwerking een beoordeling worden uitgevoerd van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens. Er moet een toezichthouder voor gegevensbescherming worden geraadpleegd (opnieuw vóór de verwerking) indien de verwerking een hoog risico zou opleveren wanneer er geen maatregelen worden genomen om het risico te beperken.

Privacy effectbeoordelingen zullen waarschijnlijk steeds gebruikelijker worden en zullen een zeer nuttig middel blijken voor bedrijven voor de aanpak van privacy risico's, zoals de beoordeling van risico's voor gegevensbeveiliging en de overweging van risico's in verband met de verwerking van persoonsgegevens, zoals het per ongeluk of op onrechtmatige wijze vernietigen van gegevens.

Is er iets veranderd aan de gegevensoverdracht aan derde landen?

Nee. De speciale bestaande voorschriften voor gegevensoverdracht van EU-lidstaten naar derde landen (inclusief de VS) blijven gelijk onder de AVG, inclusief de vereiste dat de gegevensoverdracht slechts kan plaatsvinden als deze derde landen een passend beschermingsniveau waarborgen. Onder de nieuwe regelgeving zijn deze voorschriften meer gedetailleerd geworden. Dit is een ingewikkeld onderwerp dat bovendien onderhevig is aan ontwikkeling onder de bestaande voorschriften voor gegevensbescherming die u met uw juridische afdeling moet bespreken.

Waar kan ik meer informatie vinden?

De nieuwe regelgeving staat op deze website van de Europese Commissie

Wat moet ik nu doen?

Om u voor te bereiden op het voldoen aan de AVG dient u uw middelen te begroten en te plannen (waaronder ICT). Gebruik uw planningstijd ook om u aan te passen. Dit zijn de tien belangrijkste nalevingskwesties die moeten worden aangepakt:

1. Voer een procedure voor privacy effectbeoordeling in - breng uw gegevens in kaart en stel de risicogebieden vast;
2. Voer een grondige herziening van leverancierscontracten uit - u hebt de hulp van uw leveranciers nodig, in het bijzonder voor het zeer snel melden van beveiligingsinbreuken. Zorg er daarom voor dat u contractueel het recht hebt om dit te eisen;
3. Actualiseer systemen en materialen en stel gedetailleerde nieuwe documentatie en verslagen op die klaar zijn voor productie voor officiële inspectie;
4. Toets belangrijke praktische aspecten, zoals het behoud van gegevens, aan de hand van alle gegevens die door het bedrijf worden gebruikt;
5. Zorg ervoor dat u beschikt over plannen om gegevens die u niet nodig hebt veilig te vernietigen;
6. Zorg ervoor dat nieuwe aspecten, zoals uitdrukkelijke toestemming, het recht op vergetelheid, het recht op overdraagbaarheid van gegevens en het recht op bezwaar, allemaal worden opgenomen in uw beleid en procedures;
7. Zorg voor een procedure voor het melden van inbreuk op gegevens, zoals detectie- en reactievermogen en oefen deze procedure zoals u zou doen bij een brandoefening;
8. Overweeg om een functionaris voor gegevensbescherming aan te stellen;
9. Training, training, training - train het personeel in al het bovenstaande (de toezichthouder voor gegevensbescherming schenkt hier speciale aandacht aan); en
10. Zorg voor nalevingscontroles die regelmatig plaatsvinden om problemen op te sporen en te herstellen.

Expertise

Jonathan Armstrong en **André Bywater** van **Cordery Compliance** hebben ruime ervaring in het geven van advies m.b.t. tot AVG en hebben ons geholpen om dit whitepaper op te stellen.

www.corderycompliance.com

Jonathan Armstrong
Cordery
Lexis House
30 Farringdon Street,
London, EC4A 4HH
Verenigd Koninkrijk
+44 (0)207 075 1784
jonathan.armstrong@corderycompliance.com

André Bywater
Cordery
Lexis House
30 Farringdon Street
London, EC4A 4HH
Verenigd Koninkrijk
+44 (0)207 075 1785
andre.bywater@corderycompliance.com

Over Fellowes: Fellowes' missie is het bieden van innovatieve werkplekoplossingen die men helpen om veilig, comfortabel en productief te werken, zoals kantoormachines, werkplek ergonomie en archiveringsoplossingen.

www.fellowes.com

Fellowes Ltd
Fellowes Benelux
Gesworenhoekseweg 3a
5047 TM Tilburg
Nederland
cs-benelux@fellowes.com

Cordery® Legal.Compliance

Fellowes Brands™