
checklist
in 10 stappen
voorbereid op de AVG.
randstad
human forward.

checklist: in 10 stappen voorbereid op de AVG

Het zal u vast niet ontgaan zijn: per 25 mei 2018 moet uw organisatie voldoen aan nieuwe privacyregels. Op die datum treedt de Algemene verordening gegevensbescherming (AVG) in werking en vervalt de huidige Wet bescherming persoonsgegevens (Wbp). De invoering van de AVG vraagt echter het nodige van uw organisatie. Als u nog niet met de transitie begonnen bent, is het nu echt de hoogste tijd. We helpen u met een handige checklist.

de AVG in het kort

- De Algemene verordening gegevens-bescherming (AVG) is de Nederlandse versie van de General Data Protection Regulation (GDPR), de nieuwe Europese privacywetgeving die vanaf 25 mei 2018 in alle landen van de EU geldt.

- Mensen krijgen door de nieuwe regels meer mogelijkheden om voor zichzelf op te komen bij de verwerking van hun persoonsgegevens. Uw organisatie moet voortaan kunnen bewijzen een geldige grondslag te hebben om iemands persoonsgegevens te verwerken. Ook moet het voor iedereen net zo makkelijk zijn om hun toestemming voor het gebruiken van die gegevens in te trekken, als het is om die toestemming te geven.

- Naast versterking van de bestaande rechten biedt de AVG een aantal aanvullende rechten:
  - Het recht om uw organisatie te vragen persoonsgegevens te verwijderen bestond al. Maar de nieuwe verordening maakt het mogelijk dat mensen nu ook kunnen eisen dat derden - namelijk alle andere organisaties die de gegevens van uw organisatie hebben gekregen - dat doen. Dit heet het recht op vergetelheid.
  - Ook nieuw is het recht op data-portabiliteit. Dat houdt in dat mensen, onder bepaalde voorwaarden, van uw organisatie kunnen vragen hun persoons-gegevens in een standaardformaat te ontvangen. Dat maakt het gemakkelijker om bijvoorbeeld over te stappen van de ene aanbieder naar de andere.

- De AVG geldt voor elke organisatie die persoonsgegevens verwerkt. De nadruk komt te liggen op de verantwoordelijkheid van organisaties om zich aan de wet houden. Zo krijgen organisaties een verantwoordingsplicht: zij moeten - met documenten - kunnen aantonen dat zij de juiste organisatorische en technische maatregelen hebben genomen om aan de AVG te voldoen. Bijvoorbeeld door modelbepalingen voor de doorgifte van persoonsgegevens buiten Europa.

- Alle Europese privacytoezichthouders - in Nederland is dat de Autoriteit Persoons-gegevens (AP) - hebben vanaf 25 mei 2018 dezelfde bevoegdheden om overtreders te bestraffen. Zij kunnen boetes opleggen tot 20 miljoen euro of 4% van de wereldwijde omzet van een organisatie.

- De AVG is al in mei 2016 in werking getreden, maar de wet wordt vanaf 25 mei 2018 gehandhaafd. Organisaties en toezichthouders hebben dus twee jaar de tijd gekregen om zich voor te bereiden op de AVG. Tot 25 mei 2018 geldt in Nederland nog steeds de Wet bescherming persoonsgegevens (Wbp).

checklist: 10 stappen

1
benoem een project-leider en/of -team

De strengere regelgeving en hogere boetes zijn een goede reden om voor de invoering van de AVG een projectleider en/of -team te benoemen. Zij moeten inschatten wat de impact is op uw bedrijfsprocessen en welke aanpassingen nodig zijn.

2
zorg dat de juiste mensen in uw organisatie op de hoogte zijn

Hoger management, beleids-makers, HR-medewerkers en alle andere mensen die in uw organisatie met gegevens-verwerking te maken hebben, moeten de nieuwe regels kennen. Zorg dat er genoeg mankracht en middelen beschikbaar zijn, zodat het projectteam AVG met alle betrokkenen concrete afspraken kan maken over de nieuwe werkwijze.

3
maak een overzicht van uw verwerkingen

Documenteer:

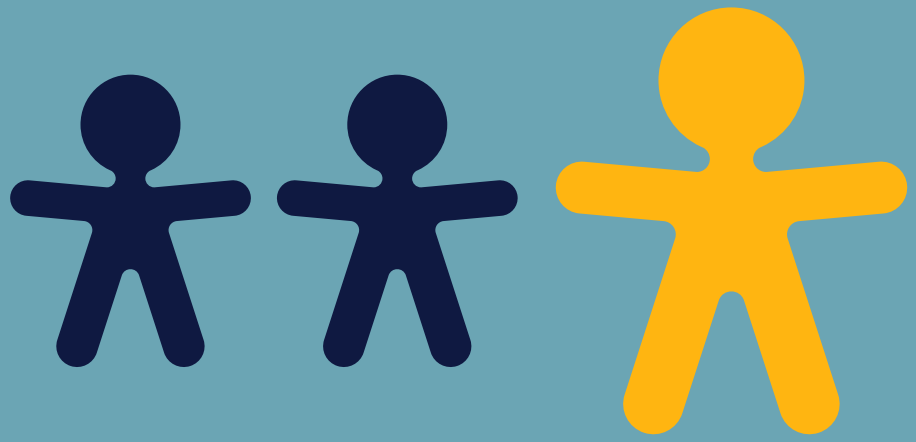
- welke persoonsgegevens u verwerkt
- met welk doel u deze persoonsgegevens verwerkt
- waar de persoonsgegevens vandaan komen
- met wie u de persoons-gegevens deelt.

4
bepaal of er een hoog privacyrisico is

Als de kans bestaat dat een gegevensverwerking die u wilt doen een hoog privacyrisico inhoudt, kunt u verplicht zijn een Data Protection Impact Assessment (DPIA) uit te voeren. Deze DPIA brengt de risico's in beeld, waardoor u maatregelen kunt nemen om die risico's te beperken. Bekijk zo snel mogelijk of u verwacht dat u straks een DPIA moet uitvoeren, en bedenk hoe u dit gaat aanpakken.

5
houd rekening met ‘privacy by design’ en ‘privacy by default’

Onder de AVG wordt uw organisatie verplicht om rekening te houden met twee uitgangspunten: privacy by design en privacy by default. Privacy by design houdt in dat u er al bij het ontwerpen van producten en diensten voor zorgt dat persoonsgegevens goed worden beschermd. Maar bijvoorbeeld ook dat u niet meer gegevens verzamelt dan noodzakelijk zijn voor het doel van de verwerking. En dat u de gegevens niet langer bewaart dan nodig. Privacy by default houdt in dat u technische en organisatorische maatregelen moet nemen om ervoor te zorgen dat u alléén persoonsgegevens verwerkt die noodzakelijk zijn voor het specifieke doel dat u wilt bereiken. Bovendien moet de gebruiker zelf actie ondernemen om aan te geven dat hij zijn persoonsgegevens wil delen of afstaan. U mag bijvoorbeeld een vakje voor het ontvangen van een nieuwsbrief niet alvast aangevinkt hebben.



6
stel vast of u een functionaris voor de gegevensbescherming moet aanstellen

Overheidsinstanties en organisaties die persoonsgegevens verwerken zijn in een aantal gevallen verplicht een functionaris voor gegevensverwerking (FG) aan te stellen. Geldt dat niet voor uw organisatie, dan bent u waarschijnlijk niet verplicht om zo’n interne toezichthouder aan te stellen. Maar het kan wel raadzaam zijn om dat toch te doen. U mag namelijk ook op vrijwillige basis een functionaris gegevensbescherming aanstellen.

7
scherp de procedures aan rond de meldplicht datalekken

De huidige Wet bescherming persoonsgegevens (Wbp) verplicht u nu al om melding te maken van een datalek bij de Autoriteit Persoonsgegevens en bij de mensen van wie de persoonsgegevens zijn gelekt. Onder de AVG blijft de meldplicht datalekken gehandhaafd. U moet datalekken documenteren, zodat de Autoriteit Persoonsgegevens kan controleren of u aan de meldplicht heeft voldaan. Zorg daarom dat u intern goede, duidelijke en voor iedereen in de organisatie bekende processen afspreekt om lekken op te sporen, vast te leggen en aan te pakken.

8
check uw huidige contracten met externe verwerkers

Besteedt u gegevensverwerking uit aan een externe bewerker - of zoals de AVG het noemt: verwerker? Dan is het zaak dat u checkt of uw bestaande afspraken en contracten voldoen aan de eisen die de AVG aan verwerkingsovereenkomsten stelt. Op Autoriteit Persoonsgegevens.nl, in het Dossier AVG, vindt u een overzicht van de onderwerpen die u schriftelijk moet vastleggen in de verwerkingsovereenkomst.

9
check de manier waarop u toestemming vraagt, krijgt en registreert

De AVG stelt strengere eisen aan de toestemming die mensen geven om hun gegevens te verwerken. Het moet nu gaan om 'geldige' en 'over het doel geïnformeerde' toestemming, en het moet net zo gemakkelijk zijn om die toestemming in te trekken als het is om hem te geven. Om een boete te voorkomen is het nodig dat u de manier waarop u toestemming vraagt, krijgt en registreert goed tegen het licht houdt - en waar nodig aanpast. Zorg dat het verzoek tot toestemming helder en begrijpelijk is geformuleerd en gemakkelijk toegankelijk is. Het moet duidelijk zijn wie u bent en wat u met de gegevens wilt doen. Als iemand toestemming wil weigeren of intrekken moet dat zonder consequentie kunnen.

10
zorg dat mensen hun privacyrechten goed kunnen uitoefenen

De AVG zorgt voor meer en betere privacyrechten en stelt u, als organisatie, verantwoordelijk voor het feit dat mensen die rechten goed kunnen uitoefenen. Zorg dat uw medewerkers, IT-systemen en technologie hier klaar voor zijn, om klachten en boetes te voorkomen. Mensen die ontevreden zijn over de manier waarop u met hun gegevens omgaat, kunnen een klacht indienen bij de Autoriteit Persoonsgegevens. De AP is vervolgens verplicht deze klachten op te volgen.

Deze checklist is geen uitputtende lijst. Voor (verdergaande) implementatie is vaak maatwerk nodig, maar met deze tien punten komt u een heel eind. De checklist is gebaseerd op de adviezen die de Autoriteit Persoonsgegevens organisaties geeft over hun voorbereiding op de AVG.

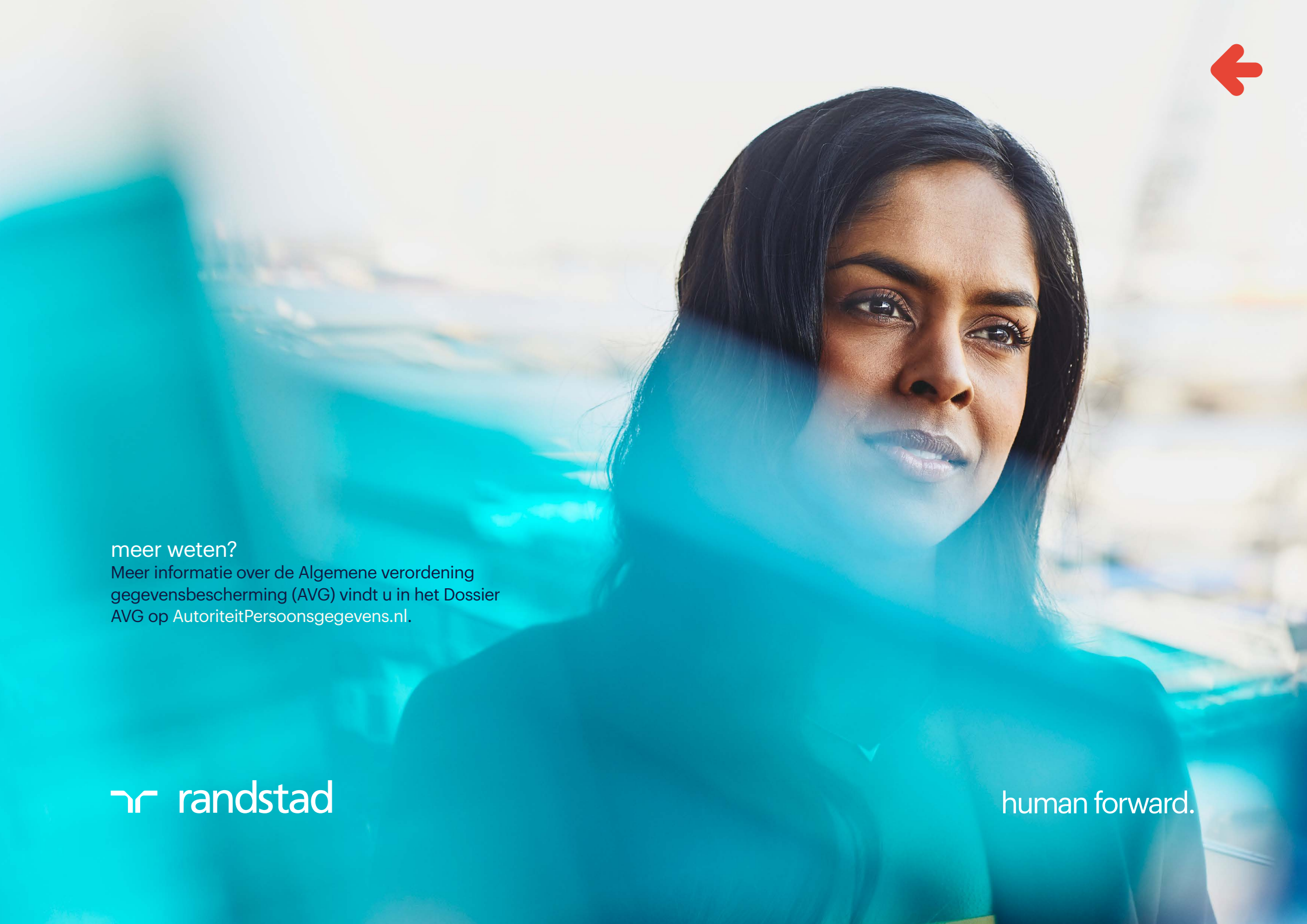
overzicht verschillen Wbp en AVG

verplichting	Wbp*	AVG**
informatie verschaffen aan betrokkene bij het verkrijgen van persoonsgegevens (doeleinden, belang, rechten betrokkene, etc.)	artikel 33 en 34	artikel 13 en 14
desgevraagd inzage verschaffen aan betrokkene van de persoonsgegevens die van hem worden verwerkt	artikel 35	artikel 15
desgevraagd corrigeren of wissen van persoonsgegevens van betrokkene	artikel 36	artikel 16 en 17
als persoonsgegevens worden gecorrigeerd of gewist moet hiervan melding worden gemaakt bij ontvangers van de persoonsgegevens	artikel 38	artikel 19
op verzoek van betrokkene moeten zijn persoonsgegevens aan hem worden overgedragen (dataportabiliteit)	-	artikel 20
privacyverhogende maatregelen bij (de ontwikkeling van) alle producten en diensten (privacy by design) en bij de standaardinstellingen kiezen voor de optie die de beste bescherming van persoonsgegevens biedt (privacy by default)	-	artikel 25
de privacy ook waarborgen als persoonsgegevens aan derden worden verstrekt, onder meer door het sluiten van een verwerkingsovereenkomst	artikel 14	artikel 28
een verwerkingsregister aanleggen met daarin alle persoonsgegevens die binnen de organisatie worden verwerkt, de doeleinden, bewaartermijnen, etc.	-	artikel 30
het melden van datalekken bij de Autoriteit Persoonsgegevens en bij de betrokkene	artikel 34a	artikel 33 en 34
bij verwerkingen van persoonsgegevens die extra risico's met zich kunnen meebrengen, moet een Data Protection Impact Assessment (DPIA) worden gemaakt	-	artikel 35
het aanstellen van een functionaris voor de gegevensbescherming (FG)	-	artikel 37

Bron: ABU

* De artikelen uit de Wbp zijn hier terug te vinden.

** De artikelen uit de AVG zijn hier terug te vinden.



meer weten?

Meer informatie over de Algemene verordening gegevensbescherming (AVG) vindt u in het Dossier AVG op AutoriteitPersoonsgegevens.nl.

randstad

human forward.