Stappenplan Compliance AVG

bureau Brandeis

Op 25 mei 2018 zal de Algemene Verordening Gegevensbescherming ("**AVG**") van toepassing zijn. Vanaf die datum werkt de AVG rechtstreeks door in alle lidstaten van de EU en moet u er dus aan voldoen. De huidige Wet bescherming persoonsgegevens ("**Wbp**"), gebaseerd op de Privacyrichtlijn uit 1995 (Richtlijn 95/46/EG), geldt dan niet meer.

De AVG verandert het juridisch kader voor de bescherming van persoonsgegevens ingrijpend. De AVG introduceert nieuwe concepten, bevat uitgebreide nieuwe verplichtingen voor het bedrijfsleven en versterkt de rechten van de betrokkenen (de mensen van wie gegevens worden verwerkt). Bovendien introduceert de AVG aanzienlijke boetes van maximaal € 20 miljoen of 4% van de wereldwijde jaaromzet van een organisatie.

De AVG heeft implicaties voor vrijwel elk bedrijf of organisatie in de Europese Unie, maar ook daarbuiten. Door strenge voorschriften gecombineerd met hoge boetes, is het verstandig dat bedrijven in een vroeg stadium al op de hoogte zijn van de inhoud van de AVG en zich daarop voorbereiden.

Hieronder laten wij zien hoe onze klanten en relaties zich in twaalf stappen zo efficiënt mogelijk kunnen voorbereiden op de AVG. bureau Brandeis staat regelmatig partijen bij in verband met de toepassing van privacyregelgeving en heeft veel ervaring met de AVG. Wij zijn u vanzelfsprekend graag behulpzaam bij uw voorbereiding op de AVG.

Disclaimer:
Dit document is bedoeld als richtsnoer en is niet bedoeld als juridisch advies.

Klaar voor de AVG in 12 stappen

1. Wijs de verantwoordelijke personen aan en stel – zo nodig – een Functionaris voor Gegevensbescherming (“FG”) aan
2. Breng verwerkingen van persoonsgegevens in kaart en maak een gap analysis
3. Voer, indien nodig, een DPIA uit
4. Voer een dataminimalisatiebeleid in (bepaal uw bewaartermijnen)
5. Leg een register/administratie aan en documenteer uw verwerkingen
6. Pas uw beveiligingsbeleid aan en pas Privacy by Design en Privacy by Default toe
7. Implementeer tools om de nieuwe rechten van betrokkenen te respecteren
8. Pas uw privacy policy aan
9. Stel een protocol datalekken op en houd een register bij
10. Check uw verwerkers en verwerkersovereenkomsten
11. Pas uw registration flow aan om rechtsgeldig toestemming te krijgen
12. Bepaal onder welke toezichthouder u valt

STAP 1

Wijs de verantwoordelijke personen aan en stel – zo nodig – een Functionaris voor Gegevensbescherming (“FG”) aan

Om te beginnen is het van belang om te bepalen wie binnen uw organisatie verantwoordelijk zijn voor privacy compliance en wie er verder betrokken zijn. Het gaat hier enerzijds om personen die bevoegd zijn om namens de organisatie over belangrijke zaken te beslissen, maar ook over personen die verstand hebben van het recht, technologie en de gegevensverwerkingen binnen een organisatie. Het is van belang dat deze personen het belang van privacy compliance onderkennen.

Wat moet u doen?

- Organiseer een *kick-off* meeting of meerdere bijeenkomsten met de relevante personen. Denk aan:
  - Directie;
  - Beleidsmakers;
  - Juristen;
  - Andere personen die veel met persoonsgegevens te maken hebben, zoals HRM medewerkers, de klantenservice, de IT-afdeling, etc.
- Geef daarbij voorlichting over de AVG en het belang van privacy compliance.
- Bepaal wat (op hoofdlijnen) de belangrijkste aandachtspunten / risico's voor uw organisatie zijn. Dit is mede afhankelijk van de *core activity* van uw organisatie.
- Bepaal wie verantwoordelijk is voor privacy compliance en hoe de taken worden verdeeld. Hoe worden beslissingen genomen? Wanneer en in hoeverre moet de directie worden betrokken? Wie is verantwoordelijk voor en/of betrokken bij de uitvoering, etc.?

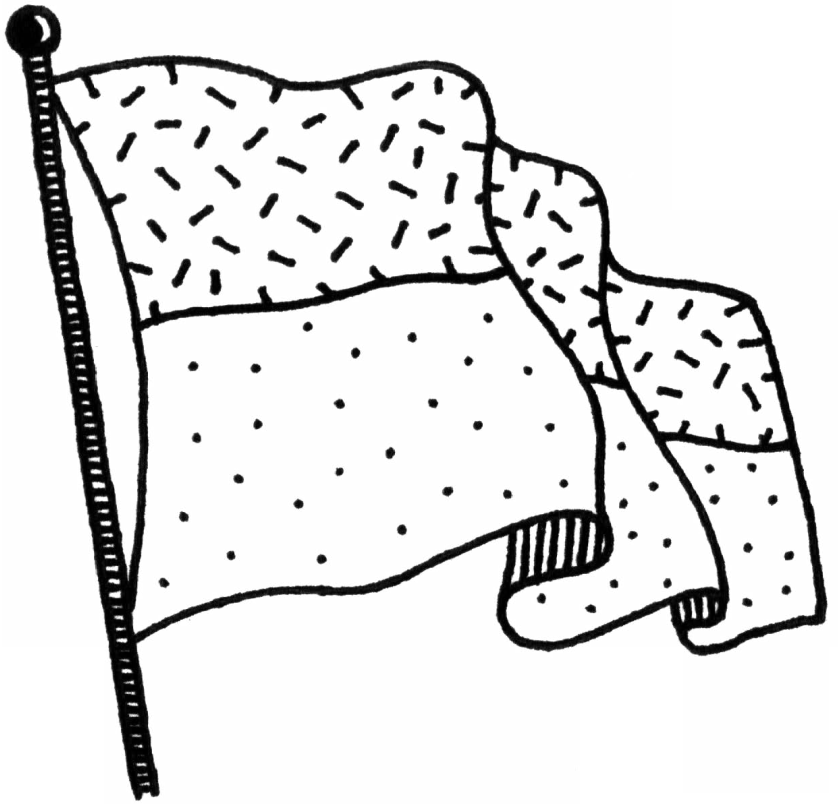
Functionaris gegevensbescherming

Onder de AVG kan uw organisatie verplicht zijn om een zogenaamde functionaris voor gegevensbescherming ("FG"; ook wel *Data Protection Officer* of "DPO") aan te stellen. Ook indien het niet verplicht is, kunt u een FG aanstellen. Bepaal nu alvast of dit voor uw organisatie geldt. U bent in ieder geval verplicht een FG aan te stellen (i) als u een overheidsinstantie of overheidsorgaan bent, (ii) als u zich bezig houdt met verwerkingen die neerkomen op regelmatige en stelselmatige observatie op grote schaal van personen, of (iii) als u zich bezig houdt met grootschalige verwerkingen van bijzondere persoonsgegevens (zie **Stap 2**).

Een FG is een soort interne toezichthouder. De FG informeert en adviseert de organisatie over verplichtingen uit de AVG en andere verplichtingen op het gebied van gegevensbescherming en ziet toe op de naleving van die verplichtingen. Ook is hij of zij de contactpersoon voor de organisatie bij de toezichthouder en voor betrokkenen.

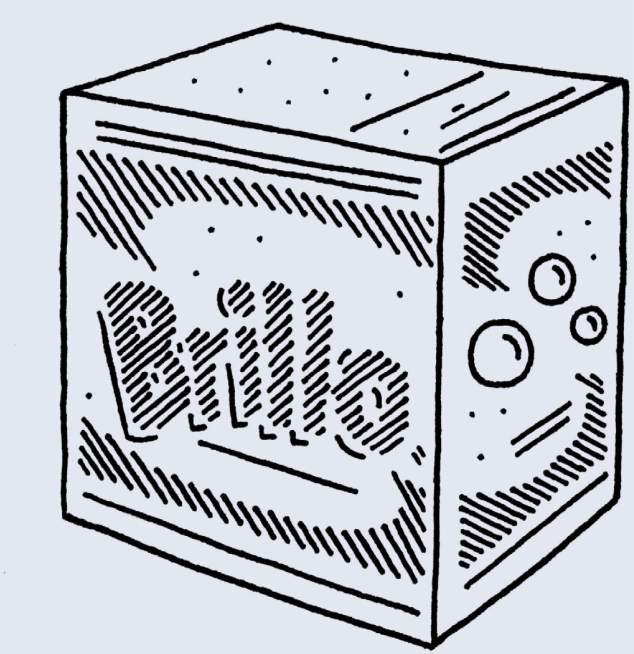
Een FG moet voor de uitvoering van deze taken deskundig zijn op het gebied van de wetgeving en de praktijk op het gebied van bescherming van persoonsgegevens. Ook moet hij of zij voldoende ondersteuning en middelen ter beschikking krijgen om deze uit te voeren en een zekere onafhankelijkheid hebben.

- Bepaal of de aanstelling van een FG vereist of wenselijk is.
- Bepaal wie FG moet worden en zorg dat deze persoon voldoende opgeleid wordt.
- Bepaal de omvang van de taken van de FG en zorg voor voldoende ondersteuning en middelen.
- Benoem de FG en meld de FG aan bij de Autoriteit Persoonsgegevens.



STAP 2

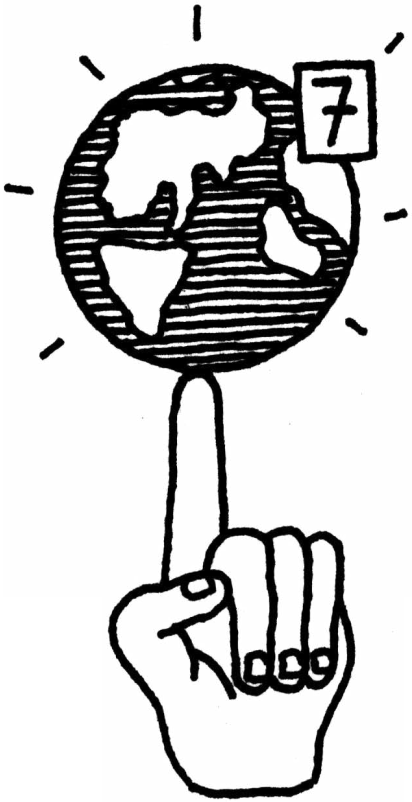
Breng verwerkingen van persoonsgegevens in kaart en maak een gap analysis



Om in overeenstemming met de AVG te kunnen handelen, moet u eerst de verwerkingen van persoonsgegevens binnen uw organisatie in kaart brengen. U moet weten welke gegevens worden gebruikt, door wie en voor welke doeleinden. Vervolgens kunt u beoordelen wat er veranderd moet worden om vanaf 25 mei 2018 compliant te zijn.

Beantwoord de volgende vragen:

- Welke persoonsgegevens worden binnen de organisatie verwerkt?
  - Welke gegevens? Bijvoorbeeld:
    - Naam;
    - Adres;
    - Functie;
    - Contactgegevens (welke?);
    - Beoordelingen;
    - Reisgegevens, etc.
  - Van welke categorieën betrokkenen? Bijvoorbeeld:
    - Klanten;
    - Werknemers;
    - Leveranciers;
    - Bezoekers;
    - Patiënten;
    - Familie van werknemers, etc.
- Verwerkt u “bijzondere categorieën” of anderszins gevoelige gegevens? Bijvoorbeeld:
  - Gezondheidsgegevens;
  - Biometrische gegevens (bijv. vingerafdruk);
  - BSN-nummers;
  - Gegevens over minderjarigen;
  - Profielen.
- Zijn er andere bijzondere risico’s?
  - Combineert u gegevens, maakt u gebruik van profielen of is sprake van geautomatiseerde beslissingen?
- Voor welke doelen worden de verschillende gegevens gebruikt?
- Op basis van welke wettelijke grondslag?
  - Blijft dit geldig onder de AVG?
- Door wie worden de gegevens verwerkt en met wie deelt u de gegevens?

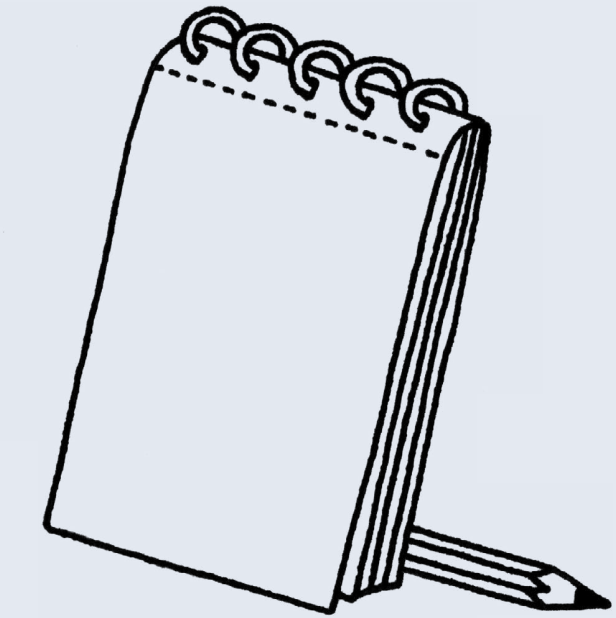


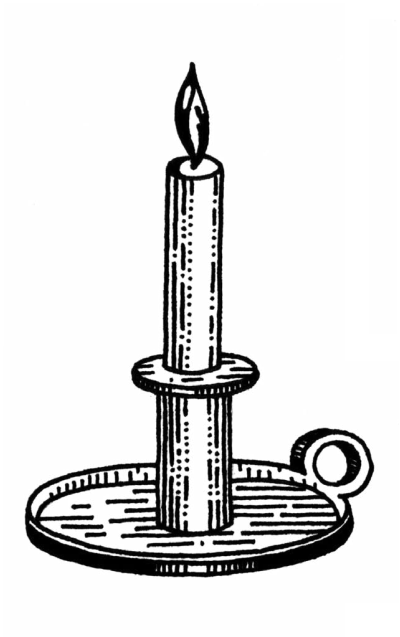
- Welke informatie wordt aan de betrokkenen verstrekt? Bijvoorbeeld:
  - Een privacy policy;
  - Een gedragscode voor werknemers.
- Is er een proces voor inzage, verbetering, verwijdering, etc. van persoonsgegevens?
- Welke dienstverleners zijn betrokken bij de (verdere) verwerking van persoonsgegevens?
  - Zijn er bewerkersovereenkomsten?
- Is er een beveiligingsbeleid?
- Doet u aan *Privacy by Design* en *Privacy by Default*?
- Is er een protocol datalekken?

Naar aanleiding van bovenstaande vragen, krijgt u een beter beeld van de gegevensverwerkingen binnen uw organisatie, de grootste risico's daarvan en wat er voor u verandert. U kunt dan bepalen welke acties genomen moeten worden tot 25 mei 2018 en welke onderwerpen voor uw organisatie prioriteit hebben.

STAP 3

Voer, indien nodig, een DPIA uit





Onder de AVG kunt u verplicht zijn een zogeheten *data privacy impact assessment* (“**DPIA**”), in het Nederlands een “gegevensbeschermingseffectbeoordeling”, uit te voeren. Een DPIA is een instrument om vooraf de privacyrisico’s van een gegevensverwerking in kaart te brengen, waarna maatregelen kunnen worden getroffen om die risico’s te verkleinen.

Wanneer een DPIA?

Een DPIA is verplicht voor (beoogde) gegevensverwerkingen die, gelet op de aard, omvang, context en doel daarvan, een hoog privacyrisico met zich meebrengen. Van een hoog risico is in ieder geval sprake in de volgende gevallen:

- Wanneer u mensen beoordeelt op basis van persoonskenmerken en daar besluiten op baseert. Het gaat hierbij onder meer om profilering en het maken van prognoses;
- Wanneer u op grote schaal bijzondere persoonsgegevens, zoals gegevens over de gezondheid, strafrechtelijke gegevens of politieke voorkeuren, verwerkt;
- Wanneer u op grote schaal en stelselmatig mensen volgt in publieke ruimten (denk aan cameratoezicht).

In alle overige gevallen, moet u zelf bepalen of een verwerking een “hoog risico” met zich meebrengt. Als uw verwerking aan twee of meer van onderstaande criteria voldoet, kunt u ervan uitgaan dat u een DPIA moet uitvoeren:

- U maakt profielen van mensen;
- U neemt geautomatiseerde beslissingen die de betrokkene wezenlijk treffen;
- Er is sprake van stelselmatige en grootschalige monitoring;
- U verwerkt bijzondere persoonsgegevens;
- Het gaat om een grootschalige gegevensverwerking, dus een verwerking die veel mensen, veel gegevens, een lange duur of een groot gebied betreft;
- U koppelt of combineert verschillende gegevensverzamelingen;
- U verwerkt gegevens over kwetsbare personen, zoals kinderen, werknemers of patiënten;
- U maakt gebruik van een nieuwe technologie. Denk aan *Internet of Things* (IoT)-toepassingen;
- U geeft persoonsgegevens door naar landen buiten de EU;
- De gegevensverwerking heeft tot gevolg dat personen een recht niet kunnen uitoefenen, een dienst niet kunnen gebruiken of een contract niet kunnen afsluiten.

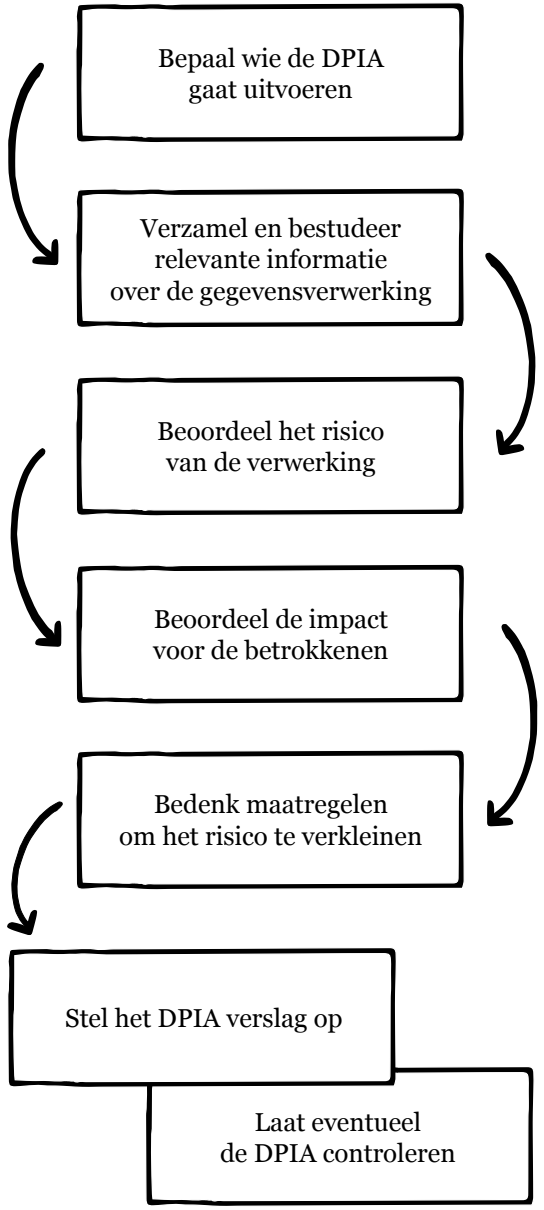
De Autoriteit Persoonsgegevens zal een lijst van verwerkingen publiceren waarvoor een DPIA verplicht is.

Hoe moet ik een DPIA uitvoeren?

U mag zelf kiezen hoe u de DPIA uitvoert, maar deze moet in ieder geval het volgende bevatten:

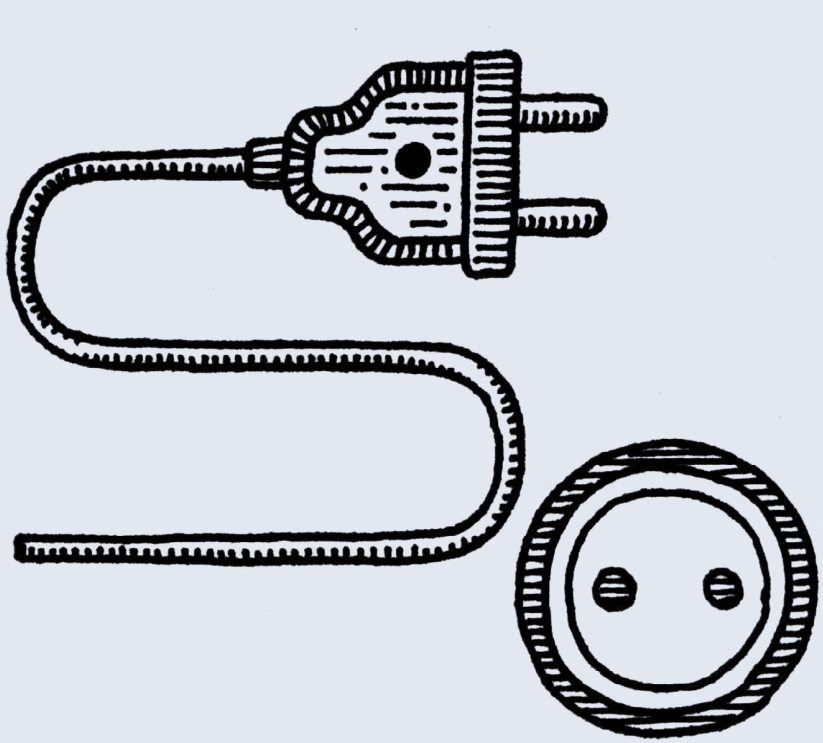
- Een systematische beschrijving van de beoogde gegevensverwerkingen en de doeleinden hiervan. Als u zich beroept op een gerechtvaardigd belang als grondslag voor de verwerking, moet u dit belang ook omschrijven in de beschrijving;
- Een beoordeling van de noodzaak en de proportionaliteit van de verwerkingen. Is de verwerking noodzakelijk om uw doel te bereiken? En is de inbreuk op de privacy van de betrokkenen niet onevenredig in verhouding tot dit doel?
- Een beoordeling van de privacyrisico's voor de betrokkenen.
- De beoogde maatregelen om (I) de risico's aan te pakken (zoals pseudonimisering) en (II) aan te tonen dat u aan de AVG voldoet.

Komt uit een DPIA naar voren dat uw beoogde verwerking een hoog risico oplevert? En lukt het u niet om maatregelen te vinden om dit risico te beperken? Dan moet u met de Autoriteit Persoonsgegevens overleggen voordat u met de verwerking start. Dit wordt een voorafgaande raadpleging genoemd. Schat nu alvast in of u DPIA's moet uitvoeren en voer die uit. Door vroeg te beginnen, is het voor u ook makkelijker te voldoen aan de andere verplichtingen van de AVG.



STAP 4

Voer een dataminimalisatie beleid in (bepaal bewaartermijnen)



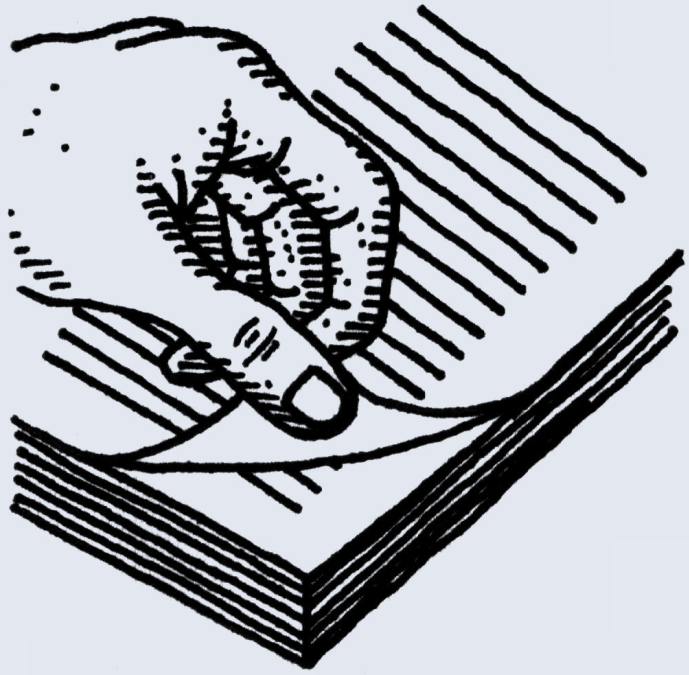
De AVG benadrukt de verplichting om niet meer persoonsgegevens te verwerken dan noodzakelijk is. Dit wordt ook wel dataminimalisatie genoemd. Het is in dit kader van belang om te bepalen hoe lang u persoonsgegevens bewaart en ervoor te zorgen dat gegevens tijdig worden verwijderd.

Wat moet u doen?

- Bepaal aan de hand van het overzicht van de verschillende gegevens dat u heeft gemaakt (zie **Stap 2**) , voor welke doeleinden u deze gebruikt en hoe lang u ze daarvoor moet bewaren.
  - Geldt er een maximale of minimale wettelijke bewaartermijn (per document- / informatie soort)? Bijvoorbeeld:
    - Persoonsgegevens van sollicitanten: maximaal 4 weken na het einde van de sollicitatieprocedure;
    - Arbeidsovereenkomsten van werknemers: maximaal 2 jaar na het einde van het dienstverband;
    - Loonbelastingverklaringen en kopie ID van werknemers: minimaal 5 jaar na einde dienstverband;
    - Opnames beveiligingscamera: maximaal 4 weken na het maken van de opname.
  - Is het daarvoor nodig dat de persoonsgegevens bewaard blijven? Kunnen wellicht bepaalde gegevens uit de dataset worden verwijderd?
  - Kunnen de gegevens worden gepseudonimiseerd?
- Bepaal de bewaartermijn, het moment waarop de termijn gaat lopen en hoe de bewaartermijn wordt gehandhaafd.
  - Maak werkafspraken, bijvoorbeeld over wanneer en hoe hard copy documentatie wordt gearchiveerd (bijvoorbeeld ieder einde van de maand in een map met datum en vernietigingsdatum) en door wie deze wordt vernietigd;
  - Stel instellingen in voor (technische) archivering of verwijdering per applicatie / database, inclusief instellingen voor verwijdering van gearchiveerde data.

STAP 5

Leg een register aan van uw verwerkingen



De AVG introduceert verplichtingen voor organisaties om duidelijke en volledige verantwoording en rekenschap af te leggen over de wijze waarop met persoonsgegevens wordt omgegaan. U moet kunnen aantonen dat uw organisatie in overeenstemming met de AVG handelt. Onderdeel hiervan is dat u een register bij moet houden van alle verwerkingsactiviteiten die binnen de organisatie, of onder verantwoordelijkheid van de organisatie, plaatsvinden. Toezichthouders kunnen inzage in deze registratie verlangen.

U kunt hiervoor het overzicht dat u onder **Stap 2** heeft gemaakt als basis gebruiken.

In het register moeten de volgende gegevens worden opgenomen:

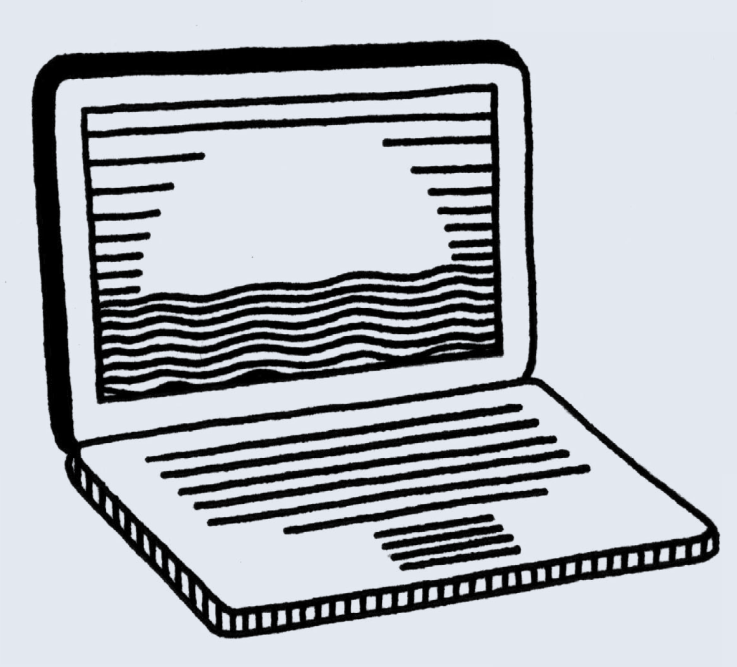
- Naam en contactgegevens verantwoordelijke (in de AVG "verwerkingsverantwoordelijke" genoemd);
- Naam en contactgegevens vertegenwoordiger en/of FG, indien van toepassing;
- Verwerkingsdoeleinden;
- Categorieën van betrokkenen;
- Categorieën van persoonsgegevens;
- Eventuele ontvangers;
- Doorgiften, indien van toepassing, inclusief naam van de entiteit of persoon aan wie wordt doorgegeven en documentatie m.b.t. passende waarborgen;
- Bewaartermijnen;
- Een algemene beschrijving van de technische en organisatorische maatregelen ter beveiliging.

Zorg er dus voor dat u een dergelijk register aanlegt en dit ook bijhoudt. Dit kan door implementatie van een *datamapping* applicatie, maar ook door bijvoorbeeld een overzicht bij te houden in een Excel bestand. Er zijn in de markt verder verschillende tools beschikbaar die u kunnen helpen om deze verplichting na te komen.

Let op: de verplichting geldt niet voor organisaties met minder dan 250 werknemers, maar geldt wel wanneer (i) de verwerking een risico inhoudt voor betrokkenen (ii) de verwerking niet incidenteel is of (iii) bijzondere categorieën van gegevens worden verwerkt.

STAP 6

Pas uw beveiligingsbeleid aan en pas Privacy by Design en Privacy by Default toe

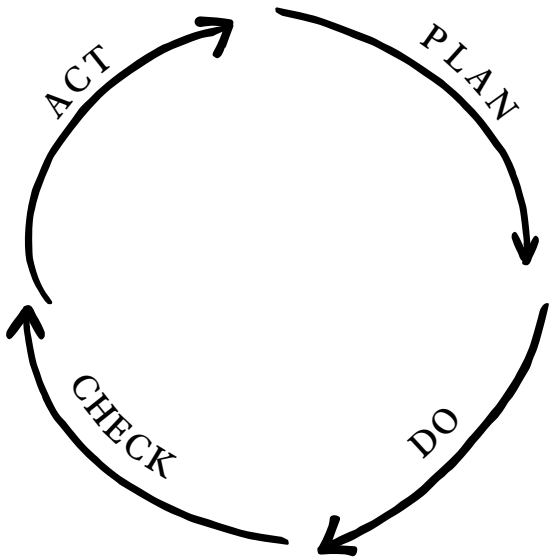


Onder de AVG moet u “passende technische en organisatorische maatregelen” nemen om persoonsgegevens te beveiligen. Wat passend is hangt af van het risico van de verwerking. U moet kunnen aantonen dat u passende maatregelen heeft getroffen en uw afwegingen in dit verband inzichtelijk kunnen maken. Het is mede daarom van belang om te controleren of uw beveiligingsbeleid nog voldoet en waar nodig aanpassingen door te voeren.

Daarnaast introduceert de AVG verplichtingen op het gebied van *Privacy by Design* en *Privacy by Default*. Dit houdt in dat u al bij de keuze voor een middel voor gegevensverwerking / in het ontwerp van systemen of applicaties rekening moet houden met de bescherming van persoonsgegevens door bijvoorbeeld beveiligingsmaatregelen en dataminimalisatie te implementeren. De standaardinstellingen moeten zodanig zijn dat alleen persoonsgegevens worden verwerkt voor een specifiek doel. Ook moet standaard, en dus ook al bij het ontwerpen van een verwerking, rekening worden gehouden met de rechten van betrokkenen.

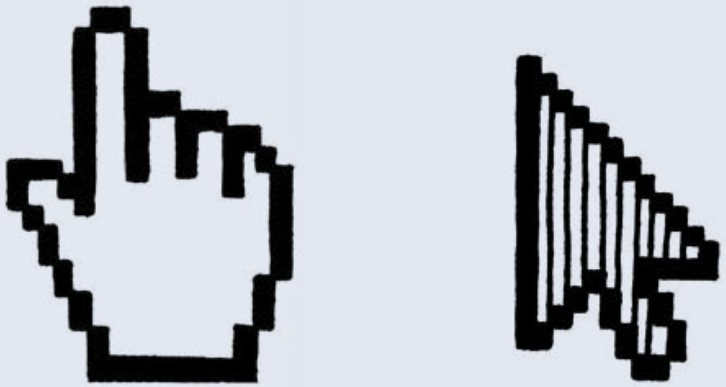
Wat u moet doen:

- Breng per type verwerking de genomen of te nemen organisatorische en technische beveiligingsmaatregelen in kaart;
- Beoordeel of dit, gezien het risico van de verwerking en de stand van de techniek, (nog) voldoende is;
- Onderzoek of gegevens gepseudonimiseerd of versleuteld kunnen worden;
- Controleer of verwerkingen en/ of bewaartermijnen beperkt kunnen worden;
- Controleer of maatregelen zijn geïmplementeerd om de rechten van betrokkenen te waarborgen (zie **Stap 7**);
- Implementeer waar nodig aanvullende maatregelen;
- Bepaal wanneer u de beveiligingsmaatregelen test en evalueert;
- Stel een beveiligingsbeleid op waarin de maatregelen, uw afweging en de periodieke evaluatie worden beschreven.



STAP 7

Implementeer tools om de nieuwe rechten van betrokkenen te respecteren



De AVG besteedt uitgebreid aandacht aan de rechten van betrokkenen. Zo hebben betrokkenen het recht op inzage in en correctie van hun gegevens. Daarnaast krijgen mensen nog meer mogelijkheden om voor zichzelf op te komen bij de verwerking van hun gegevens. Hun rechten worden versterkt en uitgebreid.

De AVG introduceert een aantal nieuwe rechten, zoals:

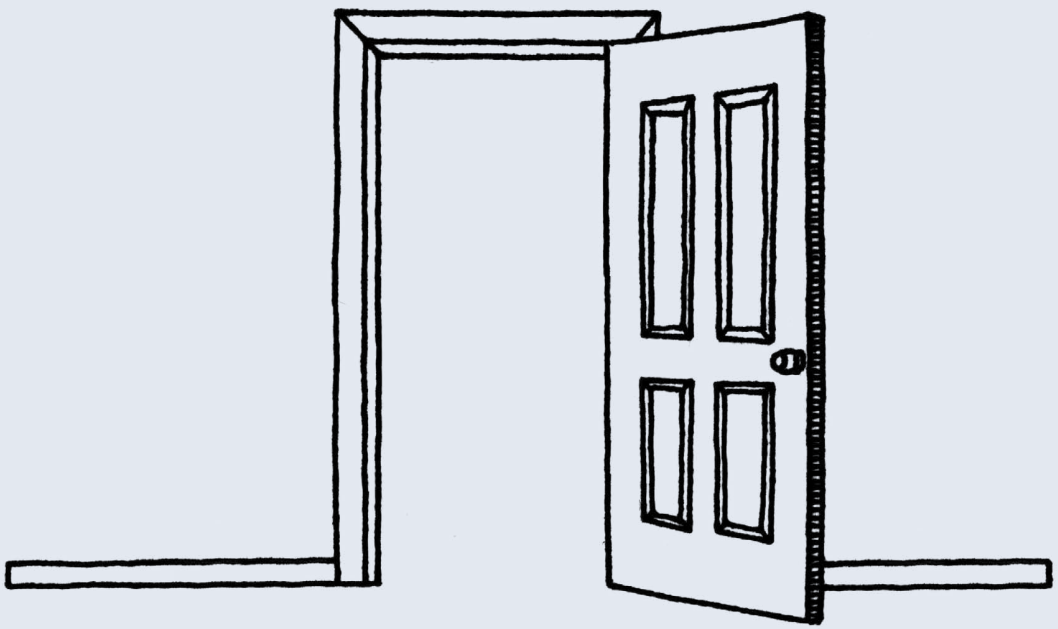
- Het recht op het ontvangen van uitgebreide informatie, waarbij de AVG specificeert welke informatie in ieder geval moet worden versterkt (zie **Stap 8**);
- Het recht om bezwaar te maken tegen profilering en geautomatiseerde besluitvorming;
- Het recht om vergeten te worden (ook wel "recht op vergetelheid" of "*right to be forgotten*"). Onder omstandigheden hebben personen het recht om hun persoonsgegevens te laten verwijderen. Indien een organisatie gegevens openbaar heeft gemaakt (bijv. op internet heeft geplaatst) moeten zelfs redelijke maatregelen genomen worden om het verzoek om verwijdering door te geven aan alle andere organisaties die de gegevens verwerken (doorzendplicht);
- Het recht op dataportabiliteit, ofwel overdraagbaarheid van persoonsgegevens. Mensen krijgen (onder voorwaarden) het recht hun persoonsgegevens in een standaardformaat te ontvangen, zodat deze makkelijk kunnen worden doorgegeven aan een andere leverancier van een vergelijkbare dienst. Bijvoorbeeld als zij zich willen uitschrijven bij de ene sociale netwerksite en zich inschrijven bij een andere. Zij kunnen zelfs verlangen dat de organisatie hun persoonsgegevens direct doorstuurt aan de nieuwe dienstverlener, mits dat technisch mogelijk is;
- Het recht om de verwerking van persoonsgegevens te beperken;
- Het recht om niet te worden onderworpen aan uitsluitend geautomatiseerde besluitvorming, zoals *profiling*.

Ook bevat de AVG een aparte bepaling over toestemming, waarover meer in **Stap 9**.

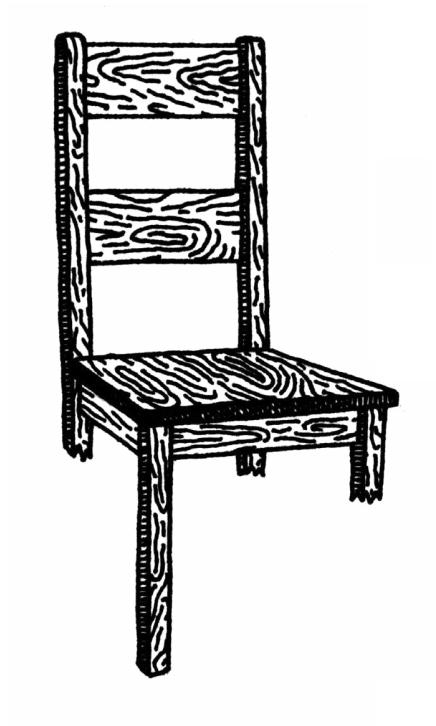
Een hoop nieuwe rechten dus, die u moet respecteren. Evalueer daarom uw procedures voor het geven van inzage, etc. en bepaal op welke wijze personen hun rechten uit de AVG binnen uw organisatie kunnen uitoefenen. Bepaal of het binnen uw organisatie gepast is om daar technische middelen, zoals bijvoorbeeld in het kader van gegevensoverdracht, voor te ontwikkelen. Denk hierbij aan downloadprogramma's waarmee personen hun gegevens eenvoudig kunnen downloaden en het aanbieden van *application programming interfaces* (API's).

STAP 8

Pas uw privacy policy aan



Onder de AVG moet u betrokkenen informeren over de verwerking van persoonsgegevens. De informatie moet beknopt, transparant, begrijpelijk en makkelijk toegankelijk zijn.



Onder de AVG bent u verplicht om onder meer informatie te verstrekken over:

- Uw identiteit en contactgegevens, en indien van toepassing, die van de FG;
- De doeleinden van de verwerking en de juridische grondslag daarvan;
- De categorieën van persoonsgegevens die u verwerkt;
- De periode dat persoonsgegevens worden opgeslagen (zie **Stap 4**);
- De rechten van de betrokkene, zoals het recht een klacht in te dienen, het recht op inzage, rectificatie en wissing, en het recht om toestemming te allen tijde in te trekken (zie **Stap 7** en **11**);
- De bron van de gegevens;
- De eventuele ontvangers of categorieën van ontvangers van persoonsgegevens;
- Of gegevens worden doorgegeven aan landen buiten de EU;
- Indien van toepassing: welk gerechtvaardigd belang is gediend met de verwerking;
- Of u aan profilering doet en, zo ja, wat de gevolgen daarvan zijn voor de betrokkene;
- Of de betrokkene verplicht is de persoonsgegevens te verstrekken en wat de gevolgen zijn van niet-verstrekking van de gegevens.

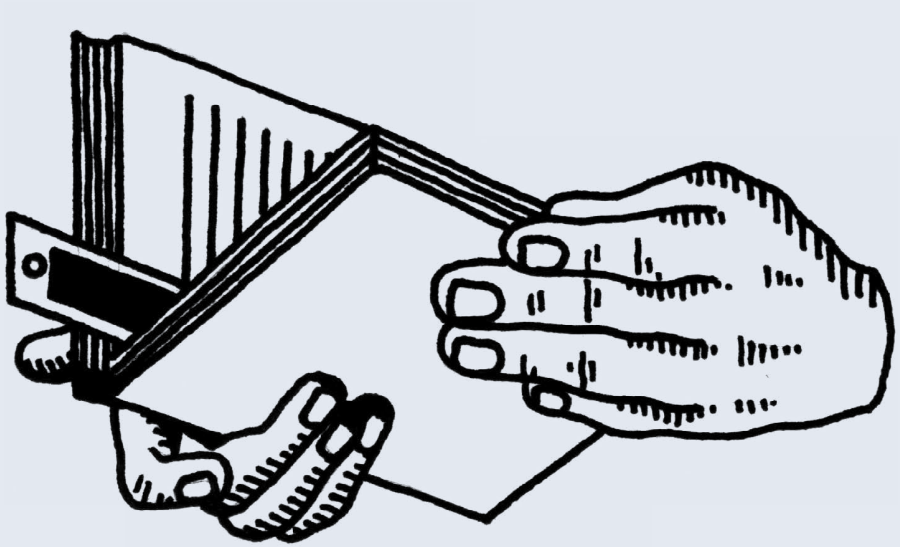
De AVG voorziet bovendien in het toekomstige gebruik van gestandaardiseerde icoontjes om consumenten op eenvoudige wijze te kunnen informeren.

De informatie moet in beginsel worden verstrekt op het moment dat de persoonsgegevens worden verzameld.

Tijd dus om uw privacy policy te actualiseren om de aanvullende informatieverplichtingen die de AVG introduceert te implementeren.

STAP 9

Stel een protocol datalekken op en houd een register bij



Onder de AVG kunt u verplicht zijn om een datalek te melden bij de bevoegde autoriteit en/of aan betrokkenen. Bij een datalek gaat het om toegang tot of vernietiging, wijziging of het vrijkomen van persoonsgegevens bij een organisatie zonder dat dit de bedoeling is. Onder een datalek valt dus niet alleen het vrijkomen (lekken) van gegevens, maar ook onrechtmatige verwerking van gegevens en onbedoelde vernietiging. Denk aan een kwijtgeraakte USB-stick met persoonsgegevens, een gestolen laptop, een inbraak in een databestand door een hacker of een brand waardoor een CRM-database (zonder back-up) verloren gaat.
Onder de AVG bent u verplicht om een datalek onverwijld, waar mogelijk binnen 72 uur, te melden aan de toezichthouder. Dit hoeft niet indien het onwaarschijnlijk is dat het datalek zal leiden tot een hoog risico voor de rechten en vrijheden van natuurlijke personen. De betrokkene moet worden geïnformeerd indien het datalek waarschijnlijk zal resulteren in een groot risico voor de rechten en vrijheden van individuen, anders niet.

Protocol datalekken

Om te kunnen voldoen aan de hiervoor genoemde verplichtingen, moet u ervoor zorgen dat u (i) op de hoogte bent zodra zich een datalek voordoet en (ii) direct adequaat handelt. Voor dit eerste punt moet u ervoor zorgen dat u maatregelen implementeert om van datalekken op de hoogte te raken in het kader van de beveiliging (zie **Stap 6**). Voor het tweede punt is het van belang om een protocol datalekken te hebben. In het protocol neemt u op (i) welke stappen er genomen moeten worden in het geval uw organisatie geconfronteerd wordt met een datalek, (ii) welke informatie er moet worden verzameld/vastgelegd en/of gemeld, (iii) door wie, en (iv) binnen welk tijdspan.

Maak ook duidelijke afspraken met uw verwerkers over datalekken. Ga na wat er in de verwerkersovereenkomst is opgenomen over datalekken (zie ook **Stap 10**).

Register datalekken

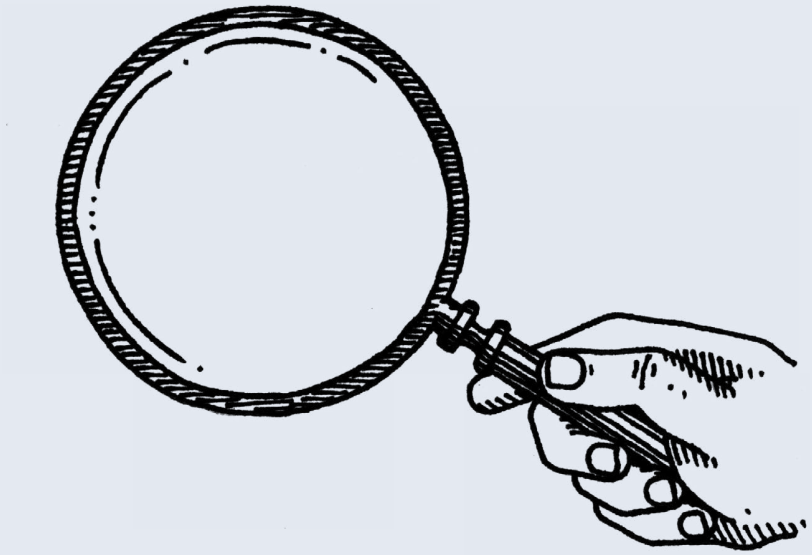
De AVG stelt daarnaast de eis dat alle datalekken – dus zowel de gemelde en niet-gemelde datalekken – die zich in uw organisatie hebben voorgedaan worden gedocumenteerd in een register. Op basis hiervan kan de bevoegde autoriteit controleren of u aan de meldplicht heeft voldaan.

Neem per datalek in ieder geval de volgende informatie op:

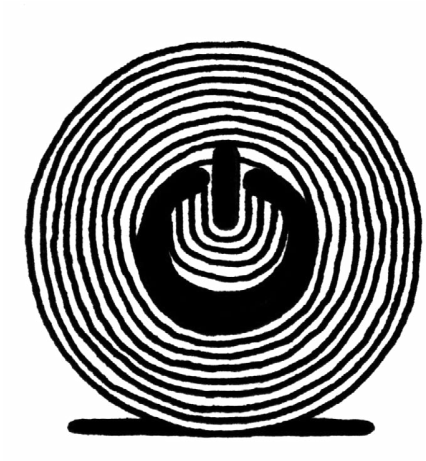
- Feiten en gegevens over de aard van het datalek;
- De categorieën van getroffen personen en – waar mogelijk – het aantal betrokkenen;
- De (waarschijnlijk) gevolgen van het datalek;
- De maatregelen die uw organisatie heeft genomen om het datalek aan te pakken en de gevolgen daarvan te beperken;
- Is het datalek gemeld aan de Autoriteit?;
- Is het datalek gemeld aan de betrokkene? Zo ja, neem dan de tekst van de kennisgeving aan de betrokkene in het overzicht op.

STAP 10

Check uw verwerkers en verwerkersovereenkomsten



Een verwerker is een derde die ten behoeve van een andere organisatie persoonsgegevens verwerkt (onder de Wbp nog “bewerker” genoemd). Denk hierbij aan dienstverleners die de salarisadministratie doen, maar bijvoorbeeld ook allerlei cloud- of andere IT diensten waarbij de dienstverlener uw persoonsgegevens opslaat of in kan zien.



U bent verplicht om een overeenkomst aan te gaan met iedere verwerker. Hierin moeten onder andere worden opgenomen dat de verwerker:

- Uitsluitend op uw instructie persoonsgegevens verwerkt;
- Passende technische en organisatorische beveiligingsmaatregelen neemt;
- De met de verwerking van persoonsgegevens belaste personen tot vertrouwelijkheid verplicht;
- Bijstand verleent bij het nakomen van verplichtingen op grond van de rechten van betrokkenen;
- De persoonsgegevens na afloop van de verwerking wist of retourneert aan de verantwoordelijke;
- Informatie ter beschikking stelt die nodig is voor audits of inspecties van toezichthouders.

Tijd dus om uw overeenkomsten met verwerkers te controleren en eventueel te heronderhandelen.

- Breng uw verwerkers in kaart;
- Check of uw overeenkomsten voldoen aan de AVG;
- Pas waar nodig de overeenkomsten aan of sluit nieuwe verwerkersovereenkomsten.

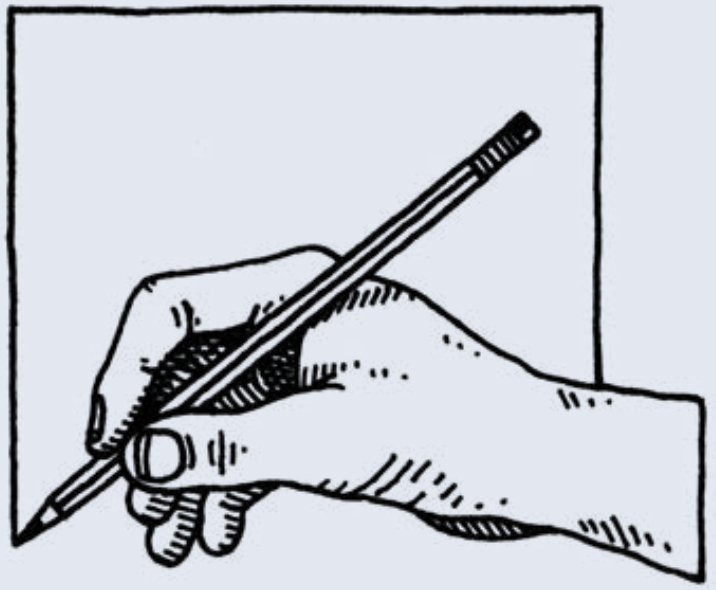
Daarnaast bevat de AVG een groot aantal verplichtingen voor de verwerker. Zo moeten verwerkers onder de AVG:

- Een register aanleggen van alle verwerkingen (zie **Stap 5**);
- Zo nodig een FG aanstellen (zie **Stap 1**);
- Toestemming vragen aan de verantwoordelijke voor het inschakelen van sub-verwerkers;
- Datalekken melden aan de verantwoordelijke;
- Medewerking verlenen aan de toezichthouder;
- Handelen in overeenstemming met de eisen voor doorgifte van persoonsgegevens naar landen buiten de EU;
- DPIA’s uitvoeren (zie **Stap 3**).

Ondanks dat deze verplichtingen al uit de AVG volgen, is het raadzaam om de punten ook met uw verwerkers te bespreken en in overleg te bepalen hoe hier in de praktijk uitvoering aan zal worden gegeven.

STAP 11

Pas uw registration flow aan om rechtsgeldig toestemming te krijgen



Een aantal van uw gegevensverwerkingen zal waarschijnlijk gebaseerd zijn op de grondslag toestemming.

Van een rechtsgeldige toestemming is pas sprake als deze zonder dwang “vrij, geïnformeerd, specifiek en ondubbelzinnig” is gegeven. Dit kan door middel van een verklaring of een actieve handeling, zoals het aanvinken van een vakje, indien daarbij voldoende informatie wordt verstrekt. Het automatisch, impliciet aannemen van toestemming of het gebruik van vooraf ingevulde vinkjes is onvoldoende om een geldige toestemming te krijgen.

Toestemming is onder de AVG niet “vrij” gegeven, als de betrokkene geen echt vrije keuze heeft. Dat wil zeggen dat hij niet in staat is om te weigeren of indien het nadelig is om de toestemming in te trekken. Dit is bijvoorbeeld het geval als het sluiten van een overeenkomst, daaronder begrepen het verlenen van een dienst, afhankelijk is van de toestemming van de betrokkene om persoonsgegevens te verwerken die niet noodzakelijk zijn voor de uitvoering van de opdracht. Een toestemming is ook niet “vrij”, indien geen afzonderlijke toestemming kan worden gegeven voor verschillende gegevensverwerkingen, terwijl dit in het individuele geval wel passend zou zijn.

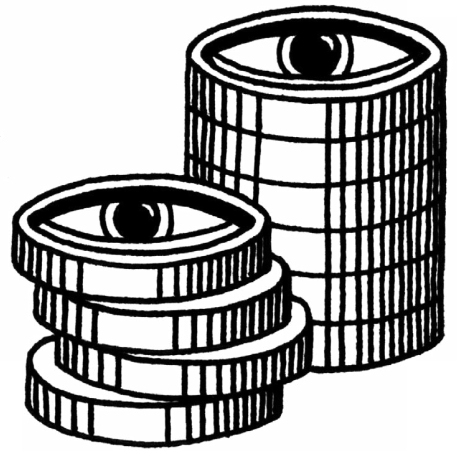
U moet kunnen aantonen dat u geldige toestemming van betrokkenen heeft gekregen om hun persoonsgegevens te verwerken.

Bovendien hebben betrokken het recht om de gegeven toestemming te allen tijde in te trekken. Dit moet even eenvoudig zijn als het geven van toestemming en vóórdat betrokkenen toestemming geven, moeten zij worden geïnformeerd over dit recht. Anders is de toestemming ongeldig.

Indien u bijzondere persoonsgegevens verwerkt, moet de toestemming (behoudens de toepasselijkheid van een uitzondering) “uitdrukkelijk” zijn. Dat betekent dat de betrokkene expliciet zijn wil moet hebben geuit in woord, geschrift of gedrag.

Wat moet u doen?

- Bepaal welke verwerkingen zijn gebaseerd op de grondslag toestemming (zie **Stap 2**);
- Controleer of de wijze waarop u toestemming vraagt, krijgt en registreert voldoet aan de AVG;
- Pas uw processen zo nodig aan;
- Zorg ook dat betrokkenen hun toestemming op eenvoudige wijze kunnen intrekken.



STAP 12

Bepaal onder welke toezichthouder u valt

De AVG gaat uit van een zogeheten “one-stop-shop”, ofwel het één-loketmechanisme.

Het idee is dat u met één toezichthouder te maken krijgt, ook als uw organisatie vestigingen heeft in meerdere EU-landen of als uw gegevensverwerkingen impact hebben in meerdere EU-landen. Deze toezichthouder wordt de “leidende toezichthouder” genoemd.

De leidende toezichthouder is de toezichthouder van de EU-lidstaat waar de hoofdvestiging (of de enige vestiging) van een organisatie is gevestigd. Dit is de plaats waar de centrale administratie van de verantwoordelijke in de EU is gelegen. Dit is anders als de beslissingen over het doel en de middelen van verwerkingen van persoonsgegevens worden genomen in een andere vestiging. Dan is dat de hoofdvestiging. Voor verwerkers is de hoofdvestiging de vestiging waar de centrale administratie is gelegen, of – bij gebreke van een centrale administratie – de vestiging waar de voornaamste verwekingsactiviteiten plaatsvinden.

De leidende toezichthouder is als eerste verantwoordelijk voor het toezicht op organisaties met grensoverschrijdende gegevensverwerkingen. De leidende toezichthouder mag ook handhavend optreden bij grensoverschrijdende verwerkingen van de organisatie onder zijn toezicht.

Vindt een verwerking uitsluitend plaats in een andere lidstaat dan die van de leidende toezichthouder, of heeft een verweking wezenlijke gevolgen voor betrokken van die lidstaat, dan kan ook bij de toezichthouder van de betreffende lidstaat een klacht worden ingediend. Deze toezichthouder – de “betrokken toezichthouder” – moet de leidende toezichthouder echter direct informeren en met hem samenwerken.

Andersom moet de leidende toezichthouder zijn optreden wel afstemmen met privacytoezichthouders in de andere EU-landen waar de gegevensverwerking impact heeft. De leidende toezichthouder coördineert de activiteiten, betrekt de andere betrokken toezichthouders bij de zaak en legt conceptbeslissingen aan hen voor.

Heeft u uw hoofdvestiging in Nederland? Met andere woorden: neemt u de beslissingen over de doelstellingen van en de middelen voor de verwerkingen in Nederland? Of heeft u alleen maar een vestiging in Nederland? Dan valt u onder toezicht van de Nederlandse privacytoezichthouder, de Autoriteit Persoonsgegevens.