HUNTER MANAGEMENT PARTNERS

Hunter Management Partners BV

Bezoekadres:
Lopikerplein 2a, Schoonhoven
2e etage "De Toren"

Postadres:
Postbus 9, 3410 CA Lopik

Tel: 0182 - 389036
Fax: 0182 - 389048
E-mail: hmp@hmp.nl
Web: www.hmp.nl
KvK Midden NL 53164946

CHECKLIST AVG

Algemene informatie voor ondernemers

Welke stappen dient u als organisatie te doorlopen om te voldoen aan de vernieuwde privacywetgeving: de AVG?

Op 25 mei 2018 treedt de Algemene Verordening Gegevensbescherming (AVG), ook wel de General Data Protection Regulation (GDPR) genoemd, in werking. De AVG is Europese wetgeving en werkt direct door in de gehele Europese Unie. De wetgeving is al vanaf 2016 van kracht. Tot 25 mei 2018 heeft men de tijd gehad om de wetgeving door te voeren. Vanaf 25 mei 2018 wordt dan ook verwacht dat je als organisatie voldoet aan de AVG.

Door de Autoriteit Persoonsgegevens kan een boete van maximaal 20 miljoen of 4% van de jaarlijkse wereldwijde omzet opgelegd worden, indien vastgesteld wordt dat de verplichtingen uit de AVG niet worden nageleefd. Daarnaast komt er een 'kliklijn' en zullen er meer controles plaatsvinden.

Met behulp van deze checklist kan worden nagegaan of u als organisatie voldoet aan de AVG-wetgeving. Vragen of wilt u weten wat Hunter Management Partners voor u kunt betekenen betreffende de vernieuwde privacywetgeving? *Neem contact op met mr. V.S. (Vera) Verlooij, junior partner en jurist bij HMP, via v.verlooij@hmp.nl.*

AVG en persoonsgegevens
De AVG ziet toe op de verwerking van persoonsgegevens van natuurlijke personen. Dit betekent indien u contact hebt met Bv's en NV's de AVG niet van toepassing is. Eenmanszaken zijn daarentegen natuurlijke personen en vallen wel onder de AVG-wetgeving.

In de AVG wordt onderscheid gemaakt tussen persoonsgegevens en bijzondere persoonsgegevens. Een bijzonder persoonsgegeven is extra gevoelige informatie en dient als zodanig verwerkt te worden.

Onder *persoonsgegevens* in de AVG wordt onder andere verstaan:
- Naam, adres, woonplaats;
- Telefoonnummer;
- E-mailadres;
- Bankgegevens.

Onder *bijzondere persoonsgegevens* wordt onder andere verstaan:
- Afkomst;
- Geaardheid;
- Medische gegevens;
- BSN-nummer;
- Paspoorten.

AVG STAPPENPLAN VOOR ORGANISATIES

Stap 1: Inventarisatie/ register van verwerkingsactiviteiten

Toelichting:

Iedere organisatie heeft in de uitoefening van bedrijfsvoering te maken met de verwerking van persoonsgegevens.
De eerste stap om te voldoen aan de AVG, is het bewust worden van de persoonsgegevens die u als organisatie verwerkt en hier een inventarisatie van te maken. Dit doet men in een register van verwerkingsactiviteiten.

Bij organisaties met meer dan 250 werknemers, is een register van verwerkingsactiviteiten verplicht. Een organisatie met minder dan 250 medewerkers moet over een register beschikken wanneer de organisatie persoonsgegevens verwerkt:

- Waarvan de verwerking niet incidenteel is. In de praktijk zijn verwerkingen zelden incidenteel;
- Die een hoog risico inhouden voor de rechten en vrijheden van de personen van wie u persoonsgegevens verwerkt; en/of
- Die vallen onder de categorie bijzondere persoonsgegevens.

Of een verwerkingsactiviteitenregister al dan niet verplicht is, het bijhouden van een register van gegevensverwerking draagt bij aan uw *verantwoordingsplicht* en maakt het voldoen aan de overige AVG-bepalingen een stuk gemakkelijker.

Een voordeel van het hebben van een verwerkingsactiviteitenregister is dat bij controle van de Autoriteit Persoonsgegevens u het register direct kunt laten zien en daarmee grotendeels voldoet aan uw verantwoordingsplicht.

Uitvoering:

In het verwerkingsactiviteitenregister wordt een inventarisatie gemaakt van de antwoorden op de volgende vragen:

- Van welke categorie personen verzamelt de organisatie gegevens? (klanten, potentiële klanten, leveranciers, werknemers)
- Welke persoonsgegevens verzamelt de organisatie? (bijvoorbeeld, naam, telefoonnummer)
- Verzamelt de organisatie ook bijzondere persoonsgegevens? (BSN, NAW gegevens, pasfoto's, camerabeelden)
- Met welk doel en met welke grondslag worden de persoonsgegevens verwerkt? (marketing, overeenkomst, verplicht vanuit andere instanties zoals de Belastingdienst)
- Hoe lang bewaart de organisatie de gegevens?
- Wie binnen de organisatie verzamelt/verzamelen de persoonsgegevens?
- Wie binnen de organisatie heeft toegang tot de persoonsgegevens?
- Worden de persoonsgegevens gedeeld met andere (internationale) organisaties?
- Heeft de organisatie een Functionaris voor de Gegevensbescherming (FG)?
- Welke maatregelen heeft de organisatie genomen om persoonsgegevens die de organisatie verwerkt te beveiligen?

In de volgende stappen worden deze vragen nader toegelicht. De antwoorden dienen in het register te worden opgenomen.

Stap 2: Doel en grondslag voor de verwerking van persoonsgegevens

Toelichting:

Gerechtvaardigd doel

Het verwerken van persoonsgegevens mag enkel plaatsvinden voor een *gerechtvaardigd doel* (doelbinding). Enkel de persoonsgegevens die noodzakelijk zijn voor het bereiken van dit doel, mogen worden verzameld. Doel is bijvoorbeeld: in contact treden met klanten, uitvoering van overeenkomst, het verzamelen van adresgegevens voor het afleveren van een bestelling enz.

Let op dat er niet meer persoonsgegevens worden verzameld dan nodig.
Voorbeeld: identificatieplicht. Veelal wordt om te voldoen aan de identificatieplicht een kopie gemaakt van het paspoort. Maar er zou ook een vinkje gezet kunnen worden: ID gezien, met het documentnummer. Hetzelfde doel, veel minder persoonsgegevens.
Ander voorbeeld: gevraagde gegevens bij een contactformulier op de website. Het doel van het contactformulier is dat klanten een vraag kunnen stellen. Het doel van de gevraagde gegevens is dat de organisatie in contact kan treden met diegene die het contactformulier verzonden heeft.
Nodig is: naam en emailadres, eventueel het telefoonnummer. Maar een geboortedatum of woonplaats is niet direct benodigd. (dit is overigens voor iedere organisatie anders, de AVG is echt maatwerk)

Gegevens die verkregen zijn voor een bepaald doel, mogen niet gebruikt worden voor andere doeleinden. Een e-mailadres ontvangen via een contactformulier, mag bijvoorbeeld niet zonder toestemming op de nieuwsbrieflijst geplaatst worden.

Grondslag

Als het doel is vastgesteld, moet vervolgens de *grondslag* bepaald worden.
Verwerking van persoonsgegevens mag alleen als er sprake is van 1 van de 6 grondslagen die zijn opgenomen in de AVG.
De grondslagen zijn:

1. *Uitvoering van de overeenkomst*: er is een overeenkomst tussen de verwerker en de betrokkene en voor deze overeenkomst is het verwerken van een aantal persoonsgegevens onontbeerlijk. Bijvoorbeeld: koopovereenkomst, arbeidsovereenkomst, opdrachten met klanten etc.
2. *Wettelijke verplichting*: hieronder vallen de verwerkingen waarvoor geldt dat het niet mogelijk is om een wettelijke plicht uit te voeren, zonder de verwerking van persoonsgegevens. Bijvoorbeeld: gegevens in de boekhouding. Bepaalde gegevens zijn noodzakelijk voor wettelijke verplichtingen zoals het betalen van belastingen en premies.
3. *Toestemming*: de organisatie verwerkt alleen persoonsgegevens na toestemming van de betrokkene. De toestemming moet een vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting bevatten. De toestemming moet vastgelegd worden (moet aantoonbaar zijn) en het moet mogelijk zijn om de toestemming weer in te trekken (opt-out)
   Een mededeling zoals: bij gebruik gaat u akkoord, is geen toestemming. De betrokkene moet echt een handeling van toestemming verrichten, zoals een checkbox aanvinken of wel of niet akkoord geven (opt-in). Toestemming is bijvoorbeeld benodigd voor het verzamelen van gegevens voor het plaatsen van cookies en het verzenden van nieuwsbrieven.
   Aan de grondslag toestemming zitten aardig wat haken en ogen. Is de verwerking te baseren op een van de andere grondslagen, dan hebben die de voorkeur.
4. *Gerechtvaardigd belang*: in de AVG worden de volgende voorbeelden gegeven: ten behoeve van direct marketing, het doorsturen van gegevens tussen verschillende onderdelen van het concern, het verzamelen van gegevens ten behoeve van netwerkbeveiliging.
   De vraag die bij een gerechtvaardigd belang gesteld moet worden: is het voor de betrokkene, logisch dat zijn gegevens verzameld en verwerkt worden: reasonable expectancy of privacy.
5. *Vitaal belang*: bij vitaal belang is gegevensverwerking gerechtvaardigd ter bestrijding van ernstig gevaar voor de gezondheid van de betrokkene of een ander persoon. Denk aan het verzamelen van gegevens ter identificatie van een persoon na een ongeval.
6. *Algemeen belang of openbaar gezag*: bestemd voor overheidsinstanties.

Uitvoering:

1. Rangschik het overzicht van verzamelde persoonsgegevens naar categorie. Bijvoorbeeld klanten, website, leveranciers, personeel e.d.;
2. Geef per categorie aan welke gegevens worden verzameld;
3. Geef per categorie aan of en welke bijzondere persoonsgegevens worden verzameld;
4. Geef per categorie aan welk gerechtvaardigd doel en welke grondslag aan de basis ligt.

Stap 3: Privacy beleid en privacyverklaring

Toelichting:

Privacy beleid

Een privacy beleid is voor een organisatie verplicht als dit in verhouding staat tot de verwerkingsactiviteiten. Dit is afhankelijk van de aard, omvang, context en doel van de gegevensverwerking. Het komt er op neer dat een privacy beleid alleen hoeft te worden opgesteld als er veel en/of bijzondere persoonsgegevens worden verzameld en verwerkt. De AVG werkt de vereisten verder niet uit.

Wederom, ook al is het opstellen van een privacy beleid voor veel organisaties niet verplicht, is het wel ten zeerste aan te bevelen. Intern is een beleid uitermate handig. Het opstellen van een privacy beleid zorgt ervoor dat de privacy van betrokkenen gewaarborgd wordt en binnen de organisatie duidelijk is hoe er met privacy omgegaan wordt.

In het privacy beleid wordt onder andere het volgende opgenomen:
Een beschrijving van welke gegevens er worden verzameld, hoe lang, waar, door wie, waarom? Kunnen de gegevens ingezien worden? Waar kunnen klachten ingediend worden? Kunnen de gegevens verwijderd worden, wat zijn de rechten van de werknemers met betrekking tot de persoonsgegevens? Hoe wordt omgegaan met datalekken en beveiliging van persoonsgegevens.

Privacyverklaring

Om als organisatie te voldoen aan de verantwoordingsplicht, de informatieplicht en om transparant met persoonsgegevens om te gaan, dient een privacyverklaring opgesteld te worden.
De privacyverklaring is wel verplicht voor iedere organisatie.
Voordat je persoonsgegevens ontvangt, dient de betrokkene op de hoogte te zijn van de privacyverklaring. Plaats hem daarom op de website, zet een link bij het contactformulier of nieuwsbriefaanmeldingsformulier.

De privacyverklaring moet voldoen aan verschillende verplichte onderdelen:

- Contactgegevens van de organisatie en eventuele Functionaris Gegevensbescherming;
- Doel en rechtsgronden voor verwerking;
- Of er gevolgen zijn van het niet verstrekken;
- Duur van de opslag;
- Rechten van betrokkenen;
- Klachtrecht;
- Eventuele doorgifte aan derde landen;
- Profilering en geautomatiseerde besluitvorming;
- Bron van verkregen persoonsgegevens.

Rechten van betrokkenen

Onder de AVG hebben betrokkenen een aantal nieuwe rechten met betrekking tot de persoonsverwerking verworven. Volgens de AVG is de organisatie verplicht de betrokkenen te informeren over deze rechten:

1. Recht van dataportabiliteit: betrokkenen hebben het recht om hun digitale gegevens te ontvangen van de organisatie. De organisatie moet dit mogelijk maken en verstrekken in een vorm die het voor betrokkenen makkelijk maakt om hun gegevens te hergebruiken en door te geven aan een andere organisatie. Denk aan het wisselen van verzekeringsmaatschappij of bank.
2. Recht van inzage: De betrokkene heeft het recht om zijn persoonsgegevens in te zien. Ze mogen aan een organisatie vragen of deze persoonsgegevens van hen heeft vastgelegd en zo ja, welke. Er hoeft geen reden voor dit inzageverzoek gegeven te worden en weigeren mag enkel met bepaalde uitzonderingen. Voor het verstrekken van inzage mogen kosten gerekend worden. Persoonlijke werkaantekeningen vallen niet onder het inzagerecht. Het gaat om de gegevens die zijn opgeslagen in een dossier, account of om de gegevens die verstrekt worden door de organisatie aan derden.
3. Recht op informatie: onder de AVG heeft u als organisatie een informatieplicht. Dat betekent dat u verplicht bent om nieuwe en bestaande klanten duidelijk te informeren over wat u met hun persoonsgegevens doet. In de praktijk gebeurt dit veelal met een (online) privacyverklaring. De privacyverklaring bestaat uit verplichte onderdelen.
4. Recht van rectificatie en aanvulling: De betrokkene heeft het recht om een correctieverzoek in te dienen voor gegevens die: feitelijk onjuist zijn, onvolledig zijn, niet ter zake doen of op een andere manier in strijd zijn met de wet.
5. Recht op vergetelheid: het recht van betrokkenen om te vragen aan de organisatie om hun persoonsgegevens te wissen. Denk bijvoorbeeld aan het uitschrijven op een nieuwsbrief of het verwijderen van een account.
   Het verzoek om vergeten te worden hoeft niet altijd geaccepteerd te worden. Een verzoek van bijvoorbeeld een klant met een betalingsregeling om vergeten te worden, hoeft natuurlijk niet. Soms is het wettelijk gezien ook niet toegestaan om alle gegevens te verwijderen, bijvoorbeeld factuurgegevens in de boekhouding voor de Belastingdienst.
   Probeer bij een verzoek wel zo veel mogelijk gegevens te wissen.
6. Recht op beperking van de verwerking: het recht om minder persoonsgegevens te verzamelen. Gegevens die mogelijk onjuist, onrechtmatig, niet meer nodig, of gegevens waartegen bezwaar gemaakt is, dienen niet verzameld te worden.
7. Recht op menselijke blik bij besluiten: sommige organisaties nemen een besluit op basis van automatisch verwerkte gegevens, bijvoorbeeld bij profilering, automatische weigering bij ingediende online kredietaanvraag of verwerking van sollicitaties via internet zonder menselijke tussenkomst. Betrokkenen hebben het recht zich te beroepen op het recht van een menselijke blik bij besluiten, wat betekent dat u een nieuw besluit moet nemen waarbij een persoon de gegevens heeft beoordeeld.
8. Het recht van bezwaar: betrokkenen hebben het recht om bezwaar te maken tegen de verwerking van hun gegevens. U moet dan stoppen met de verwerking van de persoonsgegevens, tenzij u dwingende gerechtvaardigde gronden aanvoert die zwaarder wegen dan de belangen van de betrokkenen.
9. Het recht op klagen: de betrokkenen hebben het recht om een klacht in te dienen bij de Autoriteit Persoonsgegevens over de verwerking van hun persoonsgegevens door jou als organisatie.

Uitvoering:

In het privacy beleid moet het volgende worden opgenomen:

- Het doel en de grondslag voor de verwerking van de persoonsgegevens;
- Dat de organisatie erop toeziet dat iedere verwerking van persoonsgegevens voldoet aan dit doel;
- Dat de verwerking niet verder gaat dan noodzakelijk;
- Dat de persoonsgegevens niet voor een ander doel worden gebruikt;
- Hoe men binnen de organisatie omgaat met persoonsgegevens;

- Hoe de betrokkene een klacht in kan dienen;
- De rechten van de betrokkenen met betrekking tot de persoonsgegevens.

Stap 4: privacy by design en privacy by default: Beveiliging, bewaartermijnen

Toelichting:
Privacy by design; bij het ontwerpen van nieuwe producten en/of diensten moet *vooraf* een inschatting gemaakt worden van de privacy impact en hoe u er voor zorgt dat de persoonsgegevens goed beschermd worden.

Privacy by default; bij bestaande producten en/of diensten dient u technische en organisatorische maatregelen te treffen die ervoor zorgen dat de privacy van persoonsgegevens gewaarborgd worden.

Voorbeelden:
- Niet meer gegevens verzamelen dan nodig is voor het doel (denk aan gegevens voor de nieuwsbrief, vraag niet meer gegevens dan nodig is om de nieuwsbrief te versturen);
- Bewaartermijnen: bewaar gegevens niet langer dan wettelijk vastgelegd en/of noodzakelijk;
- Checkboxen op de website niet vooraf aanvinken;
- Doelbinding: verkregen persoonsgegevens enkel gebruiken voor het verkregen doel (denk aan e-mailadressen verkregen door weggevers op de website, niet gebruiken voor de nieuwsbrief);
- Beveiliging van de gegevens: beperk de toegang, beveilig de toegang.

Uitvoering:
Voor organisaties bestaat privacy by default voornamelijk uit:
1. De bewaartermijnen bepalen van de verschillende persoonsgegevens;
2. Het beveiligen van de persoonsgegevens;
3. Bepalen wie er toegang hebben tot de persoonsgegevens;
4. De tot op heden verzamelde persoonsgegevens opruimen; onnodige persoonsgegevens verwijderen en de bewaartermijnen nalopen.

1. Bewaartermijnen
   Bepaal voor de verschillende categorieën persoonsgegevens de bewaartermijn. Sommige documenten hebben een wettelijke bewaartermijn, bijvoorbeeld fiscale documentatie. Van andere documenten moet u zelf de bewaartermijn bepalen. De bewaartermijnen moeten in ieder geval redelijk zijn en moeten worden gecommuniceerd met de betrokkenen.

2. Het beveiligen van persoonsgegevens
   Vanzelfsprekend een van de belangrijkste onderdelen van de AVG. Alle privacy beleidsplannen zijn niets waard zonder deugdelijke beveiliging.
   Het beveiligingsniveau moet afgestemd zijn op de risico's die de betreffende verwerking met zich meebrengt, u dient passende maatregelen te treffen als organisatie.
   In de AVG wordt een onderscheid gemaakt tussen technische en organisatorische maatregelen.

   Technische maatregelen:
- Up-to-date houden van software;
- Back-up maken en deze veilig opslaan;
- Versleutelen van gegevens,
- Verwijderen van verouderde gegevens;
- Goede toegangsbeveiliging: bijvoorbeeld 2-staps verificatie;
- Installeren van een virusscanner en firewall.

Organisatorische maatregelen:
- Protocol voor de afhandeling van datalekken;
- Verhogen bewustzijn van medewerkers.

3. Bepalen wie er toegang heeft tot bepaalde gegevens
   Stel per categorie persoonsgegeven vast wie er toegang moet hebben tot deze gegevens. Zorg ervoor dat diegene die geen toegang nodig hebben tot de gegevens, ook geen toegang hebben. Loop daarbij de bestaande wachtwoorden na, controleer de toegang van computerschijven etc.

4. Opruimen van bestaande persoonsgegevens
   Als het goed is, is na het voltooien van de vorige stappen duidelijk geworden, welke persoonsgegevens worden verzameld binnen de organisatie, hoe deze beveiligd zijn, wie er toegang tot heeft etc.
   Nu is het van belang dat er kritisch door alle bestaande informatie gegaan wordt.
- Ruim harde schijven op: verwijder documenten die niet nodig zijn (denk aan een Excel bestand voor de kerstkaarten van 6 jaar terug);
- Ruim dossiermappen -en kasten op;
- Maak USB-sticks leeg;
- Loop bestaande maillijsten na. Kan de toestemming voor de aanmelding op de nieuwsbrief aangetoond worden? Zo niet, vraag opnieuw toestemming.

Privacy by design komt aan de orde bij bijvoorbeeld de aanschaf van nieuwe software. Daarbij kunnen dezelfde stappen worden doorlopen als privacy by default. Enkel moet de uitkomst van de stappen bepalend zijn of de nieuwe software voldoet aan de privacy vereisten.

Stap 5: Functionaris Gegevensbescherming (FG)

Toelichting:
De Functionaris Gegevensbescherming (FG) is iemand die binnen de organisatie toezicht houdt op de toepassing en naleving van de AVG.
De FG is in 3 situaties verplicht:

1. Overheden en publieke organisaties: Overheidsinstanties en publieke organisaties zijn altijd verplicht een FG aan te stellen. (gemeente, provincie, zorg- en onderwijsinstellingen)
2. Observaties: Organisaties die als hoofdtaak hebben: het op grote schaal volgen van individuen. Denk hierbij aan profilering van mensen en cameratoezicht. (beveiligingsmaatschappijen, marketingactiviteiten op basis van gegevens, risicobeoordeling, telecommunicatie)
3. Bijzondere persoonsgegevens: Organisaties die op grote schaal bijzondere persoonsgegevens verwerken en waarvan dit de hoofdtaak is. (verzekeringsmaatschappij, bank) Niet vallen hieronder de eenpitters (de individuele arts of advocaat).

Een en ander zal in de toekomst nader opgehelderd worden. Er zal een lijst vanuit de Autoriteit Persoonsgegevens volgen, met daarin richtlijnen over op welke organisaties de verplichting van een FG rust.

Advies voor nu is: wanneer onduidelijk is of uw organisatie verplicht is om een FG aan te stellen, onderbouw goed waarom wel of niet gekozen is voor het aanstellen van een FG.

Het vrijwillig aanstellen van een FG is toegestaan. Een FB mag iemand intern of extern in de organisatie zijn.

Uitvoering:

1. Bepaal of het aanstellen van een FG noodzakelijk is;
2. Onderbouw deze keuze zorgvuldig;
3. Meld de FG aan bij de Autoriteit Persoonsgegevens via het webformulier;
4. Geef aan betrokkenen (werknemers, klanten) door wat het takenpakket is van de FG en hoe de FG te bereiken is (bijvoorbeeld in het privacy beleid of de privacyverklaring)

Stap 6: DPIA, data protection impact assessment, gegevensbeschermingseffectbeoordeling

Toelichting:

De DPIA is een instrument om vooraf privacy risico's van een gegevensverwerking in kaart te brengen en om vervolgens maatregelen te treffen om deze risico's te verkleinen.

De DPIA is enkel verplicht voor organisaties en verwerkingen met een groot privacy risico voor de betrokkenen (diegene van wie de gegevens worden verzameld). Hiervoor gelden dezelfde criteria als onder stap 5. Denk aan continu monitoren van personen, profilering en prognoses op basis van kenmerken zoals, iemands beroepsprestaties, interesses, locatie, kredietwaardigheid, het volgen van websitebezoekers, automatische vacature selectie enz.

Bij het gebruik van nieuwe technologieën is een DPIA in ieder geval verplicht.

Eveneens zal in de toekomst een gemeenschappelijke EU-lijst van verwerkingen waarvoor een DPIA verplicht is, ter beschikking worden gesteld.

Uitvoering:

1. Bepaal als organisatie of een DPIA verplicht is;
2. Zo ja, voer de beoordeling uit volgens de richtlijnen van de Autoriteit Persoonsgegevens.

Stap 7: Datalek, beleid en datalekregister

Toelichting:

Melden datalek binnen 72 uur

Sinds 2016 geldt er een meldplicht voor datalekken. Deze meldplicht houdt in dat organisaties een melding moeten doen bij de Autoriteit Persoonsgegevens zodra zij een ernstig datalek hebben. In een aantal gevallen moet het datalek ook gemeld worden aan de betrokkenen (de mensen van wie de persoonsgegevens zijn gelekt).
Een datalek levert niet per definitie een boete op; het niet melden van een datalek kan daarentegen wel een boete opleveren.

Definitie datalek

Datalek: Er heeft een beveiligingslek plaatsgevonden. Bij dit beveiligingsincident zijn persoonsgegevens verloren gegaan en/of is onrechtmatige verwerking van deze persoonsgegevens niet uit te sluiten. (Denk aan diefstal computer, inbraak hacker, kwijtraken USB stick en brand).
Het ongeoorloofd wijzigen, inzien of verstrekken van gegevens, is ook een datalek.

Melding datalek Autoriteit Persoonsgegevens: Gaat het om een datalek waarbij bijzondere persoonsgegevens, persoonsgegevens van gevoelige aard, of als er om een andere reden sprake is van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens, meld deze dan zo spoedig mogelijk maar binnen uiterlijk 72 uur aan de Autoriteit Persoonsgegevens.

Melding datalek betrokkenen: Waren niet alle gelekte gegevens (correct) versleuteld, of heeft het datalek om andere redenen waarschijnlijk ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkene, dan dient het lek gemeld te worden aan de betrokkenen.

Voorbeelden van de aard van datalekken die gemeld moet worden:
- Gegevens over de gezondheid;
- Financiële gegevens;
- Eventuele persoonlijke problemen (verslaving e.d.)
- Gebruikersnamen, inloggegevens en wachtwoorden;
- Kopieën identiteitsbewijzen en/of Burgerservicenummer.

Uitvoering:
1. Stel een datalekbeleid op.
- Maak het intern duidelijk wat een datalek is en hoe deze intern gemeld moet worden en bij wie.
- Stel een stappenplan datalek op. Datalekken moeten zo spoedig mogelijk maar uiterlijk binnen 72 uur gemeld worden.
2. Stel een datalekregister op: alle datalekken binnen de organisatie moeten worden vastgelegd in een register. Hierin moet worden opgenomen:
- Het soort gegevens
- Een omschrijving van het datalek
- Wanneer het datalek plaats vond;
- Wat er met de persoonsgegevens gebeurd is;
- Van welke personen gegevens gelekt zijn;
- Of er melding gemaakt is van het datalek;
- Binnen hoeveel uur het datalek gemeld is.

Bij controle door de Autoriteit Persoonsgegevens zal gevraagd worden om het datalekbeleid en het datalekregister.

Stap 8: Verwerkingsovereenkomsten

Toelichting:
Als een organisatie gegevensverwerking uitbesteed, dient met deze verwerker een verwerkingsovereenkomst opgesteld te worden.

Een verwerker is een persoon of organisatie die in opdracht van jou werkt met jouw verzamelde persoonsgegevens maar niet zelfstandig verantwoordelijk is voor de verwerking van de persoonsgegevens (over deze gegevens geen beslissingen mag maken). Denk aan de salarisadministratie, software, hosting partijen, (Cloud) opslag e.d.

Vereisten verwerkingsovereenkomst:
1. Algemene beschrijving: duur, aard en doel van de verwerking;
2. Beschrijving van het soort persoonsgegevens, de categorieën gegevens;
3. Instructies verwerking: bepaling doeleinden verwerking;
4. Geheimhoudingsplicht;
5. Beveiliging;
6. Sub verwerkers;
7. Privacy rechten;
8. Melden datalekken;
9. Verwijderen gegevens na afloop verwerkingsdiensten;
10. Meewerken aan audits/controles

Uitvoering:

1. Maak een overzichtslijst van alle derden die u inhuurt voor de verwerking van persoonsgegevens.
2. Stel met iedere verwerker een verwerkingsovereenkomst op of inventariseer of deze door de verwerker zelf beschikbaar is gesteld.
3. Documenteer de lijst met verwerkers en de bijbehorende verwerkingsovereenkomsten.

Disclaimer
Hunter Management Partners heeft zijn best gedaan om zich zo goed mogelijk te verdiepen in de nieuwe wetgeving en de regels zo helder mogelijk aan u uit te leggen. Desondanks kan het zijn dat er onverhoopt toch onjuiste of onvolledige informatie in deze checklist is geslopen. Zie u iets dat niet klopt of niet duidelijk is? Laat het ons weten.