AVG
Handelsonderneming Louter
Witte Paal 320^{E} Schagen

Mei 2018

Versie 1.0

Inhoud

Inleiding

Per 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing. Dat betekent dat er vanaf die datum dezelfde privacywetgeving geldt in de hele Europese Unie (EU). De Wet bescherming persoonsgegevens (Wbp) geldt dan niet meer.

De AVG is ook wel bekend onder de Engelse naam: General Data Protection Regulation (GDPR).

Bewustwording

Binnen Handelsonderneming zijn de relevante mensen in de organisatie (directie en management) op de hoogte van de nieuwe privacyregels.

Begin 2018 is er een inschatting gemaakt van wat de impact van de AVG is op de huidige processen, diensten en goederen en welke aanpassingen nodig zijn om aan de AVG te voldoen.

Acties

Acties die ondernomen zijn:

1. Vastleggen welke persoonsgegevens het bedrijf verwerkt
2. Verwerkers overeenkomsten afsluiten voor zover van toepassing
3. Overzicht maken van welke ICT-applicaties in gebruik zijn waarbij persoonsgegevens een rol inspelen, hetzij zijn opgenomen, hetzij worden verwerkt
4. Controle of de Handelsonderneming alleen de strikt noodzakelijke gegevens verwerkt
5. Na gaan of de inzet van freelancers / ZZPers, extra aandacht vraagt
6. Mogelijkheid voor klanten om zijn/haar gegevens in te zien en of te verwijderen (wanneer deze gegevens niet strikt nodig zijn of de klant niet langer klant is)
7. Worden regels met betrekking tot het bewaren van gegevens van sollicitanten nageleefd?
8. Is het verwerken van bijzondere persoonsgegevens van toepassing?
9. Is er een intern privacy beleid, voldoet deze?
10. Procedure opgesteld over hoe om te gaan met datalekken
11. Privacy verklaring / algemene voorwaarden moeten deze aangepast worden
12. Functionaris Gegevensbescherming benoemen.

Hoofdstuk 1 Inventarisatie persoonsgegevens

Intern

- Medewerkers administratie (huidig en 'oud')

Extern

Personeel

- Salaris administratie : JongeJan & Partners
- Ziekte verzuim administratie : Pantar Groep
- Pensioen administratie : Rabobank groep

Klanten

- Klanten administratie : Exact online (cloud oplossing)
  - Order administratie
  - Facturatie
  - Contactgegevens (CRM)
  - Archief contacten
- Planning administrate : Simple Simon, planning software.
  Afd. techniek
  Koppeling met Exact online
- Online nieuwsbrief : ANFY – mail chimp

Hoofdstuk 2 verwerkingsovereenkomsten

Met de volgende leveranciers moet onderzocht worden of er verwerkingsovereenkomsten moeten worden afgesloten.

1. ANFY
   ANFY maakt en verstuurt maandelijks online nieuwsbrief van Louter aan de klanten van Louter die hebben aangegeven deze nieuwsbrief willen ontvangen.

2. JongeJan & Partners
   Accountantskantoor JongeJan & Partners verzorgt de salarisadministratie voor de Handelsonderneming. JongeJan & Partners beschikken alleen over de minimale gegevens die nodig zijn om de salarisadministratie uit te voeren en de individuele salarissen te verwerken.

3. Pantar Groep
   Bij ziekte van een medewerker (m/v) wordt Pantar Groep als ARBO dienst ingezet. Pantar Groep krijgt alleen NAW gegevens van de medewerker om met medewerker te kunnen communiceren.

4. ExactOnline
   7 mei 2018 contact gezocht en verwerkingsovereenkomst ontvangen. Verwerkingsovereenkomst is als document in AVG map opgenomen.

5. Rabobank groep Nederland
   Rabobank groep verzorgt de pensioenvoorziening zoals deze is afgesloten in 2018 voor de medewerkers van Handelsonderneming Louter.

Hoofdstuk 3 Controle noodzakelijkheid gegevens

Controle

Bij controle in mei 2018 van de interne en externe gegevens is vastgesteld dat alleen strikt noodzakelijke gegevens worden vastgelegd.

Alleen die gegevens worden vastgelegd die nodig zijn voor de functie waar voor ze nodig zijn.

Controle op verwerken van gegevens

Binnen de onderneming worden alleen de strikt noodzakelijke gegevens per functie verwerkt.

Voorbeeld: voor de salaris administratie worden alleen die personeel gegevens gebruikt die nodig zijn voor de salaris administratie.

Controle op het combineren van gegevens

Door handelsonderneming worden geen gegevens verrijkt. Onder verrijken wordt verstaan het combineren van datasets tot informatie.

Verrijken zou kunnen door:

- Koppelingen met externe datasets (verrijken van datasets);
- Door het combineren van gegevens uit diverse datasets die al in het bezit zijn van de onderneming.

Het verrijken van datasets en/of het combineren van datasets zou lijden tot nieuwe informatie.

Hoofdstuk 4 privacy overeenkomst

De klant en 'stakeholder' (zoals, maar niet alleen; leveranciers, sollicitanten) privacy is belangrijk voor Handelsonderneming Louter. Om klanten duidelijkheid te geven over waar Louter hun gegevens voor gebruikt, werken wij continu aan het verbeteren van onze privacyverklaring. Met deze doelstelling in gedachten, hebben we in het licht van de nieuwe EU-regels voor gegevensbescherming, onze privacyverklaring bijgewerkt. Deze treedt eind mei in werking.

Privacyverklaring Handelsonderneming Louter

Jouw privacy is belangrijk voor ons bij Handelsonderneming. We gebruiken jouw persoonsgegevens uitsluitend om je account te beheren, onze producten en diensten aan je te leveren en om je te informeren over onze producten en diensten, voor zover je hiertoe toestemming hebt verleend. We hechten veel waarde aan de bescherming, vertrouwelijkheid en integriteit van jouw persoonsgegevens. In deze privacyverklaring leggen we uit welke persoonsgegevens wij verzamelen wanneer je van onze producten en diensten gebruikmaakt, waarom we deze gegevens nodig hebben en hoe we deze gebruiken.

Welke persoonsgegevens worden verzameld?

We hebben bepaalde persoonsgegevens nodig om jou de best mogelijke klantervaring te kunnen bieden en om, wanneer de klant expliciet daar toestemming voor heeft gegevens, je te informeren over onze producten en diensten. Sommige van deze gegevens geeft je direct, bijvoorbeeld wanneer je een bestelling doet of een service aanvraag doet.

Wanneer je bij Parkmobile een bestelling doet, een service aanvraag doet of op andere wijze van onze diensten gebruik maakt, dan verwerken we de volgende gegevens:

- Voor- en achternaam;
- Aanhef (Dhr./Mevr. etc.);
- E-mailadres;
- Je mobiele en/of vaste telefoonnummer;
- Je postadres;
- Je adres gegevens;
- Betaal- en factureringsinformatie, zoals bankrekeningnummer;
- Het KvK nummer;
- Bedrijfsnaam (indien van toepassing);
- Bedrijfsregistratienummer (indien van toepassing);
- Het BTW nummer dat hoort bij je bedrijfsnaam.

Derde Partijen

We ontvangen ook informatie van derde partijen waarmee wij samenwerken. Hoewel onze partners kunnen wijzigen, zijn dit met name: branche organisaties.

Cookies en soortgelijke technologie
Bij gebruik van onze online diensten (Website) verzamelen we gegevens via cookies en soortgelijke technologieën (bijv. web- beacons, tags en apparaat identificatiemiddelen). Cookies zijn tekstbestanden die op je apparaat worden geplaatst om standaard internet log-informatie en informatie over bezoekersgedrag te verzamelen en te analyseren. Deze informatie wordt gebruikt om het bezoekersgedrag op de website te evalueren en statistische rapporten over online-activiteiten op te stellen. We registreren jouw interactie met onze online platforms om onze content en diensten te kunnen verbeteren. Je kunt je cookie voorkeuren altijd zelf via je browser-instellingen beheren.

Hoe gebruiken we jouw persoonsgegevens?

We gebruiken jouw persoonsgegevens uitsluitend voor de doeleinden waarvoor deze zijn verzameld, en waar van toepassing, om te voldoen aan wettelijke verplichtingen. We gebruiken jouw persoonsgegevens voor de volgende doeleinden:

Uitvoering van de overeenkomsten. We verwerken jouw persoonsgegevens om je de producten en diensten van jouw keuze te leveren. Zo gebruiken wij deze informatie om betaling van de gemaakte kosten te faciliteren, services transacties te verwerken.

Klantenservice. We gebruiken jouw informatie om je te ondersteunen in het gebruik van onze diensten. Dit omvat het gebruik van persoonsgegevens om problemen met producten vast te stellen, verkeerde transacties te herstellen, en andere klantondersteuning gerelateerde diensten te leveren.

Klantcontact en communicatie. We gebruiken jouw gegevens om in verband met onze dienstverlening met je te communiceren via e-mail, sms-berichten of andere elektronische media. Zo ontvang je van ons facturen en kunnen wij met je communiceren om je account te bevestigen, je herinneringen te sturen, problemen op te lossen en om je uit te nodigen om deel te nemen aan klanttevredenheidsonderzoeken.

Marketing. We willen je graag via e-mail, sms of andere elektronische media op de hoogte houden van onze producten en diensten, of die van andere bedrijven (voor zover je hiervoor toestemming hebt verleend). Je hebt het recht om je te allen tijde af te melden voor deze informatievoorziening. Afhankelijk van jouw voorkeuren kun je je uitschrijven, je instellingen direct online wijzigen, of contact opnemen met ons om dit voor jou te doen.

***Wettelijke verplichtingen*.** We kunnen jouw informatie verwerken om te voldoen aan wettelijke verplichtingen, bijvoorbeeld het bijhouden van een administratie of om te voldoen aan legitieme verzoeken van bevoegde autoriteiten (bijvoorbeeld politie/justitie).

Onderhoud, ontwikkeling en incidentmanagement. Indien je problemen ondervindt met één van onze producten of diensten, kan het zijn dat we persoonsgegevens, zoals je naam, kenteken en klant-ID, moeten verwerken om het betreffende probleem op te lossen. We verwerken je persoonsgegevens ook voor sommige interne operationele processen, bijvoorbeeld wanneer we klantgegevens naar een nieuwe database overbrengen.

Uitvoering van algemene bedrijfsprocessen, intern management en managementrapportage. Om onze bedrijfsactiviteiten te kunnen uitvoeren, gebruiken we jouw persoonsgegevens voor algemene bedrijfsprocessen. We verwerken je gegevens bijvoorbeeld voor archiveringsdoeleinden, verzekeringen, managementrapportages, audits en andere administratieve doeleinden.

Met wie delen we jouw persoonsgegevens?

We delen jouw persoonsgegevens met derden zoals gemeentes, beheerders van parkeerplaatsen, leveranciers (hosting providers, klantenservice en e-marketing), klanten (bijv. zakelijke klanten/werkgevers) en andere partners, afhankelijk van je locatie en de diensten die je gebruikt. We delen jouw gegevens:

- Voor zover nodig om onze bedrijfsactiviteiten uit te voeren, onze diensten te verlenen en onze partnerdiensten (bijv. tankpassen) mogelijk te maken. Het gaat daarbij bijvoorbeeld om het uit kunnen voeren van parkeertransacties, het innen van betalingen, het bieden van klantondersteuning en het met jou kunnen communiceren in verband met onze diensten;
- Voor parkeercontroles, waarbij we jouw parkeerstatus communiceren met de beherende instanties zoals gemeentes. In die gevallen worden je kenteken, locatiecode en start- en eindtijd van je parkeertransactie gedeeld;
- In gevallen waarin je ons uitdrukkelijk toestemming hebt gegeven om dit te doen;
- Als wij daartoe rechtmatig worden verzocht in het kader van rechtshandhaving, bijvoorbeeld voor onderzoek naar illegale activiteiten;
- Om in voorkomend geval onze overeenkomst met jou te handhaven. Wanneer je bijvoorbeeld niet voor je parkeeracties hebt betaald, kunnen we jouw informatie met een incassobureau delen;
- Om onze rechten naar derden toe af te dwingen of onszelf te verdedigen tegen vorderingen of beweringen van derden;
- Om de veiligheid, integriteit en bescherming van onze diensten te waarborgen.

Waar worden jouw persoonsgegevens verwerkt ?

Voor hosting en onderhoud worden uw persoonsgegevens opgeslagen in de Europese Unie. Jouw persoonsgegevens worden hoofdzakelijk verwerkt door ons personeel op ons kantoor in Schagen.

Hoe lang bewaren we jouw persoonsgegevens ?

We bewaren jouw persoonsgegevens uitsluitend zo lang deze nodig zijn voor de doelen waarvoor ze zijn verzameld of worden gebruikt en/of zolang dit wettelijk is vereist.
Indien je jouw account gedurende 18 maanden niet gebruikt, markeren we deze in onze database als ‘inactief’. In dat geval maken we niet langer actief gebruik van jouw accountinformatie bijvoorbeeld om je over onze producten en diensten te informeren. Je account wordt dan gearchiveerd zodat je het op ieder gewenst moment weer kunt heractiveren, mocht je in de toekomst opnieuw van onze diensten gebruik willen maken.
Indien je jouw account wilt opzeggen, vragen we je contact op te nemen met

onze klantenservice. Na opzegging verwijderen we jouw persoonsgegevens zonder onnodige vertraging, maar met uitzondering van de informatie die we wettelijk verplicht zijn te bewaren. Wij zijn bijvoorbeeld wettelijk verplicht gegevens zoals kopieën van facturen gedurende zeven jaar te bewaren.

Toegang tot en beheer van jouw persoonsgegevens

Wanneer je een kopie van jouw persoonsgegevens wilt of als je een verzoek voor de beperking van verwerkingen wilt indienen, dan kun je contact opnemen met ons via ons webformulier. We reageren binnen 30 dagen na ontvangst van dergelijke verzoeken.

Wettelijke grondslag voor gegevensverwerking

We verzamelen en verwerken jouw persoonsgegevens uitsluitend wanneer wij hiervoor een wettelijke grondslag hebben. De volgende grondslagen zijn van toepassing:

- De verwerking is noodzakelijk voor de uitvoering van uw overeenkomst;
- De verwerking is noodzakelijk voor de behartiging van onze gerechtvaardigde bedrijfsbelangen, bijvoorbeeld i) voor het kunnen uitvoeren van onze bedrijfsactiviteiten; ii) ten behoeve van bepaalde vormen van direct marketing en profiling; iii) om fraude of misbruik van onze diensten op te sporen of te voorkomen; of iv) ten behoeve van de beveiliging van ons netwerk en systemen;
- De verwerking is noodzakelijk om aan een wettelijke verplichting te voldoen, zoals de bewaarplicht voor administratieve gegevens of om bepaalde informatie na een politiebevel te delen voor strafrechtelijk onderzoek;
- De verwerking die noodzakelijk is om taken van openbaar belang te ondersteunen, bijvoorbeeld om parkeerwachters te helpen bij het verifiëren van de geldigheid van een parkeeractie of parkeervergunning;
- Wanneer u ons uitdrukkelijk toestemming hebt gegeven voor een verwerking, bijvoorbeeld voor het delen van gegevens met partners voor commerciële doeleinden.

Wanneer de bewerking berust op toestemming, heb je te allen tijde het recht om jouw toestemming in te trekken. In dat geval zullen we de betreffende verwerking van jouw gegevens beëindigen. Het intrekken van de toestemming verandert de rechtmatigheid van de verwerking op basis van toestemming voor de intrekking daarvan niet.

Vragen en klachten

Indien je vragen hebt over de wijze waarop we jouw persoonsgegevens gebruiken, kun je contact opnemen met ons. Indien je het gevoel hebt dat een probleem niet afdoende is geadresseerd, heb je ook het recht een klacht in te dienen bij de Autoriteit Persoonsgegevens.

Verantwoordelijke entiteit

Handelsonderneming Louter VoF gevestigd te Schagen, Witte Paal 320E, 1742 LE , en geregistreerd bij het Handelsregister onder KvK nummer 52074137. beslissingen met betrekking tot de doelen en middelen van de verwerking van

persoonsgegevens vinden in principe centraal plaats bij Handelsonderneming, die als verwerkingsverantwoordelijke voor de verwerking van deze.

Hoofdstuk 5 Datalekken procedure

5.1 Inleiding

Doel van deze procedure is op gecontroleerde wijze om te gaan met de gevolgen van een datalek.

Aan de hand van een stappenplan wordt bepaald of er gemeld moet worden en hoe dit moet gebeuren. Deze procedure is bedoeld voor medewerkers van Handelsonderneming Louter die beveiligings- en privacy incidenten behandelen.

Aanleiding voor deze procedure is de meldplicht datalekken die per 01/01/2016 van kracht is. Het doel is beperking van de schade voor betrokkenen ten gevolge van 'datalekken' waarbij kans is op verlies of onrechtmatige verwerking van persoonsgegevens. De wet wordt opgenomen in de Wet bescherming persoonsgegevens (Wbp) als een nieuw artikel 34a. De meldplicht geldt voor iedere verantwoordelijke voor de verwerking van persoonsgegevens (niet: de bewerker!), zowel in de private als publieke sector.

De wet verplicht, op een enkele uitzondering na, de verantwoordelijke tot melding van een datalek aan de Autoriteit Persoonsgegevens (AP) en in bepaalde gevallen ook aan de betrokkenen. Dit laatste is afhankelijk van de ernst van de zaak en de gevolgen voor de betrokkenen.

Bij 'niet tijdige' melding kan de AP:

- een (bindende) aanwijzing geven om alsnog te melden;
- een bestuurlijke boete opleggen tot maximaal 820.000 euro per overtreding.

5.2 Wat is een datalek?

Een datalek is de inbreuk op de beveiliging van persoonsgegevens. Een persoonsgegeven is elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke levende persoon.

Persoonsgegevens kunnen direct of indirect identificeerbaar zijn. Een datalek betreft alle beveiligingsincidenten waardoor de bescherming van persoonsgegevens op enig moment is doorbroken waardoor de persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking van persoonsgegevens. Het is daarbij niet van belang of de verantwoordelijke passende technische of organisatorische beschermingsmaatregelen had getroffen of niet.

Een datalek is:

- een kwijtgeraakte USB-stick waar zich persoonsgegevens op bevinden;
- een gestolen werklaptop;
- een vastgestelde inbraak door een hacker;
- verzending van e-mail waarin de e-mailadressen van alle geadresseerden zichtbaar zijn voor alle andere geadresseerden;
- een besmetting met ransomware als er geen bruikbare back-up teruggezet kan worden;
- het verstrekken van een wachtwoord aan een derde;
- papieren met persoonsgegevens belanden op straat;

- een kwetsbaarheid in een applicatie waardoor persoonsgegevens gelekt worden.

5.3 Werkwijze

In de praktijk komt een datalek aanvankelijk binnen als een beveiligingsincident. Deze wordt behandeld volgens de procedure incidentenafhandeling en vastgelegd in Topdesk. Als het vermoeden bestaat dat het gaat om een datalek, wordt vervolgens het stappenplan gevolgd.

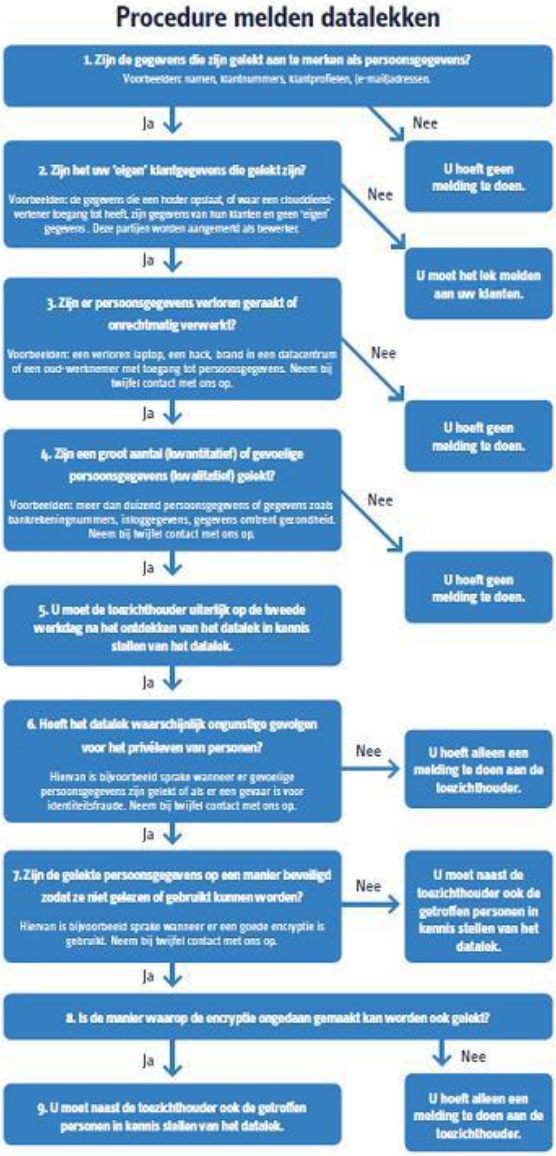
5.4 Wie moet melden?

Hieronder volgt een lijst van functionarissen die een eventuele daadwerkelijke melding aan de AP moeten doen. Voordat er wordt gemeld, wordt altijd eerst de directeur en/of de betrokken afdelingsmanager in kennis gesteld.

De eerste verantwoordelijkheid voor een eventuele melding ligt bij het hoofdbedrijfsbureau (De heer Paul Koomen). Bij afwezigheid/onbereikbaarheid ligt de verantwoordelijkheid bij de waarnemer van de Privacyfunctionaris. Bij afwezigheid/onbereikbaarheid van deze personen ligt de verantwoordelijkheid bij de directeur en/of de betrokken afdelingsmanager.

5.5 Stappenplan

Gebruik eventueel 'De meldplicht datalekken in de Wet bescherming persoonsgegeven (Wbp), beleidsregels voor toepassing van artikel 34a van de Wbp', uitgegeven door de Autoriteit Persoonsgegevens en verkrijgbaar via de website https://autoriteitpersoonsgegevens.nl voor meer informatie.
Een overzicht van het te volgen stappenplan is hierna schematisch weergegeven.


Procedure melden datalekken
1. Zijn de gegevens die zijn gelekt aan te merken als persoonsgegevens?
Voorbeelden: namen, klantnummers, klantprofielen, (e-mail)adressen.
Ja
Nee
U hoeft geen melding te doen.
2. Zijn het uw 'eigen' klantgegevens die gelekt zijn?
Voorbeelden: de gegevens die een hoster opslaat, of waar een clouddienst-verlener toegang tot heeft, zijn gegevens van hun klanten en geen 'eigen' gegevens . Deze partijen worden aangemerkt als bewerker.
Nee
U moet het lek melden aan uw klanten.
Ja
3. Zijn er persoonsgegevens verloren geraakt of onrechtmatig verwerkt?
Voorbeelden: een verloren laptop, een hack, brand in een datacentrum of een oud-werknemer met toegang tot persoonsgegevens. Neem bij twijfel contact met ons op.
Nee
U hoeft geen melding te doen.
Ja
4. Zijn een groot aantal (kwantitatief) of gevoelige persoonsgegevens (kwalitatief) gelekt?
Voorbeelden: meer dan duizend persoonsgegevens of gegevens zoals bankrekeningnummers, inloggegevens, gegevens omtrent gezondheid. Neem bij twijfel contact met ons op.
Nee
U hoeft geen melding te doen.
Ja
5. U moet de toezichthouder uiterlijk op de tweede werkdag na het ontdekken van het datalek in kennis stellen van het datalek.
Ja
6. Heeft het datalek waarschijnlijk ongunstige gevolgen voor het privéleven van personen?
Hiervan is bijvoorbeeld sprake wanneer er gevoelige persoonsgegevens zijn gelekt of als er een gevaar is voor identiteitsfraude. Neem bij twijfel contact met ons op.
Nee
U hoeft alleen een melding te doen aan de toezichthouder.
Ja
7. Zijn de gelekte persoonsgegevens op een manier beveiligd zodat ze niet gelezen of gebruikt kunnen worden?
Hiervan is bijvoorbeeld sprake wanneer er een goede encryptie is gebruikt. Neem bij twijfel contact met ons op.
Nee
U moet naast de toezichthouder ook de getroffen personen in kennis stellen van het datalek.
Ja
8. Is de manier waarop de encryptie ongedaan gemaakt kan worden ook gelekt?
Ja
Nee
9. U moet naast de toezichthouder ook de getroffen personen in kennis stellen van het datalek.
U hoeft alleen een melding te doen aan de toezichthouder.

STAP 1: PERSOONSGEGEVENS

Zijn de gegevens die zijn gelekt aan te merken als persoonsgegevens?
Een gegeven is geen persoonsgegeven, indien doeltreffende technische en organisatorische maatregelen getroffen zijn waardoor een daadwerkelijke identificatie van individuele personen redelijkerwijs wordt uitgesloten (anonimisering).
Een persoon is wel identificeerbaar als zijn identiteit redelijkerwijs, zonder onevenredige inspanning, vastgesteld kan worden. Bevatten de gegevens bijvoorbeeld namen, (e-mail)adressen of BSN's?

JA: ga naar stap 2
NEE: je hoeft geen melding te doen

STAP 2: VERANTWOORDELIJKE / BEWERKER?

Zijn het onze eigen gegevens die gelekt zijn?
De verantwoordelijke is degene die, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt (artikel 1, sub d, Wbp). Het gaat hierbij om de vraag wie uiteindelijk bepaalt welke verwerking er plaatsvindt van welke persoonsgegevens en
voor welk doel.
Ook is van belang wie er beslist over de middelen voor die verwerking: de vraag op welke manier de gegevensverwerking zal plaatsvinden. Deze bevoegdheden kunnen soms in verschillende handen liggen. In dat geval is er sprake van gezamenlijke verantwoordelijkheid.

JA: (verantwoordelijke) Ga naar stap 3.
NEE: (bewerker) De meldplicht datalekken richt zich alleen tot de verantwoordelijke voor de verwerking van persoonsgegevens (de verantwoordelijke).

Er hoeft dus geen melding bij de AP te worden gemaakt. Als bewerker heb je wel je verantwoordelijkheid richting de verantwoordelijke, zodat deze op tijd melding kan maken. De richtlijn is dit binnen 4 uur door te geven.

Meldpunt datalekken:
https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0

STAP 3: DATALEK?

In deze stap zijn er verschillende vragen om rekening mee te houden:

Stap 3A: is er sprake van een inbreuk op de beveiliging?

Een inbreuk op de beveiliging houdt in dat zich daadwerkelijk een beveiligingsincident heeft voorgedaan.
Er is niet uitsluitend sprake van een dreiging, of van een tekortkoming in de beveiliging (ook wel aangeduid als een beveiligingslek) die zou kunnen leiden tot een beveiligingsincident. Er heeft zich daadwerkelijk een beveiligingsincident voorgedaan, en de preventieve maatregelen die eventueel getroffen zijn waren niet toereikend om dit te voorkomen.

JA: (wel inbreuk) dit is een beveiligingslek. Er kan tevens sprake zijn van een datalek, ga naar stap 3B.
NEE: (geen inbreuk) dit is geen datalek. Je hoeft geen melding te doen.

Stap 3B: zijn er persoonsgegevens verloren gegaan?

Verlies houdt in dat BB de persoonsgegevens niet meer heeft. Bij het beveiligingsincident zijn de persoonsgegevens vernietigd of op een andere manier verloren gegaan, en BB beschikt niet over een complete en actuele reservekopie van de gegevens.

JA: (wel verloren) dit is een datalek, ga naar stap 4.
NEE: (niet verloren) er kan toch sprake zijn van een datalek, ga naar stap 3C.

Stap 3C: kan er uitgesloten worden dat er persoonsgegevens onrechtmatig zijn verwerkt?

Onder onrechtmatige vormen van verwerking vallen de aantasting van de persoonsgegevens, onbevoegde kennisneming, wijziging, of verstrekking daarvan. Als BB redelijkerwijs niet kunt uitsluiten dat een inbreuk op de beveiliging tot een onrechtmatige verwerking heeft geleid, dan moet u de inbreuk beschouwen als een datalek.

JA: (kan uitgesloten worden) dit is geen datalek. Je hoeft geen melding te doen.
NEE: (kan niet uitgesloten worden) dit is een datalek, ga naar stap 4.

6. Meldplicht Autoriteit Persoonsgegevens

De meldplicht valt uiteen in de meldplicht aan de Autoriteit Persoonsgegevens en die aan de betrokkenen. In dit hoofdstuk wordt omschreven wanneer en hoe er aan de Autoriteit Persoonsgegevens moet worden gemeld.

STAP 4: MELDING AP

In deze stap zijn twee vragen om rekening mee te houden:

Stap 4A: zijn er persoonsgegevens van gevoelige aard gelekt?

Bij het beantwoorden van de vraag of er sprake is van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens, moet er in ieder geval gekeken worden naar de aard van de getroffen gegevens.
Is er sprake van bijzondere persoonsgegevens of van persoonsgegevens die anderszins van gevoelige aard zijn? Bij dit laatste moet je bijvoorbeeld denken aan gegevens over betalingsachterstanden.
Bij een aantal categorieën van persoonsgegevens, in dit kader aangeduid als persoonsgegevens van gevoelige aard, kunnen verlies of onrechtmatige verwerking onder meer leiden tot stigmatisering of uitsluiting van de betrokkene, tot schade aan de gezondheid, financiële schade of tot (identiteits-)fraude. Tot deze categorieën van persoonsgegevens moeten in ieder geval worden gerekend:

- Bijzondere persoonsgegevens zoals bedoeld in artikel 16 Wbp Het gaat hierbij om persoonsgegevens over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging en om strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.
- Gegevens over de financiële of economische situatie van de betrokkene Hieronder vallen bijvoorbeeld gegevens over (problematische) schulden, salaris- en betalingsgegevens.
- (Andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene. Hieronder vallen bijvoorbeeld gegevens over gokverslaving, prestaties op school of werk of relatieproblemen.
- Gebruikersnamen, wachtwoorden en andere inloggegevens De mogelijke gevolgen voor betrokkenen hangen af van de verwerkingen en van de persoonsgegevens waar de inloggegevens toegang toe geven. Bij de afweging moet worden betrokken dat veel mensen wachtwoorden hergebruiken voor verschillende verwerkingen.
- Gegevens die kunnen worden misbruikt voor (identiteits)fraude Het gaat hierbij onder meer om biometrische gegevens, kopieën van identiteitsbewijzen en om het Burgerservicenummer (BSN).
- inloggegevens toegang toe geven. Bij de afweging moet worden betrokken dat veel mensen wachtwoorden hergebruiken voor verschillende verwerkingen.
- Gegevens die kunnen worden misbruikt voor (identiteits)fraude Het gaat hierbij onder meer om biometrische gegevens, kopieën van identiteitsbewijzen en om het Burgerservicenummer (BSN). Ook gegevens uit DNA-databanken, gegevens waar een bijzondere, wettelijk bepaalde

geheimhoudingsplicht op rust en gegevens die onder een beroepsgeheim vallen (bijvoorbeeld het medisch beroepsgeheim) in de zin van artikel 9, vierde lid, van de Wbp moeten tot de persoonsgegevens van gevoelige aard worden gerekend.

JA: (wel gevoelige gegevens) dit moet gemeld worden bij de AP, ga naar stap 5. Mogelijk moet dit ook gemeld worden aan de betrokkenen, ga daarna naar stap 6.
NEE: (geen gevoelige gegevens) ga naar stap 4B.

Stap 4B: leiden de aard en omvang van de inbreuk tot (een aanzienlijke kans op) ernstige nadelige gevolgen?

De aard en omvang van de getroffen verwerking is mede bepalend voor de beantwoording van de vraag of er bij een datalek sprake is van (een aanzienlijke kans op) nadelige gevolgen voor de bescherming van persoonsgegevens.
Een datalek bij instellingen als de Belastingdienst of bij een commerciële bank of verzekeraar kan leiden tot financieel nadeel voor de betrokkene of tot de compromittering van gegevens die beschermd worden door een geheimhoudingsplicht.
Beveiligingslekken in de omvangrijke verwerkingen van persoonsgegevens waarover de overheid beschikt kunnen ook zeer grote gevolgen hebben voor de betrokkenen.
Afgezien van de gevoelige aard van de verwerkte gegevens, die in de voorgaande paragraaf al aan de orde kwam, is voor de kans op ernstige nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens verder het volgende relevant:

- De omvang van de hierboven beschreven verwerkingen betekent dat het bij datalekken kan gaan om veel persoonsgegevens per persoon, en om gegevens van grote groepen betrokkenen. Deze beide factoren maken een gelekte dataset aantrekkelijk voor misbruik in het criminele circuit. De kans dat de gelekte dataset wordt doorverkocht, wordt daardoor ook groter, met als gevolg dat de betrokkenen langer last houden van het datalek.
- Naarmate de beslissingen die op basis van de verwerkte persoonsgegevens worden genomen ingrijpender zijn, is ook de impact van verlies of onrechtmatige verwerking groter. Bijvoorbeeld: als een organisatie financiële gegevens gebruikt om iemands kredietwaardigheid te bepalen zijn de gevolgen van verlies en onbevoegde wijziging van de gegevens ingrijpender dan bij gebruik van dezelfde gegevens voor marketingdoeleinden.
- Bij omvangrijke verwerkingen van de overheid is vaak sprake van persoonsgegevens die binnen ketens worden gedeeld. Dit betekent dat de gevolgen van verlies en onbevoegde wijziging van persoonsgegevens door de hele keten heen kunnen optreden. Voor de betrokkenen wordt het hierdoor moeilijker om de mogelijke gevolgen van een datalek te overzien en om zich daar waar mogelijk aan te onttrekken.

Als de aard en omvang van de getroffen verwerking voldoen aan het bovenstaande, dan moet IB ervan uitgaan dat er (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming
van de verwerkte persoonsgegevens aanwezig kan zijn.

JA: (wel ernstige gevolgen) dit moet gemeld worden bij de AP, ga naar stap 5. Mogelijk moet dit ook gemeld worden aan de betrokkenen, ga daarna naar stap 6.
NEE: (geen ernstige gevolgen) dit datalek hoeft niet gemeld te worden aan de AP

STAP 5: MELDING AP

De Autoriteit Persoonsgegevens stelt een webformulier beschikbaar waarmee datalekken kunnen
worden gemeld. Een overzicht van de vragen in dit webformulier zijn opgenomen in bijlage 8.

Als IB geen gebruik kan maken van het webformulier, dan kunnen volgens de AP de gevraagde gegevens per fax toegezonden worden. Je moet daarbij zorgen dat je aan kunt tonen dat je de melding tijdig heeft gedaan. Er is echter geen faxnummer te vinden op de website, wel een telefoonnummer, speciaal voor datalekken.

- Er kan melden worden gemaakt van een datalek op de website https://datalekken.autoriteitpersoonsgegevens.nl/melding/aanmaken?1.
- Het datalek moet onverwijld gemeld worden, zo mogelijk niet later dan 72 uur na de ontdekking. Mogelijk is er na 72 uur geen volledig zicht is op het incident. De melding bij de AP kan achteraf worden bijgewerkt of zelfs ingetrokken. Als er later dan 72 uur wordt gemeld, wordt er gemotiveerd waarom.
- Je ontvangt direct een ontvangstbevestiging. Deze registeren in.
- Bij die meldingen die aanleiding geven tot nadere actie door de Autoriteit
- Persoonsgegevens, zal deze contact met IB opnemen om de herkomst van de melding te
- verifiëren. Op termijn zal worden aangesloten op eHerkenning of andere gangbare
- authenticatiemiddelen.
- Melding via webformulier niet mogelijk? Bel met 0900-3282535.
- Mogelijk moet er naast een melding bij de AP, ook gemeld worden aan betrokkenen, gadoor naar stap 6.

7. Meldplicht betrokkenen

De meldplicht valt uiteen in de meldplicht aan de Autoriteit Persoonsgegevens en die aan de betrokkenen. In dit hoofdstuk wordt omschreven wanneer en hoe er aan de betrokkenen moet
worden gemeld.

STAP 6: PRIVELEVEN

Heeft het datalek waarschijnlijk ongunstige gevolgen voor het privéleven van personen? Het datalek moet aan de betrokkene worden gemeld als de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer (artikel 34a, tweede lid, Wbp).Betrokkenen kunnen door het verlies, onrechtmatig gebruik of misbruik van persoonsgegevens in hun belangen worden geschaad. De schade kan van materiële of van immateriële aard zijn. Bij dit laatste moet je bijvoorbeeld denken aan onrechtmatige publicatie, aantasting in eer en goede.

naam, identiteitsfraude of discriminatie. Identiteitsfraude kan overigens niet alleen leiden tot immateriële gevolgen, maar ook tot materiële gevolgen.
Het is aan IB om te beoordelen of een datalek aan de betrokkene gemeld moet worden. Indien er persoonsgegevens van gevoelige aard zijn gelekt, dan moet je er van uitgaan dat je het datalek niet alleen moet melden aan de Autoriteit Persoonsgegevens, maar ook aan de betrokkene. Verlies of onrechtmatige verwerking van dergelijke gegevens kunnen onder meer
leiden tot stigmatisering of uitsluiting van de betrokkene, tot schade aan de gezondheid, financiële schade of (identiteits)fraude.
In alle overige gevallen zult u op basis van de omstandigheden van het geval een afweging moeten maken.

JA: (wel gevolgen voor privéleven) ga naar stap 7.
NEE: (geen gevolgen voor privéleven) er hoeft alleen aan de AP en niet aan de betrokkenen gemeld te worden.

STAP 7: GOED BEVEILIGD?

Zijn de gelekte persoonsgegevens op een manier beveiligd zodat ze niet gelezen of gebruikt kunnen worden?

Als door de cryptografische bewerkingen die IB heeft toegepast de gelekte persoonsgegevens onbegrijpelijk of ontoegankelijk zijn voor onbevoegden, dan kunt je de melding aan de betrokkene achterwege laten. Dit is een strenge norm, die je van geval tot geval toe moet passen op basis van de actuele stand van de techniek. Als je twijfelt over de adequaatheid van de technische beschermingsmaatregelen die je heeft getroffen, dan moet je het datalek melden aan de betrokkene.

De Europese verordening 611/2013 geeft een nadere invulling aan adequate versleuteling. Volgens deze verordening mag u gegevens als onbegrijpelijk beschouwen als ze:

- op veilige wijze zijn versleuteld met een standaardalgoritme, de sleutel voor decryptie door geen enkele inbreuk gevaar heeft gelopen en de sleutel voor decryptie zodanig werd gegenereerd dat personen zonder geautoriseerde toegang de sleutel met de beschikbaretechnologische middelen niet kunnen vinden; of
- zijn vervangen door een met een cryptografisch versleutelde hashfunctie berekende hashwaarde, de sleutel die hiervoor werd gebruikt door geen enkele inbreuk gevaar heeft gelopen en deze voor datahashing gebruikte sleutel zodanig is gegenereerd dat personen zonder geautoriseerde toegang de sleutel niet kunnen vinden met de beschikbare technologische middelen.

Naast encryptie vermeldt de Nederlandse wetsgeschiedenis nog een andere technische beschermingsmaatregel waarmee persoonsgegevens kunnen worden beschermd tegen onbevoegde kennisname: het op afstand wissen van de gegevens die op een apparaat staan (*remote wiping*).

Een *remote wipe* heeft echter uitsluitend kans van slagen als er aan een aantal randvoorwaarden wordt voldaan. De eerste randvoorwaarde is dat de *remote wipe* tijdig in gang wordt gezet, zodat een eventuele aanvaller nog geen kans

heeft gehad om kennis te nemen van de gegevens. Verder moet op dat moment het apparaat waar het om gaat nog intact zijn en werken, zodat het in staat is om de *remote wipe* uit te voeren en de gegevens te wissen. Ook moet de toepassing die voor het wissen van de gegevens wordt gebruikt correct werken, zodat alle gegevens waar het om gaat daadwerkelijk worden verwijderd en er ook geen sporen achterblijven waaruit de oorspronkelijke gegevens kunnen worden gereconstrueerd.

Ook als de gelekte gegevens gepseudonimiseerd zijn zult je op basis van de specifieke omstandigheden van het geval vast moeten stellen of er aan de norm uit het zesde lid van artikel 34a Wbp wordt voldaan. Pseudonimisering wil zeggen dat je technische maatregelen hebt genomen om te voorkomen dat de persoonsgegevens worden gekoppeld aan de oorspronkelijke identiteit van de betrokkene.

JA: (wel goed beveiligd) ga door naar stap 8.
NEE: (niet goed beveiligd) Er moet naast aan de AP ook aan betrokkenen worden gemeld, ga door naar stap 9.

STAP 8:

Is de manier waarop de encryptie ongedaan gemaakt kan worden bekend gemaakt? Aandachtspunten bij de beoordeling zijn:

- Het algoritme zelf, of de wijze waarop dit is toegepast, kunnen kwetsbaarheden vertonen waardoor de encryptie of de hashing niet de bescherming biedt die je daarvan verwacht.
- Encryptie is omkeerbaar. Een onbevoegde die over de juiste sleutel beschikt, of deze zonder al te veel moeite kan vinden, kan de gelekte gegevens ontsleutelen.
- Hashing is herhaalbaar. Als er bij hashing geen salt is toegepast, of als een onbevoegde over de gebruikte salt beschikt of deze zonder al te veel moeite kan vinden, kan hij de gebruikte hashingmethode toepassen op een lijst met veelgebruikte waarden en daardoor bijvoorbeeld gestolen wachtwoorden achterhalen.

NEE: Er moet alleen aan de AP gemeld worden en niet aan de betrokkenen gemeld worden.
JA: Er moet naast aan de AP ook aan betrokkenen worden gemeld, ga naar stap 9.

STAP 9: MELDING BETROKKENEN

Er moet ook worden gemeld aan de betrokkenen. Dit moet ‘onverwijld’ gebeuren. Bij de melding aan de AP wordt een termijn afgesproken waarbinnen dit moet gebeuren. Deze termijn moet nagekomen worden. Bij melding worden minimaal de volgende gegevens verstrekt:

- de aard van de inbreuk (algemene omschrijving)
- de instanties waar de betrokkene meer informatie over de inbreuk kan krijgen (contactgegevens IB)
- en de maatregelen die IB de betrokkene aanbeveelt om te nemen om de negatieve
- gevolgen van de inbreuk te beperken (bijvoorbeeld wachtwoord wijzigen).

TENSLOTTE

Alle datalekken moeten worden bijgehouden in een overzicht. Per datalek bevat het overzicht in ieder geval feiten en gegevens omtrent de aard van de inbreuk. Als het datalek is gemeld aan de betrokkene, dan wordt ook de tekst van de kennisgeving aan de betrokkene opgenomen in het overzicht. Het overzicht hoeft niet openbaar te worden gemaakt. Het overzicht moet minstens 1 jaar bewaard worden.

Er moet rekening mee worden gehouden dat een vervolgprocedure na een datalek juridische maatregelen kan omvatten (civiel- of strafrechtelijk), en dat IB waar dat aan de orde is het bewijsmateriaal moet verzamelen, bewaren en presenteren overeenkomstig de voorschriften voor bewijs die voor het relevante rechtsgebied zijn vastgelegd.

8. Bijlage: lijst van afkortingen en termen

AP	Autoriteit Persoonsgegevens (voorheen CBP)
Betrokkene	de mensen van wie de persoonsgegevens zijn gelekt Bewerker verwerkt persoonsgegevens ten behoeve van de verantwoordelijke, zonder dat hij aan het rechtstreekse gezag van de verantwoordelijke is onderworpen. Dit kan ook een volgende partij in de keten zijn.
BSN	Burger Service Nummer
CBP	College ter Bescherming van Persoonsgegevens (nu AP)
BB	Bedrijfsbureau
Remote wipe	het op afstand wissen van de gegevens die op een apparaat staan
WBP	Wet bescherming Persoonsgegevens
Verantwoordelijke	degene die, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.

9. Bijlage: gebruikte informatiebronnen

- Autoriteit Persoonsgegevens, *De meldplicht datalekken in de Wet bescherming persoonsgegeven (Wbp), beleidsregels voor toepassing van artikel 34a van de Wbp*, 8 december 2015.
- College ter Bescherming van Persoonsgegevens, '*Meldplicht Datalekken in de Wet bescherming persoonsgegevens (Wbp) – consultatieversie*, 21 september 2015.
- Centrum voor Informatievoorziening en Privacybescherming, '*Meldplicht Datalekken*', herziende versie 0.2, november 2015.
- ICT Recht, '*Impact van de meldplicht datalekken*'